Ana Maria Andronache*

UE ŞI PROVOCĂRILE SALE ÎN MATERIE DE SECURITATE CIBERNETICĂ

CZU: 061.1 UE:004.056.5 **DOI: https://doi.org/10.5281/zenodo.12633018**

Abstract

To respond to changing security challenges, the EU and its Member States have to strengthen cyber resilience and to develop robust cyber security and defence capabilities. Cyberspace is a rapidly developing domain and new technological developments need to be supported, both in the civilian and military domains. Last, but not least, enhancing cooperation with international partners could help enhance cybersecurity within the EU and beyond, and to promote EU principles and values. This paper aims to provide an informative primer on the relevant issues facing UE in relation to cybersecurity because cybersecurity is not optional. It must form part of the design of every product, of every database, of every electronic communication. And – through education, awareness, and proactive change – we can all play a part in securing our future. Analysis of attacks over the years has revealed that cybercriminals work together exceptionally well: sharing knowledge of exploits, selling stolen data in an open market, and working together to develop new hacking techniques for infiltration. That is why the EU needs to act on different fronts to promote cyber resilience.

Keywords: *Cybersecurity, governance, resilience, dates, defence*

Creşterea gradului de conştientizare şi îngrijorare faţă de ameninţările cibernetice tot mai dese cu care se confruntă organizaţiile, guvernele şi indivizii deopotrivă impune Uniunii Europene să acţioneze, pe diferite fronturi, pentru a promova reziliența cibernetică. Astfel, sunt gândite şi propuse o serie de strategii pentru a combate criminalitatea informatică, pentru a stimula diplomaţia cibernetică şi, nu în ultimul rând, pentru o mai bună apărare cibernetică. Accentul major în ceea ce priveşte securitatea cibernetică trebuie să vizeze şi domeniul de elaborare a politicilor deoarece problemele tehnice pot afecta o largă paletă de date, de la datele cetăţenilor sau organizaţiilor guvernamentale şi nu numai, până la apărarea militară împotriva statului.

Factorii politici se confruntă cu mai multe provocări: propunerea unor noi reglementări în domeniu, gestionarea bugetelor guvernamentale reduse, negocierea parteneriatelor strategice in vederea cooperării internaţionale încerând să formuleze astfel o strategie comună în lupta impotriva ameninţărilor cibernetice. In sprijinul acestora, Comisia Europeană a propus o legislaţie care să introducă un centru de competenţe şi o reţea de centre naţionale care ar trebui să fie responsabile pentru finanţarea europeană a tehnologiei, cercetării şi educaţiei profesionale pentru următorul deceniu. Având în vedere numărul mare al părţilor implicate, de la oficiali

* Lect.univ.dr, Universitatea ”Alexandru Ioan Cuza” din Iași, Iași, România, email: anamaria.andronache@uaic.ro

guvernamentali la hackeri, factorii de decizie politică vor fi interesaţi de modul în care aceste grupuri îşi văd rolul în procesul de luare a deciziilor, precum şi de posibila lor cooperare cu entităţile existente.

În demersul de a defini sensul actual al conceptul de securitate cibernetică, voi evidenţia câteva repere istorice a securităţii cibernetice, conceptul fiind iniţiat văzut ca un proiect de cercetare. În anii 1970, Robert Thomas, cercetător pentru BBN Technologies din Cambridge, Massachusetts, a creat primul „virus" de calculator. Se numea The Creeper. Creeper, a infectat computerele afişând treptat, de la sistem la altul mesajul „EU SUNT CREEPERUL: prinde-mă dacă poţi". Ray Tomlinson, inventatorul e-mailului, a creat un program de replicare numit The Reaper, primul software antivirus, care l-ar urmări pe Creeper şi l-ar şterge ((History of cyber security, 2023). La sfârşitul anului 1988, Robert Morris a avut o idee: a vrut să testeze dimensiunea internetului Pentru a face acest lucru, el a scris un program care a trecut prin reţele, a invadat terminalele Unix şi s-a copiat. Viermele Morris a fost atât de agresiv încât a încetinit computerele până la punctul de a fi inutilizabile. Ulterior, el a devenit prima persoană care a fost condamnată în temeiul Legii privind frauda şi abuzul informatic. Din acel moment, viruşii au devenit mai mortali, mai invazivi şi mai greu de controlat, fiind impetuos necesar apariţia securităţii cibernetice (Daly, 1993:1).

Securitatea cibernetică se referă la un set de tehnici utilizate pentru a proteja integritatea reţelelor, a programelor şi a datelor de atacuri, daune sau de acces neautorizat (Ghid de securitate cibernetică, p.2). Datele care sunt stocate, transmise sau utilizate pe un sistem informatic sunt principalul punct de atracţie. Reţeaua, serverele, computerele sunt doar mecanisme pentru a ajunge la date. Securitatea cibernetică eficientă reduce riscul de atacuri cibernetice şi protejează organizaţiile şi persoanele de exploatarea neautorizată a sistemelor, reţelelor şi tehnologiilor. Implementarea robustă a securităţii cibernetice se bazează aproximativ pe trei termeni cheie: oameni, procese şi tehnologie (ENISA Report TOWARDS A COMMON ECSC ROADMAP, 2021:3). Această abordare pe trei direcţii ajută organizaţiile să se apere atât de atacurile extrem de organizate, cât şi de ameninţările interne comune, cum ar fi încălcările accidentale şi erorile umane.

Atacurile evoluează în fiecare zi pe măsură ce atacatorii devin mai inventivi, este esenţial să definiţi corect securitatea cibernetică şi să înţelegeţi elementele fundamentale ale securităţii cibernetice. Din punct de vedere informatic, securitatea cuprinde securitatea cibernetică şi securitatea fizică (Cybersecurity – Threats Challenges Opportunities, 2016:23)– ambele sunt folosite de întreprinderi pentru a se proteja împotriva accesului neautorizat la centrele de date şi la alte sisteme computerizate. Securitatea informaţiilor, care este concepută pentru a menţine confidenţialitatea, integritatea şi disponibilitatea datelor, este un subset al securităţii cibernetice (Triada CIA, 2021). Utilizarea securităţii cibernetice poate ajuta la

prevenirea atacurilor cibernetice, a încălcării datelor şi a furtului de identitate şi poate ajuta la gestionarea riscurilor. Aşadar, când vorbim despre securitate cibernetică, ne punem întrebarea: cine este inamicul şi de ce încercăm să ne protejăm de el? Ei bine, există trei aspecte principale pe care încercăm să le controlăm: acces neautorizat, ştergere neautorizată şi modificare neautorizată (Cybersecurity – Threats Challenges Opportunities, 2016:35). Aceşti trei termeni sunt sinonimi cu triada CIA care înseamnă Confidenţialitate (Confidentiality), Integritate (Integrity) şi Disponibilitate (Availability). Triada CIA este denumită cei trei piloni ai securităţii şi majoritatea politicilor de securitate sunt construite pe aceste trei principii, fiind un model de proiectare pentru a ghida companiile şi organizaţiile pentru a-şi formula politicile de securitate. Componentele triadei sunt considerate a fi cele mai importante componente ale securităţii. Confidenţialitatea este protecţia informaţiilor personale. Confidenţialitatea înseamnă păstrarea informaţiilor unui client, cetăţean, compani etc., iar măsurile standard pentru stabilirea confidenţialităţii includ: criptarea datelor, autentificare cu doi factori, verificare biometrică, Tokeni /Jetoane de securitate. Integritatea, în contextul sistemelor informatice, se referă la metode de asigurare a faptului că datele sunt reale, exacte şi protejate de modificările neautorizate ale utilizatorului. Măsurile standard pentru garantarea integrităţii includ: sume de control criptografice, utilizarea permisiunilor pentru fişiere, surse de alimentare neîntrerupte şi backup-uri de date. Disponibilitatea, în contextul unui sistem informatic, se referă la capacitatea unui utilizator de a accesa informaţii sau resurse într-o locaţie specificată şi în formatul corect. Măsurile standard pentru garantarea disponibilităţii includ: copiere de rezervă a datelor pe unităţi externe, implementarea firewall-urilor, surse de alimentare de rezervă şi redundanţă de date(Prakash, 2023).

Toate atacurile cibernetice au potenţialul de a ameninţa una sau mai multe dintre cele trei părţi ale triadei CIA. Confidenţialitatea, integritatea şi disponibilitatea trebuie să lucreze împreună pentru ca informaţiile să fie păstrate în siguranţă (Kidd, 2023). Deci, este important să înţelegem ce este triada CIA, cum este folosită pentru a planifica şi implementa o politică de securitate de calitate, înţelegând în acelaşi timp diferitele principii din spatele acesteia.

Plecând de la ideea că ameninţările la adresa securităţii cibernetice sunt mult mai mult decât o chestiune de IT, observăm interesul sporit al UE care doreşte să construiască un spaţiu cibernetic deschis şi securizat, tocmai pentru a spori încrederea cetăţenilor în instrumentele şi serviciile digitale. Istoria reţelei europene de securitate cibernetică începe cu adoptarea Convenţiei de la Budapesta privind criminalitatea informatică în 2001, a Cadrului comun privind reţelele şi serviciile de comunicaţii electronice în 2002 şi cu înfiinţarea ulterioară a ENISA, o agenţie independentă a UE pentru securitate cibernetică, în 2004. Principala atribuţie a ENISA a fost dezvoltarea unei culturi a securităţii reţelelor şi a informaţiilor în beneficiul cetăţenilor,

consumatorilor, întreprinderilor şi organizaţiilor din sectorul public din Uniunea Europeană, contribuind astfel la buna funcţionare a pieţei interne (Regulation (EC) No 460/2004). Modelul iniţial de guvernanţă era încă modelul de piaţă, schimbul de informaţii fiind un principiu-cheie al unei guvernanţe de succes. Modificarea condiţiilor internaţionale au condus, de asemenea, la o evoluţie a legislaţiei europene în materie de securitate cibernetică, Strategia de securitate cibernetică a UE din 2013 (actualizată în 2017) a subliniat necesitatea cooperării dintre statele membre, sectorul privat şi agenţiile UE – ENISA (NIS), EC3/Europol (aplicarea legii) şi AEA (apărare) – pentru a promova sensibilizarea cu privire la ameninţările la adresa securităţii cibernetice, pentru a încuraja investiţiile, precum şi pentru a face schimb de bune practici(Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace , 2013).

Agenda europeană privind securitatea din 2015 se axează pe combaterea criminalităţii informatice ca prioritate-cheie, care poate fi realizată printr-un "răspuns coordonat la nivel european", inclusiv punerea în aplicare a politicilor existente şi adaptarea legislaţiei existente(The European Agenda on Security, 2015). Directiva privind securitatea reţelelor şi a sistemelor informatice în UE (Directiva NIS) din 2016 este un exemplu de act legislativ general la nivelul UE axat pe securitatea cibernetică. Acesta a instituit grupul NIS care coordonează cooperarea strategică între statele membre, stabilind orientări pentru capacităţile naţionale, precum şi promovând schimbul de informaţii. Cadrul de politici al UE în domeniul apărării cibernetice, adoptat în 2014, a fost actualizat în 2018 pentru a corespunde mai bine noilor provocări în materie de securitate cibernetică (EU cyber defense policy framework , 2018).

Printre primele domenii in care s-a discutat despre acest concept este cel al justitiei, mai mult, tema dezbătută in 2016 făcea referire la combaterea activităţilor infracţionale în spaţiul cibernetic (Consiliul UE, iunie 2016). In 2017, Instituţiile UE au făcut un pas important în direcţia consolidării cooperării lor în ceea ce priveşte combaterea atacurilor cibernetice. Printr-un acord interinstituţional s-a înfiinţat un Centru de răspuns la incidente de securitate cibernetică (CERT-UE) permanent, pentru toate instituţiile, organele şi agenţiile UE (Cronologie – securitatea cibernetica). Apărarea cibernetică este elementul cheie in 2018. UE consolidează rezistenţa la atacurile cibernetice, statele membre ale UE cooperează tot mai mult în domeniul apărării cibernetice, în scopul de a-şi consolida capacităţile, Consiliul adoptă, cum am precizat mai sus, o versiune actualizată a cadrului de politici pentru apărarea cibernetică a UE. În versiunea actualizată sunt stabilite domeniile prioritare pentru apărarea cibernetică şi sunt explicate rolurile actorilor implicaţi (Comunicat de presă, decembrie 2018). In 2019 Consiliul a stabilit un cadru care îi permite UE să impună măsuri restrictive specifice pentru a descuraja şi a răspunde la atacurile cibernetice care reprezintă o ameninţare externă la adresa UE sau a statelor sale

membre.Mai precis, această decizie permite UE, pentru prima dată, să impună sancţiuni unor persoane sau entităţi care: sunt responsabile de atacuri cibernetice sau de tentative de atacuri cibernetice, oferă sprijin financiar, tehnic sau material pentru astfel de atacuri sau sunt implicate în alte moduri(Consiliul UE, Comunicat de presă, mai 2019). Acest cadru se aplică, de asemenea, atacurilor cibernetice asupra unor state terţe sau organizaţii internaţionale, în cazul în care măsurile restrictive sunt considerate necesare pentru realizarea obiectivelor politicii externe şi de securitate comune (PESC). La 9 aprilie 2019, Consiliul a adoptat regulamentul cunoscut şi sub denumirea de „Regulamentul privind securitatea cibernetică", care introduce: un ansamblu de sisteme de certificare la nivelul UE şi creare unei noi Agenţii a Uniunii Europene pentru Securitate Cibernetică(Regulamentul (UE) 2019/881), pentru a prelua responsabilităţile actualei Agenţii a Uniunii Europene pentru Securitatea Reţelelor şi a Informaţiilor (ENISA).

În următorul an, 2020, Consiliul îndeamnă la consolidarea rezilienţei şi contracararea ameninţărilor hibride, inclusiv a dezinformării. Consiliul a constatat că noile tehnologii şi crize, precum actuala pandemie, oferă actorilor ostili ocazii de a-şi extinde ingerinţa. Aceasta reprezintă o provocare în plus pentru statele membre şi instituţiile UE, pe lângă criza în sine. Consiliul a recunoscut că pandemia de COVID-19 face ca UE şi statele sale membre să fie mai vulnerabile la ameninţările hibride. Printre aceste ameninţări se numără răspândirea intensificată a dezinformării şi a ingerinţei manipulatoare. Combaterea acestor ameninţări, în special a activităţilor cibernetice răuvoitoare, a dezinformării şi a ameninţărilor pentru securitatea economică, necesită o abordare cuprinzătoare, care implică o cooperare şi o coordonare eficace(Conturarea viitorului digital al Europei – comunicat de presă, iunie 2020). Oraşul Bucureşti (România) a fost selectat de reprezentanţii guvernelor statelor membre ale UE pentru a găzdui viitorul sediu al noului Centru de competenţe european industrial, tehnologic şi de cercetare în materie de securitate cibernetică, centru ce va îmbunătăţi coordonarea cercetării şi a inovării în domeniul securităţii cibernetice în UE (Selectarea sediului, 2020). Acesta va fi principalul instrument al UE de punere în comun a investiţiilor pentru cercetarea şi dezvoltarea tehnologică şi industrială în domeniul securităţii cibernetice.

În 2021 Consiliul a adoptat concluzii privind Strategia de securitate cibernetică a UE pentru deceniul digital prin care se stabileşte cadrul de acţiune a UE pentru a proteja cetăţenii şi întreprinderile din UE împotriva ameninţărilor cibernetice, pentru a promova sisteme informatice securizate şi pentru a proteja un spaţiu cibernetic deschis, liber şi securizat la nivel mondial (Comunicat de presă, 2021). Concluziile afirmă că securitatea cibernetică este esenţială pentru construirea unei Europe reziliente, verzi şi digitale. Acestea stabilesc ca obiectiv cheie atingerea autonomiei strategice, menţinând în acelaşi timp o economie deschisă, dar şi consolidarea

capacităţii de a face alegeri autonome în domeniul securităţii cibernetice, cu scopul de a consolida poziţia de lider a UE în domeniul digital.

În contextul creşterii numărului de atacuri cibernetice sofisticate împotriva administraţiei publice a UE, în 2022, Consiliul şi Parlamentul European au ajuns la un acord provizoriu cu privire la măsurile menite să asigure un nivel comun ridicat de securitate cibernetică în întreaga Uniune, pentru a îmbunătăţi şi mai mult reziliența şi capacităţile de răspuns la incidente atât ale sectorului public, cât şi ale sectorului privat, precum şi ale UE în ansamblu. Odată adoptată, noua directivă, denumită NIS 2, va înlocui actuala directivă privind securitatea reţelelor şi a sistemelor informatice (Directiva NIS). Noua legislaţie va asigura o mai bună cooperare în materie de riscuri şi incidente şi o mai bună gestionare a acestora precum si extinderea domeniul de aplicare al normelor (Comunicat de presă, 2022).

Având în vedere că spaţiul cibernetic este un domeniu de concurenţă strategică, riscurile pentru securitatea şi apărarea UE cresc într-o perioadă de tensiuni geopolitice şi în care dependența de tehnologiile digitale este din ce în ce mai mare, Consiliul adoptă concluzii privind politica UE în domeniul apărării cibernetice in 2023. Acestea subliniază necesitatea ca UE şi statele sale membre să consolideze în continuare rezilienţa acestora pentru a face faţă ameninţărilor cibernetice şi să îşi sporească securitatea cibernetică comună şi apărarea cibernetică comună împotriva comportamentelor răuvoitoare şi a actelor de agresiune în spaţiul cibernetic (Comunicat de presă, 2023).

O serie de sectoare critice precum transporturile, energia, sănătatea şi finanţele au devenit tot mai dependente de tehnologiile digitale pentru a-şi desfăşura activităţile de bază. Digitalizarea oferă oportunităţi enorme şi asigură soluţii pentru multe dintre provocările cu care se confruntă Europa, nu în ultimul rând în timpul crizei provocate de pandemia de COVID-19, dar, în acelaşi timp, expune economia şi societatea la ameninţări cibernetice. Atacurile cibernetice şi criminalitatea informatică sunt tot mai numeroase şi mai sofisticate în întreaga Europă. Se preconizează că această tendinţă va continua să crească în viitor, date fiind previziunile conform cărora 41 miliarde de dispozitive la nivel mondial vor fi conectate la internetul obiectelor până în 2025(International Data Corporation).

Pentru a construi un spaţiu cibernetic deschis şi securizat, în care cetăţenii pot avea încredere în instrumentele şi serviciile digitale este necesară o bună guvernanţă a securităţii cibernetice, aşa cum am precizat la inceputul lucrării. Astfel, voi prezenta mai multe modele de guvernare a securităţii cibernetice chiar dacă ştim că nu există un model universal pentru guvernanţă. În lucrarea sa clasică, Powell (Powell, 1990 : 296) discută trei modele de guvernare: piaţa, ierarhia şi reţeaua. Dacă ne referim la guvernanţa securităţii cibernetice putem spune că mâna invizibilă a pieţei este deschisă, schimbul economic păstrează în mare măsură autonomia actorilor ale căror costuri şi beneficii sunt autoevaluate (de exemplu, costul software-ului vs costul

posibilei pierderi de date) şi nu apare niciun sentiment pe termen lung de încredere şi obligaţie. În cazul în care lipseşte o abordare generală coerentă de reglementare a organismelor naţionale şi ale UE, mecanismele pieţei intervin pentru a soluţiona problemele apărute deoarece ameninţările cibernetice au potenţialul de a le submina profiturile. Cu toate acestea, necesitatea de a adăuga măsuri complementare, care nu sunt determinate de piaţă, este evidentă pentru securitatea statului sau confidenţialitatea datelor utilizatorilor. Datorită faptului că ameninţările la adresa securităţii cibernetice sunt intr-o continuă evoluţie se poate observa ineficienţa guvernanţei bazate exclusiv pe piaţă şi necesitatea unei noi abordari. Modelul ierarhic, cu distribuţia clară a sarcinilor şi schema de bază a regulilor birocratice, conform lui Powell (Powell, 1990 : 301), este potrivit pentru producţia de masă, de mare viteză, compensând cu stabilitate şi predictibilitate pentru mecanismele incerte ale pieţei. Cu toate acestea, o critică a stabilităţii este lipsa de flexibilitate necesară atât pentru reacţia la schimbări, cât şi pentru a reuşi anticiparea acestora. Dorinţa de predictibilitate generează, de asemenea, tendinţe spre conformitate şi "bifarea căsuţelor" în locul unei analize adecvate a riscurilor (Massacci, Ruprai, Collinson, Williams, 2015 :53).

Totuşi, pentru a reacţiona la mediul de securitate cibernetică aflat într-o rapidă schimbare rapidă, flexibilitatea de mare viteză este crucială. Organizaţiile ierarhice necesită, de asemenea, o rezervă de resurse comune pentru a proteja împotriva consecinţelor inevitabile. Cu toate acestea, cererea de a pune în comun resurse suplimentare de către organizaţiile responsabile cu securitatea este întotdeauna vulnerabilă la inflaţia ameninţărilor de către ceea ce preşedintele american Eisenhower a numit complexul militar-industrial şi pentru care există dovezi în domeniul cibernetic (Brito, Watkins, 2011). Cea mai grea provocare este că acest model necesită angajamentul unui grup mare de actori, incluzând nu doar industriile şi consumatorii, ci şi reprezentanţi ai organismelor politice naţionale şi supranaţionale, precum şi grupuri ale societăţii civile de a respecta organizarea ierarhică. Un obiectiv unificator al cooperării internaţionale în materie de securitate cibernetică răspunde provocărilor moderne ale elaborării politicilor, în mod similar cu modul în care prototipurile UE au fost răspunsul la provocările consolidării păcii în Europa postbelică. Un obiectiv european comun este cel mai bine realizat în modelul de guvernanţă a reţelei, aşa cum este descris de Powell – "îndatorarea şi dependenţa pe termen lung" (Powell, 1990 : 308). O caracteristică a unui model de reţea de succes este facilitarea schimbului de date şi cunoştinţe, pentru care un mediu de încredere şi sentimentul de a fi impreuna este esenţial. Pupillo (Pupillo, 2018) menţionează, de asemenea, că "relaţiile bazate pe încredere sunt esenţiale pentru politica de securitate cibernetică şi reziliență", dezvoltând stimulentele inerente contradictorii ale pieţei (costuri private vs beneficii comune). Cu alte cuvinte, lăsarea securităţii cibernetice în domeniul relaţiilor bazate pe piaţă nu va reuşi probabil să creeze condiţiile necesare

pentru răspunsuri politice comune eficiente, în timp ce structura ierarhică, cu limite clare de autoritate poate fi inadecvată pentru provocarea de a uni comunitatea de cercetare în domeniul securităţii cibernetice printr-un obiectiv comun. Modelul de reţea nu este imun la provocări cum ar fi pierderea independenţei sau responsabilităţi neclare şi este important să nu le ignorăm. Guvernanţa colaborativă, şi anume "încercările de a reuni toate părţile interesate şi relevante pentru discuţii faţă în faţă în cursul cărora sunt elaborate politici" (Bevir, 2012), va contribui la abordarea provocărilor suplimentare şi va asigura dezvoltarea durabilă a modelului de guvernanţă. Pe scurt, o bună guvernanţă a securităţii cibernetice ar trebui să răspundă următoarelor criterii de calitate: eficienţa şi capacitatea resurselor de alocare a resurselor, potenţialul de dezvoltare şi disponibilitatea, legitimitate şi responsabilitate, transparenţă şi partajare, permiţând în acelaşi timp confidenţialitatea datelor. Se pare că există un consens general cu privire la faptul că flexibilitatea modelului de reţea pare cea mai adecvată pentru a face faţă provocărilor dinamice ale securităţii cibernetice şi pentru a oferi flexibilitatea de a se adapta la condiţiile economice şi politice ale diferitelor state.

Un alt consens există şi cu privire la problemele de securitate pe care le voi discuta în continuare, acestea fiind şi principalele provocări ale UE în materie de securitate cibernetică. Un rol esenţial în asigurarea unor standarde ridicate de securitate cibernetică pentru produsele, serviciile şi procesele TIC îl joacă sistemul de certificare a securităţii cibernetice la nivelul UE. Faptul că diferitele ţări din UE utilizează în prezent diferite sisteme de certificare a securităţii generează fragmentarea pieţei şi obstacole de reglementare. Prin Regulamentul privind securitatea cibernetică UE s-a introdus un cadru unic de certificare la nivelul UE care va consolida încrederea, va stimula şi mai mult creşterea pieţei securităţii cibernetice şi va facilita comerţul în întreaga Uniune (Grupul european de certificare a securităţii cibernetice (ECCG)).

Referitor la piaţa securităţii cibernetice a UE ştim că ţările europene ocupă 18 din primele 20 de locuri în indicele mondial al securităţii cibernetice. Valoarea pieţei securităţii cibernetice a UE este estimată la peste 130 de miliarde EUR şi creşte cu o rată de 17% pe an şi UE numără peste 60 000 de întreprinderi în domeniul securităţii cibernetice şi peste 660 de centre de expertiză în materie de securitate cibernetică (Securitatea cibernetică)

O provocare aparte este combaterea criminalităţii informatice, ce îmbracă diferite forme şi multe infracţiuni comune sunt facilitate de mijloace informatice. De exemplu, infractorii pot: să preia controlul asupra dispozitivelor personale utilizând programe malware, să fure sau să compromită date cu caracter personal şi proprietate intelectuală pentru a comite fraude online, să utilizeze internetul şi platformele de comunicare socială pentru a distribui conţinut illegal, să utilizeze „darknetul” pentru a vinde bunuri ilicite şi servicii de piratare. Unele forme de criminalitate informatică, cum ar fi exploatarea sexuală online a copiilor, provoacă prejudicii grave victimelor

lor (Europol). Se preconizează că suma de 5,5 mii de miliarde EUR ar fi costul anual al criminalităţii informatice la nivel Mondial. În cadrul Europolului a fost creat un Centru european specializat de combatere a criminalităţii informatice, pentru a ajuta ţările UE să ancheteze infracţiunile online şi să dezmembreze reţelele infracţionale. Platforma multidisciplinară europeană împotriva ameninţărilor infracţionale (EMPACT) este o iniţiativă pentru securitate sub comanda statelor membre având ca scop identificarea, prioritizarea şi abordarea ameninţărilor reprezentate de criminalitatea organizată internaţională(Directiva UE privind atacurile împotriva sistemelor informatice (Jurnalul Oficial al UE)).

O ameninţare gravă la adresa securităţii UE o reprezintă frauda în legătură cu mijloacele de plată fără numerar (Comunicat de presă, aprilie, 2019) ce poate constitui un venit semnificativ pentru criminalitatea organizată. În plus, acest tip de fraudă afectează încrederea consumatorilor în securitatea tehnologiilor digitale. În aprilie 2019, UE a adoptat noi norme de combatere a fraudelor legate de mijloacele de plată fără numerar, iar statele membre ar fi trebuit să le pună în aplicare începând cu 2021.

Îmbunătăţirea siguranţei copiilor în mediul online (Comunicat de presă, aprilie, 2021) este o altă provocare la care UE trebuie să raspundă. Astfel, în mai 2022, Comisia Europeană a propus o nouă legislaţie pentru a combate abuzurile sexuale asupra copiilor şi exploatarea sexuală a acestora în mediul online, noile norme fiind în prezent discutate în cadrul Consiliului. Între timp, se aplică un acord provizoriu cu privire la măsurile temporare care le permit furnizorilor de servicii de comunicaţii electronice precum serviciile de webmail şi de mesagerie să continue să detecteze, să elimine şi să semnaleze abuzul sexual online asupra copiilor, ceea ce include şi măsurile de combatere a ademenirii copiilor în scopuri sexuale, până la adoptarea măsurilor legislative permanente. Măsurile au intrat în vigoare în august 2021 şi vor expira în 2024(Abuzul sexual asupra copiilor).

Normele şi politicile UE abordează şi alte aspecte legate de justiţie şi de asigurarea respectării legii ale combaterii criminalităţii informatice şi a criminalităţii în general, cum ar fi accesul la probele electronice, criptarea şi păstrarea datelor (Un acces mai bun la probele electronice, pentru combaterea criminalităţii). Infractorii exploatează tehnologia digitală pentru a comite infracţiuni şi pentru a ascunde activităţi ilicite. Prin urmare, autorităţile de aplicare a legii şi autorităţile judiciare se bazează tot mai mult în anchetele şi urmările lor penale pe probele electronice, precum texte, e-mailuri sau aplicaţii de mesagerie. Acesta este motivul pentru care UE lucrează la norme noi care vor facilita şi vor accelera accesul transfrontalier la probele electronice. UE se străduieşte să stabilească o discuţie activă cu industria tehnologiei pentru a se obţine echilibrul adecvat între asigurarea continuării utilizării unei tehnologii de criptare solide şi garantarea exercitării competenţelor autorităţilor de aplicare a legii şi ale autorităţilor judiciare în aceleaşi condiţii ca în mediul offline. În decembrie 2020, Consiliul a adoptat o rezoluţie privind criptarea, evidenţiind nevoia

atât de securitate prin criptare, cât şi de securitate în pofida criptării (Comunicat de presă, decembrie,2020).

În prezent, pentru a combate criminalitatea în mod eficace, este important ca prestatorii de servicii să păstreze anumite date care pot fi divulgate în anumite condiţii stricte în scopul combaterii criminalităţii. Cu toate acestea, păstrarea datelor poate încălca drepturile fundamentale individuale, în special drepturile la viaţă privată şi la protecţia datelor cu caracter personal. Consiliul a adoptat concluzii privind păstrarea datelor din comunicaţiile electronice în scopul combaterii criminalităţii (Comunicat de presă, iunie, 2019) şi a însărcinat Comisia să colecteze informaţii suplimentare şi să organizeze consultări specifice, în cadrul unui studiu cuprinzător privind posibile soluţii pentru păstrarea datelor, inclusiv luarea în considerare a unei viitoare iniţiative legislative.

Uniunea Europeană şi statele sale membre promovează cu fermitate un spaţiu cibernetic deschis, liber, stabil şi securizat, în care drepturile omului, libertăţile fundamentale şi statul de drept să fie pe deplin respectate în scopul stabilităţii sociale, al creşterii economice, al prosperităţii şi al integrităţii unor societăţi libere şi democratice. UE face eforturi mari pentru a se proteja împotriva ameninţărilor cibernetice provenind din ţări terţe, în special prin intermediul unui răspuns diplomatic comun denumit „setul de instrumente pentru diplomaţia cibernetică"(Comunicat de presă, mai, 2019). Acest răspuns include cooperare şi dialog diplomatice, măsuri preventive împotriva atacurilor cibernetice şi sancţiuni. Strategia de securitate cibernetică a UE, adoptată de Comisia Europeană şi de SEAE în decembrie 2020, consolidează răspunsul diplomatic al UE la atacurile cibernetice.

Spaţiul cibernetic este considerat al cincilea câmp de luptă, la fel de important pentru operaţiunile militare ca şi domeniile terestru, maritim, aerian şi spaţial. Este un domeniu care cuprinde totul, de la reţelele de informaţii şi telecomunicaţii, infrastructură şi datele pe care le deţine până la sistemele informatice, operatori şamd (Comunicat de presă, noiembrie, 2022). UE cooperează în domeniul apărării în spaţiul cibernetic prin activităţile Agenţiei Europene de Apărare (AEA), în colaborare cu Agenţia UE pentru Securitate Cibernetică şi cu Europolul. AEA sprijină statele membre în construirea unei forţe de muncă militare competente în domeniul apărării cibernetice şi asigură disponibilitatea unei tehnologii proactive şi reactive în domeniul apărării cibernetice.

Securitatea cibernetică este una dintre priorităţile UE în răspunsul la pandemia de COVID-19, în timpul căreia atacurile cibernetice s-au intensificat. Planul include investiţii suplimentare, iar găsirea unor soluţii inovatoare care să poată proteja statele membre împotriva celor mai recente şi mai avansate ameninţări cibernetice este esenţială. Din acest motiv, securitatea cibernetică este o parte importantă a programelor-cadru de finanţare a cercetării şi inovării ale UE, Orizont 2020 şi succesorul acestuia, Orizont Europa. În mai 2020, UE a angajat 49 de milioane

EUR pentru a stimula inovarea în domeniul securităţii cibernetice şi al sistemelor de protecţie a vieţii private (Comunicat de presă, mai 2020). În cadrul programului Europa digitală pentru perioada 2021-2027, UE s-a angajat să investească 1,6 miliarde EUR în capacitatea de securitate cibernetică şi în implementarea pe scară largă a infrastructurilor şi instrumentelor de securitate cibernetică în întreaga UE pentru administraţii publice, întreprinderi şi persoane fizice (The Digital Europe Programme).

După cum am văzut, Strategia UE de securitate cibernetică (Comunicat de presă, decembrie 2020) îşi propune să creeze rezistenţa la ameninţările cibernetice şi să se asigure că cetăţenii şi întreprinderile beneficiază de tehnologii digitale de încredere. Numărul atacurilor cibernetice continuă să crească, atacuri din ce în ce mai sofisticate ce provin dintr-o gamă largă de surse atât din interiorul, cât şi din afara UE. Prin urmare, UE ar trebui să-şi canalizeze eforturile pentru o digitalizare sigură. Ar trebui să găsească soluţii inovatoare, să crească standardele de securitate cibernetică pentru serviciile esenţiale şi infrastructurile critice, precum şi să contribuie la dezvoltarea şi aplicarea de noi tehnologii. Guvernele, întreprinderile şi cetăţenii ar trebui să îşi împartă responsabilitatea în vederea asigurării unei transformări digitale securizate. Suveranitatea tehnologică a UE trebuie să se bazeze pe reziliența tuturor serviciilor şi produselor conectate. Toate cele patru comunităţi cibernetice – cele care se ocupă de piaţa internă, de aplicarea legii, diplomaţie şi apărare – trebuie să colaboreze pentru o conştientizare comună a ameninţărilor.

BIBLIOGRAFIE

Abuzul sexual asupra copiilor, Child sexual abuse, https://home-affairs.ec.europa.eu/policies/internal-security/child-sexual-abuse_en

Apărarea cibernetică: concluziile Consiliului subliniază importanţa consolidării în continuare a rezilienţei UE pentru a face faţă ameninţărilor cibernetice (comunicat de presă, 23 mai 2023), https://www.consilium.europa.eu/ro/press/press-releases/2023/05/23/cyber-defence-council-conclusions-stress-the-importance-of-further-strengthening-the-eu-s-resilience-to-cyber-threats/

Artificial intelligence cybersecurity challenges(2021). European Union Agency for Cyber- security (ENISA), https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges

Atacurile cibernetice: Consiliul poate de acum să impună sancţiuni (comunicat de presă, 17/05/2019), https://www.consilium.europa.eu/ro/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions

Bevir M., *Governance: A very short introduction*, OUP Oxford

Brito J., Watkins T.(2011). *Loving the cyber bomb-the dangers of threat inflation in cybersecurity policy*.Harv. National Security J., p.3

Centrul de răspuns la incidente de securitate cibernetică pentru instituţiile, organele şi agenţiile UE (CERT-UE), https://european-union.europa.eu/institutions-law-

budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/computer-emergency-response-team-eu-institutions-bodies-and-agencies-cert-eu_ro

Centrul european de combatere a criminalităţii informatice (Europol), https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

Combaterea abuzului online asupra copiilor – acord informal cu Parlamentul European privind normele temporare(Comunicat de presă, 29 aprilie 2021) https://www.consilium.europa.eu/ro/press/press-releases/2021/04/29/combating-child-abuse-online-informal-deal-with-european-parliament-on-temporary-rules/

Concluziile Consiliului Uniunii Europene privind păstrarea datelor în scopul combaterii criminalităţii, Comunicat de presă , iunie 2019, https://data.consilium.europa.eu/doc/document/ST-9663-2019-INIT/ro/pdf

Consiliul adoptă concluzii privind Strategia de securitate cibernetică a UE (comunicat de presă, 22 martie 2021), https://www.consilium.europa.eu/ro/press/press-releases/2021/03/22/cybersecurity-council-adopts-conclusions-on-the-eu-s-cybersecurity-strategy/

Consolidarea securităţii cibernetice şi a rezilienţei la nivelul UE – acord provizoriu al Consiliului şi al Parlamentului European (comunicat de presă, 13 mai 2022) https://www.consilium.europa.eu/ro/press/press-releases/2022/05/13/renforcer-la-cybersecurite-et-la-resilience-a-l-echelle-de-l-ue-accord-provisoire-du-conseil-et-du-parlement-europeen/

Conturarea viitorului digital al Europei – Consiliul adoptă concluzii (comunicat de presă, 9 iunie 2020), https://www.consilium.europa.eu/ro/press/press-releases/2020/06/09/shaping-europe-s-digital-future-council-adopts-conclusions/

Convenţia de la Budapesta privind criminalitatea informatică (2001), https://polis.osce.org/file/11311/download?token=M5C2qnQI

Criptarea: Consiliul adoptă o rezoluţie privind securitatea prin criptare şi securitatea în pofida criptării, Comunicat de presă, decembrie 2020, https://www.consilium.europa.eu/ro/press/press-releases/2020/12/14/encryption-council-adopts-resolution-on-security-through-encryption-and-security-despite-encryption/

Cronologie – securitatea cibernetică https://www.consilium.europa.eu/ro/policies/cybersecurity/timeline-cybersecurity/

Cybersecurity challenges in the uptake of artificial intelligence in autonomous driving (2021). European Union Agency for Cybersecurity, https://www.enisa.europa.eu/publications/enisa-jrc-cybersecurity-challenges-in-the-uptake-of-artificial-intelligence-in-autonomous-driving

Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. (2013) Joint communication to the European Parliament, the Council, the European economic and social committee and the com- mittee of the regions, [Online]:

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

Cybersecurity – Threats Challenges Opportunities (2016) p.1-70 https://www.acs.org.au/

Cyber Defence: EU boosts action against cyber threats, Comunicat de presă, 22 noiembrie 2022, https://ec.europa.eu/commission/presscorner/detail/en/IP_22_6642

Daly Joseph P.(1993), *The Computer Fraud and Abuse Act - A New Perspective: Let the Punishment Fit the Damage*, 12 J. Marshall J. Computer & Info. L. 445, p.1-23, https://repository.law.uic.edu/cgi/viewcontent.cgi?article=1377&context=jitpl

Despre Grupul european de certificare a securității cibernetice (ECCG)- https://digital-strategy.ec.europa.eu/ro/policies/cybersecurity-certification-group

Directiva UE privind atacurile împotriva sistemelor informatice (Jurnalul Oficial al UE) https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32013L0040

DIRECTIVA 2002/21/CE A PARLAMENTULUI EUROPEAN ŞI A CONSILIULUI din 7 martie 2002 privind un cadru de reglementare comun pentru reţelele şi serviciile de comunicaţii electronice (Directivă-cadru) (JO L 108, 24.4.2002, p. 33) https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:02002L0021-20091219

ENISA Report (2021) , *TOWARDS A COMMON ECSC ROADMAP*, European Union Agency for Cybersecurity, p.1-50, www.enisa.europa.eu

EU cyber defense policy framework (2018) http://data.consilium.europa.eu/doc/document/ST-14413-2018- INIT/en/pdf

EU grants nearly €49 million to boost innovation in cybersecurity and privacy systems, Comunicat de presă, mai 2020, https://digital-strategy.ec.europa.eu/en/news/eu-grants-nearly-eu49-million-boost-innovation-cybersecurity-and-privacy-systems

Ghid de securitate cibernetică, p.1-30, https://www.sri.ro/assets/files/publicatii/ghid_de_securitate_cibernetica.pdf

History of cyber security (2023), articol disponibil pe https://cyber-security.degree/resources/history-of-cyber-security/

International Data Corporation- https://digital-strategy.ec.europa.eu/ro/policies/internet-things-policy

Kidd Chrissy (2023), Is the CIA Triad Relevant ?, https://www.splunk.com/en_us/blog/learn/cia-triad-confidentiality-integrity-availability.html

Kononenko V.(2021), *Improving the common level of cybersecurity across the EU*, Initial Appraisal of a European Commission Impact Assessment, EPRS, European Parliament

Lupta UE împotriva criminalității organizate (informaţii generale) - https://www.consilium.europa.eu/ro/policies/eu-fight-against-crime/

Massacci F., Ruprai R., Collinson M., Williams J. (2015) *Economic impacts of rules-versus risk-based cybersecurity regulations for critical infrastruc- ture providers*. IEEE Security & Privacy, 14(3), p.52-60

Negreiro M.(2019), *ENISA and a new cybersecurity act*, Briefing, EPRS, European Parliament

Negreiro M., Belluomini A.(2020), *The new European cybersecurity competence centre and network*, Briefing, EPRS, European Parliament

New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient, Comunicat de presă, decembrie 2020, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391

Prakas Mrinal (2023), *CIA Triad in Cyber Security: Definition, Examples, Importance*, https://www.knowledgehut.com/blog/security/cia-in-cyber-security

Pupillo L.(2018), *EU Cybersecurity and the Paradox of Progress*, CEPS Policy Insight

Regulamentul UE privind securitatea cibernetică, https://eur-lex.europa.eu/RO/legal-content/summary/the-eu-cybersecurity-act.html

Powell, W. W. (1990), *Neither market nor hierarchy: network forms of organisation*, Research in Organisational Behaviour, 12,p. 295 – 336.

Securitatea cibernetică- https://www.consilium.europa.eu/ro/policies/cybersecurity/

Security economics and the internal market. https://www.enisa.europa.eu/ publications/archive/economics-sec.

Selectarea sediului Centrului de competenţe european industrial, tehnologic şi de cercetare în materie de securitate cibernetică (informaţii generale) https://www.consilium.europa.eu/ro/policies/cybersecurity/seat-selection-cybersecurity-centre/

The Digital Europe Programme (DIGITAL) , https://digital-strategy.ec.europa.eu/en/activities/digital-programme

The European Agenda on Security (2015). Comm. to the European Parliament, the Council, the European economic and social committee and the committee of the regions, http://www.europarl.europa.eu/cmsdata/125863/EU%20agenda%20on%20security.pdf

Triada CIA explicate (2021) https://www.routech.ro/triada-cia-confidentialitate-integritate-si-disponibilitate-explicate/

UE instituie norme mai stricte pentru combaterea fraudelor legate de mijloacele de plată fără numerar (comunicat de presă, 9 aprilie 2019) https://www.consilium.europa.eu/ro/press/press-releases/2019/04/09/eu-puts-in-place-tighter-rules-to-fight-non-cash-payment-fraud/

UE va deveni mai rezistentă la atacurile cibernetice: Consiliul sprijină acordul privind certificarea comună şi o agenţie consolidată (comunicat de presă, 19/12/2018) ,

https://www.consilium.europa.eu/ro/press/press-releases/2018/12/19/eu-to-become-more-cyber-proof-as-council-backs-deal-on-common-certification-and-beefed-up-agency/

Un acces mai bun la probele electronice, pentru combaterea criminalităţii, https://www.consilium.europa.eu/ro/policies/e-evidence/

Understanding the increase in supply chain security attacks. https://www.enisa.europa.eu/news/enisa- news/understanding- the- increase- in-supply-chain-security-attacks.

Zygierewicz A.(2020), *Directive on security of network and information systems* (NIS Directive), Implementation appraisal briefing, EPRS, European Parliament