REVOLUȚIA DIGITALĂ ȘI PROTECȚIA DREPTURILOR OMULUI: ÎNFRUNTAREA ATACURILOR CIBERNETICE

THE DIGITAL REVOLUTION AND THE PROTECTION OF HUMAN RIGHTS: FACING CYBER ATTACKS

CZU: [343.53:004]:342.7 **DOI:**https://doi.org/10.59295/ssdoed2024.25

Andreea-Nicoleta DRAGOMIR[1],
Ana MORARI (BAYRAKTAR)[2],
Ștefana-Magdalena MAGDAN[3]

ABSTRACT. *In recent decades, the development of information technologies has been a significant force in the evolution of our society. Amongst other advantages and conveniences, the dynamics of digital innovations have influenced the way we interact socially and access information systems globally. However, we need to be aware of the challenges associated with digitisation, such as data security, unequal access to technology and threats to privacy.*

To remedy this problem, law and legal science needs new theoretical and practical solutions to formulate principles and models of digital development that would restore the effectiveness of law enforcement in the context of frequent cyber attacks. The effective development and implementation of cyber security policy is a prerequisite for the development of a knowledge-based society. In this context, the provision of training and guidance in this area is a key element in raising staff awareness of potential threats and preventive measures. Establishing well-defined access policies, limiting privileges and using specialised monitoring software facilitates early detection of suspicious activities or intrusion attempts.

This article aims to analyse the implications of cyber attacks on fundamental human rights. In doing so, we aim to examine the cost-effectiveness of existing legal instruments and the response of the international community to strengthening a system of human rights protection in the context of the digital revolution.

Keywords: *cyber-attack, security, threats, technologies, civil infrastructure, protection system*

REZUMAT. *În ultimele decenii, dezvoltarea tehnologiilor informaționale a reprezentat o forță semnificativă în evoluția societății noastre. Cunoscând printre altele o serie de avantaje și facilități, dinamica inovațiilor digitale a influențat modul de interacționare socială și accesul la sistemele informaționale la nivel global. Cu toate acestea, trebuie să fim conștienți de provocările asociate cu digitalizarea, cum ar fi securitatea datelor, accesul inegal la tehnologie și amenințările la adresa intimității.*

Pentru a remedia această problemă, legislația și știința juridică are nevoie de noi soluții teoretice și practice pentru a formula principii și modele de dezvoltare digitală care ar re-

[1] Andreea-Nicoleta DRAGOMIR, Universitatea ”Lucian Blaga” din Sibiu, Facultatea de Drept ”Simion Bărnuțiu”, andreea.dragomir@ulbsibiu.ro, **https://orcid.org/0000-0002-9358-8098**

[2] Ana MORARI (BAYRAKTAR), Universitatea ”Lucian Blaga” din Sibiu, Facultatea de Drept ”Simion Bărnuțiu”, ana.morari@ulbsibiu.ro, **https://orcid.org/0009-0002-9363-8718**

[3] Ștefana-Magdalena MAGDAN, Universitatea ”Lucian Blaga” din Sibiu, Facultatea de Drept ”Simion Bărnuțiu”, magdalena.magdan@ulbsibiu.ro, **https://orcid.org/0009-0002-0238-3087**

dresa eficacitatea aplicării legii în contextul frecventelor atacuri cibernetice. Elaborarea și implementarea efectivă a politicii de securitate cibernetică reprezintă o condiție prealabilă pentru dezvoltarea unei societăți bazate pe cunoaștere. În acest context, furnizarea de formare și îndrumare în acest domeniu reprezintă un element-cheie pentru sensibilizarea personalului cu privire la amenințările potențiale și la măsurile preventive. Stabilirea de politici de acces bine definite, limitarea privilegiilor și utilizarea de software-uri specializate de monitorizare facilitează detectarea rapidă a activităților suspecte sau a tentativelor de intruziune.

Acest articol își propune să analizeze implicațiile atacurilor cibernetice asupra drepturilor fundamentale ale omului. În acest sens, ne propunem să examinăm rentabilitatea instrumentelor legale existente și răspunsul comunității internaționale cu privire la consolidarea unui sistem de protecție a drepturilor omului în contextul revoluției digitale.

Cuvinte-cheie: *atac cibernetic, securitate, amenințări, tehnologii, infrastructura civilă, sistem de protecție.*

În epoca societății informaționale, caracterizată de o preeminență a mediului digital, s-au manifestat schimbări care, în ciuda elementelor benefice, nu se limitează exclusiv la aspecte favorabile. Principalele inconveniente derivă din riscurile asociate incidentelor cibernetice, fenomen în creștere.

Dispozitivele și structura *Tehnologiilor Informației și Comunicațiilor (TIC)* manifestă un grad înalt de complexitate și inter-conectivitate, unde perturbarea unei componente poate cauza efecte adverse semnificative asupra funcționalității celorlalte componente. În ultimul timp, specialiștii și factorii de decizie au manifestat o crescută îngrijorare cu privire la necesitatea protejării sistemelor TIC împotriva atacurilor cibernetice, acțiuni intenționate ale indivizilor neautorizați care vizează accesul ilicit la sisteme în scopul furtului, distrugerii sau a altor activități ilegale.

Procesul de asigurare a securității sistemelor TIC și a conținutului acestora a fost consacrat sub termenul de **securitate cibernetică**. Cu toate că securitatea cibernetică reprezintă un concept amplu, insuficient de detaliat în unele contexte, termenul este util, deși nu poate fi circumscris unei definiții concrete.

Din punct de vedere etimologic, termenul ”*cyber*” cuprinde *lato sensu* orice activități, dispositive și evenimente legate de calculatoare, informațiile electronice și/sau rețelele digitale [1]:

- Securitatea ciberneică reprezintă termenul definitoriu al protecției calculatoarelor, a informațiilor electronice și/sau rețelele digitale împotriva scurgerilor, transmiterii, interceptării, modificării sau distrugerii neautorizate, accidentale sau intenționate;
- Spațiu cybernetic se referă la reprezentarea spațială în care se desfășoară toate procesele digitale asupra rețelelor electronice și informaționale;
- Un atac cibernetic constituie actul militar de deturnare a calculatoarelor, a informațiilor electronice și/sau a rețelelor digitale, care are ca scop deplasarea, expulzarea, distrugerea sistemelor critice, financiare sau de informații.

Amenințările cibernetice derivă din activitățile desfășurate sau susceptibile de a fi întreprinse de către indivizi specializați în atacuri cibernetice. Acești atacatori se aliniază cu una sau mai multe categorii distincte, precum[2]:

- infractori cu intenții orientate către dobândirea de avantaje financiare prin practici precum furtul sau șantajul cibernetic;
- spioni care își propun să sustragă informații clasificate sau brevetate, utilizate de entități guvernamentale sau din sectorul privat;
- practicanți ai războiului cibernetic la nivel guvernamental, dedicați dezvoltării de capacități și efectuării de atacuri cibernetice în susținerea obiectivelor strategice ale unei țări;
- "Hacktiviști", care desfășoară atacuri cibernetice din motive neasociate cu beneficii financiare;
- Teroriștii care adoptă atacurile cibernetice ca formă de război, fie cu aprobarea oficială a unui stat, fie independent de aceasta.

Atacatorii cibernetici își focalizează eforturile asupra exploatării acestor vulnerabilități umane. Aceștia folosesc tehnici sofisticate de inginerie socială pentru a câștiga încrederea utilizatorilor și pentru a-i determina să dezvăluie informații sensibile, cum ar fi parole sau date personale. Atacurile cibernetice pot utiliza și metode psihologice pentru a manipula comportamentul utilizatorilor și a-i convinge să desfășoare acțiuni care să favorizeze atacatorii.

Rolul atacatorilor cibernetici nu se rezumă doar la exploatarea vulnerabilităților umane, ci și la identificarea și exploatarea erorilor sistemelor tehnologice. Ei profită de vulnerabilitățile de securitate software și hardware pentru a pătrunde în sisteme și rețele, iar odată ajunși acolo, pot să compromită integritatea, confidențialitatea sau disponibilitatea datelor.

Cu toate acestea, fiecare atac cibernetic și influența lui asupra drepturilor omului trebuie analizat în strânsă concordanță cu contextul unei situații concrete, sau cel puțin în legătură cu un domeniu bine definit pentru a putea identifica aplicabilitatea instrumentelor legale și, prin urmare, pentru a putea stabili un șir de măsuri legale și tehnice adecvate.

Categorizarea și clasificarea amenințărilor cibernetice

Când elemente fundamentale ale societății, cum ar fi sistemele de comunicare, infrastructurile critice, instituțiile bancare și guvernamentale, devin ținta atacurilor cibernetice, ne confruntăm cu o nevoie stringentă de a dezvolta competențe avansate în identificarea și înțelegerea amenințărilor cibernetice. Aceasta presupune nu doar o abordare reactivă, ci și una proactivă, orientată spre anticiparea și prevenirea posibilelor atacuri. Prin urmare, este esențial să catalogăm tipurile de amenințări cu care ne confruntăm:[3]

- **Drive-by exploits/download:** se referă la atacurile care descarcă automat programe malware în calculatorul utilizatorului fără știrea sau consimțământul acestuia. Acest tip de atac se realizează prin exploatarea vulnerabilităților browserelor web și a plugin-urilor. Prejudiciile pot include scurgerea de date, ceea ce duce la

pierderi financiare.[4] Aplicațiile mobile elaborate cu scopul de a sustrage informații de plată, date de identificare și fonduri din conturile bancare ale utilizatorilor au înregistrat o creștere de 50%, conform ultimelor statistici, în cursul primei jumătăți a anului 2019.[5]

- **Ransomware:** Atacurile ransomware au continuat să fie una dintre cele mai mari amenințări cibernetice în 2022. În același timp, acestea devin din ce în ce mai complicate. Conform datelor citate de Agenția UE pentru Securitate Cibernetică, cererea cea mai mare de ransomware a crescut de la 13 milioane EUR în 2019 la 62 milioane EUR în 2021. În 2021 ransomware-ul global a produs daune în valoare de 18 miliarde de euro – de 57 de ori mai mult decât în 2015. [6]

Zeus, troianul cel mai des folosit pentru furtul datelor bancare: Pentru a crea link-urile de download și fisierele executabile Zeus, virusul folosește data și ora de pe computerul victimei. Virusul colectează anul, luna, ziua, ora și minutul sistemului, creează doua cuvinte duble, adaugă un nume popular de domeniu web și completează apoi link-ul cu „iforum". Practic, victima plătește o sumă de bani, dar nu primește fișierul promis.[7]

- **Virușii**: virușii informatici sunt aplicații cu efecte adesea distructive, concepute pentru a infecta un sistem informatic. Virușii au două caracteristici principale: se autoexecută și se automulțumesc în sistemul infectat.[8]
- **Rogueware**: aplicație care induce în eroare utilizatorii să plătească bani pentru a elimina infecțiile false detectate în sistemul de operare. De cele mai multe ori, acest tip de aplicație pretinde că elimină programele malware detectate în calculatoare, dar în realitate instalează aplicații cu efect distructiv.[9]
- **DoS / DDoS**: are ca efect compromiterea funcționării anumitor servicii de internet. Unul dintre cele mai frecvente atacuri DDoS este atacul de tip "packet flood", care trimite un număr mare de pachete către sistemul victimă, care are ca efect blocarea pachetelor deschise conexiuni deschise și încărcarea traficului de rețea, ceea ce duce la întreruperea serviciilor furnizate de către sistemul atacat.[10]

Aceste categorii de atacuri au experimentat o diversificare semnificativă recent, iar unele dintre ele pot fi caracterizate ca potențiale epidemii globale, întrucât manifestă o propagare extinsă și rapidă, contribuind astfel la o rata considerabilă de diseminare.

Dreptul internațional în operațiuni cibernetice

Legislația privind operațiunile cibernetice în dreptul internațional se confruntă cu o serie de provocări complexe, generate de natura specifică a cyberspațiului și de absența unor delimitări clare între frontierele statelor. În acest context, stabilirea unor norme coerente pentru calificarea operațiunilor cibernetice, determinarea jurisdicției și definirea răspunsurilor statelor poate fi în mod evident calificată ca fiind una dificilă și necesară.

În era cyberspațiului, unde frontierele fizice devin din ce în ce mai abstracte, necesitatea reglementării operațiunilor cibernetice la nivel internațional devine imperativă. Războiul cibernetic afectează o gamă diversă de domenii, impunând o adaptare continuă a cadrului legal pentru a gestiona provocările emergente și a asigura securitatea în acest spațiu virtual dinamic.

În contextul spațiului extraterestru, se propune actualizarea a trei tratate-cheie: Tratatul privind spațiul extraterestru, Tratatul privind Luna și Convenția privind răspunderea. Obiectivul acestor propuneri este stabilirea unui cadru legal robust pentru a aborda amenințările cibernetice în aceste domenii specifice, reflectând necesitatea ajustării normelor la dinamica cyberspațiului.[11]

În sfera aviației, se explorează reglementări care să integreze atacurile cibernetice în convenții existente, cum ar fi Convenția de la Montreal din 1971 și Convenția de la Chicago din 1944. Aceste propuneri vizează adaptarea legislației curente pentru a proteja aviația civilă împotriva amenințărilor cibernetice în evoluție continuă.

În ceea ce privește legea mării, se examinează potențialul Convenției Națiunilor Unite din 1982 de a servi drept cadru descurajator pentru operațiunile de război cibernetic, evidențiind articolele 19 și 109[12]. Aceste propuneri reflectă efortul de a ajusta dreptul maritim la noile realități ale cyberspațiului. De asemenea, în domeniul telecomunicațiilor, se propun reglementări pentru atacurile cibernetice sub egida Convenției internaționale privind telecomunicațiile.[13]

Aceste inițiative subliniază necesitatea unui cadru legal internațional coeziv și adaptabil pentru a gestiona amenințările cibernetice în diversele sectoare ale cyberspațiului. Adaptarea continuă a normelor legale este esențială pentru a ține pasul cu dinamica rapidă a tehnologiilor cibernetice și pentru a asigura un mediu securizat în cyberspațiu.

Convenția privind criminalitatea informatică[14] reprezintă un avans semnificativ, încercând să ofere o bază pentru combaterea infracțiunilor cibernetice. Totuși, chiar și aceasta are limitări și nu abordează în mod exhaustiv întreaga diversitate a operațiunilor cibernetice, iar problemele privind jurisdicția rămân neclare, mai ales în contextul cyberspațiului global.

În cadrul atacurilor cibernetice, dificultățile apar în evaluarea impactului acestora și în determinarea aplicării dreptului la autoapărare, conform prevederilor Cartei ONU. Absența unei practici clare și a unui consens internațional în privința definirii unui atac cibernetic drept "armat" adaugă un grad suplimentar de complexitate și incertitudine.

În ceea ce privește cyberwarfare, distincția esențială dintre Jus ad bellum și Jus in bello devine evidentă.[15] Regulile de purtare a războiului întâmpină dificultăți în aplicarea lor la atacurile cibernetice, având în vedere evoluția rapidă a tehnologiei și a capacităților cibernetice. Principiile fundamentale ale proporționalității și distincției între obiectivele civile și cele militare devin problematice în contextul atacurilor cibernetice, unde consecințele pot fi dificil de evaluat și de diferențiat.

Cu toate acestea, deși evoluția tehnologiei permite o acuratețe și precizie a țintei, rezultatul raportat la cum sunt afectați civilii este dezastruos de cele mai multe ori. Întreaga infrastructură se află într-o indisolubilă legătură cu populația civilă.

La nivel internațional, unul dintre cele mai recente documente care încearcă să reglementeze problematica în discuție este Manualul Tallinn. Acesta a fost elaborat și construit de un grup de experți care au afirmat că Dreptul internațional umanitar (DIU) are aplicabilitate în cazul războiului cibernetic și, prin intermediul manualului, oferă detalii despre modul în care regulile DIU vor fi implementate în acest domeniu [16].

Evaluarea conformității cu dreptul a armelor noi este de interes pentru toate statele, contribuind la asigurarea faptului că forțele armate acționează în conformitate cu angajamentele lor internaționale. Articolul 36 al Protocolului I adițional la Convențiile de la Geneva din 1977 impune fiecărui stat parte să verifice că orice armament nou pe care îl implementează sau ia în considerare respectă regulile dreptului internațional umanitar (DIU), aspect subliniat și în Manualul Tallinn, cu privire la cyberspațiu și arme cu tehnologie avansată utilizată din ce în ce mai frecvent în prezent.

La cea de-a 28-a Conferință Internațională a Crucii Roșii și Semilună Roșie din 2003, statele parte la Convențiile de la Geneva au solicitat o "revizuire riguroasă și multidisciplinară"[17] a noilor arme, mijloacelor și metodelor de război, pentru a se asigura că normele legale nu sunt depășite de progresul tehnologic. Utilizarea operațiunilor cibernetice în conflictele armate reprezintă un exemplu concret al acestei dezvoltări tehnologice rapide.

În ceea ce privește terorismul cibernetic, lacunele din legislația internațională devin evidente. Acordurile regionale și rezoluțiile ONU existente nu abordează pe deplin provocările actuale ale terorismului cibernetic. Astfel, se impune revizuirea și actualizarea legislației internaționale pentru a reflecta adecvat amenințările cibernetice în evoluție.

Sancțiunile UE împotriva Amenințărilor CiberneticePartea superioară a formularului

Uniunea Europeană desfășoară o serie de inițiative cu scopul de a consolida reziliența cibernetică, a contracara fenomenul criminalității informatice și a promova diplomația și apărarea cibernetică.

Uniunea Europeană desfășoară o serie de inițiative cu scopul de a consolida reziliența cibernetică, a contracara fenomenul criminalității informatice și a promova diplomația și apărarea cibernetică.

Măsurile restrictive specifice adoptate ca răspuns la amenințările cu atacuri cibernetice, atât la adresa Uniunii și a statelor membre, cât și a statelor terțe, constituie o bun răspuns diplomatic la adresa activităților cibernetice rău intenționate.

La data de 16 aprilie 2018, Consiliul a emis concluzii în care a condamnat utilizarea ilegală a tehnologiilor informației și comunicațiilor, inclusiv în cazul atacurilor cibernetice cunoscute sub numele de **"WannaCry"** și **"NotPetya"**, care au cauzat daune economice semnificative în Uniune și în afara acesteia [18].

Prin urmare, Consiliul a ajuns la ideea implementării unor restricții sub forma includerii a a **șase persoane**[19] și **trei entități** [20] răspunzătoare de atacurile cibernetice menționat anterior sau implicate în acestea, pe lista celor cărora li se aplică interdicții de călătorie și o înghețare a activelor [21].

La 16 decembrie 2020, o nouă strategie de securitate cibernetică a UE, **"*The EU's Cybersecurity Strategy for the Digital Decade*"** a fost adoptată. Principalele obiective ale acesteia au fost:

- propunere de actualizare a directivei NIS pentru o mai bună protecție a rețelelor și a sistemelor informatice
- propunere de directivă privind reziliența entităților critice.

În general, strategia își propunea să furnizeze un șir de garanții capabile să susțină securitatea și un mediu "safe" de navigare pe rețelele net, acesta fiind structurată pe 3 piloni [22]:

- rezilienţă, suveranitate tehnologică și poziția de lider a UE;
- consolidarea capacității operaționale de prevenire, descurajare și răspuns;
- promovarea unui spațiu cibernetic global și deschis printr-o cooperare sporită.

Propunerea de Directiva privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune (Directiva NIS revizuită/„NIS 2")[23] – extinde domeniul de aplicare al directivei NIS și propune un șir de măsuri juridice capabile să construiască un sistem al securității cibernetice, asigurând următoarele [24]:

•Pregătirea statelor membre, solicitând ca acestea să fie echipate în mod corespunzător. De exemplu, cu o echipă de răspuns la incidente de securitate informatică **(CSIRT)** și cu o autoritate națională competentă pentru rețele și sisteme informatice **(NIS)**;

- Cooperarea între toate statele membre, prin înființarea unui grup de cooperare care să sprijine și să faciliteze cooperarea strategică și schimbul de informații între statele membre.
- Cultură a securității în toate sectoarele care sunt vitale pentru economia și societatea noastră și care se bazează în mare măsură pe TIC, cum ar fi energia, transporturile, apa, sectorul bancar, infrastructurile pieței financiare, asistența medicală și infrastructura digitală.

Propunerea de Directivă privind reziliența entităților critice în baza acestei directive statele membre vor stabili o strategie națională de consolidare a rezilienței entităților critice, să efectueze o evaluare a riscurilor cel puțin o dată la patru ani și să identifice entitățile critice care furnizează servicii esențiale [25]. Această directivă cuprinde zece sectoare: energia, transporturile, activitatea bancară, infrastructurile pieței financiare, sănătatea, apa potabilă, apa reziduală, infrastructura digitală, administrația publică și spațiul [26].

Riscuri - prejudicii aduse de atacuri cibernetice

În ultimii ani, am asistat la o serie de atacuri cibernetice de amploare, evenimente care au atras atenția întregii lumi. Aceste atacuri au vizat atât infrastructuri fizice critice, exemplificate de atacul asupra Colonial Pipeline [27], care a paralizat distribuția de gaze, cât și infrastructuri digitale critice, precum atacul SolarWinds [28], ce a oferit hackerilor acces la rețelele guvernamentale americane. În plus, spitalele și serviciile de sănătate, alături de industriile comerciale, au fost afectate de atacuri profitabile de tip ransomware. Deși consecințele fizice durabile au fost limitate, aceste atacuri s-au dovedit mult mai severe decât s-ar fi crezut la o primă vedere.

Rezultatul imediat al acestor atacuri a fost o scădere semnificativă a încrederii publicului în capacitatea guvernelor de a-i proteja împotriva daunelor. În același timp, milioane de oameni au experimentat anxietate intensă față de noua percepție a vulnerabilității lor la astfel de atacuri, generând solicitări pentru politici de securitate cibernetică mai stricte și alimentând o dispoziție de a sacrifica libertățile civile digitale în numele securității.

Întrucât atacul cibernetic nu are limite, acesta se regăsește pretutindeni și implică riscuri substanțiale, atunci când este folosit, pentru cei vizați și nu numai. Astfel, s-au identificat cinci puncte cheie sub care impactul generat de un atac cibernetic poate fi clasificat:

1. Fizic/digital;
2. Economic;
3. Psihologic;
4. Reputațional;
5. Social. [29]

Atacurile cibernetice generează niveluri similare de stres psihologic. Acest lucru ridică provocări semnificative pentru normele și practicile de securitate internaționale și naționale. În primul rând, suferința psihologică provocată de atacurile cibernetice ar putea fi suficientă pentru a încadra aceste incidente ca atacuri armate, conform definiției dreptului internațional. Aceasta ar putea declanșa dreptul de autoapărare armată în fața unor atacuri considerate până acum lovituri limitate. În același timp, daunele psihologice vizibile din conflictul cibernetic pot afecta calculele de proporționalitate și pot impune restricții operațiunilor cibernetice.

În ansamblu, aceste elemente evidențiază complexitatea și profunzimea riscurilor asociate atacurilor cibernetice, subliniind necesitatea unei abordări atente și adaptabile pentru a gestiona aceste amenințări în evoluție în cyberspațiu.

În era digitală, amenințările cibernetice reprezintă o provocare majoră pentru companii din diverse domenii, iar evaluarea riscurilor asociate acestor atacuri devine esențială pentru asigurarea securității operaționale. Riscurile unui atac cibernetic în cyberspațiu sunt variate și pot afecta nu doar entitatea în cauză, ci și părțile terțe cu care aceasta interacționează. Astfel, este imperios necesară o înțelegere aprofundată

a consecințelor pe care aceste amenințări le pot avea asupra întregului ecosistem de afaceri.

Unul dintre cele mai evidente riscuri este furtul de informații confidențiale, inclusiv secrete comerciale și patente [30]. Companiile investesc resurse semnificative în dezvoltarea și menținerea unui avantaj competitiv, iar pierderea acestor informații poate compromite serios poziția pe piață și inovația.

Pierderile financiare sunt, de asemenea, o consecință directă a atacurilor cibernetice, în special atunci când datele sunt obținute fraudulos și folosite în mod malefic. Aceste pierderi nu afectează doar situația financiară imediată a companiei, ci pot avea și impacturi pe termen lung, afectând încrederea investitorilor și a acționarilor.

Daunele aduse reputației și prestigiului firmei reprezintă un alt aspect crucial. Neîncrederea partenerilor de afaceri și a clienților poate duce la scăderea vânzărilor și la pierderea poziției de lider în piață. Construirea și menținerea unei reputații solide necesită timp și efort, iar atacurile cibernetice pot anula aceste eforturi într-un timp foarte scurt.

Pierderile de echipamente și programe, irecuperabile în unele cazuri, adaugă la complexitatea riscurilor. De la infrastructură hardware la date critice, aceste pierderi pot afecta funcționarea normală a afacerii și pot implica costuri substanțiale pentru înlocuire și recuperare.

Cheltuielile neprevăzute cu anchetele extinse necesare în urma unui atac cibernetic reprezintă un alt aspect major. Firmele sunt adesea nevoite să investească în expertiză tehnică și legală pentru a identifica și soluționa vulnerabilitățile, ceea ce poate implica resurse financiare semnificative.

În plus, riscul unor războaie cibernetice prelungite poate intensifica pierderile financiare și poate crea un climat de insecuritate în cadrul cyberspațiului. Este esențial ca firmele să adopte atât măsuri active, precum implementarea unor politici de securitate cibernetică robuste, cât și măsuri pasive, precum asigurările împotriva riscurilor cibernetice, pentru a se proteja eficient împotriva consecințelor nefaste ale unui atac cibernetic în cyberspațiu.

Oferind o descompunere detaliată a modurilor diferite în care un atac cibernetic poate afecta o afacere și terțe părți, aceasta oferă membrilor consiliului și altor cadre superioare o înțelegere mai bună a daunelor directe și indirecte ale atacurilor cibernetice atunci când iau în considerare amenințările cu care se confruntă organizația lor. Acest lucru se aplică la fel de bine și altor organizații și chiar guvernelor sau celor care administrează infrastructura națională critică.

Măsuri tehnice și legale în prevenirea atacurilor cibernetice

Progresele tehnologice legate de securitatea cibernetică și criminalitatea cibernetică impun o revizuire a cadrului legislativ. Chiar dacă într-o anumită măsură legile tradiționale pot fi aplicate, este esențial ca legislația să se adapteze la noile concepte

și entități, cum ar fi "datele informatice" intangibile, care nu sunt abordate în mod convențional de actele normative [31].

Criminalitatea și securitatea cibernetică sunt două aspecte care nu pot fi separate într-un mediul digital interconectat. Există mai multe tipuri de crime cibernetice care au provocat sistemul legislative pentru stabilirea unor măsuri legale adecvate. De exemplu, încălcarea confidențialității datelor, fiind și cea mai frecventă "crimă informațională", are un cadrul legislative domestic și internațional bine stabilit.

În Kenya, **Înalta Curte din Nairobi** s-a pronunțat în 2020 în cauza **Nubian Rights Forum** că guvernul nu poate pune în aplicare o nouă sistem cuprinzător de identitate digitală fără să existe o lege adecvată privind protecția datelor în ceea ce privește supravegherea, Înalta Curte din Africa de Sud a constatat, în cauza amaBhungane că o anchetă în masă supravegherea masivă și interceptarea comunicațiilor de către Centrul național de comunicații au fost ilegale. Aceste evoluții urmează dezvoltării rapide a legislației privind protecția datelor în întreaga lume de la intrarea în vigoare a **Regulamentului general privind protecția datelor al Uniunii Europene (GDPR) în 2018**. GDPR a stabilit un nou standard pentru protecția datelor cu caracter personal online, și a servit drept model pentru legislația a numeroase alte țări [32].

În ceea ce privește politica de incriminare a actelor în spațiul cibernetic (cyber), în cadrul unui atelier de lucru privind criminalitatea informatică, organizat în cadrul celui de-al **X-lea Congres al Națiunilor Unite în aprilie 2000**, s-a afirmat că țările membre ar trebui să încerce să armonizeze dispozițiile referitoare la incriminarea, dovada și procedurile (statele ar trebui să încerce să armonizeze dispozițiile relevante privind incriminare, probe și proceduri)[33].

Cinci lucruri trebuie să fie luate în considerare de către legiuitori pentru a incrimina criminalitatea cibernetică, și anume[34]:

- Incriminarea trebuie să fie un efort care să sprijine scopul final al politicii penale, și anume protejarea și prosperarea comunității;
- Comunitatea denunță fapta care va fi incriminată;
- Este necesar să se țină cont de avantajele și dezavantajele incriminării;
- Trebuie să se facă eforturi pentru a preveni supra-criminalizarea care poate avea un efect secundar asupra publicului;
- Este necesar să se realizeze o ajustare a capacității de aplicare a legii

Există o serie de motive pentru care colaborarea între industria, guvernul și autoritățile de aplicare a legii pentru a combate criminalitatea informatică reprezintă un punct cheie în viitoarele proiecte de prevenire a atacurilor cibernetice. Infrastructura internetului este deținută de sectorul privat, iar comunitatea de afaceri operează servicii prin intermediul acesteia [35].

Natura tehnologiei face ca aceasta să se schimbe rapid, pe măsură ce se schimbă adoptarea unei tehnologii sau când apare o nouă tehnologie. tehnologie este introdusă. Noile modele de criminalitate se dezvoltă și trebuie să le urmărim pentru a ne asigura că putem reacționa eficient în vederea reducerii impactului acestora [36].

Concluzii

Evoluția digitală a adus cu sine transformări semnificative în modul în care societatea funcționează și interacționează. Cu toate acestea, o provocare majoră cu care ne confruntăm astăzi este securitatea în cyberspațiu și protecția drepturilor omului în contextul atacurilor cibernetice.

Atacurile cibernetice reprezintă amenințări la adresa vieții private, libertății individuale și a altor drepturi fundamentale ale omului. În acest context, este imperativ să tragem unele concluzii cheie ce vor fi evidențiate în cele ce urmează.

Odată cu extinderea dependenței noastre de tehnologie, drepturile omului devin tot mai vulnerabile la atacurile cibernetice. Accesul neautorizat la informații personale, restricționarea libertății de exprimare online și alte practici similare amenință temelii ale societății bazate pe drepturi și libertăți. În fața acestor amenințări, există o necesitate imperioasă de a dezvolta și implementa reglementări clare și eficiente pentru ciberspațiu. Reglementările ar trebui să protejeze drepturile individuale, să stabilească standarde clare de securitate cibernetică și să impună sancțiuni adecvate pentru cei care încalcă aceste norme.

Dat fiind caracterul transfrontalier al atacurilor cibernetice, cooperarea internațională este esențială. Comunitatea internațională ar trebui să lucreze împreună pentru a dezvolta strategii comune de prevenire a atacurilor, schimb de informații și sprijin reciproc în investigații. De asemenea, îmbunătățirea nivelului de educație și conștientizare în rândul utilizatorilor de tehnologie este crucială. Oamenii trebuie să înțeleagă riscurile asociate utilizării necorespunzătoare a tehnologiei și să adopte practici de securitate cibernetică pentru a-și proteja drepturile.

În paralel cu eforturile de securitate cibernetică, inovația tehnologică trebuie să fie ghidată de principii etice și responsabile. Companiile și dezvoltatorii ar trebui să acorde o atenție deosebită protecției drepturilor omului în proiectarea și implementarea noilor tehnologii. Construirea unei capacități de răspuns rapid la atacurile cibernetice este esențială. Autoritățile guvernamentale, organizațiile internaționale și sectorul privat ar trebui să colaboreze pentru a dezvolta mecanisme eficiente de reacție în fața amenințărilor iminente.

În concluzie, protecția drepturilor omului în era digitală presupune o abordare cuprinzătoare, care să integreze reglementarea eficientă, cooperarea internațională, educația și inovația responsabilă. Numai prin eforturi comune și determinare putem asigura că revoluția digitală servește drepturilor omului și nu le compromite.

Referințe bibliografice:

1. *КІБЕРБЕЗПЕКА ЕРИ ГДОБАЛЬНОІ КОМУНИКАЦІІ,* pag.2. [citat 03.12.2023]. Disponibil: https://elibrary.ivinas.gov.ua/4701/1/Evoliutsiia%20stratehii%20kiberbezpeky%20SShA.pdf.

2. MIHAI Ioan-Cosmin, CIUCHI Costel, PETRICĂ Gabriel, *Current Challenges in the Field of Cybersecurity – The Impact and Romania's Contribution to the Field*, Strategy and Policy Studies Spos 2017, Bucharest 2018, pag.10-11. [citat 03.12.2023], Disponibil: http://ier.gov.ro/wp-content/uploads/2018/10/SPOS_2017_Study_4_FINAL.pdf.
3. DOGARU Olguța, *Noi provocari in securitatea cibernetica*, Studii de Securitate Public, Vol. 3, Nr. 4(12), Octombrie - Decembrie 2014. [citat 03.12.2023]
4. MONTHER Aldwairi, Analysis of Drive-by Downloads and Malicious Websites, College of Technological Innovation Zayed University, Abu Dhabi, UAE 144534. [citat 03.12.2023]
5. ENISA, Raportul ENISA privind situația amenințărilor Malware, Ianuarie 2019 – aprilie 2020, pag. [citat 03.12.2023]. Disponibil: https://www.enisa.europa.eu/publications/report-files/ETL-translations/ro/etl2020-malware-ebook-en-ro.pdf.
6. Parlamentul European, *Securitate cibernetică: principalele amenințări*. [citat 03.12.2023] Disponibil:https://www.europarl.europa.eu/pdfs/news/expert/2022/1/story/20220120STO21428/20220120STO21428_ro.pdf.
7. SECAREANU Marian, *The New Scientific Revolution - Types of Cyber Attacks Police Taken into Consideration on a European and International Level*, 3 PUB. Sec. Stud. 215 (2014), pag.3 [citat 03.12.2023].
8. MITRA Silviu-Elian, The Structure of Cyber Attacks, 9 INT'l J. INFO. Sec. & CYBERCRIME 43 (2020). [citat 03.12.2023].
9. Serviciul Român de informații, Glosar de termeni pentru domeniul securităţii cibernetice, pag. 41. [citat 03.12.2023]. Disponibil: https://www.sri.ro/assets/files/publicatii/GLOSAR-TERMENI-CYBER-12-09-2019.pdf
10. PORTER Evan, Ce Este un Atac DDoS și Cum să Previi Unul în 2023. [citat 03.12.2023]. Disponibil: https://ro.safetydetectives.com/blog/ce-este-un-atac-ddos/.
11. Papanastasiou Afroditi, *Application of International Law in Cyber Warfare Operations,* Disponibil: file:///C:/Users/User/Downloads/SSRN-id1673785.pdf. [citat 03.12.2023].
12. Convenția Națiunilor Unite asupra dreptului mării din 10.12.1982. Disponibil: 6.1.Conventie-1982-Conventia-Natiunilor-Unite-asupra-dreptului-marii-10.12.1982.pdf (gov.ro). [citat 02.12.2023]
13. Ibidem. [citat: 02.12.2023]
14. Convenția privind cirminalitatea informatică din 23.11.2001. Disponibil: file:///C:/Users/User/Downloads/CoE-HUN-RPT-3657-RO-2849.pdf. [citat 05.12.2023].
15. LAZĂR Elena, *Operațiunile cibernetice și reglementarea juridică lacunară a acestora în dreptul international.* Disponibi: https://www.juridice.

ro/701958/operatiunile-cibernetice-si-reglementarea-juridica-lacunara-a-acestora-in-dreptul-international.html. [citat:02.12.2023]
16. ICRC, *Cyberwarfare and international humanitarian law: the ICRC's position*, Disponibil: https://www.icrc.org/en/doc/assets/files/2013/130621-cyberwarfare-q-and-a-eng.pdf. [citat: 03.12.2023].
17. Ibidem. [citat: 03.12.2023].
18. Official Journal of the European Union, COUNCIL DECISION (CFSP) 2020/1127 of 30 July 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, par.(3). [citat 06.12.2023]. Disponibil: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32020D1127&from=EN.
19. Ibidem. GAO Qiang and ZHANG Shilong (China); Alexey Valeryevich MININ, Aleksei Sergeyvich MORENETS, Evgenii Mikhaylovich SEREBRIAKOV, Oleg Mikhaylovich SOTNIKOV (Federația Rusă). [citat 06.12.2023]
20. Ibidem. *Main Centre for Special Technologies (GTsST) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU)*. [citat 06.12.2023]
21. Consiliul UE, *UE: primele sancțiuni impuse vreodată împotriva atacurilor cibernetice*. [citat 03.12.2023]. Disponibil: https://www.consilium.europa.eu/ro/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/.
22. Ministerul Afacerilor Externe, *Problematica securității cibernetice în cadrul organizațiilor internaționale şi implicarea României ca membru al acestorai*. [citat 06.12.2023]. Disponibil: https://www.mae.ro/node/28369.
23. Ibidem. [citat 06.12.2023]
24. Comisia Europeană, *Directiva privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune (Directiva NIS2)*. [citat 06.12.2023]. Disponibil: https://digital-strategy.ec.europa.eu/ro/policies/nis2-directive.
25. Consiliul UE, *Reziliența UE: Consiliul adoptă o directivă pentru consolidarea rezilienței entităților critice*. [citat 06.12.2023]. Disponibil: https://www.consilium.europa.eu/ro/press/press-releases/2022/12/08/eu-resilience-council-adopts-a-directive-to-strengthen-the-resilience-of-critical-entities/.
26. Ministerul Afacerilor Externe, *Problematica securității cibernetice în cadrul organizațiilor internaționale şi implicarea României ca membru al acestorai*. [citat 06.12.2023]. Disponibil: https://www.mae.ro/node/28369.
27. EASTERLY Jen & FANNING Tom, *The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years*. Disponibil: https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years. [citat: 05.12.2023]

28. ICRC, *The SolarWinds hack: Lessons for international humanitarian organizations*. Disponibil: https://international-review.icrc.org/sites/default/files/reviews-pdf/2022-06/the-solarwinds-hack-lessons-for-international-humanitarian-organizations-919.pdf. [citat: 05.12.2023].
29. Researchers identify negative impacts of cyber attacks. Disponibil: https://www.ox.ac.uk/news/2018-10-29-researchers-identify-negative-impacts-cyber-attacks. [citat: 05.12.2023].
30. RUSU Răzvan, Atacul cibernetic – Riscurile acestui tip de fraudă asupra firmelor și cum poate fi prevenit. Disponibil: https://leaderteam.ro/atacul-cibernetic-riscurile-acestui-tip-de-frauda-asupra-firmelor-si-cum-poate-fi-prevenit/. [citat: 03.12.2023]
31. APPAZOV Artur, *Legal Aspects of Cybersecurity*, pag. 35. [citat 06.12.2023]. Disponibil: https://www.justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Forskningspuljen/Legal_Aspects_of_Cybersecurity.pdf.
32. Media Defence, *CYBERCRIMES - Summary Modules on Litigating Digital Rights and Freedom of Expression Online*, pag.8. [citat 06.12.2023]. Disponibil: https://www.mediadefence.org/ereader/wp-content/uploads/sites/2/2020/12/Module-7-Cybercri [citat 06.12.2023]
33. MUDZALIFAH Milla, THE POLITICS OF CRIMINAL LAW IN CYBERCRIME: AN EFFORTS TO COMBAT INFORMATION TECHNOLOGY CRIMES IN INDONESIA, Jurnal Pembaharuan Hukum Volume 10, Number 1, April 2023, pag.8-9. [citat 06.12.2023].
34. Ibidem. [citat 06.12.2023].
35. Home Office, Cyber Crime Strategy, pag.29-30. [citat 06.12.2023]. Disponibi: https://assets.publishing.service.gov.uk/media/5a7c716fed915d48c240fc37/7842.pdf
36. Ibidem. [citat 06.12.2023].