ANALELE ŞTIINŢIFICE ALE UNIVERSITĂŢII „ALEXANDRU IOAN CUZA” DIN IAŞI
TOM LXX, 4, ŞTIINŢE JURIDICE, 2024

DOI: 10.47743/jss-2024-70-4-12

Terorismul cibernetic

Cyber terrorism

Ioana ŢURCANU[1]

Rezumat: Prezentul articol își propune o analiză asupra modalității de înfăptuire în prezent a fenomenului terorismului cibernetic, cunoscut și drept *cyber terrorism*, a raționamentelor care stau la baza tranziției de la deja cunoscutele manifestări la cele contemporane, precum și a încercărilor de a identifica în concret indivizii predispuși la comiterea acestui tip de fapte, tot astfel cum prezintă și o perspectivă asupra capacității concrete de prevenire, stopare sau controlare a terorismului cibernetic.

Cuvinte-cheie: terorism cibernetic, probe digitale, World Wide Web, prevenție.

Abstract: The present article aims to analyze the current means by which the phenomenon of terrorism, also known as cyber terrorism, is carried out, the reasoning behind this transition from the already known manifestations to contemporary ones, as well as the attempts to concretely identify individuals predisposed to committing this type of acts. It also provides a perspective on the actual capacity to prevent, stop, or control cyber terrorism.

Keywords: cyber terrorism, digital evidence, World Wide Web, prevention.

1. Introducere

În jurul noțiunii de terorism gravitează în mod indisolubil și cea de globalizare. Deși termen cu profunde conotații pozitive pentru societatea umană și evoluția sa privită ca imagine de ansamblu, în acest demers pare să fie unul dintre factorii prielnici în ceea ce se traduce a fi terorismul de tip transnațional. Astfel, se trasează liniile directoare ale unei noi dimensiuni, în care *„terorismul este generat și sprijinit prin dispute politice, conflicte îndelungate și nu în ultimul rând prin incapacitatea sau refuzul unor state de a asigura un control riguros pe teritoriul lor, creând astfel adevărate paradisuri ale activității infracționale.*[2]*”*. Evoluția globalizării a deschis două noi paliere, în primul rând augmentarea dinamismului geografic și a

[1] Absolvent studii juridice, Master în Drept, e-mail: ioanaturcanu99@gmail.com .

[2] S. Ordzhorikidze, fost Secretar General adjunct și Director General al ONU, discurs citat în R. Stănoiu, E. Stănișor, C. Sima, A. Preda, V. Teodorescu, *Marea criminalitate în contextul globalizării*, Editura Universul Juridic, București, 2012, p. 67.

modalităților de înfăptuire a terorismului, iar în al doilea rând deschiderea orizontului statelor spre luarea în considerare și chiar realizarea unei colaborări în scopul prevenirii și combaterii acestui fenomen, determinând schimbări deloc de neglijat și în politica abordată de organizații de gen militar precum NATO. Astfel, se constată, odată cu evoluția societății, inclusiv evoluția motivațiilor, trecându-se de la justificări de tip religios la cele de ordin etnic, în care teroristul părăsește sfera fanatismului și se îndreaptă mai mult spre o combinație între radicalism, îndoctrinare și repere științifice clare, determinând astfel necesitatea luării în considerare de noi perspective asupra modului de cercetare a faptelor considerate de natură teroristă[3].

Mai mult decât atât, pentru a sublinia aceeași idee, se impune o dublare a perspectivelor anterior menționate și o conectare cu o pârghie de legătură, respectiv cea a radicalismului, concept imposibil de neglijat pentru înțelegerea acestui fenomen și implicit pentru facila și temeinica sa investigare. În această ordine de idei, apare ca imposibilă și fără de temei trecerea cu vederea a esențialului, a faptului că la baza acestei manifestări infracționale este în sine un sentiment, o aparență emoțională clară, cvasiinstantanee, iar nu în mod absolut o cauză, ci mai precis un cumul de contexte orientate spre aspirația evidențierii *„unui discurs"* ce apare ca un parcurs argumentativ pentru un scop concretizat și exprimat prin violență.

Ținând cont de modalitatea în care criminalitatea a fost modelată pe parcursul ultimilor ani de evoluția tot mai pregnantă a tehnologiilor din sfera digitală, și fenomenul terorismului a cunoscut mutații specifice acestor modificări, cele mai ușor vizibile făcând referire la procesul de diseminare a informațiilor specifice propagandei teroriste, la activitatea de recrutare sau la schimbul de date ori opinii între simpatizanții manifestărilor de acest gen, nefiind de neglijat nici modificările mai puțin sesizabile în rândurile populației, respectiv facilitarea finanțării actelor sau chiar posibilitatea înfăptuirii lor de la distanță prin intermediul sistemelor electronice.

2. Spațiul de desfășurare a activităților aparținând sferei terorismului cibernetic

Terorismul cibernetic este indisolubil legat de World Wide Web sau mai precis un fragment al mediului online care însumează Deep Web-ul, Deep Net-ul, dar și Web Invizibilul sau Dark Web-ul, și la care nu se poate face accesul utilizându-se motoare obișnuite de căutare, fiind impregnat de informații care sunt în majoritatea cazurilor ilegale sau promotoare ale unor conduite profund antisociale. Având în vedere aceste coordonate, Surface Web sau rețeaua utilizată în mod uzual de orice persoană, nu poate oferi teroriștilor protecția anonimatului sau siguranța schimbului de informații atât de relevant în procesul de construire a grupurilor sau de pregătire a atentatelor, aspect demonstrat printr-un studiu de specialitate care a confirmat că într-o proporție de aproximativ 57% din componența

[3] M. Tutunaru, *Terorismul în lumea contemporană*, în Revista Română de Criminalistică nr. 1, februarie 2018, p. 2812.

totală a Dark Web-ului este formată, pe lângă pornografie, trafic de droguri sau armament, din comunicații de natură teroristă[4] .

Această preocupare a grupărilor teroriste pentru comunicarea facilitată de diverse platforme online s-a manifestat cu precădere după finalul anilor 1990, când după încercări nereușite de a utiliza paginile de *„internet de suprafață"*, eșecuri datorate intervenției serviciilor secrete de informații care puteau cu ușurință să ia poziție prin monitorizarea site-urilor cu grad ridicat de pericol, s-au reprofilat prin mutarea activităților în Dark Web. Un exemplu în acest sens este și o piață de desfacere denumită Silk Road, al cărui deținător, Ross William Ulbright, a fost judecat și încarcerat deoarece permitea comercializarea de stupefiante. Aceeași evoluție, mai precis modernizare a tehnicilor utilizate în domeniul criminalității, a fost înregistrată și prin prisma ușurinței scurgerilor de informații, manifestare asociată cu sintagma *„WikiLeaks"*, precum și cu amploarea pe care au câștigat-o criptomonedele prin prisma apariției Bitcoin, folosite ca monede de schimb principale, o estimare realizată pe doi ani evidențiind că prin platforma Silk Road a fost înlesnită realizarea de tranzacții de ordinul miliardelor de dolari. Un exemplu în acest sens este și *Found the Islamic Struggle without Leaving a Trace*, site care se ocupă cu strângerea de fonduri și oferă în această direcție și o adresă a unui portofel virtual în care se pot dona bani sub forma monedele Bitcoin, existând inclusiv un ghid online cu scopul de a învăța membrii grupărilor utilizarea corectă, denumit *„Bitcoin wa Sadaqat alJihad"* sau tradus *„Bitcoin și Caritatea pentru Jihad"*.

Deși, utilizând Dark Web-ul, teroriștii s-au bucurat în activitatea de schimb de informații de masca anonimatului pentru o bucată de timp considerabilă, fiind folosit ca metodă de comunicare cu succes și în prezent, aceștia nu au renunțat complet la a recurge și la paginile de internet sau la platformele online, inclusiv site-urile de socializare la care orice individ are acces, risc asumat în vederea realizării campaniilor de recrutare și de promovare a ideilor la care aderă. În urma atacurilor petrecute în noiembrie 2015, la Paris, acțiunile DAESH au fost mutate aproape integral în mediul mult mai sigur adăpostit de Dark Web, mesaj distribuit către militanți prin intermediul Telegram, de către *Al-Hayat Media Center*, centrul media al grupării, prin care se aducea la cunoștință transferarea site-ului *Isdarat*, de profil de altfel pentru descoperirea de materiale și manifeste cu un profund și evident caracter de propagandă, din cauza campaniilor lansate și susținute de către grupul *Anonymus* care, prin acțiuni constante, a reușit să determine închiderea a sute de site-uri cu profil terorist[5].

Motivația pentru care sunt alese aceste moduri de comunicare, tipice pentru o parte mai puțin accesibilă a internetului, a fost demonstrată inclusiv prin dovezi tangibile, în luna august a anului 2013 descoperindu-se de către NSA sau Agenția Națională de Securitate din SUA prezența în spațiul online a unei rețele private utilizată de către teroriști în vederea pregătirii viitoarelor atentate, astfel reușindu-se interceptarea unei serii *„de comunicații criptate între Ayman al-Zawahiri, liderul Al-Qaeda, și Nasir al-Wuhaysi, liderul filialei yemenite Al-Qaeda*

[4] V. C. Voinea, *Teroriști în lumea virtuală*, în Intelligence, nr. 44, 2022, p. 84.

[5] *Ibidem.*

în peninsula Arabă"[6], Institutul pentru Studii de Securitate Națională dezvăluind mai mult decât atât că pentru mai bine de zece ani corespondența dintre liderii mai multor grupări teroriste a fost realizată cu ajutorul Dark Web, dar și că în principal DAESH, dar și alte grupări teroriste își distribuie mesajul făcând uz de platforma Telegram, la finele lunii mai anul 2016 fiind identificate 700 de canale noi cu profil terorist.

De asemenea, datorită capturării în august 2015 de către poliția franceză a unui specialist IT, s-au descoperit informații valoroase despre o aplicație folosită în scopul criptării comunicațiilor, denumită *TrueCrypt*. Reda Hame a explicat cum a primit instruirea necesară să utilizeze programul și instrucțiuni clare de a introduce și a folosi aplicația în Europa. Programul a fost creat în 2004 de Paul LeRoux, un fost lider al unei alte grupări teroriste cu sediul central în Filipine.

3. Identificarea făptuitorilor și direcțiile de luat în calcul în procesul de investigare

Statisticile oferite în 2023 de către *EUROPOL – TE – SAT (European Union – Terrorism Situation and Trend Report)* au confirmat faptul că în ultimul deceniu societatea se confruntă cu un fenomen alarmant și greu gestionabil, respectiv mutarea activităților specifice pregătirii atentatelor în mediul online și caracterizarea acestora de discreția și intimitatea oferite de mediul în care autorii își desfășoară viața de zi cu zi, subliniindu-se astfel încă o dată direcția nouă pe care fenomenul terorismului o parcurge, aplecarea către înrolarea de indivizi marcați de incapacitatea adaptării la normele ce conturează realitatea socială actuală, exploatarea frustrărilor generate de incoerența opiniilor referitoarea la sfera politică, religioasă sau profesională, precum și a lipsei de implicare și sprijin necesare indivizilor ce fac parte din grupuri ce implică o asistență specială, cum este cazul minorilor ori al persoanelor cu probleme de stabilitate emoțională ori mintală, racolate astăzi prin intermediul unor metode mult mai eficiente, particulare erei digitalizării, de exemplu crearea de conexiuni pe platforme, forumuri ori chiar prin jocurile video[7]. Practica înregistrată recent a subliniat că *„organizațiile teroriste sau extremiste își îndreaptă atenția către școli, universități, lăcașuri de cult sau chiar închisori, acestea din urmă fiind un teren fertil pentru radicalizare, din cauza izolării specifice mediului carceral și a unei scheme personale care nu permite detectarea activităților teroriste sau extremiste*"[8], reala amenințare, în ciuda existenței grupurilor de tip organizat, marcate de ideologii specifice extremei dreapta sau stânga, fiind în continuare atacatorii izolați, găsiți responsabili pentru marea parte dintre atacurile teroriste înregistrate pe parcursul anului 2022.

Printre activitățile considerate specifice terorismului cibernetic sau *cyberterrorism*-ului se numără și schimbarea de informații cu ajutorul e-mail-ului

[6] *Idem*, p. 86.

[7] M. M. Maria, *Terorismul în pas cu moda tehnologiei digitale*, în Intelligence, nr. 47, 2023, p. 15.

[8] *Idem*, p. 16.

în vederea planificării de atentate sau recrutării de membri, sabotarea programelor care asigură monitorizarea asupra traficului aerian, în vederea producerii de dezastre aeriene concretizate fie în prăbușiri, fie în ciocniri, atacarea sistemelor ce facilitează aprovizionarea cu apă potabilă a populației dintr-o zonă delimitată ori contaminarea directă a apei, accesul nepermis în bazele ce conțin informații referitoare la identitatea, starea de sănătate și schema de tratament a bolnavilor cu scopul de a realiza modificări asupra medicației prescrise și de a se înregistra astfel cât mai multe persoane decedate, ori accesul în sistemele care controlează rețelele electronice determinând astfel întreruperea alimentării electrice și pagube însemnate din punct de vedere economic, precum și starea de temere în rândul populației[9]. În cazul investigării criminalistice a acestor tipuri de infracțiuni, o importanță crescută o are procesul de determinarea a obiectelor ce au fost utilizate sau afectate săvârșirii faptei ilicite, fiind denumite și corpuri delicte și care constituie în linii mari mijloacele prin care infracțiunea este realizată, dar și o sursă vastă de probe. În plus, se acordă atenție și identificării informațiilor rezultate în urma infracțiunilor, ce vor putea fi sechestrate având în vedere proveniența ilegală a acestora, relevante fiind cu precădere liste ce conțin coduri de acces, diverse parole pentru programe guvernamentale, care prin natura lor și a faptului că au fost obținute pot ridica suspiciunea pregătirii unor acte teroriste. De asemenea, în mod uzual se procedează la constatarea rezultatelor delictului, iar mai apoi la identificarea autorului și împrejurărilor care au facilitat producerea evenimentului[10], stabilindu-se modul concret prin care acesta a realizat accesul la sistemele informatice și dacă au existat sau nu și alți participanți pentru a se putea exclude sau confirma ulterior, prin coroborarea cu alte probe, ipoteza existenței unui grup organizat.

În acest cadru se circumscrie și sintagma de probe digitale, folosită în cadrul investigării în vederea atingerii acelorași idealuri ca cele fizice, deosebirea radicală ce se evidențiază între cele două categorii supuse analizei fiind reprezentată de faptul că cele digitale pot fi considerate valori, neavând o existență tangibilă, palpabilă. Cu toate acestea, probele digitale au o esență materială întrucât se prezintă sub forma unor semnale electromagnetice, recunoscute de altfel din punct de vedere științific drept o formă a existenței materiei și *„se exprimă sub formă binară, manifestată prin existența unor impulsuri electrice, cu două valori standardizate, sau prin două stări fundamentale de existență a câmpului magnetic”*[11]. Pentru a putea fi utile, în domeniul probelor digitale este necesară respectarea unui set de principii care confirmă importanța neaducerii de modificări acestora, a accesului permis doar persoanelor competente privind tehnica criminalistică sau a consemnării în scris a tuturor detaliilor privind analiza, modul de depozitare și examinare, precum și desemnarea unei organizații, respectiv persoane responsabile cu păstrarea lor. În aceeași ordine de idei, organisme precum *„International*

[9] A. C. Moise, *Metodologia investigării criminalistice a infracțiunilor informatice*, Editura Universul Juridic, București, 2011, p. 26.

[10] E. Stancu, *Tratat de criminalistică*, Editura Universul Juridic, București, 2015, p. 780.

[11] A. C. Moise, *op. cit.*, p. 174.

Association of Computer Investigative Specialists" au prevăzut o serie de standarde privind examinarea probelor digitale, impunând conservarea de manieră a păstra starea în care au fost descoperite, realizarea unui exemplar care să reflecte cu exactitate caracteristicile originalului cu scopul de a nu îl distruge în timpul analizei pe cel din urmă, dar și etichetarea și înregistrarea lor[12].

Mai mult decât atât, probele digitale sunt caracterizate de mai multe trăsături speciale raportate la celelalte categorii de probe, fiind mult mai fragile, cu referire la prelucrarea și colectarea lor, probabilitatea de a exista erori de utilizare a sistemelor informatice ce pot conduce la ștergerea sau modificarea lor fiind considerabilă. De aici se desprinde și problematica susceptibilității de alterare, relativ ușoară, și unul dintre principiile care reprezintă fundamentul investigării infracțiunilor informatice, mai exact necesitatea conservării integrității probelor digitale și realizarea documentației integrale a procesului prin care au fost obținute, aspecte esențiale pentru demonstrarea nealterării lor. De asemenea, este de notorietate că aceste probe nu au o aparență evidentă, fiind indispensabilă utilizarea unor programe speciale pentru a fi relevate, iar mai apoi întrebuințate. Totodată, raportat la persistența[13] datelor, probele digitale pot fi împărțite în *probe digitale volatile*, memoria sistemului fiind într-o relație de cauzalitate cu alimentarea la energia electrică în sensul conservării informațiilor, și *probe digitale nevolatile* care presupun stocarea datelor pe suporturi de tipul hard-disc și care nu sunt afectate de o posibilă întrerupere a alimentării, motiv pentru care pot fi ridicate fără a fi necesară o intervenție rapidă. Una dintre cele mai importante caracteristici rămâne totuși construcția de gen binar care impune interpretarea de către un specialist a probelor înainte ca acestea să fie utilizate de către un investigator.

În general, probele digitale sunt căutate în zone cheie, fiind regăsite în cele mai multe dintre cazuri în fișiere care au fost create de către utilizator, cum este cazul bazelor de date, agendelor, foilor de calcul ori calendarelor, în fișiere protejate, exemple fiind cele criptate, ascunse, care se pot deschide doar folosind o parolă, sau în fișierele pe care computerul le creează, cum sunt cele backup, temporare, cookies, log sau swap[14].

Având în vedere unele acte de urmărire penală, în cazul percheziției, în cazul în care un calculator este considerat *fructul crimei* (terminologie preluată din doctrina nord americană), deci practic instrumentul prin care infracțiunea a putut fi realizată, mandatul va fi emis în vederea ridicării și analizării computerului în principal și doar în subsidiar a informațiilor ce se regăsesc pe acesta. Mandatul este esențial să fie cât mai detaliat, date referitoare la componentele ce urmează a fi preluate, informații despre fabricant, model și orice alt mijloc de identificare fiind profund relevante[15]. Dacă în mod uzual atunci când se emite un mandat de percheziție se menționează locul în care această acțiune ar trebui să se desfășoare, deci de unde obiectele pot fi ridicate, în cazul calculatoarelor este conturată mai mult o

[12] *Idem*, p. 176.
[13] *Idem*, p. 178.
[14] *Idem*, p. 179.
[15] E. Stancu, *op. cit.*, p. 782.

lume virtuală ce conține informații intangibile. Acest fapt determină dificultatea stabilirii spațiale a informației, concretizându-se trei direcții: existența unei locații externe cunoscute, a unei locații externe necunoscute, sau a unei locații interne despre care anchetatorii cunosc că datele s-ar afla în zonă. Aspecte care nu trebuie scăpate din vedere în aceste cazuri sunt în principal modalitatea, precum și capacitatea de stocare a aparatelor, acestea fiind și diferențele majore între lumea virtuală și cea fizică, un hard-drive obișnuit având aptitudinea de a cuprinde 100.000 de pagini de date, dar și ipoteza infracțiunilor informatice flagrante, unde este fundamentală respectarea aceluiași set de reguli precum în cazul percheziților, modul de acțiune fiind similar, aceasta pentru a se asigura conservarea pe cât posibil a probelor digitale și a tuturor urmelor care pot confirma că s-a produs o manifestară încadrată în sfera ilicitului penal[16].

În cazul infracțiunilor informatice există și o serie de particularități în privința procedeului de cercetare la fața locului, centrul atenției căzând primordial pe calculator, monitor, tastatură, dispozitivele de stocare externe, modemuri ori chiar imprimante, fiind corectă și în această situație distincția dintre faza statică și faza dinamică a investigație. Cu toate că procesul de cercetare la fața locului este tipic pentru organele judiciare, o cerință ce nu poate fi ignorată este prezența pe parcursul tuturor operațiunilor a unui specialist în domeniu, respectiv un informatician cu pregătire profesională și dacă este posibil și cu experiență în sectorul infracțiunilor informatice. Cu referire la faza statică, se procedează la constatarea stării de fapt, la îndepărtarea dacă este cazul a persoanei care se află în proximitatea sistemului informatic, fiind singura modificare care poate fi permisă în economia spațiului, o posibilă greșeală putând fi reprezentată inclusiv de oprirea alimentării cu energie electrică a aparaturii. Fixarea scenei se realizează prin intermediul fotografiilor și înregistrărilor de tip video, relevante pentru investigație fiind toate aparatele din încăpere, precum și programele ce rulau pe monitoare în momentul descoperii calculatoarelor, daca este cazul. În ceea ce privește faza dinamică a cercetării, s-a constat din rațiuni de ordin practic necesitatea colaborării organelor judiciare cu un specialist din domeniul informaticii, în permanență, atât pentru ridicare, fixarea urmelor, cât și pentru manipularea lor în vederea unui posibil transport[17].

4. Dezideratul prevenției

Referitor la activitatea de prevenție a terorismului cibernetic, este de remarcat faptul că atacurile executate prin intermediul calculatoarelor prezintă o dificultate particulară în ceea ce privește preîntâmpinarea lor, securitatea națională fiind într-o stare de perpetuu pericol și de dezechilibru, ceea ce generează de la sine o aparență de teamă. Pe lângă impedimentele de ordin tehnic, se remarcă și unele inconveniente legislative, mai exact neputința statelor din întreaga lume de a crea un sistem armonizat de norme care să guverneze problema terorismului cibernetic, ideal greu de îndeplinit prin raportare la imaginea juridică de ansamblu, atât de

[16] *Idem*, p. 783.
[17] *Ibidem.*

diversificată și greu de adaptat la un standard comun, unele dintre bariere fiind chiar interesele variate, raportarea eterogenă la sfera penală și chiar sistemele de drept diferite care funcționează în state.

La nivel european au fost înregistrate diverse încercări în această direcție, una dintre ele fiind și apariția *Convenției asupra Criminalității informatice de la Budapesta* prin care s-a tins spre constituirea unei baze pentru state privind infracțiunile care vizează confidențialitatea, integritatea, dar și disponibilitatea datelor precum și a sistemelor informatice care au fost accesate sau captate prin orice manieră ilegală[18].

Potrivit doctrinei de specialitate, se consideră că în ciuda beneficiilor mult mai mari pe care atentatele teroriste le înregistrează în sfera informatică, atuuri printre care riscul scăzut de a fi oprite sau chiar costurile mult mai mici de execuție, organizațiile teroriste nu vor renunța nici la atacurile clasice, respectiv cele cu bombă care prin frecvență și efecte și-au demonstrat eficiența. Cu toate acestea, ipoteze vehiculate până în prezent prezintă probabilitatea crescută ca cele două tipuri de acțiuni să fie combinate în scopul găsirii unui melanj care să satisfacă cât mai multe dintre deziderateле clasice, mai exact numărul mare de victime, răspândirea cu viteză și către cât mai multe persoane a mesajelor propagandiste, precum și impunerea la nivelul populației a unei senzații de pericol și frică pe o perioadă cât mai lungă de timp, un exemplu de scenariu în acest sens fiind *„detonarea unei încărcături explozive convenționale, concomitent cu lansarea de atacuri cibernetice asupra rețelei locale de telecomunicații”*[19], realizându-se în acest fel un blocaj în ceea ce privește locul în care s-a produs incidentul și autoritățile responsabile cu acordarea de ajutor victimelor sau cu minimizarea pe cât posibil a efectelor pe care atentatul le-a produs.

De asemenea, tot pentru a susține acest demers al prevenției atentatelor cibernetice, statele din Occident au elaborat planuri de protejare a sistemelor de infrastructură, strategii potrivite structurilor armate și au alocat fonduri considerabile serviciilor de informații angajând specialiști în IT, toate aceste încercări dovedindu-se cu neputință a se ridica la standardele rezultatelor dorite, evoluția permanentă și imposibil de oprit a internetului, precum și incompatibilitatea securizării depline a acestuia, contrară naturii și scopului pentru care a fost creat, respectiv deschiderea cât mai mare, fiind adevărate piedici în efortul de a asigura o prevenție eficientă în cazul terorismului cibernetic[20].

Concluzii

Având drept indicator ideile anterior exprimate, se poate conchide însăși evoluția care pare să marcheze acest fenomen al terorismului, de la reputatele atentate cu bombă, la o atenție centrată astăzi în jurul noțiunii de terorism ciber-

[18] T. Vătuiu, *Terorismul informatic: Măsuri pentru prevenirea și combaterea lui*, în Revista Română de Criminalistică, nr. 2, aprilie 2018, p. 2874.

[19] *Ibidem.*

[20] *Ibidem.*

netic, practică marcată de acțiuni mult mai „curate” raportat la imaginea vizuală caracterizată de urmările atacurilor fizice, dar cu consecințe profunde. În această ordine de idei, a apărut ca un demers rațional prezentarea unor date relevante referitoare la activitățile de răspândire a materialelor cu conotație propagandistă, la modalitățile de recrutare ori chiar de finanțare a organizațiilor teroriste prin intermediul platformelor online, precum și la spațiul din internet în care aceste acțiuni au loc, dar și a unor principii de investigare tipice infracțiunilor informatice, utilizate și în cazul cercetării actelor specifice terorismului cibernetic.

Referințe

Maria M. M., *Terorismul în pas cu moda tehnologiei digitale*, în Intelligence, nr. 47, 2023.

Moise A. C., *Metodologia investigării criminalistice a infracțiunilor informatice*, Editura Universul Juridic, București, 2011.

Stancu E., *Tratat de criminalistică*, Editura Universul Juridic, București, 2015.

Stănoiu R., Stănișor E., Sima C., Preda A., Teodorescu V., *Marea Criminalitate în contextul globalizării*, Editura Universul Juridic, București, 2012.

Tutunaru M., *Terorismul în lumea contemporană*, în Revista Română de Criminalistică nr. 1, februarie 2018.

Vătuiu T., *Terorismul informatic: Măsuri pentru prevenirea și combaterea lui*, în Revista Română de Criminalistică, nr. 2, aprilie 2018.

Voinea V. C., *Teroriști în lumea virtuală*, în Intelligence, nr. 44, 2022.