IMPACTUL PSIHOLOGIC AL TERORISMULUI CIBERNETIC

Anca SAVU
Doctorand, Universitatea Națională de Apărare ,,Carol I", București

Florentina-Ștefania NEAGU
Doctorand, Academia de Studii Economice, București

Orice act de terorism constituie, pentru societățile democratice, o adevărată agresiune psihologică și emoțională, capabilă să producă temeri în mentalitatea populației. Din punct de vedere semantic, terorismul își atinge obiectivul final, prin crearea unui climat de insecuritate, frică și teroare. Actul în sine, care poate fi un atac terorist convențional sau unul care are loc în mediul online, este suficient pentru a influența activitățile profesionale, timpul liber și călătoriile persoanelor. Prin urmare, natura profund intruzivă și violentă a terorismului cibernetic poate încuraja apariția unor tulburări psihiatrice sau a unui comportament cu un nivel crescut de risc.

Pentru a putea estima impactul terorismului cibernetic, trebuie să identificăm, în primul rând, profilul psihologic al teroristului cibernetic. În al doilea rând, terorismul cibernetic este, cel mai adesea, parte a terorismului convențional și, prin urmare, are un impact similar.

Cuvinte-cheie: crimă organizată, impact psihologic, spațiu cibernetic, mass-media, terorism cibernetic.

INTRODUCERE

După atentatele din 11 septembrie 2001, un element-cheie al politicilor de securitate din SUA, dar și din celelalte state ale lumii l-a reprezentat consolidarea securității naționale. Mai mulți analiști politici, militari și economici, precum și academicieni și jurnaliști au estimat că, după aceste evenimente, vor urma atacuri teroriste asupra infrastructurii computerizate sau prin intermediul acestora[1].

Orice act de terorism constituie, pentru societățile democratice, o adevărată agresiune psihologică și emoțională, capabilă să determine schimbarea percepției populației cu privire la siguranța lor fizică sau la integritatea datelor personale care se regăsesc în mediul online.

Dacă, în cazul atentatelor teroriste cu dispozitive explozive care provoacă daune materiale și pierderi de vieți omenești, impactul mediatic și psihologic este mare, fiind resimțit imediat de către oameni, în cazul incidentelor cibernetice, impactul asupra insfrastructurilor IT este și mai mare, generând costuri semnificative de remediere a acestora. În același timp, au și un impact psihologic asupra persoanelor, deoarece acestea nu își mai consideră datele personale sau activele virtuale[2] în siguranță.

În primul rând, terorismul cibernetic are un impact pihologic indirect asupra persoanelor, adică indivizii nu conștientizează imediat că ceea ce se întâmplă în jurul lor reprezintă rezultatul unor atacuri cibernetice sau al utilizării unor dispozitive electronice. Pentru a demonstra acest lucru, vom prezenta câteva exemple ale utilizării unor astfel de atacuri. Astfel, în anul 1999, Pentagonul a dezvăluit că a folosit o *„armă specială"* care i-a permis să perturbe rețeaua de electricitate a mai multor orașe din fosta Iugoslavie[3]. În anul 2002, președintele G.W. Bush a semnat o directivă, *„ordonând guvernului american să pregătească planuri naționale pentru războiul electronic ofensiv împotriva potențialilor inamici"*[4].

În aprilie 2005, SUA au înființat Comandamentul Strategic NATO (StratCom), care a devenit funcțional din ianuarie 2014[5]. Această unitate de elită militară

[1] Maura Conway, *Le cyber-terrorisme. Le discours des médias américains et ses impacts*, Cités, 2009/3 (no 39), pp. 81-94, disponibil la https://www.cairn.info/revue-cites-2009-3-page-81.htm

[2] Activele virtuale reprezintă bunuri necorporale care pot fi constituite în investiții alternative cu riscuri specifice, unități de cont, monede virtuale etc., disponibil la http://www.cdep.ro/afaceri_europene/afeur/2019/st_2643.pdf

[3] *Truth behind America's raid on Belgrade*, în *The Guardian*, 28 noiembrie 1999, disponibil lahttps://www.theguardian.com/theobserver/1999/nov/28/focus.news1

[4] J.P. Manach, *Le cyberterrorisme est virtuel*, la cyberguerre en préparation, 2006, disponibil la http://www.internetactu.net/2006/02/24/le-cyberterrorisme-est-virtuel-la-cyberguerre-en-preparation/

[5] *About us*, NATO StratCom Centre of Excellence, 2019, disponibil la https://www.stratcomcoe.org/about-us

nu protejează doar infrastructurile vitale ale Americii, ci le poate ataca și pe ale inamicilor săi[6]. În decembrie 2005, Forțele Aeriene ale SUA au adăugat *„dominația spațiului cibernetic”* în misiunea sa, iar un document recent declasificat arată că obiectivul lui Donald Rumsfeld, fost secretar al Apărării în mandatele președinților Gerald Ford și George W. Bush, dorea, încă din 2003, să *„lupte cu internetul*”, pe care îl asemăna cu un *„sistem de arme inamice”*[7].

MĂSURAREA IMPACTULUI PSIHOLOGIC AL TERORISMULUI CIBERNETIC PRIN INTERMEDIUL MASS-MEDIEI

Dezvoltarea agendelor structurilor de presă se bazează pe premisa că mass-media are o influență semnificativă asupra modului în care publicul identifică subiectele cele mai importante, o presupunere teoretică bazată pe mai multe studii empirice. În acest domeniu, există două tipuri principale de abordare, una care se concentrează pe elită și cealaltă, care este fundamental pluralistă. Abordarea de elită se concentrează asupra puterii politice instituționale și a factorilor de decizie, în timp ce a doua extinde conceptul de *„agendă politică”* pentru a include factori precum agenda sau agendele mass-media[8]. Se va sublinia că mass-media acționează ca principală sursă de informații politice a maselor în interiorul statului, dar și în străinătate și, cu atât mai mult, din cauza dezvoltării programelor de televiziune prin satelit, dar și ainternetului.

Ele servesc, de asemenea, drept *„canal principal”* pentru comunicarea temerilor și dorințelor publice atât ale elitelor politice, cât și ale actorilor guvernamentali. Media tradițională este un mare operator de putere în societatea contemporană, cu o influență inegalabilă asupra diseminării informațiilor și a știrilor. Acționează ca un intermediar nu numai între populație și guvern, ci și în cadrul organelor guvernamentale.

Relațiile dintre terorismul cibernetic, ca parte a terorismului convențional, și mass-media sunt la fel de complexe, ambigue, menținând o legătură organică și funcțională între ele[9]. Conform psihologului francez Évelyn Josse, *„fără mass-media, terorismul modern nu ar supraviețui”*[10]. În era informațională, în societatea noastră globalizată, mass-media oferă spațiul necesar pentru hackeri și teroriști de a răspândi mesajul și teroarea prin intermediul mediului online.

[6] J. Lasker, *U.S. Military's Elite Hacker Crew*, 2005, disponibil la https://www.wired.com/2005/04/u-s-militarys-elite-hacker-crew/

[7] A. Brookes, *U.S. plans to 'fight the net' revealed*, BBC, 2006, disponibil la http://news.bbc.co.uk/2/hi/americas/4655196.stm

[8] Maura Conway, *Le cyber-terrorisme, ibidem.*

[9] Pierre Mannoni, Christine Bonardi, *Terrorisme et Mass Médias*, în *Topique Revue*, 2003, nr. 83, pp. 55-72.

[10] Évelyn Josse, *Les médias face au terrorisme et aux populations affectées, l'impossible équation*, 2015, disponibil la www.resilience-psy.com

Rolul principal al mass-mediei în cazul producerii unui atentat cibernetic este acela de a disemina știrea privind atacul, în mediul online, dar și pe posturile de televiziune, prezentând care au fost daunele produse de acesta și ce măsuri au fost luate pentru a putea fi combătute efectele pe termen scurt.

IMPACTUL PSIHOLOGIC PRODUS DE PROPAGANDA TERORISTĂ

Rețelele teroriste recrutează adepți nu doar pentru a produce atentate teroriste, dar și pentru a-i folosi în funcție de cunoștințele de specialitate pe care le au, pentru a penetra rețelele de calculatoare și a le virusa sau a le cripta datele, cu scopul obținerii de bani de pe urma furnizării cheii unice de decriptare. Acești recruți sunt folosiți și pentru a disemina propaganda teroristă în mediul online prin intermediul rețelelor sociale sau prin deturnarea website-urilor unor companii private sau instituții de stat. Un exemplu elocvent de deturnare a unui website, dar care a constituit și un atac cibernetic major, este reprezentat de atacul efectuat în luna august 2012 asupra companiei de stat Saudi Aramco, care a dus la scoaterea din funcțiune a 30.000 de calculatoare. Reţeaua de calculatoare a companiei a fost infectată cu un virus, într-un act de sabotaj fără precedent. Atacul a fostrevendicat de o grupare numită Sabia de tăiere a Justiţiei, care acuza guvernul saudit de crime și atrocităţi în mai multe ţări. Virusul a cauzat ștergerea datelor pentru treisferturi din calculatoarele companiei, înlocuindu-le cu imaginea unui drapel american ars[11].

Pe 18 ianuarie 2016, Observatorul *Paalga* a publicat în mod succesiv o fotografie cu Mokhtar Belmokhtar[12], pe care îl descriau drept *„presupusul creier al atacurilor din Ouagadougou”*[13]. În numărul din ianuarie al revistei *Le Pays* au fost publicate fotografiile tuturor victimelor, oferind organizațiilor teroriste sponsorizate o idee despre masacrul pe care l-au produs.

De asemenea, imaginile au fost este preluate sub forma altor titluri și diseminate prin intermediul altor trei ziare online. Scopul acestor diseminări este de a arăta care este amploarea pagubelor, hrănind psihoza teroriștilor, pentru a transmite ideea unui terorism militar mai puternic decât forțele militare consacrate. Teroriștii sunt prezentați de cele trei ziare ca *„ființe anormale”, „nebuni ai lui Allah”, „minți criminale care nu cred nici în Dumnezeu, nici în Diavol”*[14].

[11] *Saudi Aramco Oil Giant Recovers from Virus Attack News Technology*, BBC, 27 august 2012, disponibil la https://www.bbc.com/news/technology-19389401.

[12] Mokhtar Belmokhtar este un lider algerian al grupului Al-Murabitoun, fost comandant militar al grupării Al-Qaeda din Magreb; disponibil la https://en.wikipedia.org/wiki/Mokhtar_Belmokhtar.

[13] *Burkina-Faso. De Sankara à Compaoré et la rivalité entre Daech et l'Aqmi*, pe *À l'encontre*, 18 ianuarie 2016, disponibil la https://alencontre.org/category/afrique/burkina-faso

[14] B. Labasse, P. Savary și Thierry Watine, *Les Cahiers du journalisme*, vol. 2, nr. 1, trimestrul I, 2018, Les Presses de l'Université d'Ottawa.

Teroriștii masacrează oamenii printr-un război fizic, iar mass-media și rețelele sociale amplifică impactul psihologic al acestor fapte. Groaza este dramatizată și prezentată pe un ton plin de compasiune, astfel dispare linia dintre jurnalistul care scrie știrea și omul emoțional care o citește[15]. Moartea este pusă în scenă, amestecând emoții și groază. Istoricul francez Jean-Pierre Filiu vorbește despre *„teroare mediatică”* pentru a ilustra voracitatea presei pentru actul terorist. Căutarea informațiilor despre șoc îi determină, adesea, să servească drept vehicule de propagandă teroristă. Media devine, astfel, complicele involuntar al teroriștilor a căror existență și acțiuni le face cunoscute[16].

EFECTELE PSIHOLOGICE ASUPRA ȚINTELOR

Înainte de a vedea care sunt efectele asupra țintelor, trebuie identificat care este profilul teroristului cibernetic, care sunt motivațiile și țintele sale. În ceea ce privește profilul și motivațiile teroristului cibernetic, putem spune că acestea sunt aproape similare cu cele ale teroristului clasic, diferind doar mediul de luptă.

Teroristul cibernetic este o persoană ce are cunoștințe avansate în domeniul IT. Scopul acestuia este atingerea unui deziderat, cum ar fi cel asimilat fenomenului terorist, context în care atacurile realizate de aceștia sunt aparent bazate pe convingerile politice sau pe dorința de a contesta legitimitatea organizațiilor sau a guvernelor țintă. Analitic, se constată faptul că agresiunile realizate de aceste grupuri nu relevă un tipar anume.

Din cercetările realizate până acum, rezultă faptul că majoritatea teroriștilor nu suferă de boli mintale, ci sunt oameni raționali, care evaluează foarte bine costurile și implicațiile actului terorist, indiferent de natura acestuia, ajungând, într-un final, la concluzia că este profitabil.

Aderarea la un grup terorist îi conferă nou-venitului un sentiment de apartenență la o comunitate, de putere și de identitate a unui om care are probleme de adaptare socială, și nu numai. Pentru atacator, beneficiile nu sunt neapărat materiale, ci ele constau în satisfacerea unor nevoi de ordin spiritual și social.

Cei care ajung să facă parte din cadrul unei organizații teroriste sunt recrutați astfel încât să satisfacă nevoile organizației. În acest sens, recrutorul organizației teroriste are mai multe criterii după care se ghidează în procesul de recrutare. Acestea variază începând de la vârstă, sex, mediul social până la diferite calități pe care aceștia le caută pentru îndeplinirea anumitor misiuni de natură teroristă.

[15] Lassané Yaméogo, *Les médias, un allié du terrorisme*, 2016, disponibil la http://cahiersdujournalisme.org/V2N1/CaJ-2.1-R007.html

[16] J.P. Filiu, *Barbarie jihadiste et terreur* médiatique, Cités, 2015, pp. 27-38.

Etapa-cheie pentru crearea profilului psihologic al unui terorist cibernetic este identificarea unor caracteristici comune care trebuie investigate. Caracteristicile cuprind aspecte înnăscute, cum ar fi deschiderea, conștientizarea, extroversia, agreabilitatea și nevroticul. De asemenea, trăsăturile și caracteristicile personale sunt modelate de experiențe și evenimente de viață care duc, astfel, la machiavellianism, narcisism, psihopatie, senzație care caută maturitate, agresivitate, probleme de abilități sociale, superficialitate, lipsa autostimei și integritate personală. Factorii motivanți ai criminalității cibernetice ajung la hacktivism, câștig monetar, spionaj, sabotaj, credințe politice și religioase, curiozitate, emoții, sporirea valorii de sine și intenția de a controla și manipula pe alții.

Din punct de vedere motivațional, există următoarele tipuri psihologice de teroriști, și anume[17]:

Răzbunătorul – acesta acționează sub impulsul determinant al dorinței de revanșă pentru un afront personal anterior. Acesta este dispus să plătească cu viața sau cu libertatea.

Infractorul de drept comun – urmărește satisfacerea cauzei prin violență, interesele fiind, de cele mai multe ori, materiale. Acest lucru se poate realiza fie direct, prin deposedarea victimei de bunurile existente, fie pe un timp mai îndelungat, prin formularea unor pretenții față de apropriații victimei (recompensa).

Criminalul plătit – care acționează la indicația și cu sprijinul financiar și material al unor organizații teroriste, având drept obiectiv suprimarea vieții unor personalități politice sau militare, care se opun ideilor și intereselor organizației. Teroriștii din această categorie sunt, de obicei, oameni profesioniști, cunoscători ai mai multor limbi străine sau de diferite domenii, cu calități fizice și psihice deosebite, fapt ce le permite să se angajeze în acțiuni extrem de riscante.

Bolnavul mintal – acționează indiferent de caz, de situație sau de consecințe. Acesta este puternic radicalizat și acționează dintr-un impuls maladiv și irațional.

Fanaticul religios – aceasta acționează violent, considerând că este condus de o forță divină să apere ideile și concepțiile religioase al căror este adept, victima fiind orice persoană sau entitate care contrazice aceste idei. Acesta este condus de instinctul religios ce îl orbește și îl face să creadă că, prin acțiunile sale, îl slăvește pe Allah. De obicei, această categorie de teroriști sunt formați încă din copilărie, fiindu-le insuflată violența, ura față de *„necredincioși”* și fiind crescut în spiritul fanatismului religios.

[17] S.A. Jalil, *Countering Cyber Terrorism Effectively: Are We Ready to Rumble?*, Global Information Assurance Certification Paper, disponibil la https://www.giac.org/paper/gsec/3108/countering-cyber-terrorism-effectively-ready-rumble/105154

Martirul național – are drept motivație sacrificiul pentru o cauză măreață și de interes național. Aceasta va atenta la acele personalități care, în opinia sa și a organizației din care face parte, constituie o problemă în calea promovării intereselor lor naționale, precum și a grupului din care face parte.

Protestatarul politic – are o motivație similară cu cea a martirului național, însă interesele sale sunt de natură politică.

Din punctul nostru de vedere, teroristul cibernetic este un pic diferit de cel clasic, prin prisma faptului că acesta își desfășoară activitatea în mediul online. Din perspectivă psihologică, o persoană nu se naște terorist sau terorist cibernetic, ci suferă pe parcurs un set de transformări. Organizațiile teroriste sunt interesate în mod special de grupurile de indivizi nemulțumiți sau marginalizați.

Potrivit piramidei lui Maslow, pentru organizațiile teroriste sunt importante trei categorii de persoane care pot fi transformați în teroriști cibernetici, și anume: persoane cu nevoi sociale de incluziune și afirmare, persoane cu nevoie de securitate, persoane cu nevoi de bază[18].

Pentru persoanele cu nevoi de bază, este foarte atrăgătoare ideea de a se alătura unei organizații teroriste din prisma faptului că aceasta îi poate oferi beneficii materiale atât ei, cât și familiei sale. Frustrarea este un element-cheie în cadrul acestor persoane. O parte din comportamentul teroriștilor este legat de frustrarea privind imposibilitatea de a-și satisface anumite nevoi personale, fie că sunt de natură psihologică sau fiziologică, iar acest lucru duce la acte de agresiune.

În strânsă legătură cu neîmplinirea anumitor nevoi este și izolarea de restul societății. Astfel, dacă o persoană nu reușește să își satisfacă acele nevoi, începe să nege orice fel de comportament uman și, astfel, se izolează de restul societății. Devine lipsit de empatie față de nevoile altora și dezvoltă un comportament antisocial distructiv față de semenii săi.

Un alt element în acest sens este sindromul grandomaniei. În acest caz, individul are o părere idealizată despre el însuși și nu posedă niciun respect pentru semenii săi. Aceasta poate deveni violent dacă ajunge la concluzia că societatea nu îl respectă, nu îi respectă credințele și idealurile, devenind frustrat că nu poate avansa pe treptele piramidei lui Maslow. Acest tip de individ are nevoie de afirmare puternică și simte nevoie de a-i distruge pe cei care i se opun.

Potrivit unui document elaborat de Oficiul Națiunilor Unite pentru Droguri și Criminalitate (UNODC), Al-Qaeda a început, de ceva timp, să recruteze minori pentru a face față lipsei de resurse umane. Se pare că organizația și-a îndreptat

[18] European Union Agency for Network and Information Security, *ENISA overview of cybersecurity and related terminology*, septembrie 2017, disponibil la https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology

atenția asupra minorilor cu dezabilități mentale, cu un IQ scăzut sau care provin din familii destrămate ori din medii sociale nefaste. Media de vârstă în rândul acestor minori este de 13-16 ani[19].

O altă categorie care este de interes pentru organizațiile teroriste sunt femeile. Aceastea nu sunt neapărat folosite în actele de terorism, însă pot fi folosite în procesul de recrutare și propagandă pe internet[20].

Terorismul cibernetic este un domeniu atractiv pentru teroriștii moderni și din motivul că este mult mai ieftin decât metodele clasice de terorism. Teroristul modern are nevoie doar de un computer personal și de o conexiune online, nu trebuie să cumpere arme sau explozivi, ci poate crea și livra viruși de calculator printr-o linie telefonică, un cablu sau o rețea. Este anonim față de terorismul tradițional, acest lucru punând în dificultate agențiile de securitate să urmărească sau să identifice sursa atacului.

Varietatea și numărul de ținte sunt foarte mari, teroristul cibernetic putând viza mai multe computere și rețele în același timp. Potrivit studiilor, infrastructurile critice sunt vulnerabile în fața atacurilor teroriștilor, deoarece sunt extrem de complexe, ceea ce face dificil de eliminat toate punctele slabe. Atacul poate fi realizat de la distanță, acest lucru fiind foarte atractiv pentru teroriștii cibernetici, deoarece elimină restul investițiilor pe care ar fi trebuit să le facă în cazul unui atac terorist tradițional (tabere de antrenament, investiții în arme, psihologice etc.). Terorismul cibernetic poate afecta un număr mai mare de oameni decât terorismul tradițional, generând, astfel, un impact mai mare asupra mass-mediei.

Categoriile de ținte afectate de terorismul cibernetic sunt: cetățenii, instituțiile statului, companiile private.

Infrastructurile critice ale unui stat sau operațiunile financiare (ca, de exemplu, comerțul online, schimbul valutar, plata facturilor) sunt afectate, în mare măsură, de actele teroriștilor cibernetici, însă persoanele care sunt direct afectate vor suferi un stres psihologic mult mai mare, așa cum este în cazul unui furt de date de pe cardul de debit, care poate lăsa un individ fără toți banii din contul bancar. Nu putem subestima impactul pe care atacurile cibernetice le-ar putea avea asupra oamenilor, deoarece diferite persoane reacționează diferit la astfel de situații. Unora dintre persoane, direct afectate de terorismul cibernetic, în cazuri

[19] United Nations Office on Drugs and Crime (UNODC), *Handbook on Children Recruited and Exploited by Terrorist and Violent Extremist Groups: The Role of the Justice System*, 2017, Viena, disponibil la https://radical.hypotheses.org/files/2016/04/Handbook_on_Children_Recruited_and_Exploited_by_Terrorist_and_Violent_Extremist_Groups_the_Role_of_the_Justice_System.E.pdf

[20] D.E. Denning, *Activism, Hacktivism, and Cyberterrorism: the Internet as a Tool for Influencing Foreign Policy*, în J. Arquilla, D. Ronfeldt (Eds.), *Networks and netwars. The future of terror, crime and militancy*, Chapter eight, 239-288. Santa Monica: RAND Corporation, disponibil la https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf

precum pierderea informațiilor vitale ale companiei, care pot fi utilizate pentru a amenința starea de bine a organizației sau a persoanei vizate, li se poate induce sentimentul de teamă, iar persoana afectată va trăi sub un stres sever. Persoana implicată va suferi emoțional și acest lucru ar putea afecta starea sănătății sale mintale. În alte cazuri, în care atacurile de dezinformare folosind site-uri web, e-mail și alte mijloace electronice ar putea fi efectuate pentru a disemina zvonuri despre o anumită situație, organizație sau o persoană, pot duce la un haos în rândul publicului larg. Oamenii vor intra în panică și, astfel, operațiunile financiare și modul normal de viață vor fi perturbate. Prin urmare, este necesar ca publicul larg să fie bine informat despre terorismul cibernetic și să poată identifica pașii care pot fi făcuți pentru a face față îngrijorării cât mai bine[21].

COPIII, O ȚINTĂ A TERORISMULUI CIBERNETIC?

Conform legilor naționale din mai multe țări ale lumii, copiilor minori le sunt protejate demnitatea și integritatea împotriva oricăror încălcări din partea altor persoane. De exemplu, legislativul tunisian are o politică ce urmărește să lupte împotriva exploatării minorilor de către criminalitatea organizată și să prevină toate formele de îndoctrinare ideologică. Printre alte fenomene cu care se poate confrunta un copil atunci când navighează pe internet se află: instigarea la ură, stimularea pentru a se alătura unor rețele teroriste, propagarea mesajelor teroriste prin intermediul terorismului cibernetic și rasismul cibernetic, care se referă la jignirea și instigarea altor persoane la rasism. Lupta împotriva ambelor tipuri de implicare este o necesitate absolută, care necesită vigilență din partea serviciilor competente în domeniu.

Există, în spațiul cibernetic, multiple atacuri asupra demnității și integrității copiilor. Acestea constituie amenințări la adresa demnității lor umane. Aceste leziuni apar în mai multe forme, cum ar fi traficul de organe, traficul de copii prin intermediul internetului, *„cyber-droguri”* și *„cyber-rasism”*[22]. În al doilea rând, în ceea ce privește traficul de copii prin internet, legislațiile naționale interzic exploatarea copiilor sub diferite forme de criminalitate organizată. Însă, protecția copiilor în spațiul cibernetic nu se limitează la aceste trei fenomene, existând și alte fenomene care pot constitui amenințări la demnitatea și integritatea copiilor.

[21] S.A. Jalil, *Countering Cyber Terrorism Effectively: Are We Ready to Rumble?, ibidem.*

[22] M. Gargouri, *La protection de l'internaute mineur face aux actes de cyber-terrorisme*, Village de la Justice. La Communauté des métiers du droit, disponibil la https://www.village-justice.com/articles/protection-internaute-mineur-face-aux-actes-cyber-terrorisme, 32235.html

În prezent, internetul este la baza riscurilor și pericolelor prin care copiii devin victime. Copiii care utilizează internetul pot cădea pradă pedofililor, teroriștilor și mișcărilor rasiste. Acest instrument este un mijloc de recrutare a teroriștilor. Grupuri teroriste și recrutori consultă paginile de Facebook și blogurile de chat cu mesaje în căutarea persoanelor receptive, în special a tinerilor vulnerabili, pentru a-i implica într-un grup online privat, în spatele căruia se află un grup terorist. Activiștii recrutați din mediul online de către teroriști sunt, în mare parte, minori și tineri. Majoritatea teroriștilor morți din zonele de conflict sau prinși sunt tineri cu o vârstă mai mică de 18 ani. Tinerii de astăzi sunt idealiști și cred că au puterea de a schimba lumea. Teroriștii profită de această etapă normală a dezvoltării lor intelectuale, psihologice și biologice pentru a atrage și a manipula insidios acești tineri.

Conform avocatului tunisian Mohamed Gargouri, infracțiunile din domeniul terorismului cibernetic în detrimentul copiilor pot lua două forme, fie prin prezentarea informațiilor teroriste, fie prin recrutarea electronică a copiilor ca activiști teroriști. În statele arabe, cu precădere, un fenomen care a luat amploare în ultimii ani îl constituie activismul cibernetic; deși este răspândit în lume, acest subiect este marcat în lumea arabă prin represiune și anonimat. Reprimarea se manifestă prin cenzura folosită de autorități și, chiar dacă teroriștii nu și-au propus decât să treacă de la provocarea de pe internet la acțiunea de concretizare a răului, faptul rămâne real.

Site-urile și paginile de facebook sunt considerate de legislația tunisiană *„alte materiale sau echipamente”*, folosite de o organizație sau persoane fizice pentru a comite infracțiuni de terorism în cyberspațiu.

Trebuie subliniat faptul că propaganda și publicitatea nu sunt doar activități strâns legate de războiul psihologic, deoarece există și altele, precum pirateria. Hackingul computerizat reprezintă un atac țintit, eficient și automatizat, suficient de coordonat menit să paralizeze activitățile computerizate ale unui copil pe internet. Pirateria poate submina demnitatea umană a minorului prin exploatarea ilegală a fotografiilor sau a informațiilor sale. Grupurile de hackeri au interese lucrative și folosesc know-how-ul tehnologic, prin infiltrarea în rețele sociale și punându-și talentul în slujba convingerilor sale prin organizarea de atacuri informatice în scopul piratării și al deturnării datelor personale ale copiilor. Hackerii sunt motivați de bani, sunt legați de organizații criminale și sunt dispuși să-și vândă serviciile către cel mai bun ofertant. Printre formele de activism cibernetic se numără strângerea de fonduri, mobilizarea, schimbul de informații, planificarea, coordonarea și, mai ales, recrutarea teroriștilor[23].

[23] Goubin Yang, *Cyber-activism [draft] [#digitalkeywords]*, 9 iunie 2014, disponibil la http://culturedigitally.org/2014/06/cyber-activism-draft-digitalkeywords/

CONCLUZII

Terorismul cibernetic are un impact direct și indirect asupra persoanelor, în primul caz, persoanele nu conștientizează imediat că ceea ce se întâmplă în jurul lor reprezintă rezultatul unor atacuri cibernetice, iar în cel de al doilea caz, oamenii pot dobândi un sentiment de teamă, de stres.

Principalul rol al mass-mediei în cazul producerii unui atentat cibernetic este acela de a disemina știrea privind atacul în mediul online, dar și pe posturile de televiziune, prezentând care au fost daunele produse de acesta și ce măsuri au fost luate pentru a putea fi combătute efectele pe termen scurt.

De asemenea, influențează populația prin intermediul mass-mediei, care diseminează știrile în flux și care un caracter negativ, de cele mai multe ori, deoarece știrile negative aduc un rating crescut unui post de televiziune sau un număr mult mai mare de accesări ale unei pagini web.

Terorismul cibernetic are si un impact psihologic produs de propaganda teroristă, persoanele recrutate de organizații fiind folosite pentru a disemina propaganda acestora în mediul online prin intermediul rețelelor sociale sau prin deturnarea website-urilor unor companii private sau instituții de stat. O categorie de țintă care este din ce în ce mai afectată sunt copiii minori, care, de cele mai multe ori, au acces la internet și pot cădea foarte ușor pradă unor persoane rău intenționate. Trebuie subliniat faptul că propaganda și publicitatea nu sunt doar activități strâns legate de războiul psihologic, deoarece există și altele, precum pirateria. Hackingul computerizat reprezintă un atac țintit, eficient și automatizat, suficient de coordonat, menit să paralizeze activitățile computerizate ale unui copil pe internet.

BIBLIOGRAFIE:

1. ***, *About us*, NATO StratCom, Centre of Excellence, 2019, disponibil la https://www.stratcomcoe.org/about-us
2. ***, *Burkina-Faso. De Sankara à Compaoré et la rivalité entre Daech et l'Aqmi*, în À *l'encontre*, 18 ianuarie 2016, disponibil la https://alencontre.org/category/afrique/burkina-faso
3. ***, *ENISA overview of cyber security and related terminology*, European Union Agency for Network and Information Security, septembrie 2017, disponibil la https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology
4. *Handbook on Children Recruited and Exploited by Terrorist and Violent Extremist Groups: The Role of the Justice System*, United Nations Office on Drugs and Crime (UNODC), 2017, Viena, disponibil la https://radical.hypotheses.org/files/2016/04/Handbook_on_Children_Recruited_and_Exploited_by_Terrorist_and_Violent_Extremist_Groups_the_Role_of_the_Justice_System.E.pdf

5. *Saudi Aramco Oil Giant Recovers from Virus Attack News Technology*, BBC, 27 august 2012, disponibil la https://www.bbc.com/news/technology-19389401
6. *Truth behind America's raid on Belgrade*, *The Guardian*, 28 noiembrie 1999, disponibil la https://www.theguardian.com/theobserver/1999/nov/28/focus.news1
7. A. Brookes, *U.S. plans to 'fight the net' revealed*, BBC, 2006, disponibil la http://news.bbc.co.uk/2/hi/americas/4655196.stm
8. Maura Conway, *Le cyber-terrorisme. Le discours des médias américains et ses impacts*, Cités, 2009/3 (no 39), disponibil la https://www.cairn.info/revue-cites-2009-3-page-81.htm
9. D.E. Denning, *Activism, Hacktivism, and Cyberterrorism: the Internet as a Tool for Influencing Foreign Policy*, în J. Arquilla, D. Ronfeldt (Eds.), *Networks and netwars. The future of terror, crime and militancy*, Chapter eight, 239-288, Santa Monica: RAND Corporation, disponibil la https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf
10. J.P. Filiu, *Barbarie jihadiste et terreur médiatique*, Cités, 2015.
11. M. Gargouri, *La protection de l'internaute mineur face aux actes de cyber-terrorisme*, Village de la Justice. La Communauté des métiers du droit, disponibil la https://www.village-justice.com/articles/protection-internaute-mineur-face-aux-actes-cyber-terrorisme,32235.html
12. S.A. Jalil, *Countering Cyber Terrorism Effectively: Are We Ready to Rumble?*, Global Information Assurance Certification Paper, disponibil la https://www.giac.org/paper/gsec/3108/countering-cyber-terrorism-effectively-ready-rumble/105154
13. Évelyn Josse, *Les médias face au terrorisme et aux populations affectées, l'impossible équation*, 2015, disponibil la www.resilience-psy.com
14. B. Labasse, P. Savary, Thierry Watine, *Les Cahiers du journalisme*, vol. 2, nr. 1, trimestrul I, 2018, Les Presses de l'Université d'Ottawa.
15. J. Lasker, *U.S. Military's Elite Hacker Crew*, 2005, disponibil la https://www.wired.com/2005/04/u-s-militarys-elite-hacker-crew/
16. J.P. Manach, *Le cyberterrorisme est virtuel*, la cyberguerre en préparation, 2006, disponibil la http://www.internetactu.net/2006/02/24/le-cyberterrorisme-est-virtuel-la-cyberguerre-en-preparation/
17. P. Mannoni, Christine C. Bonardi, *Terrorisme et Mass Médias*, *Topique Revue*, 2003, nr. 83.
18. Lassané Yaméogo, *Les médias, un allié du terrorisme*, 2016, disponibil la http://cahiersdujournalisme.org/V2N1/CaJ-2.1-R007.html
19. Goubin Yang, *Cyber-activism [draft] [#digitalkeywords]*, 9 iunie 2014, disponibil la http://culturedigitally.org/2014/06/cyber-activism-draft-digitalkeywords/