FORME DE MANIFESTARE A TERORISMULUI CIBERNETIC

WAYS OF CYBERTERRORISM

FORMES D'ACTION DU CYBERTERRORISME

Cdor.prof.univ.dr. Sorin TOPOR*

Atacurile cibernetice, în prezent, devin tot mai complexe, mai frecvente şi cu efecte distructive tot mai mari. Indiferent de tipul sau dimensiunea unei organizaţii, aceasta afectează informaţiile infrastructurilor publice şi private.

Terorismul contemporan, care urmărește comiterea de acţiuni cu obiective clare, desfășurate o singură dată sau în serie, având, ca motivaţii, rezistenţa la schimbarea de ordin politic, economic sau social, efecte asupra informaţiilor globale, utilizează și metode de atac cibernetic prin implementarea noilor tehnologii informaționale.

În acest articol mi-am propus ca, pornind de la analizarea principalilor factori de insecuritate publică și de dezordine socială, pe care îi consider ca determinanți în dezvoltarea unor forme moderne de terorism, să formulez conținutul conceptului de terorism cibernetic, în raport cu care să evidențiez acele aspecte relevante pentru înțelegerea modalităților sale de aplicare.

Cyber attacks are now becoming more and more complex, more frequent and with increasing destructive effects. Regardless of the type or value of an organization, it affects information of public and private infrastructures.

In this context, the terrorism aims to execute actions, driven only once or in series, motivating as resistance to political, economic or social changes and producing global information effects. It is well known the development of terrorism is favored by the development of information technology. Last but not least, the social factor and the arms proliferation determine the adapt of objective aspect of terrorism, often the modeling of terrorist ideology based on issues of population discontent with the ease of acquisition of weapons, munitions and destructive materials through various forms of trade.

In this work we propose to determine the content of the concept of cyber terrorism, starting from the analysis of the main factors of public insecurity and social disorder that facilitate the development of modern forms of terrorism. In this order we propose to underline the base aspects to understand the ways of its application.

Les cyberattaques sont, à l'heure actuelle, de plus en plus complexes, de plus en plus fréquentes et de plus en plus destructrices. Quelle que soit la nature ou la dimension d'une organisation, elles portent préjudice aux informations des infrastructures publiques et privées.

Le terrorisme contemporain, qui cherche à engager des actions ponctuelles ou successives, avec des objectifs bien définis, ayant pour motivation la résistance aux changements politiques, économiques ou sociaux, ayant des effets sur les informations globales, utilise également des méthodes de cyberattaque par la mise en œuvre de nouvelles technologies de l'information.

À partir de l'analyse des principaux facteurs d'insécurité publique et de désordre social, considérés, à mon avis, comme déterminants pour le développement des formes modernes du terrorisme, j'ai l'intention, dans cet article, d'établir le contenu du concept de cyberterrorisme, par rapport auquel je devrais souligner les aspects pertinents pour comprendre ses modalités de mise en pratique.

Cuvinte-cheie: terorism; terorism cibernetic; spionaj cibernetic; fraude cibernetice; e-propaganda; e-instruire; radicalizare.

Keywords: *terrorism; cyber terrorism; cyber spying; cyber frauds; e-propaganda; e-training; radicalization.*

Mots-clés: *terrorisme; cyberterrorisme; cyber-espionnage; cyber fraude; e-propagande; e-learning; radicalisation.*

**** Universitatea Națională de Apărare „Carol I”***
e-mail: *sorin.topor@yahoo.com*

În prezent, în cadrul societății informațiile circulă extrem de rapid prin capabilitățile moderne oferite de tehnologia informațională. Astfel, mass-media își consolidează funcția de instrument de bază pentru analiza, transmiterea, formarea curentelor de opinii, pentru stabilirea sau pentru corectarea unor agende de lucru ale factorilor decizionali etc., toate acestea având, ca principal obiectiv, „comerțul cu informații”. De aceea informațiile vândute trebuie să fie frumos prezentate, în imagini sugestive, dacă este vorba despre o situație materială și/sau cu însușiri carismatice, dacă acestea provin din situații specifice vieții socioumane. Pentru aceasta, au apărut adevărate „științe”, așa cum sunt neuromarketingul, consilierea de imagine, consultanța vestimentară etc.

Putem aprecia că toate aceste caracteristici ale cotidianului au, ca scop principal, captarea atenției unui public, devenind „ținta” lui de interes, fie acesta instruit ori nu, educat sau nu. Se observă că, pentru atingerea acestui obiectiv, în prezent nu mai pot fi utilizate doar metodele tradiționale de comunicare. Pentru ca o agenție mediatică să aibă succes, va trebui ca publicul vizat să fie „sedus” cu informații. Iar pentru a ajunge la sufletul oamenilor, sunt necesare tehnici și tehnologii moderne care să permită optimizarea abilităților de comunicare la nivel global. Mă refer la accesul facil la serviciile Internet, la servicii de știri, furnizate prin diverse canale TV, radio și presă scrisă, la alte servicii de comunicare, la comunicații de tip satelitar, la telefonia celulară etc.

Organizațiile teroriste, promovând violența extremă, au și acestea publicul lor. Persoanelor care formează acest segment de public le sunt stimulate percepțiile pentru a considera că dețin un nivel ridicat de „psiho-putere” asupra altor indivizi. Numai așa se explică de ce acest tip de public ascultă şi susţine mesajul transmis de liderii organizațiilor teroriste.

Cele mai elocvente exemple provin din spaţiile actuale de conflict, şi anume: din Afganistan, din Orientul Mijlociu, din Africa etc., zone unde se încurajează reacția armată prin stimularea percepţiei populației că războiul, declanșat de SUA, se desfășoară împotriva islamului; din zona Palestina – Israel, unde se promovează ideea de aplicare discreţionară a politicilor de acordare a drepturilor cetăţeneşti ori a modului de eliberare a vizelor, pe fondul situaţiei extrem de complexe a migraţei dinspre zonele controlate de ISIS/Daesh; din alte zone din arealul global, caracterizate printr-o puternică „rezistenţă socială”, manifestată de grupări anarhiste şi de justiţiari care militează, prin violență, pentru o așa-zisă „apărare a drepturilor omului”, violența fiind considerată singura formă de reacție față de abuzurile serviciilor de informaţii şi instituțiilor guvernamentale (de exemplu, lupta vestelor galbene în Franța, în anul 2018).

Apreciez că obiectivul nemijlocit al terorismului este de obţinere sau de menţinere a unei stări de insecuritate publică şi de dezordine socială în spații tot mai întinse. Iar dacă în societatea informațională, atribut tot mai des folosit pentru a caracteriza actualul stadiu de evoluție socială, informația a devansat celelalte dimensiuni sociale și organizațiile teroriste suferă transformări, fiind nevoite să își adapteze metodele de comunicare la cerințele consumatorilor de informații. Bazându-mă pe aceste particularități, „terorismul cibernetic” devine metoda cea mai atractivă pentru organizațiile teroriste contemporane, foarte bine adaptată mediului informațional contemporan. Astfel, Internetul devine un suport de furnizare de informații controlate de organizații teroriste, efectele asimilării lor de către publicul vizat fiind de amplificare a pericolului terorist, perceput de populație. Mai mult decât atât, rețeaua Internet a devenit un instrument de control și de manipulare, persoana manipulată emoțional fiind încurajată să ucidă, să provoace rănirea altor persoane, să se autodistrugă sau să provoace distrugeri materiale.

Apreciez că această metodă este mult mai complexă decât hacktivismul și infracționalitatea cibernetică, fiind exploatată de organizațiile teroriste pentru propagandă, pentru obținerea de sprijin financiar, de informaţii și pentru comunicare între membrii organizaţiilor lor[1].

Gabriel Weimann[2] a identificat cel puţin şase moduri diferite de utilizare a spaţiului cibernetic în scopuri teroriste:

1. *ca instrument al războiului psihologic* – se cunosc imaginile difuzate în scopul provocării terorii în rândul populaţiei ţintă (imagini cu ostatici executaţi prin decapitare şi care aparţineau unei naţionalităţi sau erau angajaţii unei corporaţii);

2. *ca instrument de propagandă* – organizaţiile teroriste pot face publicitate acţiunilor lor prin emisiuni în direct, oriunde în lume. Difuzarea de informaţii le facilitează popularizarea realizărilor şi diminuarea greşelilor lor;

3. *ca instrument financiar* – se cunoaște că Al-Qaeda a primit ajutor financiar, graţie averii lui Bin Laden şi contribuţiei mai multor organizaţii neguvernamentale, prin diverse metode de sponsorizare. În prezent, experţi, precum Jimmy Gurule, atrag atenţia asupra Bitcoin, ca reprezentând un mijloc potrivit pentru acordarea sprijinului financiar unei organizaţii teroriste[3]. Activităţile specifice crimei organizate, desfăşurate de Daesh, și ne referim, aici, la contrabanda cu benzină, pot fi încadrate acestui tip de sponsorizare, dacă plăţile se efectuează cu moneda cibernetică;

4. *ca instrument de recrutare* – folosind Internetul, Daesh şi-a înmulţit numărul de luptători străini, în comparaţie cu Al-Qaeda. Distribuirea masivă, în rândul populaţiei, a imaginilor şi videoclipurilor care arată viaţa „corectă” a mujahedinilor, precum şi succesul acţiunilor Daesh împotriva duşmanilor nonmusulmani (inclusiv execuţiile umane) au ajutat la deschiderea de birouri de informare şi de recrutare în întreaga lume. Succesul acestor metode, aşa cum era de aşteptat, a trezit un real interes printre tinerii musulmani;

5. *ca instrument de ascundere/disimulare a sistemului organizaţional şi conducerii sale* – practic, modelul de organizare și ierarhia structurilor unei grupări teroriste au putut fi ascunse prin stabilirea unor reţele multiple de posturi de comunicare. Astfel, importanţa elementelor de conducere, tradiționale unei ierarhii verticale, a fost estompată de conducerea în rețea, pe orizontală. Membrii sau grupările teroriste s-au putut sprijini reciproc, şi-au putut coordona şi planifica atacurile etc. într-un mod mai ieftin şi mai sigur. În Al-Qaeda, pentru ca liderii să nu poată fi detectaţi, s-a făcut apel către toţi „fraţii în jihad” să folosească serviciul PalTalk;

6. *ca depozit de documente* – oricine poate găsi în paginile web numeroase manuale şi ghiduri referitoare la fabricarea explozivelor, la lupta în mediul urban, la tactici de gherilă şi de supravieţuire etc.

Aspectele pe care le consider ca fiind definitorii pentru activitatea terorismului cibernetic, pe care le-am identificat prin analiza celor mai frecvente evenimente teroriste contemporane, le-am grupat în patru forme de manifestare, descrise în continuare. Având în vedere că majoritatea provin din surse deschise, unde informațiile nu prezintă întotdeauna un grad mare de credibilitate, precizez că această clasificare se bazează pe informații identificate în unele surse bibliografice și pe interpretarea personală a unor posibilități ipotetice de atac ale teroriștilor cibernetici.

Spionaj cibernetic

Apreciez că spionajul cibernetic este una dintre cele mai importante şi alarmante probleme internaţionale ale societăţii contemporane, prin aspectele pe care le voi prezenta succint în continuare.

Realitatea actuală ne confirmă că un sistem informaţional nu trebuie să mai fie protejat doar de cei identificaţi sau autointitulaţi „băieţi răi”, ci de oricine, care, în mod voit sau întâmplător, intră în „zona de confort” a ţintei. De aceea una dintre cele mai mari probleme care dă multe bătăi de cap guvernanţilor este definirea spionajului cibernetic. Multe organizații și-au creat propriile definiţii, care, de regulă, se rezumă la factorii care pot produce distrugeri de date și de informații, pe timpul unui atac, într-o rețea informatică, ori care ascund identitatea atacatorului sau felul în care au fost utilizate informaţiile furate etc.

În analiza de față, avem, ca reper, definiţia din Manualul Tallinn, care, sub regula 32, precizează că spionajul cibernetic reprezintă „orice act executat clandestin sau utilizarea de false pretenţii prin folosirea capabilităţilor cibernetice, în intenţia de a obţine informaţii”[4]. Aparent, nu ar trebui să abordăm această definiție atunci când analizăm terorismul cibernetic ca formă de manifestare a războiului asimetric. Însă Manualul Tallinn ne prezintă și unele concluzii ale grupului de experţi, potrivit cărora atacul Al-Qaeda, din 11 septembrie 2001, asupra SUA, este asimilat, sub aspect juridic internaţional, dreptului la autoapărare în faţa unui atac armat[5], situație care îmi permite utilizarea acesteia în continuare.

Plecând de la aceste opinii, analiza mea se complică, atunci când suprapun definiției speţa ”Snowden”, în care Edward Snowden a demonstrat că practic oricine poate spiona, Internetul oferind un mare nivel de anonimat. O multitudine de date şi de informaţii pot fi procurate din dispozitivele mobile conectate la diversele servicii de Internet, aşa cum sunt ipaduri, tablete, telefoane mobile, smartphone-uri etc. Toate aceste dispozitive electronice pot fi simultan în relații multiple, în diverse reţele cibernetice şi în rețele de comunicaţii.

Deşi există norme legislative care prevăd sancţiuni pentru interceptarea apelurilor telefonice celulare de către unele structuri guvernamentale, s-a dovedit că și structurile de crimă organizată pot intercepta și monitoriza convorbirile de pe un telefon mobil. Când telefonul emite, o rețea de telefonie digitală permite urmărirea dispunerii geografice a acelui dispozitiv. Identificat ca abonat, sub un număr de telefon celular, emisiile acestuia permit stabilirea activității desfășurate pe timpul deplasării între site-urile celulare şi prin Internet.

Având aceste oportunități, oferite de tehnologie, nimic nu îi împiedică pe teroriști să utilizeze tehnicile de interceptare și de monitorizare a unor emisii a dispozitivelor pe care le consideră de interes. Prin urmare, spionajul cibernetic poate fi utilizat și în sprijinul săvârşirii de acte teroriste. Acesta asigură: facilitarea accesului neautorizat; interceptarea pachetelor de date; virusarea sistemelor informatice; blocarea procesului de comunicare a datelor; piratare software; clonarea mijloacelor electronice de plată; activităţi de inginerie socială; identificarea de activități planificate prin aplicațiile de management al proiectelor, aplicații existente în orice telefon celular; alte particularităţi comportamentale ale ţintei.

În general, din perspectiva securității, riscurile şi implicaţiile unui atac major de securitate cibernetică, cu origini teroriste, pot fi comparabile celor din perioada Războiului Rece. Extrapolând aceste riscuri la un nivel mult mai mare asupra interesului național ori asupra interesului comun într-o alianță internațională, vom observa că, procedural, nu se schimbă cu nimic. Spre exemplu, infrastructurile reţelelor de transport al energiei electrice, instalaţiile de tratare a apei, nodurile de management feroviar şi rutier, facilităţile aeroportuare etc., toate sunt vulnerabile spionajului cibernetic și altor amenințări informaţionale. Spionajul cibernetic poate pregăti lovirea directă a unor ţinte, poate procura informaţii în sprijinul acțiunilor maliţioase și care nu vizează executarea unui atac direct, ori poate extrage informaţii, în scopul șantajării țintei și obținerii de fonduri.

Este evident că, pentru un astfel de efort de realizare a spionajului prin și cu dispozitive cibernetice, este nevoie de o forţă reală, de o capabilitate specializată, despre care nu avem cunoștință că ar exista în organizarea niciunei structuri teroriste contemporane. Însă, lipsa acestor infomații nu trebuie să ne „încurajeze” prea mult. Lecțiile învățate, în urma acțiunilor contrateroriste, ne atenționează că, atunci când un lider puternic al unei organizaţii teroriste dispune de fonduri suficiente, poate achiziționa de pe piaţa neagră cam tot ce își propune. Având bani, pot cumpăra serviciile unor indivizi recunoscuți ca având reale performanțe în activitatea infracțională pe Internet, ori a unor simpatizanţi ai ideologiilor teroriste, buni specialişti în utilizarea instrumentelor de spionaj cibernetic, iar stimulându-le orgoliile, să-și „rezolve” toate obiectivele informaționale propuse.

Fraude cibernetice, comise în sprijinul activităţii teroriste

Potrivit Codului penal din România, frauda informatică reprezintă „introducerea, modificarea sau ştergerea de date informatice, restricţionarea accesului la aceste date ori împiedicarea în orice mod a funcţionării unui sistem informatic, în scopul de a obţine un beneficiu material pentru sine sau pentru altul, dacă s-a cauzat o pagubă unei persoane”[6]. După cum se observă, în această definiție nu se face legătura cu terorismul. Definiția face trimitere către o zonă specifică infracţionalităţii.

În prezent, tot mai mulți infractori, în vederea comiterii de activităţi infracţionale, în afara graniţelor fizice sau administrative, exploatează viteza, confortul şi anonimatul oferit de mediul informatic, afectând grav victima prin atacurile cibernetice efectuate sau prin exercitarea de ameninţări asupra oricărei persoane aflate oriunde în lume.

Deşi nu există o definiţie universală şi recunoscută pentru infracțiuni cibernetice, pe baza cazuisticii penale privind infracţiunile legate de Internet, clasific activitatea infracțională specifică în:

• infracţionalitate informatică avansată (sau infracţiuni înalt tehnologizate) – cuprind atacuri sofisticate împotriva componentelor şi programelor informatice;

• infracţionalitate cu caracter informatic – cuprind infracţiuni „tradiţionale” care au suferit „modernizări”, odată cu apariţia Internetului. Între acestea, includem infracţiunile împotriva copiilor, infracţiuni financiare şi chiar acele activități infracționale din zona terorismului.

Încă o dată doresc să subliniez că, oricât de schimbătoare este natura infracţionalităţii

informatice, determinată de aceste noi tendinţe în dezvoltarea sistemelor şi reţelelor informatice, nu toate activităţile din Internet, specifice crimei organizate, reprezintă terorism cibernetic.

În general, activitatea recunoscută ca fiind desfăşurată de structurile de crimă organizată se orientează în vederea maximizării profitului, în cel mai scurt timp. Dintre acestea, amintim furtul, frauda, jocurile ilegale, vânzarea de medicamente contrafăcute etc.[7] Am considerat necesar să fac aceste precizări pentru a înţelege că structurile poliţiei sunt angajate în neutralizarea tuturor fraudelor informatice, pentru combaterea organizaţiilor teroriste, primind sprijin şi de la alte structuri specializate în combaterea activităţilor logistice sau financiare destinate susţinerii terorismului. De altfel, miniştrii de interne din cadrul G7 au solicitat, în cadrul întâlnirii de la Ischia, Italia, în octombrie 2017, partajarea informaţiilor, din platforma globală, despre aşa-anumiţii „luptători teroriști străini” (”foreign terrorist fighters – FTFs”) pe timpul schimbului de date şi analizei activităţii preponderent extremiste. În finalul acestui summit, miniştrii de interne au susţinut, printr-o declaraţie comună, că vor „sprijini rolul INTERPOL ca platformă globală pentru schimbul de informaţii despre documentele de călătorie pierdute şi furate, precum şi pentru examinarea sistematică a călătorilor internaţionali, incluzând schimbul de informaţii biometrice şi de date colectate în spaţiul de luptă. Nu în ultimul rând se angajează să încurajeze toate statele să intensifice utilizarea bazelor sale de date”[8]. De altfel, INTERPOL a fost pionierul schimbului de informaţii pentru sprijinul juridic al acţiunilor militare încă din anul 2005, prin Proiectul Vennlig, în Irak şi, ulterior, prin Proiectul Hamah, în Afganistan. Informaţiile furnizate prin INTERPOL permit subminarea activităţilor grupărilor teroriste, interzicerea deplasării luptătorilor-teroriști care urmăresc întoarcerea în zonele de conflict, evaluarea nivelurilor de risc şi sprijinirea investigaţiilor necesare executării arestărilor conexe.

De ce toate aceste alarme? Pentru că, începând cu anul 2018, pe baza evoluţiilor îngrijorătoare a ameninţărilor geopolitice, ideologice şi tehno-logice, care fac ca prevenirea fraudelor cibernetice să fie o problemă preponderent de protecţie a afacerilor împotriva noilor forme şi a celor emergente de infracţionalitate financiară, se observă şi o serie de efecte asupra stării de securitate naţională a unui stat. Astfel, în perioada 20-24 noiembrie 2017, printr-o iniţiativă EMMA (European Money Mule Action), îndreptată împotriva spălării banilor transnaţionali, s-a reuşit identificarea unor transferuri ilegale de fonduri legate de crimina-litatea informatică[9], în valoare de aproximativ 31 de milioane de dolari. Conform EMMA, 90% dintre aceşti bani puteau fi destinaţi sprijinirii activităţii teroriste a unor grupări, precum Boko Haram, Statul Islamic şi Hezbollah. Aceste fonduri proveneau din aşa-numitele transporturi de bani şi criptofonduri, transporturi despre care autorităţile afirmă că sunt esenţiale pentru operaţiunile care fac ca activitatea să treacă de la scopuri infracţionale la terorism.

Mai mult decât atât, în cazul operaţiilor militare de destabilizare a puterii militanţilor din Irak, din Siria, din Somalia etc., grupările extremiste par să se orienteze către infracţionalitatea financiară online, prin eforturi de finanţare a radicalizării[10], pentru recrutare din interiorul naţiunilor occidentale şi, nu în ultimul rând, pentru achiziţionarea de arme de foc necesare executării de atacuri individuale şi locale, cu obiective limitate. Se estimează că, în viitor, extremiştii din ţările occidentale ar putea dezvolta diverse metode de obţinere de venituri prin infracţiuni cibernetice pentru testarea de noi tehnologii, dintre care cele vizate sunt dronele încărcate cu exploziv[11]. De altfel, cele mai frecvente obiective ale fraudelor informatice pe care se sprijină activitatea teroristă sunt cele destinate achiziţionării online de diverse materiale, de componente explozive, chimice şi/sau biologice, închirierii de maşini şi apartamente.

Organizaţiile teroriste şi sponsorii lor pot folosi Internetul pentru finanţarea acestor activităţi. Modul în care teroriştii utilizează Internetul pentru strângerea de fonduri şi pentru achiziţionarea de resurse poate fi clasificat în patru categorii generale (indicare sursă a clasificării):

- cererea directă – se referă la utilizarea site-urilor web, grupurilor de chat, mesageriei electronice şi comunicărilor direcţionate pentru a solicita donaţii de la adepți;
- comerţul electronic – după cum se cunoaşte, în cadrul Internetului se poate desfăşura comerţ electronic, existând site-uri web care pot fi organizate ca magazine online cu diverse produse şi unde se pot oferi

susţinătorilor cărţi, înregistrări audio şi video, alte articole;

- exploatarea instrumentelor de plată online – dispozitivele de plată online oferă servicii specializate prin intermediul site-urilor dedicate sau al platformelor de comunicaţii, facilitează transferul fondurilor electronic între părţi;
- sponsorizare din partea unor organizaţii caritabile – transferurile de fonduri sunt adesea efectuate prin transfer bancar electronic, card de credit sau facilităţi alternative de plată, disponibile prin intermediul serviciilor, precum PayPal sau Skype.

„Spălarea banilor” este o altă activitate a crimei organizate, importantă pentru sprijinul organizaţiilor teroriste. Un exemplu în acest sens este cazul hackerului Younis Tsouli, care, în Marea Britanie, a spălat câştiguri ilicite, obţinute prin furtul din carduri bancare, în scopul finanţării unor acte de terorism[12]. Pentru aceasta, el a apelat la mai multe metode, inclusiv la transferul prin intermediul conturilor electronice de plată online, fondurile fiind direcţionate prin mai multe ţări, înainte de a ajunge la destinaţia dorită. Banii astfel spălaţi au fost utilizaţi atât pentru a plăti înregistrarea de către Tsouli a 180 de site-uri, unde se difuzau videoclipuri de propagandă ale Al-Qaeda, cât şi pentru a achiziţiona echipamente necesare activităţilor teroriste, în mai multe ţări. Se pare că au fost utilizate circa 1.400 de carduri de credit, care au generat aproximativ 1,6 milioane de lire sterline, în fonduri ilicite pentru finanţarea terorismului.

E-propaganda, educaţia şi radicalizarea

Exploatând Internetul, grupările teroriste pot „beneficia” de promovarea propriilor ideologii în vederea incitării la ură şi la violenţă, ori pentru pregătirea atentatelor teroriste, pentru atragerea de simpatizanţi, pentru instruire asistată etc. Reţelele informaţionale ale utilizatorilor casnici, ale firmelor şi ale instituţiilor, care permit conectarea diverselor tehnologii informaţionale, pot fi programate să execute simultan un atac în spaţiul cibernetic, din diverse zone ale lumii, asupra unui serviciu sau unei reţele conectate la Internet.

Una dintre cele mai cunoscute metode de atac pe Internet este difuzarea de materiale de propagandă. În general, propaganda prin Internet adoptă forma comunicărilor multimedia prin care se pune la dispoziţie cititorului o mulţime de informaţii care constituie instrucţiuni ideologice sau practice, explicaţii, justificări, sau care promovează aspecte specifice vieţii într-o organizaţie teroristă. Acestea pot include mesaje virtuale, prezentări, reviste, tratate, fişiere audio, video şi jocuri video, realizate de organizaţiile teroriste sau de simpatizanţi. Cu toate acestea, spre deosebire de abordarea legitimă a unui punct de vedere, ceea ce constituie propaganda teroristă este adesea o evaluare subiectivă a tuturor aspectelor prezentate.

Difuzarea propagandei nu este o activitate interzisă. Unul dintre principiile de bază ale dreptului internaţional privind protecţia drepturilor omului include dreptul la libertatea de exprimare. Aceasta garantează unei persoane dreptul de a împărtăşi o opinie sau de a distribui un conţinut, care, în mod normal, poate fi sau nu acceptat de către alte persoane (sub rezerva anumitor excepţii limitate).

Una dintre excluderile general acceptate în ceea ce priveşte acest drept este interzicerea distribuirii anumitor materiale cu conţinut sexual explicit, interdicţie considerată a fi în interesul public pentru protejarea grupurilor vulnerabile. Alte excluderi, prevăzute de lege şi dovedite a fi necesare, se referă la mesaje care, în mod vădit, sunt dăunătoare protecţiei securităţii naţionale şi internaţionale, precum şi la cele de natură să incite la acte de violenţă împotriva indivizilor sau anumitor grupuri de persoane.

Aşa după cum se cunoaşte, promovarea violenţei este o temă comună în propaganda legată de terorism. Acesta este unul dintre motivele principale care explică de ce un mesaj distribuit prin Internet, care se referă la terorism, creşte exponenţial audienţa, publicul fiind afectat emoţional. Propaganda pe Internet poate include conţinut, cum ar fi înregistrări video ale unor acte de terorism violente sau simulări ale acestora, încurajând utilizatorul să se angajeze prin joc virtual pentru a acţiona ca un terorist.

Promovarea retoricii extremiste, care încurajează actele violente, este o altă tendinţă comună, identificată în cadrul platformelor informatice care găzduiesc conţinut extremist pe Internet. Este evident că acest conţinut poate fi distribuit ulterior publicului şi personal, şi prin mijloace media fizice, aşa cum sunt CD-urile şi DVD-urile. Însă, de bază rămâne Internetul, spaţiul

care oferă o gamă largă de instrumente constând în site-uri web dedicate, camere de video-chat şi forumuri de discuţii, reviste on-line, platforme de socializare în reţea, aşa cum sunt Twitter şi Facebook, site-uri video populare şi de partajare a fişierelor media, de tipul YouTube, Rapidshare etc.

Propaganda teroristă are ca principale obiective recrutarea de simpatizanţi, radicalizarea şi incitarea la violenţă. Mesajele difuzate vor căuta să transmită factori incitanţi de mândrie, de realizare şi de dedicare scopurilor extremiste. Acestea pot fi utilizate pentru a demonstra eficienţa atacurilor teroriste, angajamentul şi corectitudinea faţă de cei care au oferit sprijinul financiar.

Alte obiective ale propagandei teroriste pot include folosirea manipulării psihologice, în scopul subminării credinţei unui anumit individ în valorile sale sociale sau promovării sentimentelor de anxietate, frică sau panică în rândul populaţiei sau al unui segment al acesteia. Aceasta se poate realiza prin diseminarea dezinformării, prin zvonuri, prin ameninţări cu violenţă sau prin imagini legate de acte de violenţă. Audienţa vizată poate include spectatori direcţi şi/sau public afectat de publicitatea potenţială, generată de astfel de materiale.

Internetul este locul idel pentru stabilirea de conexiuni şi pentru relaţionarea cu cei interesaţi, tinerii reprezentând victimele ideale, adesea, prinşi în mrejele teribilismului, ale reacţiunii faţă de ce e perimat şi haterismului. Mai mult decât atât, pe baza abilităţile lor de utilizare a Internetului, tinerii pot dezvolta o publicitate implicită prin redifuzarea conţinutului online, prin discuţii şi mesaje în care îşi comunică părerile faţă de administratorii site-ului sau/şi cu ceilalţi membri. Grupurile teroriste au recunoscut „puterea” acestui instrument şi au început să-l folosească cu abilitate. Astfel, acestea difuzează pe aceleaşi platforme mesaje şi programe de îndoctrinare a tineretului cu mesaje radicale.

Deşi nu se poate măsura amploarea succesului acţiunii lor, se recunoaşte că Internetul riscă să devină un instrument performant de recrutare şi de radicalizare. Pentru aceasta, Daesh prezintă diverse aspecte care ţin de oportunităţile profesionale, de viaţa de familie sau de apartenenţa la o comunitate. Această metodă nu vizează doar tinerii sau persoanele deja intrate în procesul de recrutare, ci pe oricine intră în contact cu produsele lor propagandistice, fie printr-un link redirecţionat, fie prin notificări de tip ”push”. Mesajele utilizate nu sunt simple naraţiuni, ci ele sunt atent fabricate pentru a realiza o influenţare psihologică cu efecte graduale. Modalitatea în care acestea vor fi recepţionate este influenţată de mai mulţi factori, dintre care enumerăm: educaţie, vârstă, ocupaţie, mediu relaţional, modalitate de abordare etc.

Radicalizarea unei persoane depinde de contextul familial, emoţional, politic, financiar etc. al individului la acel moment. Nizar Trabelsi, acuzat că a amplasat o bombă într-o unitate militară din Belgia, în numele Al-Qaeda, pe timpul interogatoriului din cadrul anchetei penale a afirmat că elementul iniţial care l-a determinat să adere la cauza teroristă a fost prezentarea de către recrutori a unei fotografii cu o fetiţă ucisă în Fâşia Gaza, în anul 2001[13].

Instruire asistată prin sisteme informatice

Observăm că organizaţiile teroriste utilizează Internetul și pentru diseminarea informaţiilor. Dintre produsele lor, enumerăm o serie de ghiduri practice, sub formă de manuale online, clipuri audio şi video, informaţii şi alte sfaturi pe platforme online, toate asigurând o platformă de instruire asistată prin calculator. Mai mult decât atât, aceste platforme cibernetice pun la dispoziţie instrucţiuni detaliate, într-o formă extrem de facilă, mai mult intuitivă (adesea, în format multimedia, în limbi de circulaţie preponderent locală, dar şi internaţională), pe teme diverse, precum: particularităţile construirii unui dispozitiv exploziv improvizat; modalităţi ale uzului armelor de foc, armelor albe sau altor arme improvizate; modalităţile de combinare a unor substanţe, în mod curent, nepericuloase şi transformarea lor în otrăvuri sau în alte elemente periculoase; particularirăţile planificării şi organizării atacurilor teroriste etc.

Prin urmare, platformele de instruire cibernetică, astfel constituite, pot fi considerate tabere virtuale de instruire, urmând ca antrenarea fizică să se execute în mod individual, cu sau fără asistenţă de specialitate. De asemenea, aceste platforme pot fi folosite pentru discuţii sau pentru distribuirea observaţiilor identificate în cadrul experimentelor, pentru comunicarea lecţiilor învăţate despre metodele, tehnicile sau cunoştinţele operaţionale specifice executării de acţiuni teroriste.

De exemplu, revista online *Inspire*, despre care se presupune că este publicată de Al-Qaeda, are ca obiectiv iniţial declarat instruirea musulmanilor pentru jihad. Acestă publicaţie conţine o cantitate mare de materiale ideologice, destinate încurajării terorismului, inclusiv declaraţii atribuite lui Osama Bin Laden, Sheikh Ayman al-Zawahiri, altor persoane reprezentative ale organizației Al-Qaeda.

Elementele de instruire, disponibile online, includ, printre altele, instrumente necesare activităţilor contrainformative, activităților de protecție și celor de hacking, instrumente pentru îmbunătăţirea securităţii legăturilor de comunicaţii şi a altor activităţi de menținere a legăturii online, instrumente de selectare, de propunere a unor metode de criptare şi tehnici de ascundere a identității. Se pare că natura interactivă a platformelor digitale în spațiul cibernetic ajută la consolidarea acelor sentimente de comuniune dintre indivizii aflați în diverse locaţii şi dispuneri geografice, încurajând, astfel, crearea de reţele de schimb de materiale instructive şi tactice. Mai mult decât atât, Internetul poate fi folosit nu numai ca mijloc de a publica retorica extremistă și videoclipuri, ci și ca o modalitate de dezvoltare a relațiilor, o modalitate de a solicita sprijinul celor responsabili cu propaganda orientată etc.

Demn de remarcat în ceea ce privește pericolul radicalizării prin Internet este că spațiul cibernetic poate constitui un mediu eficient de recrutare și de instruire a minorilor, cunoscut fiind faptul că această categorie este semnificativă pentru o mare parte a utilizatorilor. Propaganda făcută în scopul recrutării minorilor poate lua forma unor desene animate, a unor videoclipuri muzicale populare sau a unor jocuri pe suport informatic. De regulă, produsele propagandistice, difuzate pe site-urile web aflate sub controlul teroriștilor sau afiliaţilor acestora, au ca scop vizionarea lor de către minori. De aceea ele includ un melanj de desene animate şi de povestioare cu mesaje care promovează şi glorifică diverse acte de terorism, așa cum este martiriul și atacurile suicidare.

Alte structuri teroriste creează și promovează jocuri digitale. Caracterul lor online le transformă în reale instrumente de recrutare şi de instruire. Astfel de jocuri pot promova violenţa de orice fel, îndreptată împotriva unui stat sau unui individ marcant pentru un partid politic, pot stabili scale de valori și alte recompense pentru „succesul” parcurgerii etapelor virtuale, putând fi oferite unui public tot mai larg, adesea fiind traduse în mai multe limbi de circulație pentru spațiul geografic de interes.

Pe baza celor prezentate, putem observa că și atacul lui Brenton Tarrant ar putea fi încadat ca făcând parte dintr-o etapă de instruire online. Imaginile video, difuzate simultan în rețeaua Facebook, *atenție*, imagini produse și postate în direct de atacator printr-o cameră video, aflată în permanență deschisă, îl arăta cum, la data de 08.03.2019, conducea o mașină spre o moschee, cum intra în clădire și cum deschidea focul asupra celor aflați înăuntru, în mod nediscriminatoriu. Ulterior, îl prezenta cum îi executa pe cei răniți căzuți în stradă, cum își schimba arma, cum trăgea asupra curioșilor de pe stradă, mascat fiind de parbrizul mașinii și de faptul că nu a deschis geamul acesteia în timpul mersului.

Este clar că evenimentul a fost un atac terorist, fiind susținut și de „manifestul”, publicat pe Internet, în care îi denunța pe imigranți ca invadatori. Legat de Internet, Facebook, Twitter și Google au permis susținerea a numeroase discuții și difuzarea de materiale cu conținut extremist în cadrul platformelor lor, ca urmare a distribuirii imaginilor video și a filmelor rezultate din acest eveniment. *Daily Mail*, citându-l pe Clement Thibault, analist la platforma globală a piețelor financiare Investing.com, remarca că „streaming-ul live al filmărilor din Noua Zeelandă va aduce cu siguranță mai multe întrebări privind regulile și controlul asupra Facebook. Aceasta a oferit o platformă pentru atacul oribil de astăzi și, fără îndoială, va fi pusă sub semnul întrebării pentru facilitarea răspândirii acestui eveniment”[14].

Concluzii

După cum se observă, terorismul cibernetic trebuie considerat ca o etapă a evoluţiei infracţiunilor cibernetice, adaptată scopurilor teroriste. Este evident că resursele oferite de spaţiul cibernetic şi mecanismele de comitere a acţiunilor informatice se întrepătrund, ele fiind exploatate la maximum de către cei proveniţi atât din zona criminalităţii informatice, cât şi din zona terorismului.

Din punctul de vedere al dezvoltării terorismului cibernetic, apreciez că pot fi identificate trei scenarii de bază, ale căror diferenţe provin din raporturi diferite de cauzalitate. Nu exclud

posibilitatea existenţei şi altor scenarii, pe care le consider derivate sau soluţii adoptate, în funcţie de resursele avute la dispoziţie şi de instruirea în domeniu.

Cele trei scenarii de dezvoltare a terorismului cibernetic sunt:

Scenariul 1 – instruirea unor teroriști tradiționali în hacktivism;

Scenariul 2 – angajarea unor hackeri pentru organizarea și executarea unor atacuri teroriste cu sprijin informatic și informațional, dat de Internet, atacuri similare modelului „mercenarilor cibernetici”;

Scenariul 3 – hackeri simpatizanţi, care împărtăşesc ideologiile organizaţiei teroriste şi, ulterior, devin membri activi ai acesteia.

Principalele metode utilizate în sfera criminalităţii informatice și care ar putea fi exploatate în scopul desfăşurării unui atac terorist sunt: atacurile prin parolă; atacuri prin accesarea reţelei şi interceptarea pachetelor de date; atacuri care exploatează accesul liber (trusted access); atacuri prin IP (IP spoofing); atacuri prin inginerie socială; atacuri cu predicţia numărului secvenţei; atacuri cu deturnarea sesiunii; atacuri care exploatează slăbiciunile tehnologiei; atacuri care exploatează bibliotecile partajate etc. Toate aceste metode pot configura un scop infracţional, din care să se aprecieze motivaţia pentru care ele au fost lansate.

Concluzionez că nu este nicio diferenţă între cunoştinţele necesare şi setul de instrumente folosite de către hackeri şi teroriști cibernetici, efectele finalizării atacului şi motivaţia lui fiind singurele elementele care le diferenţiază. Sinergia măsurilor terorismului convenţional şi ale războiului informaţional se constituie într-un element foarte periculos şi, totodată, avantajos pentru teroriști, deoarece acesta combină scopurile letale cu obiectivul major de generare de frică.

Pentru teroriştii cibernetici, adoptarea acestor măsuri informaţionale permite o acţiune liberă în diverse spaţii geografice, cu încălcarea graniţelor convenţionale fizice ale statelor contemporane. În acelaşi timp, teroriştii tradiţionali pot folosi războiul informaţional pentru a limita costul unui atac de acest tip, în comparaţie cu cel al unui atac convenţional.

De asemenea, războiul informaţional furnizează anonimatul atacatorului și obţine un efect sporit propagării schizofreniei în cadrul ţintei, fără limitarea capacităţilor teroriste de a spori efortul pe timpul atacului. Astfel, raportul „cost scăzut/efecte sporite” este de departe mult mai atractiv pentru teroriştii care utilizează războiul informaţional, faţă de cei care se opun acestui fapt.

Trebuie acceptat că terorismul cibernetic este o realitate care a depășit de mult domeniul strict limitat al propagandei pe Internet. Însă, prin sintagma că întărirea terorismului tradiţional se va realiza prin alegerea și dezvoltarea tehnicilor și metodelor specifice războiului informaţional, nu trebuie să înţelegem că au apărut noi tipuri de teroriști.

Terorismul cibernetic nu este război informaţional și nici un cumul de infracțiuni cibernetice. Este ceva nou, extrem de versatil, care se confundă cu alte forme sociocibernetice și care are un mare potențial de dezvoltare. Cum se va adapta cerințelor tradiționale ale terorismului clasic rămâne doar o opțiune a managementului organizației teroriste respective. Vom vedea...

NOTE:

1 Manuel R. Torres Soriano, ”Guerras por delegación en el ciberespacio – Proxy wars in cyberspace”, *IEEE* – Revista institutului spaniol de studii strategice –, nr. 9, 2017.

2 Gabriel Weimann, ”Special Report”, United States Institute of Peace, martie 2004, https://www.usip.org/sites/default/files/sr116.pdf, accesat la 14.09.2018.

3 Apud. Jimmy Gurule, în Dru Stevenson, ”Effect of the national security paradigm on criminal law”, https://law.stanford.edu/wp-content/uploads/2018/03/stevenson.pdf, accesat la 16.10.2018.

4 Michael N. Schmitt (general editor), Liis Vihul (managing editor), *Tallinn Manual 2.0 On the International Law Applicable to Cyber Operations*, University Press, Cambridge, 2017, p. 168.

5 *Ibidem*, p. 345.

6 https://legeaz.net/noul-cod-penal/art-249, accesat la 15.02.2019.

7 Uptin Saiidi, ”Inside Interpol’s Singapore cybercrime-fighting complex”, https://www.cnbc.com/2017/05/17/inside-interpols-singapore-cybercrime-fighting-complex.html, accesat la 16.02.2019.

8 *** *G7 Ministers call for sharing of battlefield data on terrorists via INTERPOL*, https://www.interpol.int/News-and-media/News/2017/N2017-144, accesat la 16.02.2019.

9 Liam Tung, ”Australia helps EU in latest crack down on money mules”, https://www.cso.com.au/article/630544/australia-helps-eu-latest-crack-down-money-mules/, accesat la 12.01.2019.

10 Timothy L. Quintero, ”The Connected Black Market: How the Dark Web Has Empowered LatAm Organized Crime”, https://www.insightcrime.org/news/analysis/connected-black-market-how-dark-web-empowered-latam-organized-crime/, accesat la 12.01.2019.

11 *** *Threat Lens 2018 Annual Forecast*, https://worldview.stratfor.com/article/threat-lens-2018-annual-forecast-excerpt, accesat la 12.01.2019.

12 Michael Jacobson, ”Terrorist Financing and the Internet”, *Studies in Conflict & Terrorism*, https://www.tandfonline.com/doi/pdf/10.1080/10576101003587184, accesat la 10.11.2018.

13 Melodie Bouchaud, ”Belgium Condemned Over Unlawful Extradition of Terrorist to the US”, https://news.vice.com/en_us/article/3kegx3/belgium-condemned-over-unlawful-extradition-of-terrorist-to-the-us, accesat la 03.11.2018.

14 https://www.dailymail.co.uk/news/article-6814269/Facebook-shares-drop-execs-quit-Christchurch-live-stream-shooting-stirs-outrage.html, accesat la 15.04.2019.

BIBLIOGRAFIE

*** „Anders Breivik, autorul atacurilor din Norvegia, ar putea primi «impresionanta» pedeapsă de 30 de ani de închisoare!”, http://www.ghimpele.ro

*** ”Cyber-attack: US and UK blame North Korea for WannaCry”, https://www.bbc.com

*** *Decret nr. 212, din 31 octombrie 1974, pentru ratificarea Pactului internațional cu privire la drepturile economice, sociale și culturale și Pactului internațional cu privire la drepturile civile și politice*, publicat în B.Of. nr. 146/20 1974, http://www.cdep.ro

*** „Efectul Breivik: Circa o sută de norvegieni vor să devină «teroriști solitari», http://www.financiarul.ro

*** ”Facebook shares drop execs quit Christchurch live stream shooting stirs outrage”, https://www.dailymail.co.uk

*** ”G7 Ministers call for sharing of battlefield data on terrorists via INTERPOL”, https://www.interpol.int

*** ”Hacked: The Bangladesh Bank Heist”, https://www.aljazeera.com

*** *Noul cod penal*, https://legeaz.net

*** *Threat Lens 2018 Annual Forecast*, https://worldview.stratfor.com

Bălan George, „Noua concepţie internaţională de acţiune doctrinară şi practică în combaterea terorismului”, http://fs.legaladviser.ro

Bouchaud Melodie, ”Belgium Condemned Over Unlawful Extradition of Terrorist to the US”, https://news.vice.com

Bumiller Elisabeth, Thom Shanker, ”Panetta Warns of Dire Threat of Cyberattack on US”, https://www.nytimes.com

Fedotov Yury, ”Taking action where we can to stop cybercrime”, https://www.unodc.org

Flynn Matthew J., *Is There a Cyber War?*, Excelsior College, National Cybersecurity Institute Journal, vol. 1, Issue 2, 2014.

Jacobson Michael, ”Terrorist Financing and the Internet”, *Studies in Conflict & Terrorism*, https://www.tandfonline.com

Jurj-Tudoran Remus, „Instigarea publică la săvârșirea unei infracțiuni de terorism și libertatea de exprimare în practica Curții Europene a Drepturilor Omului”, http://revistaprolege.ro

Quintero Timothy L., ”The Connected Black Market: How the Dark Web Has Empowered LatAm Organized Crime”, https://www.insightcrime.org

Saiidi Uptin, ”Inside Interpol’s Singapore cybercrime – fighting complex”, https://www.cnbc.com

Schmitt Michael N. (general editor), Liis Vihul (managing editor), *Tallinn Manual 2.0,* On the International Law Applicable to Cyber Operations, Cambridge, University Press, 2017.

Soriano Manuel R. Torres, ”Guerras por delegación en el ciberespacio – Proxy wars in cyberspace”, *IEEE* – Revista institutului spaniol de studii strategice –, nr. 9, 2017.

Stevenson Dru, ”Effect of the national security paradigm on criminal law”, https://law.stanford.edu

Tanasă Remus, „Benedict Anderson şi destinul «Comunităţilor imaginate»”, https://www.lapunkt.ro

Tung Liam, ”Australia helps EU in latest crack down on money mules”, https://www.cso.com.au

Weimann Gabriel, ”How modern terrorism uses the Internet, United States Institute of Peace”, https://www.usip.org