BULETINUL
UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I"
https://buletinul.unap.ro

Implicații ale terorismului jihadist în spațiul cibernetic

Implications of the jihadist terrorism in cyberspace

Drd. Bianca BRANDEA*
*Universitatea din București, Facultatea de Limbi și Literaturi Străine
Școala Doctorală „Limbi și identități culturale", România

Abstract

Atacul terorist din 11 septembrie 2001 a marcat schimbarea percepției Occidentului asupra Orientului Mijlociu și viceversa. Urmat de prezența militară a SUA în Orientul Mijlociu, acest eveniment a contribuit la dezvoltarea mijloacelor de acțiune teroristă din întreaga lume și la popularizarea jihadului. Atitudinea ostilă a Occidentului astfel succedată a întreținut starea de tensiune dintre cele două spații. De-a lungul timpului, grupărilor jihadiste și teroriste li s-au alăturat membri originari din Occident, care au fost convinși de importanța „misiunilor" pe care și le-au asumat ulterior. În prezenta lucrare, ne vom concentra asupra transpunerii și continuării ostilităților în spațiul geografic și cibernetic, ținând cont inclusiv de conflictul israeliano-palestinian actual.

The terrorist attack on the 11th of September, 2001, marked the change in the West's perception of the Middle East and vice versa. Followed by the US military presence in the Middle East, this event contributed to the development of the means of terrorist actions around the world and the popularization of jihad. The hostile attitude of the West thus succeeded in maintaining the state of tension between the two spaces. Over time, jihadist and terrorist groups have been joined by members originating from the West who were convinced by the importance of the "missions" they later undertook. In the present paper, we will focus on the transposition and continuation of hostilities in both geographic and cyber spaces, with reference even to the current Israeli-Palestinian conflict.

Cuvinte-cheie:
terorism; jihad; securitate; conflict; hacktivism; propagandă; apărare; terorism cibernetic.

Keywords:
terrorism; jihad; security; conflict; hacktivism; propaganda; defense; cyberterrorism.

Info articol
Primit: 12 februarie 2024; Evaluat: 28 februarie 2024; Acceptat: 13 martie 2024; Disponibil online: 5 aprilie 2024
Citare: Brandea, B. 2024. „Implicații ale terorismului jihadist în spațiul cibernetic".
Buletinul Universității Naționale de Apărare „Carol I", 13(1): 78-86. https://doi.org/10.53477/2065-8281-24-05

Începutul secolului XXI a adus schimbări majore în percepția Occidentului asupra Orientului Mijlociu, fapt ce a contribuit la delimitarea, respectiv segregarea celor două spații. Progresul tehnologic occidental perpetuu se desfășoară în același timp cu evoluția mentalităților și măsurilor orientale de ostilitate față de supremația Occidentului. În prezenta lucrare, vom analiza situații în care interferența celor două spații a fost necesară pentru îndeplinirea unor acțiuni ofensive și combative, de la mediul fizic până la mediul virtual.

Conflictele armate internaționale din ultimul deceniu – cu precădere cele desfășurate în Europa de Est și Orientul Mijlociu[1] – au consolidat rivalitatea dintre SUA și Rusia și au repornit negocierile pozițiilor aliaților fiecăreia. Conflictul Israelului împotriva Palestinei este cel mai important pe care îl vom avea în vedere în cele ce urmează, fapt pentru care vom observa câteva dintre cele mai importante implicații ale acestuia de-a lungul istoriei.

[1] Zona la care ne vom referi în prezenta lucrare este denumită de istorici drept Orientul Apropiat, fiind inclusă în aria amplă a Orientului Mijlociu.

Cu prilejul tensiunilor militare internaționale, în general, fenomenul radicalizării devine din ce în ce mai frecvent în rândul civililor interesați să susțină în mod activ cauza în care cred. Accesul neîngrădit la internet facilitează circulația materialelor menite să atragă noi adepți care fie împărtășesc deja convingerile promovate, fie devin interesați sau atrași de ele. În cazul radicalizării atacatorilor din spațiul cibernetic, propaganda la care sunt expuși are scopul de a forma „trupe" invizibile pentru a contribui la ostilitățile dintr-un „front", la rândul său, invizibil. Este de menționat faptul că astfel de „trupe" nu sunt create doar prin intermediul propagandei accesibile pe internet, ci includ membri care au concepții extremiste provenite din alte surse, în special de natură politică.

Mediul cibernetic este expus în mod constant amenințărilor atât psihologice, cât și cu repercusiuni în mediul fizic. Așadar, în contextul conflictelor armate actuale din proximitatea României, UE și NATO, gradul ridicat de alertă în spațiul cibernetic este necesar pentru a încerca preîntâmpinarea și contracararea amenințărilor, atacurilor de diverse tipuri, propagandei și dezinformării, ținând cont de faptul că astfel de evenimente au avut deja loc, sub pretextul contestării poziției României.

Jihad cibernetic sau terorism cibernetic?

Propaganda jihadistă răspândită în mediul online de către organizații teroriste precum Al-Qaida sau ISIS reprezintă un mod de intimidare a occidentalilor, dar și de recrutare a musulmanilor din ambele spații, respectiv încurajarea nonmusulmanilor de a se converti la islam pentru a se alătura jihadului. Este important de precizat faptul că, într-un asemenea context, islamul este folosit drept instrument de manipulare și radicalizare, încurajându-se valori care

nu se regăsesc în islamul autentic sau care chiar i se opun, promovându-se astfel o imagine incompletă și incorectă a religiei (Toma 2013, 72).

În cazul anumitor jihadiști, radicalizarea a însemnat adoptarea unui nou mod de viață, în care sunt urmărite scopuri precum înființarea unui nou califat, uciderea celor care nu urmează regulile și valorile pe care ei le consideră ca fiind ale islamului, distrugerea sau remodelarea Occidentului și în special a marilor puteri etc. (Leiken 2012, 142-144). Cu toate că grupările jihadiste sunt divizate în funcție de scopuri și ideologii, susținerea cauzei palestiniene reprezintă un ideal comun. De exemplu, abordarea online a grupării Al-Qaida nu este concentrată doar asupra ofensării Israelului, ci presupune și incriminarea statelor arabe care susțin perspectivele Occidentului în conflictul din Palestina. În plus, din analizele efectuate de Europol asupra propagandei online a grupării Al-Qaida în anul 2021, reieșea că aceasta susține că jihadul implică angajarea fiecărui musulman în susținerea cauzei palestiniene, încurajând, totodată, atacurile împotriva Israelului, „cruciaților" și țărilor arabe „zioniste" (Europol 2022, 39). Întreținând astfel de convingeri, informațiile publicate de ISIS sunt menite să convingă audiența că jihadiștii sunt, de fapt, musulmanii reali (Frampton, Fisher și Prucha 2017, 24).

În alt studiu, publicat de Europol, în anul 2017, jihadul cibernetic este descris drept „exploatarea globalizată a internetului de către Statul Islamic, care se identifică drept Califatul Cibernetic, prin intermediul discursului specific având scopul de a atrage hackeri din întreaga lume pentru a se implica în războiul din media împotriva «cruciaților» și a se alătura Califatului Cibernetic Unit" (Antinori 2017, 6).
Acestea sunt doar câteva dintre conceptele care stau la baza amenințărilor în plan real, însă în cele ce urmează, ne vom concentra asupra situației din „frontul" cibernetic și asupra motivațiilor comune, identificate în ambele planuri.

Este notabil faptul că jihadul și terorismul sunt două concepte distincte. Potrivit *Dicționarului de securitate internațională*, jihadul, deși tradus adesea ca „război sfânt", este descris ca punct central al islamului, semnificând luptă, străduanie sau efort. Jihadul poate avea caracter ofensiv cu scopul de răspândire a islamului, sau defensiv, în situațiile în care islamul este atacat (Robinson 2010, 119). În ceea ce privește terorismul, acestuia nu i s-a atribuit o definiție precisă, fiind descris ca un fenomen care „constă în utilizarea ilegală a forței de către actorii nonstatali cu scopul de a crea teroare în rândul populațiilor civile și de a forța guvernele la concesii politice. Folosirea violenței ilegale este ceea ce deosebește terorismul de activitatea politică normală, de violența legală/judiciară și de războiul convențional" (Robinson 2010, 227).

Cât despre diferențierea dintre jihad cibernetic și terorism cibernetic, este de precizat faptul că informațiile difuzate în numele unei organizații teroriste sau al unui jihadist care acționează singur se încadrează în jihadul cibernetic. În schimb, terorismul cibernetic are ca scop desfășurarea atacurilor cu scopul de a contribui la conflicte economice, politice și psihologice (Babanoury 2014), și, în sens strict, la folosirea spațiului cibernetic drept instrument pentru a vătăma fizic indivizi și obiecte (Torres 2016, 109).

Așadar, plasând cele două concepte în domeniul securității cibernetice, observăm că propaganda jihadistă utilizează pretextul religios pentru a atrage adepți, islamul fiind, de fapt, aparența acțiunilor politice intenționate, în timp ce terorismul reprezintă starea tensionată și atacurile motivate de pretexte similare.

Terorismul în pas cu progresul cibernetic

În studiul său asupra fenomenului radicalizării celei de-a doua generații de imigranți asiatici și africani în Europa, Robert S. Leiken menționează atracția tinerilor extremiști față de identitatea aleasă, în detrimentul celei moștenite. O astfel de identitate este conturată ca urmare a eșecului integrării atât în rândul nativilor europeni, cât și a neidentificării cu familia extinsă și comunitatea originară a părinților imigranți. În consecință, discursul justificativ, oferit de grupările teroriste, împreună cu sentimentul de apartenență la o comunitate unită reprezintă contextul ideal de canalizare a furiei simțite de-a lungul vieții (Leiken 2012, 410).

Diverși specialiști argumentează că terorismul, asociat extremismului islamist, nu este suficient de dezvoltat din punct de vedere tehnologic pentru a reprezenta o amenințare majoră. Hunker (2010) remarcă faptul că atacurile cibernetice perturbatoare, provocate de teroriști, sunt probabile și posibile, având mai degrabă rolul de a provoca enervarea maselor, cibernetica în sine nefiind o armă a terorii (Hunker 2010, 12). Torres (2016) susține că jihadiștii nu au pregătirea tehnică necesară unui război cibernetic, tendința acestora fiind mai degrabă către propagandă și *hacktivism* (Torres 2016, 108-9).

Interesul față de progresul tehnologic continuu și expunerea la rețelele de socializare, unde pot circula materiale propagandiste și știri de interes, alături de principiul expus de Leiken (2012), pot constitui un factor de risc la adresa securității generale și cibernetice, inclusiv a României. Potrivit Strategiei Naționale de Apărare a Țării pentru perioada 2020-2024, în rândul riscurilor enumerate se încadrează și „intensificarea propagandei islamist-jihadiste globale care alimentează riscurile radicalizării pe teritoriul național, inclusiv în rândul cetățenilor români, conferind perspective dificil de anticipat și contracarat" (Administrația Prezidențială, 27).

În general, atenția organizațiilor teroriste islamiste este îndreptată, cu precădere, spre statele care sprijină SUA în acțiunile desfășurate în Orientul Mijlociu. Din acest punct de vedere, România ar putea constitui o țintă „legitimă", fapt motivat și de implicarea permanentă a României în consiliile și comitetele internaționale de securitate (Andreescu și Radu 2015, 273). „Expusă indirect, prin asociere cu NATO, UE, SUA și statele europene implicate articulat în combaterea flagelului, țara noastră rămâne o țintă de oportunitate" (Administrația Prezidențială, 25).
România a fost deja ținta atacurilor de tip DDoS, revendicate de gruparea prorusă de hackeri Killnet și prilejuite de sprijinul militar și social, acordat Ucrainei, ca urmare

a războiului început de Rusia (Oancea 2022). Pentru asemenea atacuri efectuate de hacktiviști, sunt în continuare eligibile statele care susțin Ucraina, cel puțin până la finalul conflictului militar (SRI 2022).

Hackingul și *hacktivismul*: armele voluntarilor în timpul conflictelor armate

Între *hacktivism* și terorism cibernetic, există atât asemănări, cât, în special, deosebiri. *Hacktivismul* presupune un nivel scăzut de perturbare a funcționalității țintelor, obiectivele principale fiind umilirea acestora și câștigarea vizibilității. În ceea ce privește terorismul cibernetic, autorii urmăresc să rămână nedepistați, iar scopurile principale sunt de a submina securitatea instituțională și încrederea publică prin atacarea infrastructurilor critice și a serviciilor de urgență. Caracteristicile comune ale celor două concepte sunt răspândirea propagandei, intențiile de recrutare și strângerea de fonduri, respectiv instrumente și tehnici similare de atac. În cazurile în care *hacktiviștii* și teroriștii cibernetici au viziuni opuse, nu este exclus ca, între cele două tipuri de grupări, să existe atacuri cibernetice (Baldi, Gelbstein și Kurbalija 2003, 18-19).

Implicarea grupării Killnet în conflictul dintre Palestina și Israel nu reprezintă cu certitudine intenția de a susține Palestina sau gruparea Hamas, fiind mai degrabă o oportunitate de a lansa atacuri cibernetice împotriva Israelului. Acțiunile acesteia beneficiază de interesul altor grupări cu interese similare din lume, așa după cum reiese din cooperarea cu Anonymous Sudan în campania împotriva „regimului Israel" (Hollingworth 2023). Deși nu există dovezi concrete ale apartenenței membrilor grupărilor sus-numite la organizații teroriste sau jihadiste, putem identifica două elemente importante care fac parte din tiparul amenințărilor teroriste.

Primul element este redat de alegerea țintelor de nivel înalt. Comiterea cu succes a unor atacuri asupra unui guvern simbolizează interacțiunea dintre atacator și victimă. În acest mod, atacatorul are certitudinea transmiterii mesajelor ostile și a recunoașterii potențialului distructiv. Obținerea controlului asupra unui spațiu cibernetic guvernamental înseamnă, drept urmare, abilitatea de a deține controlul asupra securității întregului stat vizat.

Al doilea element este constituit din implicarea voluntară a străinilor în susținerea cauzelor și/sau realizarea atacurilor. Analog aderării nonarabilor și nonmusulmanilor la grupări jihadiste, observăm motivația grupărilor proruse și sudaneze de a contribui la vătămarea spațiului cibernetic guvernamental israelian.

Pe de altă parte, radicalizarea reprezintă un principiu cheie în comportamentul și mentalitatea jihadiștilor și teroriștilor. În ceea ce privește *hacktiviștii*, radicalizarea nu este neapărat un element definitoriu, ținând cont de faptul că majoritatea atacurilor importante sunt înfăptuite în perioade de tensiuni politice. În schimb, caracterul

extremist este mai degrabă comun atât *hacktiviștilor*, cât și jihadiștilor și hackerilor. În plus, imaginile civililor palestinieni răniți în timpul conflictului – în special ale copiilor – au contribuit, de-a lungul timpului, la creșterea numărului de jihadiști și la amplificarea dorinței acestora de a acționa împotriva Israelului, în mod special, dar și a statelor occidentale care îl susțin. În lucrarea *Ways of cyberterrorism* este menționat exemplul lui Nizar Trabelsi, un jihadist acuzat de amplasarea unei bombe într-o bază militară din Belgia, care a mărturisit că imaginile unei fete omorâte în Fâșia Gaza l-au încurajat să devină membru Al-Qaida în anul 2001 (Topor 2019, 87).

Pentru o mai bună claritate asupra tensiunilor internaționale actuale, este relevant să amintim câteva aspecte importante din istoria ultimelor decenii. În studiul său, publicat în anul 1990, privind tensiunile politice arabo-israeliene și Războiul Rece, Jerome Slater prezintă conflictul ca fiind prins în rivalitatea dintre SUA și Uniunea Sovietică, unde URSS și-ar fi urmat ideologia expansionistă asupra Orientului Mijlociu, eliminând influențele SUA și NATO din zonă și, în special, independența energetică a Occidentului, Japoniei și SUA (Slater 1990, 557-559). În plus, Slater amintește de susținerea activă, din partea URSS, pentru înființarea statului Israel, incluzând recunoașterea diplomatică declarată Israelului, în anul 1948, în cadrul Consiliului ONU; unii istorici motivează poziția URSS din respectiva perioadă prin intenția acesteia de a diminua influența britanică în Orientul Mijlociu (Slater 1990, 562).

La nivel formal, evoluția conflictului depinde în mare măsură de atitudinea „marilor puteri" și a „superputerii", respectiv de definirea celei din urmă. Conform studiului Alexandrei Sarcinschi, statutul de „superputere" ar putea fi atribuit Statelor Unite ale Americii, însă în ultimele decenii, este luat în considerare declinul puterii SUA, urmat de posibila atribuire a acestui rang unui alt stat. Cât despre „marile puteri" actuale, recunoscute internațional ca având acest statut sunt SUA, Marea Britanie, China, Franța, Rusia, Japonia și Germania (Sarcinschi 2010, 20-21). În contextul în care Israelul joacă rolul principal în conflictul declanșat în anul 1948 și intensificat în 2023, sunt relevante teoriile conform cărora Israelul intenționează să devină o superputere în Orientul Mijlociu (Khashan 2020), la nivel mondial (Kor 2021), în domeniul tehnologiei (Forbes 2015), respectiv al inteligenței artificiale în domeniul războiului (Williams 2023).

Pe „frontul" cibernetic, se conturează astfel două aspecte definitorii pentru perspectivele extremiștilor, alăturați fiecăreia dintre părțile oponente: partea aliată Israelului urmărește obținerea supremației cibernetice și, în special, informaționale, în timp ce partea aliată Palestinei se opune acestor acte, acționând mai degrabă în replică la ofensivele continue ale Israelului. În general, atacurile cibernetice de natură teroristă sunt catalogate drept atacuri perturbatoare, comise de actori statali și nonstatali, iar războiul cibernetic este considerat o formă specială de atac perturbator. Într-un război cibernetic, este inclusă atacarea perturbatoare a spațiului unui stat de către alt stat, fapt ce se poate încadra în rândul acțiunilor de utilizare a forței (Hunker 2010, 2-4).

Într-un articol referitor la perspectiva cibernetică a conflictului din Fâșia Gaza, publicat de compania singaporeză Cyfirma, securitatea cibernetică este deosebit de importantă nu numai pentru statele implicate, dar și pentru aliații lor. Această concluzie se bazează, cu precădere, pe desfășurarea atacurilor cibernetice de către grupuri de *hacktiviști* și pe amenințările din partea altor tipuri de actori din diverse regiuni care au țintit site-uri guvernamentale, sectoarele educațional și media, panouri publicitare, centrale electrice, sisteme de alertă și chiar informații militare sensibile. De asemenea, articolul menționează posibilitatea Iranului și a aliaților săi de a conduce acțiuni „preventive" în viitorul apropiat, ca urmare a atacurilor Israelului împotriva Palestinei (Cyfirma 2023).

Într-un alt articol al Cyfirma privind atacurile hackerilor și *hacktiviștilor* în contexte conflictuale ale relațiilor internaționale, este recomandată intervenția diplomatică a guvernelor cu scopul de a diminua tensiunile geopolitice. Într-o astfel de abordare, este prevăzută prevenirea activităților *hacktiviste* prin eliminarea motivațiilor pe care se bazează (Cyfirma 2024).

Concluzii

Conflictele internaționale în care sunt implicate Occidentul și Orientul Mijlociu atrag inclusiv interesul civililor din ambele zone, care, în acest scop, își pot desfășura acțiunile ofensive în mediul cibernetic. Conflictul dintre Palestina și Israel constituie un prilej pentru intensificarea propagandei de factură jihadistă și teroristă, căreia i se alătură adepți atât din spațiul occidental, cât și oriental.

Argumentele folosite pentru a justifica ura și eventuala poziție ofensivă împotriva Occidentului sunt, în prezent, sporite, ca urmare a susținerii oferite de Occident Israelului, fapt ce poate implica creșterea numărului amenințărilor de natură teroristă în mediul cibernetic și în afara lui. Dezacordul față de pozițiile adoptate de guvernele occidentale este exprimat inclusiv în rândul anumitor civili originari din Occident, care, motivați de empatie și cu convingerea că pot contribui la schimbarea peisajului politic internațional, aderă la o formă interpretată a religiei care oferă aparența concordanței cu ideologiile după care aceștia se ghidează. Astfel, o parte importantă a amenințărilor din contextele conflictuale sunt concretizate prin exploatarea factorului psihologic atât al atacatorilor, care au ocazia de a-și satisface nevoia de validare, cât și al țintelor în rândul cărora este instalată starea de teroare.

România este o posibilă țintă, din cauza apartenenței la UE și în tratate, precum NATO, însă tocmai această apartenență este crucială pentru menținerea și sporirea nivelului de securitate, precum și a cooperării în vederea îndeplinirii acestor scopuri. În concluzie, complementar implicării militare și logistice în zonele de conflict, reziliența și dimensiunea defensivă a mediului cibernetic al României rămân extrem de importante, indiferent de evoluția evenimentelor.

Referințe

Administrația Prezidențială. 2020. „Strategia Naţională de Apărare a Ţării pentru perioada 2020-2024.” https://www.presidency.ro/files/userfiles/Documente/Strategia_Nationala_de_Aparare_a_Tarii_2020_2024.pdf.

Andreescu, Anghel și Nicolae Radu. 2015. *Jihadul islamic. De la „înfrângerea terorii” și „războiul sfânt” la „speranța libertății”.* București: Editura RAO.

Antinori, Arije. 2017. *The "Jihadi Wolf" threat the evolution of terror narratives between the (cyber-)social ecosystem and self-radicalization "ego-system".* Haga: Europol Public Information.

Babanoury, Julien. 2014. "Cyber Jihad: The Internet's contribution to Jihad". https://incyber.org/en/cyber-jihad-the-internets-contribution-to-jihad-par-julien-babanoury-ceis/.

Baldi, Stefano, Gelbstein, Eduardo și Kurbalija, Jovan. 2003. *Hacktivism, cyber-terrorism and cyberwar. The activities of the uncivil society in cyberspace.* Msida: DiploFoundation.

Cyfirma. 2023. "Israel Gaza conflict: the cyber perspective". https://www.cyfirma.com/outofband/israel-gaza-conflict-the-cyber-perspective/.

—. 2024. "Caught in the Crossfire : How International Relationships Generate Cyber Threats". https://www.cyfirma.com/outofband/caught-in-the-crossfire-how-international-relationships-generate-cyber-threats/.

Cyware. 2019. "Flame 2.0 spyware found using strong encryption algorithm to avoid detection". https://cyware.com/news/flame-20-spyware-found-using-strong-encryption-algorithm-to-avoid-detection-36939d76.

Europol. 2022. *Online Jihadist Propaganda 2021 in review.* Luxemburg: Publications Office of the European Union.

Forbes, Steve. 2015. "How The Small State Of Israel Is Becoming A High-Tech Superpower". https://www.forbes.com/sites/steveforbes/2015/07/22/how-the-small-state-of-israel-is-becoming-a-high-tech-superpower/.

Frampton, Martyn, Ali Fisher și Nico Prucha. 2017. *The New Netwar: Countering Extremism Online.* Londra: Policy Exchange.

Hollingworth, David. 2023. "Killnet and Anonymous Sudan join forces to target Israel in widespread hacking campaign". https://www.cyberdaily.au/security/9652-killnet-and-anonymous-sudan-join-forces-to-target-israel-in-widespread-hacking-campaign.

Hunker, Jeffrey. 2010. *Cyber war and cyber power: Issues for NATO doctrine.* Roma: NATO Defense College.

Khashan, Hilal. 2020. "Israel Becomes the Middle East's Superpower". https://geopoliticalfutures.com/israel-becomes-the-middle-easts-superpower/.

Kor, Moira. 2021. "I'm going to turn Israel into a world superpower". https://www.jns.org/im-going-to-turn-israel-into-a-world-superpower/.

Leiken, Robert S. 2012. *Islamiștii europeni. Revolta tinerei generații.* Traducere de Sorin Șerb. București: Corint Books.

Oancea, Dorin. 2022. „Grupul de hackeri pro-rus Killnet a revendicat atacul cibernetic ce a afectat mai multe site-uri ale instituţiilor din România". https://www.mediafax.ro/externe/grupul-de-hackeri-pro-rus-killnet-a-revendicat-atacul-cibernetic-ce-a-afectat-mai-multe-site-uri-ale-institutiilor-din-romania-20782645.

Robinson, Paul. 2010. *Dicționar de securitate internațională.* Traducere de Monica Neamț. Cluj-Napoca: CA Publishing.

Sarcinschi, Alexandra. 2010. *Rolul actorilor statali în configurarea mediului internațional de securitate.* București: Editura Universității Naționale de Apărare „Carol I".

Slater, Jerome. 1990. "The Superpowers and an Arab-Israeli Political Settlement: The Cold War Years." *Political Science Quarterly* 105 (4): pp. 557-577.

SRI. 2022. "Buletin Cyberint." II Semester. https://sri.ro/assets/files/publicatii/buletin-cyber-sem-2-2022-RO.pdf.

Toma, Gabriel. 2013. *Terorismul internațional. Reacții ale actorilor regionali și globali.* Iași: Institutul European.

Topor, Sorin. 2019. "Ways of cyberterrorism." *Bulletin of "Carol" National Defence University* 8 (3): 82-90.

Torres, Manuel. 2016. *The limits of cyberterrorism*. Editor H. Giusto. *Daesh and the terrorist threat: from the Middle East to Europe* (Foundation for European Progressive Studies -Fondazione Italianieuropei) 108-114.

Williams, Dan. 2023. "Israel aims to be «AI superpower», advance autonomous warfare". https://www.reuters.com/world/middle-east/israel-aims-be-ai-superpower-advance-autonomous-warfare-2023-05-22/.