Coordonatori:

Darius-Antoniu Ferenț [Coordonatorul Grupului de Lucru pentru Securitate și Apărare Cibernetică al Asociației Ofițerilor în Rezervă din România, specialist în securitate cibernetică - End-user security, Formator, doctorand la Universitatea Babeș-Bolyai].

Lector univ. dr. Silviu-Valentin Petre [Colaborator extern al Grupului de Lucru pentru Securitate și Apărare Cibernetică, cadru didactic la Academia Națională de Informații „Mihai Viteazul" din București].

Alida-Monica-Doriana Barbu [Membru susținător al AORR și voluntară la Grupul de Lucru pentru Securitate și Apărare Cibernetică al AORR, absolventă a masteratului „Managementul crizelor și prevenirea conflictelor" din cadrul Universității Naționale de Apărare „Carol I" din București, doctorand la Universitatea Babeș-Bolyai].

Autori:

Colonel (r.) Elena Onu [Membru al AORR și membru al Grupului de Lucru pentru Securitate și Apărare Cibernetică]

Locotenent-colonel (r.) Ing. fiz. Nicolae Sfetcu [Membru al AORR și membru al Grupului de Lucru pentru Securitate și Apărare Cibernetică]

Alexia-Gabriela Szabo [Membru susținător al AORR și voluntară la Grupul de Lucru pentru Securitate și Apărare Cibernetică]

Andreea Pop [Membru susținător al AORR și voluntară la Grupul de Lucru pentru Securitate și Apărare Cibernetică]

Alexia Oprea [Membru susținător al AORR și voluntară la Grupul de Lucru pentru Securitate și Apărare Cibernetică]

Oana-Melisa Țolea [Membru susținător al AORR și voluntară la Grupul de Lucru pentru Securitate și Apărare Cibernetică].

ISBN 978-606-062-924-5

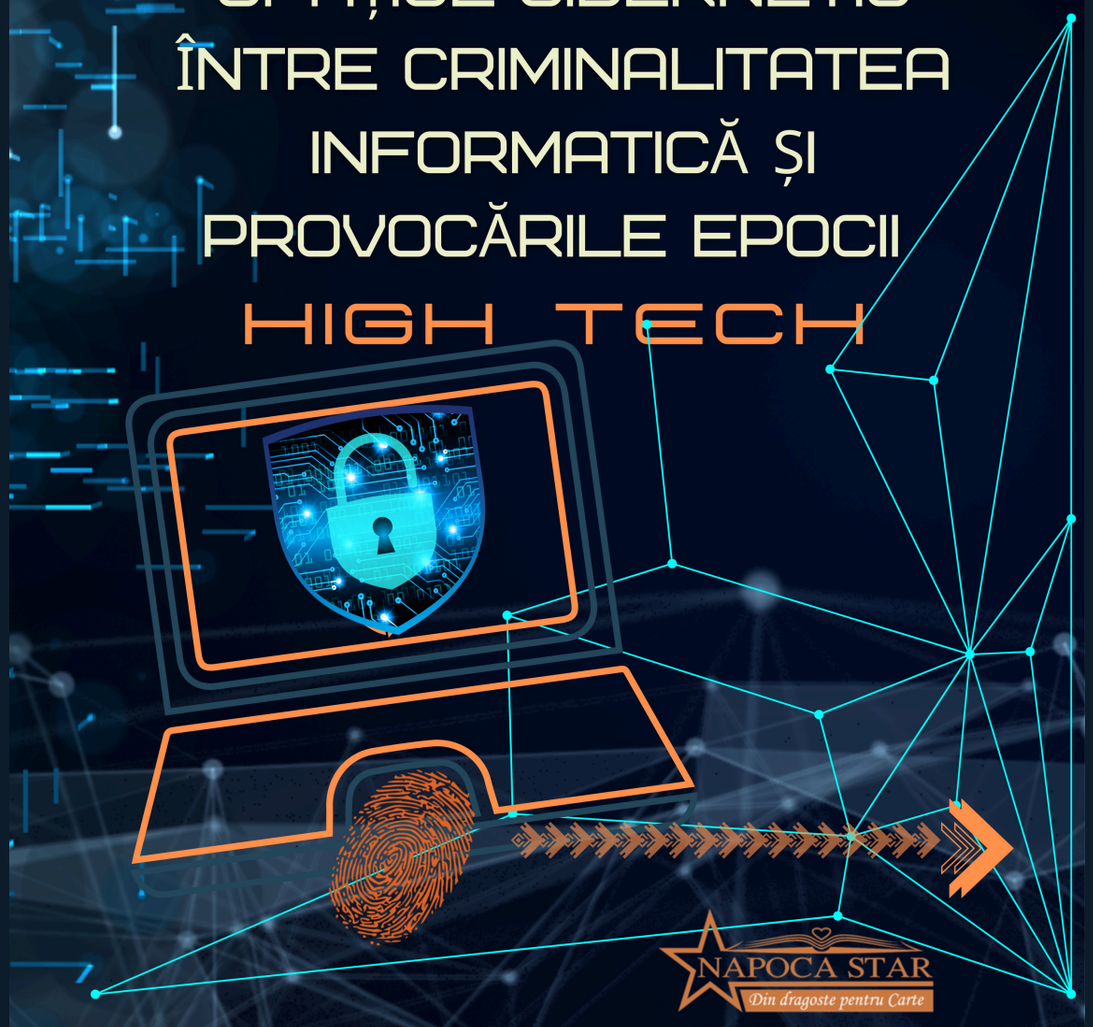
SPAȚIUL CIBERNETIC ÎNTRE CRIMINALITATEA INFORMATICĂ ȘI PROVOCĂRILE EPOCII HIGH TECH

Asociația Ofițerilor în Rezervă din România | Multicultural Bussiness Institute | Academia Elitelor Modelelor si Valorilor | Platforma Valori Românești | Institutul pentru Dezvoltare Umană și Comunitară

SERIA STUDII DE APĂRARE

SPAȚIUL CIBERNETIC ÎNTRE CRIMINALITATEA INFORMATICĂ ȘI PROVOCĂRILE EPOCII

HIGH TECH



NAPOCA STAR
Din dragoste pentru Carte

SPAȚIUL CIBERNETIC ÎNTRE CRIMINALITATEA INFORMATICĂ ȘI PROVOCĂRILE EPOCII HIGH TECH

Coordonatori:
Darius-Antoniu Ferenț
Silviu-Valentin Petre, Alida-Monica-Doriana Barbu

Autori:
Darius-Antoniu Ferenț
Alida-Monica-Doriana Barbu
Elena Onu, Nicolae Sfetcu, Alexia-Gabriela Szabo, Andreea Pop,
Alexia Oprea, Oana-Melisa Țolea

Coordonatori
Darius-Antoniu Ferenț
Silviu-Valentin Petre, Alida-Monica-Doriana Barbu

Autori
Darius-Antoniu Ferenț
Alida-Monica-Doriana Barbu
Elena Onu, Nicolae Sfetcu, Alexia-Gabriela Szabo, Andreea Pop, Alexia Oprea, Oana-Melisa Țolea

SPAȚIUL CIBERNETIC ÎNTRE CRIMINALITATEA INFORMATICĂ ȘI PROVOCĂRILE EPOCII HIGH TECH

Editura Napoca Star
2024

Design copertă: Diana-Cristina Frăteanu

Editura Napoca Star
Strada București, nr. 1
Cluj-Napoca, România
+40 264 432547
+40 740 167461
dinuvirgil2000@gmail.com
www.napocastar.ro

Descrierea CIP a Bibliotecii Naţionale a României
Spaţiul cibernetic între criminalitatea informatică şi provocările epocii High Tech / Darius-Antoniu Ferenţ, Alida-Monica-Doriana Barbu, Elena Onu, ... ; coord.: Darius-Antoniu Ferenţ, Silviu-Valentin Petre, Alida-Monica-Doriana Barbu.
Cluj-Napoca : Napoca Star, 2024
Conţine bibliografie
ISBN 978-606-062-924-5
I. Ferenţ, Darius-Antoniu
II. Barbu, Alida Monica Doriana
III. Onu, Elena
IV. Petre, Silviu-Valentin (coord.)
004.056

Cuprins

Association of Reserve Officers in Romania (AORR)

Darius-Antoniu Ferenț
(*Coordinator of the AORR Cyber Security and Defence Working Group)*

The Association of Reserve Officers in Romania (AORR) is an active and responsible non-governmental organization. In line with its fundamental goals and objectives, AORR, a member of the Interallied Confederation of Reserve Officers CIOR-NATO, established the Cyber Security and Defence Working Group (GLSAC) on May 6, 2023. The group is based in Cluj-Napoca, a city with a distinguished military tradition and currently home to the 4th Infantry Division Headquarter "Gemina".

In a society that involves the intensive use of electronic data and information across all sectors of human existence, with significant socio-economic and security implications, securing IT&C systems has become a major concern for organizations, as well as for NATO and EU member states. These entities are undertaking efforts and measures to ensure the security and uninterrupted operation of special or critical infrastructures.

As interconnectivity increases and sectors of human life digitize, the volume of data stored on servers, clouds, computer equipment and data in motion (shared) continues to rise, which necessitates measures to ensure its confidentiality and integrity.

For the Armed Forces, ensuring the security and resilience of military cyber infrastructures against risks and threats from cyberspace remains a fundamental objective.

Among many other activities, GLSAC organizes information and awareness campaigns on cyber security threats aimed at users of computing devices and seeks to cultivate a cyber security culture among Romanian citizens.

GLSAC is a team composed of reserve and retired military personnel, cybersecurity specialists and civilian volunteers. We have a young team of volunteers (aged between 20 and 25 years old), who contribute to areas such as technical (IT&C), secretarial, administrative, graphic design and online communication. Entry into GLSAC is based on personal skills, abilities, and competencies, and candidates must also meet the conditions stipulated in the Statute of the Association of Reserve Officers in Romania.

Non Sibi Sed Omnibus

From China with Love: Spionajul chinezesc în epoca contemporană

Alida-Monica-Doriana Barbu
(Membru susținător al Asociației Ofițerilor în Rezervă din România și voluntară la Grupul de Lucru pentru Securitate și Apărare Cibernetică al AORR)

Introducere

Guvernul Chinei desfășoară activități de spionaj peste granițe prin intermediul Ministerului Securității Publice (MPS), Ministerului Securității Statului (MSS), Armatei de Eliberare a Poporului (PLA) – prin Intelligence Bureau of the Joint Staff Department, organizații și întreprinderi de stat, Departamentului de Lucru al Frontului Unit (UFWD). Se utilizează SIGINT (Signal Intelligence), HUMINT (Human Intelligence), spionajul cibernetic, pentru accesarea informațiilor sensibile de la distanță, precum și operațiuni de influențare prin cooptarea comunităților din diaspora chineză.[1] Spionajul industrial din partea Guvernului chinez vizează colectarea de tehnologie și informații în sprijinul economiei proprii, dar și reprimarea dizidenților din străinătate (uigurii, partizanii mișcării de independență tibetane, a Taiwanului și a Hong Kong-ului, critici ai Partidului Comunist Chinez (PCC),

[1] Alexander, Bowe, "China's Overseas United Front Work: Background and Implications for the United States" (PDF). United States-China Economic and Security Review Commission, 24 August 2018, https://www.uscc.gov/sites/default/files/Research/China%27s%20Overseas%20United%20Front%20Work%20-%20Background%20and%20Implications%20for%20US_final_0.pdf.

considerați anti-democratici sau mișcarea Falun Gong.[2] Oficiali americani susțin că în urma activității chineze de Intelligence în Statele Unite, s-au cauzat daune economice și furturi tehnologice în valoare de 320-445 miliarde USD anual.[3]

Prin obținerea secretelor tehnologice, comerciale și militare, spionajul chinez urmărește conservarea securității naționale.[4] Agențiile de informații chineze acționează altfel față de alte organizații de spionaj, angajând studenți sau cadre universitare care vor petrece puțin timp în țara gazdă, în loc să cultive ani de zile agenți dubli sau surse de nivel înalt.[5] Articolul 14 din Legea națională a informațiilor din China (2017) statuează că agențiile de informații chineze pot solicita sprijinul și cooperarea organizațiilor, instituțiilor și a oricărui cetățean considerat util.

From China with Love

Dezertorii oferă multe din informațiile disponibile publicului în legătură cu serviciile de informații chineze, RPC acuzându-i

[2] Nicole, Perlroth; Kate Conger; Paul Mozur, "China Sharpens Hacking to Hound Its Minorities, Far and Wide", The New York Times, 22 October 2019, https://www.nytimes.com/2019/10/22/technology/china-hackers-ethnic-minorities.html.

[3] Zack Cooper, Understanding the Chinese Communist Party's Approach to Cyber-Enabled Economic Warfare, FDD PRESS, A division of the Foundation for Defense of Democracies, Washington DC, September 2018, https://s3.us-east-2.amazonaws.com/defenddemocracy/uploads/documents/REPORT_China_CEEW.pdf.

[4] "Report: China spies threaten U.S. technology", CNN, 15 November 2007, https://web.archive.org/web/20080120120103/http://www.cnn.com/2007/TECH/11/15/us.china.tech.ap/

[5] David Johnston, "The Nation; Finding Spies Is the Easy Part", The New York Times, 23 May 1999, https://www.nytimes.com/1999/05/23/weekinreview/the-nation-finding-spies-is-the-easy-part.html

că promovează o agendă mincinoasă anti-RPC.[6] O excepție e cazul Katrinei Leung, suspectată că a început o legătură amoroasă cu un agent FBI pentru a dobândi documente sensibile de la el, acuzații respinse în instanță de către judecătorul federal la data de 5 ianuarie 2005, pe motiv de conduită greșită a procurorului. Leung a fost acuzată de deținere și copiere neautorizate de materiale clasificate. Numele de cod dat de FBI era „Parlor Maid" și a furnizat informații despre China timp de 20 de ani. În aprilie 2003, Katrina Leung și agentul special FBI J.J. Smith au fost arestați. Guvernul a acuzat-o pe Leung că a acționat în favoarea Chinei, cu sprijinul lui Smith, cu care a avut o relație timp de două decenii. Katrina copia documente secrete sau clasificate din servieta lui Smith, existând bănuiala unei complicități a agentului FBI, ceea ce a pus sub semnul întrebării aproape fiecare informație de contraspionaj despre China adunată de Statele Unite în ultimii douăzeci de ani.

Fostul șef al FBI de contrainformații din San Francisco, Ed Appel, a atras atenția asupra posibilității producerii unor consecințe negative, precum compromiterea guvernului SUA și a informațiilor privitoare la China. Leung și Smith nu au fost acuzați de spionaj, dar guvernul a susținut că Smith a dat dovadă de neglijență gravă prin oferirea accesului la documente clasificate lui Leung, care le-a copiat. Ambii au pledat nevinovați. Guvernul SUA a susținut că Leung, de fapt agent chinez cu numele de cod „Luo", a efectuat călătorii regulate în China, pentru întâlniri cu oficiali de rang înalt, cărora le livra informații.

William Cleveland, unul dintre cei mai buni agenți chinezi de contraspionaj ai biroului FBI din San Francisco, a fost primul care a bănuit că „Parlor Maid" ar fi putut da informații chinezilor. În 1991, Cleveland a fost trimis de FBI să călătorească în China. La întoarcere, i s-a pus la dispoziție o înregistrare audio dinainte

[6]"Beijing Denies Involvement in China Spy Case", VOA, 1 April 2008, https://web.archive.org/web/20080406010708/http://www.voanews.com/english/2008-04-01-voa34.cfm

de călătoria sa în China, în care o femeie cu numele de cod „Luo" oferă detalii despre călătoria unui agent numit „Mao", vocea femeii semănând extrem de mult cu cea a lui Leung. Dar Cleveland, la rândul său, a fost timp de trei ani amantul lui Leung. Cartierul general nu a aflat despre relația dintre Smith sau Cleveland cu Leung, trimițând-o înapoi în teren, sub supravegherea lui Smith. Ulterior, chiar și după ce au descoperit că Leung lucrează cu chinezii, atât agentul Cleveland, cât și agentul Smith au continuat să împărtășească informații despre importante investigații de contraspionaj chineze cu „Parlor Maid".Fostul agent Cleveland nu a fost acuzat de guvernul federal, colaborând cu anchetatorii săi.

Filmul 'From China with Love' detaliază drama din spatele problemelor profunde care au afectat FBI-ul de mai bine de un deceniu, în opinia producătorului *Frontline* Michael Kirk, precum vulnerabilitățile controlului de management, dar și ale relației dintre agenți și surse, și nu în ultimul rând, eficiența capcanelor sentimentale.

Autorul cărții „A Convenient Spy", Dan Stober, afirmă că Cleveland era implicat în cazurile Gwo-Bao Min, Wen Ho Lee și Peter Lee, iar în eventualitatea în care ar fi discutat cu Katrina aceste cazuri, iar ea le-ar fi transmis chinezilor, ar fi făcut un rău important SUA.

Larry Wu-Tai Chin[7], născut la Beijing, a început în timpul celui de-al Doilea Război Mondial să lucreze pentru Statele Unite, în urma recrutării de către armata SUA ca interpret și traducător pentru Biroul de Legătură al Armatei SUA. În 1948, a primit aceleași sarcini la Consulatul SUA din Shanghai, moment în care a început să dezvolte contacte în cadrul serviciilor de informații chineze.

Chin a ajutat în 1951 Departamentul de Stat să intervieveze prizonierii de război chinezi în Coreea, iar în 1952, le-a dezvăluit

[7] Dan Stober, A Convenient Spy: Wen Ho Lee and the Politics of Nuclear Spionage, Simon and Schuster, New York, 2001.

identitățile chinezilor și s-a alăturat unei divizii a CIA din Okinawa, Japonia, și anume Serviciul de Informații Externe de Radiodifuziune (FBIS). A continuat legătura cu contactele sale chineze și s-a întâlnit cu acestea la Hong Kong pentru schimb de informații. FBIS l-a transferat în 1961 pe Chin în California, în timp ce serviciile de informații chineze i-au pus la dispoziție în Canada un om de contact, căruia îi putea oferi informații. În 1965, Chin a devenit cetățean american.

După ce a trecut testul poligrafului în 1970, Chin a fost promovat într-o poziție FBIS în Arlington, Virginia, gestionând informații extrem de sensibile, precum documente referitoare la planul președintelui Nixon de normalizare a relațiilor cu China și rapoarte de la agenții americani din străinătate. La retragerea sa în 1981, Chin a primit o medalie de la CIA pentru serviciile aduse, iar mai târziu a fost celebrat printr-o ceremonie similară de către chinezi.

După ce a primit în 1982 un pont de la Yu Qiangsheng, un ofițer chinez de informații care a dezertat în Statele Unite, FBI a început să suspecteze că Chin era spion. În urma confruntării lui Chin cu dosarul adus de Yu Qiangsheng despre el și cu dovezile relației cu responsabilul său din Ministerul Securității de Stat (MSS), Chin a mărturisit la interogatoriul FBI că a spionat pentru China, devenind una dintre cele 14 persoane acuzate de spionaj în 1985, supranumit „Anul spionului”.

La procesul de spionaj din februarie 1986, Chin s-a apărat că a transmis informațiile Chinei pentru a ajuta la îmbunătățirea relațiilor dintre cele două țări, însă juriul l-a găsit vinovat de conspirație, spionaj și evaziune fiscală. Chin s-a sinucis în celula sa de închisoare înainte de a putea fi condamnat.

În 2023, îngrijorările legate de spionajul chinez asupra Statelor Unite au aruncat umbre asupra vizitei planificate în China a Secretarul de stat al SUA, Antony Blinken, în timp ce cele două superputeri încercau să îmbunătățească legăturile deteriorate, urmărindu-se în același timp cu priviri atente una pe

cealaltă. Antony Blinken a aterizat la Beijing după amânarea călătoriei sale anterioare, planificată pentru luna februarie, amânare datorată unui balon de supraveghere chinez ce trecuse deasupra țintelor militare strategice americane, înainte de a fi doborât de un avion de luptă american. În ciuda încercărilor de a repara comunicarea fracturată dintre SUA și China, o altă controversă a fost stârnită de balonul de spionaj chinez, chiar dacă președintele Xi a afirmat că nu știa despre prezența balonului deasupra teritoriului SUA. Balonul a utilizat un furnizor de servicii de internet american pentru a trimite transmisii periodice și scurte de date legate de navigare și locație înapoi în Beijing, China. Prin această conexiune, SUA au putut să adune informații despre balon în timpul tranzitului deasupra Statelor Unite. Conexiunea la rețea nu a fost folosită pentru a transmite informații înapoi în China, deși informațiile (date și imagini) erau stocate, China a menținut afirmația că balonul a fost un balon meteorologic cu un curs deviat. Comunitatea americană de Intelligence e de părere că liderii Partidului Comunist Chinez nu aveau în intenție ca balonul să survoleze Statele Unite. Directorul Biroului de Informații Naționale și FBI au refuzat să comenteze [8]

Înlănțuirea de acuzații de spionaj dintre cele două state subliniază modul în care strângerea de informații – o activitate menită să se desfășoare fără a fi detectată, în afara ochiului publicului – devine un punct de foc din ce în ce mai proeminent în relația SUA-China.

[8] Katie Bo Lillis, Chinese spy balloon used US internet provider to communicate its location, CNN, Published 2:33 PM EST, Fri December 29, 2023, https://edition.cnn.com/2023/12/29/politics/chinese-spy-balloon-us-internet-provider/index.html

Bernard Boursicot în mrejele „Frumoasei" din Beijing

Cazul Bernard Boursicot, născut la 12 august 1944 la Vannes, Franța, este un o ilustrare a modului lipsit de scrupule de recrutare a personalului din ambasadele străine de către serviciile secrete chineze. Întâi se identifică veriga slabă: în cazul ambasadei franceze, agentul contractual Bernard Boursicot, care din cauza vârstei fragede – 20 de ani -, a lipsei de experiență și a naivității, se îndrăgostește de o solistă de operă chineză, care de fapt e bărbat. Stratagemele cântărețului chinez au rezistat testului timpului, Boursicot crezând această mascaradă decenii întregi, în care, din dorința de a nu o pierde pe „femeia" iubită și pe „copilul" lor (de fapt, un copil înfiat de chinez), a încredințat serviciilor secrete chineze informații despre ambasade străine. Relația dintre Shi Pei Pu, cântărețul chinez de operă și diplomatul francez Bernard Boursicot, desfășurată în timpul Revoluției Culturale din China, se încadrează în categoria înșelăciune personală profundă și spionaj internațional.

Shi Pei Pu, spion sub masca de cântăreț de operă chinez, celebru pentru rolul său feminin de *dan* din *Povestea unui fluture*[9], "un tânăr misterios, zvelt și scund, superb în costumul cu guler a la Mao, având totodată un chip tulburător"[10], l-a cunoscut în 1964 pe Boursicot, un contabil de 20 de ani al ambasadei Franței la Beijing. Acesta din urmă a fost încântat de Shi, iar când Shi i-a dezvăluit în timpul unei plimbări în 1965 că e femeie, dar că a fost forțat să trăiască ca bărbat din cauza presiunii familiale, romantismul a prins contur, la fel ca relația lor în timpul Revoluției Culturale și a deceniilor ce vor urma. Povestea cuplului a inspirat „M. Butterfly", piesa câștigătoare a

[9] Carl Samson, Shi Pei Pu: The opera singer who faked being a woman to spy for China, Next Shark, 11 aprilie 2024, https://nextshark.com/shi-pei-pu-bernard-boursicot-espionage

[10] Roger Faligot, Serviciile secrete chineze de la Mao la Xi Jinping, Meteor Publishing, București, 2019, p. 469.

premiului Tony în 1988 a lui David Henry Hwang, jucată de BD Wong și filmul cu același titlu al lui David Cronenberg din 1993.[11]

Ministerul Francez de Externe a dispus în decembrie 1965 plecarea lui Boursicot la Ambasada Franceză din Arabia Saudită și la Ministerul de Externe din Paris, însă a revenit la Beijing în 1969 pe postul de arhivar și ofițer responsabil cu valiza diplomatică, un post sensibil prin prisma secretelor ambasadei la care avea acces.

Shi a continuat să îl manipuleze pe Boursicot, prezentându-i „fiul" de 4 ani, Shi Dudu, pretinzând că era al lor. În urma înscenării răpirii ei de către masele populare din cartier, în speranța asigurării securității ei și a copilului lor, Bernard s-a întâlnit la finele primăverii anului 1970 cu Kang Gesun, despre care știa de la Shi că lucra la Municipalitatea Beijing-ului, dar care era de fapt funcționar al Ministerului Securității Publice – Ministerul de Interne, căruia i-a înmânat un plic sigilat preluat de la registratura ambasadei. Kang și tovarășul său „Zhao", pe numele adevărat Peng Zhe, făceau parte din Diaochabu, serviciul de informații al Comitetului Central al PCC, în cadrul căruia o secție se ocupa de compromiterea și recrutarea străinilor trimiși să lucreze în China. Secția a fost activă inclusiv în timpul Jocurilor Olimpice din 2008 de la Beijing, reorganizată în cadrul serviciului Guoanbu. Kang i-a fost ofițerul de caz din 1970 până în 1981, ușurat că îl recrutase pe Bertrand, căci îi mărturisese că nu prea aveau de lucru în timpul Revoluției Culturale. Între 1970 și 1972, când a plecat pe postul de arhivist-criptograf la Dublin, și între 1979 și 1981, când era detașat la ambasada din Mongolia Exterioară, Boursicot le-a înmânat chinezilor documente diplomatice, însă niciodata documente ștampilate „confidențial" sau „secret" referitoare la Franța, ci cu privire la intențiile

[11] Carl Samson, Shi Pei Pu: The opera singer who faked being a woman to spy for China, Next Shark, 11 aprilie 2024, https://nextshark.com/shi-pei-pu-bernard-boursicot-espionage

americane în Vietnam, la puterea militară a sovieticilor cu care chinezii au avut dispute teritoriale în 1969. La un moment dat, când i se cereau tot mai multe informații despre URSS, Japonia, India, Mongolia, SUA, Hong Kong, Boursicot a început să decupeze articole din *Le Figaro*, să le rescrie la mașina de scris în stilul său literar și furând ștampila ambasadorului, să le pună inscripția „secret". Bernard s-a întors în Franța din Ulan Bator în 1981. Fiind urmat de Shi Peipu în 1982, a încheiat contactul cu agenții chinezi, dar a fost arestat la Paris la data de 30 iunie 1983 pentru dispariția a 100 de documente de la ambasada din Beijing. [12]

În timpul anchetei care l-a vizat și pe Shi Peipu, comisarii de la DST au aflat că acesta era nepotul lui Ding Xilin (decedat în 1974), dramaturgul și ministru adjunct al culturii, dar și vicepreședintele Asociației Poporului Chinez pentru Relații Culturale cu Țările Străine., asociație care servea drept acoperire pentru operațiuni de Intelligence, inclusiv când a fost invitat Președintele Mitterrand la Beijing. Celălalt vicepreședinte era Zou Dapeng (destituit și omorât în 1967 de către Gărzile Roșii), directorul adjunct al serviciului de informații Diaochabu, cel care îl prinsese în cursa predării documentelor ambasadei pe Bernard. Deși regimul se liberalizase, serviciile secrete chineze permițându-i lui Shi să onoreze invitația unei universități franceze în octombrie 1982 și să rămână cu copilul lor alături de Bernard, artistul chinez a ținut legătura cu atașatul cultural de la ambasada chineză din Paris, Wang Erqing, dobândind notorietate în lumea chineză din Franța și primind invitații la postul TV TF1.[13] În plus, venise în Hexagon pentru a-l reactiva pe Boursicot care urma să devină diplomat, cadru B.

În mod interesant, Bruno Laroche, judecătorul de instrucție l-a acuzat pe Bernard de spionaj alături de agenți ai unei puteri

[12] Roger Faligot, *Serviciile secrete chineze de la Mao la Xi Jinping*, Meteor Publishing, București, 2019, pp. 473-479.
[13] Roger Faligot, *op. cit.*, pp. 480-481.

străine și pe Shi Peipu de complicitate, în loc să îl acuze pe chinez de spionaj și pe Boursicot de complicitate. În urma aflării rezultatului examenului medical de la postul de radio France Inter care a confirmat sexul masculin al lui Shi Peipu, Bernard și-a pierdut cunoștința în celula inchisorii Fresnes unde se afla și a încercat o săptămâna mai târziu să își reteze jugulara cu o lamă de ras. Raportul medicilor psihiatri Defer și Roper a explicat confuzia oficialului francez ân privința sexului chinezului prin faptul că relațiile sexuale se desfășurau în întuneric, iar Shi ar fi avut o hemoragie în timpul primului contact sexual, hemoragie ce simula virginitatea. Artistul chinez a avut chiar manifestările unei sarcini, dar a întrerupt-o de comun acord cu Boursicot. La semnele noii graviditățI din decembrie 1965, oficialul francez a fost convins de realitatea sarcinii. Bernard a plecat din China, la întoarcerea sa în septembrie 1969, fiind înștiințat că Shi încredințase fiul născut în august 1966 unei doici în provincie, de la care copilul a fost recuperat în 1973 și adoptat. Copilul era de origine uigură (grup etnic turc) din Xinjiang, pentru a da impresia că e metis europeano-asiatic.[14]

Shi Peipu ar fi suferit de criptorhidie până în 1965, conform declarației chinezului, criptorhidie care ar fi fost operată chirurgical și tratată hormonal. Joyce Wadler, colaboratoare la Washington Post, a scris în 1993 cartea ”Liaison” la editura Bantam Books în New York, carte în care explica cum criptorhidia făcea posibile contacte sexuale superficiale. Cartea nu a putut fi însă publicată în Franța din cauza ridicării opoziției lui Shi Peipu că ar reprezenta un atentat la viața sa privată. Shi Peipu, deși era spion chinez condamnat, beneficia de protecție în Franța. Spionul chinez a fost chiar răsplătit pentru mărturia împotriva lui Boursicot prin punerea în libertate provizorie de către curtea de apel în februarie 1984. Mitterrand însuși l-a grațiat în 1987 pe Shi Peipu, deși fusese condamnat la 6 ani de

[14] Roger Faligot, *Serviciile secrete chineze de la Mao la Xi Jinping*, Meteor Publishing, București, 2019, pp.481-483.

închisoare, fiind primul spion condamnat care nu a fost declarat *persona non grata*. Statul francez dorea aplanarea incidentului diplomatic în urma presiunilor chineze. Generalul de Gaulle a fost printre primii care a recunoscut Beijing-ul, prietenie cultivată și de Chirac, apoi de Sarkozy prin călătoria în China și considerarea Taiwan-ului și a Tibetului indestructibil legate de China.[15]

Bernard a rămas în închisoare toți cei 6 ani de condamnare. Foști colegi ai ambasadei din Beijing ar fi încercat să îi obțină eliberarea, dar nu și Etienne Manac'h, ambasadorul, indicat de către un transfug sovietic trecut de partea CIA drept agent al serviciilor secrete sovietice, cu numele de cod Taksim, recrutat pe când era în 1942 reprezentantul Franței Libere în Turcia și apreciat de Zhou Enlai în fața lui Alain Peyrefitte, autor al cărții „*Quand la Chine s'éveillera*" și jurnalist la *Le Figaro* drept punte de legătură între China și Occident. Ambasadorul francez predase Chinei pe transfugul Zhang Shirong, ce a fost posibil executat după repatriere, caz în care Boursicot se opusese pentru salvarea vieții chinezului.[16]

După grațierea din 1987, Shi a continuat cu spectacolele de operă la Paris, dar și cu călătorii dese la Beijing, al cărui viceprimar era un apropiat al său. Avea în proprietate inclusiv un apartament aproape de *Orașul Interzis*. Boursicot însă a avut de-a face cu oprobiul public și umilința privitoare la aventura lor. Shi a decedat într-un azil de bătrâni din Paris pe 30 iunie 2009, la 70 de ani. Cu câteva luni înainte de moartea sa, i-a mărturisit lui Boursicot că încă îl iubește. Boursicot, care locuise și el într-un azil de bătrâni francez, a comentat moartea lui Shi pentru New York Times în fața lui Joyce Wadler, autoarea cărții „Liaison: The True Story of the M. Butterfly Affair": „*A făcut atâtea lucruri împotriva mea de care nu i-a fost milă, cred că este o prostie să joc un alt joc acum și să spun că sunt trist. Placa*

[15] Roger Faligot, op. cit., pp.483-484, 486, 489-450.
[16] *Ibidem*., pp. 484, 486-488.

este curată acum. Sunt liber." Povestea cuplului a inspirat piesa lui David Henry Hwang, câștigătoare a premiului Tony în 1988, „M. Butterfly", cu BD Wong și filmul cu același titlu al lui David Cronenberg din 1993.[17]

În Franța există mulți „prieteni pentru China", adică surse, agenți de influență, corespondenți, ale căror corzi sensibile sunt ușor de atins, fie prin stratagema femeii frumoase, cinele rafinate, atracția culturală mutuală, naivitatea lumii economice în privința contractelor înșelătoare, deschiderea prea mare a lumii universitare care permite intruziunea chineză, tradiția înfrățirii regionale, existența curentului maoist din anii 1960 reconvertit, antiamericanismul și creșterea comunității chineze din Franța.[18]

Moartea Violettei – nu Valéry, Zhang

Violetta Zhang (13.11.1965-26.06.1999) a fost găsită moartă în apartamentul deținut de Departamentul de Studii Chineze al Institutului de Studii pentru Orientul Îndepărtat al Universității Ludwig-Maximilian din München. Violetta, sinoloaga cu ochi albaștri, de origine germană, divorțase de soțul Zhang Zhongping din Beijing, de proveniență chinez. Cauza decesului său la vârsta de 34 ani a fost declarată necunoscută în urma anchetei. Instanța bavareză a interzis în 2006 publicarea numelui adevărat al comisarului de poliție, cunoscut sub pseudonimul Stephanie Glück, în urma acuzării de către jurnalistul Armin Witt, partenerul defunctei, de incompetență și încercare deliberată de ascundere a adevărului. Nici RTL II, postul de televiziune unde lucrase Violetta, nu s-a lăsat mai prejos, și a ridicat în documentarul realizat despre circumstanțele ciudate ale decesului lui Witt:

[17] Carl Samson, Shi Pei Pu: The opera singer who faked being a woman to spy for China, Next Shark, 11 aprilie 2024, https://nextshark.com/shi-pei-pu-bernard-boursicot-espionage
[18]Roger Faligot, *op. cit*., 489-491.

problema neconcordanței între raportul poliției, serviciilor de urgență și personalului judiciar privind ora găsirii cadavrului; aspectul tăierii venelor, conform raportului poliției, nu se regăsea în autopsie; lipsa sângelui pe corpul decedatei sau în apartamentul institutului; absența interogatoriului rezidenților complexului; raportul criminalistic care afirma prezența unei seringi înfipte în pieptul său; veridicitatea biletului de adio al Violettei, care denota o atitudine depresivă, în opoziție cu mulțumirea de sine și de viață, demonstrată cu doar două zile înainte în fața familiei.[19]

Violetta studiase chineza și epoca Tang în trecut la Shanghai, reîntorcându-se în China alături de Armin în 1998 și planificând o nouă călătorie în 1999 la bordul iahtului Galaxy, achiziționat de prietenul ei din Iugoslavia. Au trezit însă suspiciunea autorităților chineze prin intrarea în țară a lui Armin ca și turist, deși era jurnalist, a deținerii asupra lor a unor hărți nautice clasificate și a unei cărți a autorului Sterling Seagrave, neagreat de China, despre rețelele de chinezi din străinătate. Stabilirea contactelor cu sprijinul lui Krüger, consulul german din Shanghai și a unui amic, atașat militar la Ambasada Germaniei din Beijing, dar și dorința de a trimite cetățeni germani cu nava Galaxy prin firma de turism înființată de ei pe insula Hainan din sudul Chinei, insulă ce deținea multe instalații militare de interceptare electronică, a trezit bănuiala rezonabilă din partea chinezilor că ar fi lucrat pentru BND, Serviciul Federal de Informații German. În Hainan, în 2001, avioanele de luptă chineze au determinat aterizarea forțată a avionului-spion al armatei americane EP-3E. Guvernatorul Ruan Chongwu, fost director al Gonganbu, consilier între 1978 și 1983 la Ambasada Chinei din Bonn, ocupându-se cu spionajul tehnologic și științific, era interesat în continuare de Germania de Vest. Sediul BND de pe Pullachstraße, aproape de consulatul chinez de pe Romanstraße, era urmărit de agenții Guoanbu, iar în eventualitatea

[19] *Ibidem.,* pp.308-309.

în care Violetta, deși divorțată, ar fi lucrat pentru BND, s-ar fi considerat de către autoritățile chineze că ar fi încălcat obligația de fidelitate față de statul chinez, prin prisma numelui chinez pe care încă îl purta.[20]

Armin Witt era de părere că Violetta aflase informații pe care nu trebuia să le știe fie despre institutul său, fie despre ChinaForum, societate infiltrată de chinezi pe care o superviza. Îl privea pe fostul soț drept un posibil suspect prin drumurile pe care le făcea între München, unde avea locuința și Suedia, unde lucra la o companie de telefonie.[21]

Chinezii sunt atenți la cei care observă China și erau familiariati cu practica angajării în cadrul institutelor de cercetare a agenților germani, practică utilizată și de ei. Încă din epoca lui Jiang Zemin (1997-2004), chinezii stabileau schimburi universitare și aveau specialiști, precum Lu Yaokan, care scriau rapoarte despre institutele vest-germane, inclusiv Institutul de Orientalism și Studii Internaționale. Lu Yaokan era analistă la CICIR (Institutul de Relații Internaționale Contemporane din China) – centrul de analiză al serviciului de informații Guoanbu. Împreună cu profesorul specializat în Germania și Franța, Feng Zhongling, care a tradus de asemenea biografia lui Deng Xiaoping scrisă de Uli Franz, Lu a ales țintele de spionaj din Germania în numele Guoanbu, printre care e posibil să se fi numărat și Violetta, al cărei deces are parfumul unei crime comandate de China și mascată în sinucidere, acoperită de Germania pentru evitarea tensionării relațiilor cu Țara Dragonului.[22]

[20] Roger Faligot, *Serviciile secrete chineze de la Mao la Xi Jinping*, Meteor Publishing, București, 2019, pp. 310-311.
[21] Roger Faligot, *op. cit.*, p. 311.
[22] *Ibidem*., p. 312.

Spionajul tehnologic al Chinei

Tehnologia de rețea dezvoltată de armata chineză a spionat mai multe națiuni, conform SUA, cazuri de intruziuni de computere suspectate a fi chineze întâlnindu-se în Canada, Noua Zeelandă, Australia, Germania, Franța, Regatul Unit, India, Țările de Jos și Statele Unite.[23]

În urma *Shadow Network*, operațiune de spionaj computerizat, experții în securitate au susținut că activiștii tibetani erau vizați de guvernului chinez, deoarece hackerii privați chinezi urmăresc doar informații economice.[24] Cercetătorii canadieni de la *Centrul Munk pentru Studii Internaționale* de la Universitatea din Toronto au examinat în 2009 computerele din biroul lui Dalai Lama, descoperind astfel *GhostNet*, o rețea extinsă de spionaj cibernetic. Hackerii chinezi au obținut acces la computere ale organizațiilor guvernamentale și private din 103 țări, deși cercetătorii susțin că nu există nicio dovadă că guvernul chinez ar fi fost în spatele acesteia. Calculatoarele accesate aparțineau lui Dalai Lama, organizațiilor afiliate cu Dalai Lama din Bruxelles, Londra, India și New York, exilaților tibetani, ambasadelor, ministerelor de externe și ale altor birouri guvernamentale, fiind vizate și guvernele din Asia de Sud și Asia de Sud-Est.[25]

---

[23] Peter Brookes, "Flashpoint: The Cyber Challenge: Cyber attacks are growing in number and sophistication", Family Security Matters, 13 March 2008, https://web.archive.org/web/20080329074454/http://www.familysecuritymatters.org/homeland.php?id=1386912

[24] Nicole Perlroth, "Case Based in China Puts a Face on Persistent Hacking", The New York Times, 29 March 2012, https://www.nytimes.com/2012/03/30/technology/hacking-in-asia-is-linked-to-chinese-ex-graduate-student.html

[25] John Markoff, "Vast Spy System Loots Computers in 103 Countries", The New York Times, 28 March 2009, https://www.nytimes.com/2009/03/29/technology/29spy.html.

A doua rețea de spionaj cibernetic a fost descoperită în 2010, printre documentele furate numărându-se materiale clasificate despre securitatea sistemelor de rachete indiene, documente confidențiale ale ambasadei despre relațiile Indiei în Africa de Vest, Rusia și Orientul Mijlociu. Hackerii email-ului lui Dalai Lama erau conectați cu universități din China. Beijingul a negat din nou implicarea.[26] În 2019, hackeri chinezi și-au luat identități false, pretinzând că sunt reporteri *New York Times* sau *Amnesty International*, vizând biroul privat al lui Dalai Lama, membrii parlamentului tibetan și organizațiile neguvernamentale tibetane. Twitter și Facebook au distrus o rețea extinsă de roboți chinezi care răspândeau dezinformare cu privire la protestele din Hong Kong din perioada 2019-2020, iar atacul împotriva companiilor media din Hong Kong a fost urmărit de hackeri chinezi.[27]

Tehnologia inteligenței artificiale (AI) de recunoaștere facială și de supraveghere dezvoltată în China pentru a identifica minoritatea musulmană a uigurilor[28] este utilizată pe întreg teritoriul chinez și, în pofida îngrijorării legate de implicarea Chinei în rețelele wireless 5G, este exportată de către *China National Electronics Import & Export* și Huawei în Zimbabwe, Ecuador, Uzbekistan, Kenya, Pakistan, Emiratele Arabe Unite,

[26] Tania Branigan, "Cyber-spies based in China target Indian government and Dalai Lama", The Guardian, 6 April 2010, https://www.theguardian.com/technology/2010/apr/06/cyber-spies-china-target-india.

[27] Robert McMillan; Maria Armental, "Twitter, Facebook Target Accounts Spreading Misinformation on Hong Kong Protests", The Wall Street Journal, 19 August 2019, https://www.wsj.com/articles/twitter-facebook-target-accounts-spreading-misinformation-on-hong-kong-protests-11566242944.

[28] Paul Mozur, "One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority", The New York Times, 14 April 2019,https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html?action=click&module=RelatedCoverage&pgtype=Article&region=Footer.

Bolivia, Venezuela, Angola și Germania.[29] MIT, Princeton, Fundația Rockefeller sprijină start-up-urile AI chineze *SenseTime, Hikvision* și *Megvii,* care vând versiuni mai ieftine ale sistemelor de supraveghere cu inteligență artificială dezvoltate de statul chinez, deși utilizarea lor este redusă în urma declarării drept amenințări la adresa securității naționale și încălcării drepturilor omului, dar și în urma preocupărilor legate de competiția economică dintre China și SUA.[30] China a reușit să depășească SUA în investițiile în startup-uri americane de inteligență artificială.[31]

În iulie 2020, în raportul său anual, agenția națională de informații a Germaniei, BfV (Bundesamt für Verfassungsschutz) a avertizat consumatorii că datele personale pe care le furnizează companiilor de plată chineze sau altor firme de tehnologie, cum ar fi *Tencent, Alibaba*, etc., ar putea ajunge în mâinile guvernului chinez.[32]În septembrie 2020, o companie chineză, *Shenzhen Zhenhua Data Technology*, a intrat sub lupa întregii lumi pentru capacitățile și intențiile sale legate de utilizarea BIG DATA și de extragere și integrare a datelor,[33] directorul executiv Wang

[29] Paul Mozur, Jonah M. Kessel, Melissa Chan, "Made in China, Exported to the World: The Surveillance State", The New York Times, 24 April 2019.

[30] Ryan Mac, "The US Just Blacklisted China's Most Valuable Facial Recognition Startups Over Human Rights Abuses", Buzz Feed, 8 October 2019. "Research Brief: China Is Starting To Edge Out The US in AI Investment". CB Insights. 12 February 2019.

[31] "Research Brief: China Is Starting To Edge Out The US in AI Investment". CB Insights. 12 February 2019, https://www.cbinsights.com/research/china-artificial-intelligence-investment-startups-tech/.

[32] German intel warns against giving data to Chinese tech firms, AP, Published 5:48 PM EEST, July 9, 2020, https://apnews.com/article/48ee7ff615ce6f5fa05047782abd11a4

[33] Daniel Hurst; Lily Kuo; Charlotte Graham-McLay, "Zhenhua Data leak: personal details of millions around world gathered by China tech company", the Guardian, 14 September 2020,

Xuefeng afirmând că e un susținător al războiului psihologic, hibrid, și al influențării opiniei publice.[34]

Concluzii

Fiecare întreprindere chineză de anvergură din întreaga lume deține o „celulă" internă care răspunde în fața Partidului Comunist Chinez (PCC) care se asigură că compania respectă directivele și agenda politică chineză. PCC operează deseori sub acoperirea naturală a afacerilor. „Mașina de partid este peste tot. Pentru China, afacerile sunt inseparabile de politică".[35] Dintre cele 93 de milioane de membri ai Partidului Comunist Chinez, mulți sunt plasați sau ascunși în organizații în afara granițelor, în vederea culegerii de informații, în special din sfera tehnologiei și telecomunicațiilor. Potrivit Raportului Cox de 700 de pagini al SUA din 1999, China aflase secretele militare americane, informații despre bombele cu neutroni, computerele pentru ghidarea rachetelor, focoasele nucleare multiple, au furat planuri tehnice și brevete, dar și companiile americane se făceau vinovate de transmiterea tehnologiilor de vârf către chinezi prin societățile mixte. Era o doar o chestiune de timp până când chinezii aveau să producă prototipele copiate.[36] Serviciile de

https://www.theguardian.com/world/2020/sep/14/zhenhua-data-full-list-leak-database-personal-details-millions-china-tech-company.

[34] Ben Graham, "Zhenhua Data: 35,000 Aussies being spied on by China as part of 'psychological war", news.com.au., 13 September 2020, https://web.archive.org/web/20200917043528/https://www.news.com.au/technology/online/security/zhenhua-data-35000-aussies-being-spied-on-by-china-as-part-of-psychological-war/news-story/3ce5b88c00e3ae81d59976911a96319b.

[35] Frank Gardner, „The spying game: China's global network*",* BBC News, 8 July 2020, https://www.bbc.com/news/uk-53329005

[36] Roger Faligot, Serviciile secrete chineze de la Mao la Xi Jinping, Meteor Publishing, București, 2019, p. 367.

informații profesioniste chineze interesate în dobândirea cunoștințelor tehnologice sunt Departamentul de Informații Militare (DIM) al Statului-Major al AEP (AEP-2) și Ministerul Securității Statului (MSS- Guoanbu). Companiile industriale și institutele de cercetare sunt controlate de guvernul chinez, pierderile cele mai importante de tehnologie americană producându-se în urma interacțiunilor științifice, comerciale și academice dintre China și SUA.[37]

La Conferința „Salutări tovarășilor de pe frontul misiunilor speciale" susținută de Guoanbu, [38] de AEP – 2 și Departamentul de Muncă al Frontului Unit din 1997, viceprim-ministrul Zhou Jiahua a declarat că aceste organisme deschiseseră agenții de informații în 50 țări și peste 170 de orașe, sub denumirea de baze generale, stații și substații.[39]

Metodele de recrutare a agenților sau persoanelor străine din poziții-cheie în companii străine, guverne, universități, ambasade, etc. includ stimulente pozitive, precum invitații la întâlniri importante de afaceri, la evenimente culturale, schimburi de experiență sau colaborări în mediul universitar și de cercetare în China, oferte de ajutor financiar pentru companiile aflate în dificultate sau oferirea unui loc neexecutiv într-un consiliu director, nu în ultimul rând mita printr-o sumă substanțială de bani. Pe teritoriul Chinei însă, metodele de recrutare devin mai incisive, incluzând presiunea asupra membrilor familiei chineze și *„honeytraps"*- capcanele amoroase pentru oficialii sau oamenii de afaceri occidentali imprudenți. Întâlnirea „întâmplătoare" cu o femeie atractivă, aleasă în funcție de profilul psihologic al persoanei vizate, este urmată apoi de episoade romantice

[37] Roger Faligot, *op.cit*., p. 371.
[38] Ministerul Securității Statului (MSS sau Guóānbù) este agenția de poliție secretă a Republicii Populare Chineze, cu sediul în districtul Haidian din Beijing, în ale cărei atribuții intră informațiile externe, contrainformațiile și securitatea politică a Partidului Comunist Chinez (PCC).
[39] Roger Faligot, op.cit., p. 307.

înregistrate pe ascuns și utilizate ca „kompromat" - material compromițător folosit ca șantaj.[40]

Bibliografie

Monografii. volume de referință

1. Faligot, Roger, Serviciile secrete chineze de la Mao la Xi Jinping, Meteor Publishing, București, 2019.
2. Stober, Dan, A Convenient Spy: Wen Ho Lee and the Politics of Nuclear Spionage, Simon and Schuster, New York, 2001

Documente Online

3. Bowe, Alexander, "China's Overseas United Front Work: Background and Implications for the United States" (PDF). United States-China Economic and Security Review Commission, 24 August 2018, https://www.uscc.gov/sites/default/files/Research/China%27s%20Overseas%20United%20Front%20Work%20-%20Background%20and%20Implications%20for%20US_final_0.pdf.
4. Cooper, Zack Understanding the Chinese Communist Party's Approach to Cyber-Enabled Economic Warfare, FDD PRESS, A division of the Foundation for Defense of Democracies, Washington DC, September 2018, https://s3.us-east-2.amazonaws.com/defenddemocracy/uploads/documents/REPORT_China_CEEW.pdf.

[40] Frank Gardner, *op.cit.*

Resurse web

- https://www.bbc.com/
- https://www.nytimes.com/
- https://www.cbinsights.com/
- https://apnews.com/
- https://www.theguardian.com/
- https://www.news.com.au/
- http://www.familysecuritymatters.org/
- https://www.wsj.com/
- https://nextshark.com/
- https://edition.cnn.com/
- http://www.voanews.com/

Actualul context de securitate și folosirea de către Moscova a narativelor privind arsenalul nuclear

Colonel (r.) Elena Onu
Membru al Asociației Ofițerilor în Rezervă din România și membru al Grupului de Lucru pentru Securitate și Apărare Cibernetică

Abstract

Declarațiile Moscovei privind posibilitatea unui atac nuclear care au succedat acțiunile militare ale Federației Ruse în Ucraina, demarate în februarie 2022, au fost percepute de cea mai mare parte a comunității internaționale drept o modalitate de a intimida Ucraina și țările UE și NATO.

Această tactică a avut cu siguranță un efect inițial, oprind sau amânând sprijinul militar acordat Ucrainei din partea unor mari puteri occidentale. Pornind de la realitatea că președintele Vladimir Putin folosește declarațiile privind armele nucleare pentru a comunica cu publicul – intern și extern, iar ignorarea unei astfel de retorici poate fi la fel de dăunătoare ca și exagerarea ei, folosind analiza declarațiilor oficialilor din Federația Rusă și NATO, articolul încearcă să clarifice ipoteza potrivit căreia intensificarea retoricii nucleare ar putea fi folosită de Moscova, alături de China, pentru a crea un ”avantaj strategic” într-o eventuală negociere cu SUA privind împărțilea sferelor de influență și inițierea unui nou Război Rece.

Introducere

Începând cu anul 1999, Federația Rusă a folosit în mod constant amenințările nucleare pentru atingerea obiectivelor politicii sale externe și de securitate, mai ales pentru descurajarea atacurilor directe la adresa sa și asigurarea câștigurilor teritoriale,

pentru schimbarea politicilor și practicilor statelor vecine sau aflate în sfera sa de influență dar și ale adversarilor, inclusiv SUA și NATO.

Utilizarea armelor nucleare de către Moscova este reglementată de Doctrina militară a Federației Ruse[41] - un sistem de principii pentru apărarea armată a țării care descrie și posibilele amenințări externe și interne dar și modalitățile de răspuns la acestea [42].

Punctul fundamental al acestei doctrine (ediția 2020)[43] îl reprezintă punctul 17 potrivit căruia „Federația Rusă își rezervă dreptul de a folosi arme nucleare ca răspuns la utilizarea armelor nucleare și a altor tipuri de arme de distrugere în masă împotriva acesteia și (sau) aliaților săi, precum și în cazul agresiunii împotriva Federației Ruse folosind arme convenționale, când însăși existența statului este amenințată" (Decretul Președintelui Federației Ruse din 02.06.2020 Nr.355, Указ Президента Российской Федерации от 02.06.2020 г. № 355, pct.17). De aici rezultă că Rusia poate lansa nu numai o lovitură nucleară, ci poate și răspunde prima dacă este atacată cu arme convenționale, dar în același timp viitorul său este pus în pericol.

Totodată, cuprinde și Fundamente ale politicii de stat în domeniul descurajării nucleare (Основах государственной политики Российской Федерации в области ядерного сдерживания) și enumeră pericolele împotriva cărora Moscova ar fi dispusă să folosească armele nucleare[44]. Acestea includ, dar nu se limitează la situațiile în care:

- Moscova are informații fiabile despre lansarea de rachete balistice care atacă teritoriul rus și/sau teritoriul aliaților săi;
- Rusia este atacată cu arme convenționale, ceea ce amenință însăși existența statului;

[41] *Adoptată la 25 decembrie 2014*
[42] *http://www.scrf.gov.ru/security/military/document129/*
[43] *Reactualizată la 2 iunie 2020*
[44] *http://www.kremlin.ru/acts/bank/45562*

- inamicul folosește arme nucleare sau alte tipuri de arme de distrugere în masă împotriva Rusiei și/sau aliaților săi;
- adversarul acționează împotriva guvernului rusesc sau a instalațiilor militare critice, care ar putea perturba răspunsul forțelor nucleare ruse.

De asemenea, la punctul 20 documentul precizează că decizia de a folosi arme nucleare trebuie să fie luată numai de președintele Rusiei, care poate informa autoritățile altor țări și/sau organizații internaționale despre acest lucru. *„Președintele Federației Ruse poate, dacă este necesar, să informeze conducerea politico-militar a altor state și (sau) organizații internaționale despre disponibilitatea Federației Ruse de a folosi arme nucleare sau despre decizia luată de a folosi arme nucleare, precum și despre folosirea lor" (Decretul Nr.355, pct.20).*

Odată cu escaladarea operațiunii militare speciale în Ucraina, subiectul descurajării nucleare a revenit însă în prim-plan[45] și chiar dacă în 2023, în contextul participării la ședința plenară a celei de-a XX–a ședințe aniversare a Clubului Internațional de Discuții Valdai, președintele rus Vladimir Putin[46] a dat asigurări că nu este nevoie de o modificare a doctrinei nucleare prin scăderea pragului nuclear[47], evoluțiile ulterioare, dar mai ales decizia Administrației Biden (din luna martie 2024) de a aproba reorientarea strategiei de descurajare nucleară a SUA, pentru a face față „posibilelor confruntări nucleare coordonate

---

[45] *A XX-a reuniune anuală a Clubului Internațional de Discuții Valdai pe tema: „Multipolaritate corectă: cum să asigurăm securitatea și dezvoltarea pentru toți" a avut loc în perioada 2-5 octombrie 2023 la Soci. La întâlnire au participat 140 de experți, politicieni, diplomați din 42 de țări din Eurasia, Africa, America de Nord și de Sud. https://ru.valdaiclub.com/events/own/xx-ezhegodnoe-zasedanie-mezhdunarodnogo-diskussionnogo-kluba-valday/*

[46] *Desfășurat la 5 octombrie 2023, la Soci*

[47] *http://kremlin.ru/events/president/news/72444*

cu Rusia, China și Coreea de Nord", ar putea influența decizia părții ruse.

Descurajarea nucleară și contextul geopolitic actual

După demararea operațiunii militare ruse în Ucraina, amenințările nucleare coercitive rusești și teama de escaladare nucleară au jucat un rol decisiv în stabilirea domeniului și momentului de acordare a ajutorului militar occidental Kievului.

Încă din anunțul oficial din 24 februarie 2022 privind începerea acestei operațiuni, Vladimir Putin s-a adresat celor „care pot fi tentați din exterior să intervină în evenimentele care au loc" avertizând că cei încearcă să „creeze amenințări la adresa țării ar trebui să știe că răspunsul Rusiei va fi imediat și va duce la consecințe pe care nu le-ați întâlnit niciodată în istoria voastră" (Vladimir Putin, Moscova, 24 februarie 2022)[48]. Mesajul a fost însoțit de decizia de a declanșa starea de alertă a forțelor nucleare ruse și întărit prin publicarea unei fotografii de la întâlnirea avută de președintele Vladimir Putin cu ministrul apărării Serghei Șoigu și cu șeful Statului Major Valeri Gerasimov[49]. Demersul a fost interpretat de experții în domeniu drept un mod de a întârit mesajul doctrinei sovietice, reînviat în timpul președintelui Boris Elțin, potrivit căruia armele nucleare rusești pot fi lansate numai cu acordul unanim și simultan al președintelui, ministrului apărării și al șefului Statului Major[50].

---

[48] *https://tass.ru/politika/13825671*

[49] *Caitlin Kennedy, Bradley Peniston, „What Just Happened With Putin's Nuclear Forces? Here's What Experts Say", Defence One, 27 februarie 2022, https://www.defenseone.com/threats/2022/02/what-just-happened-putins-nuclear-forces-heres-what-experts-say/362501/ (accesat la 29 august 2024)*

[50] *David Hoffman, "Cold War Doctrines Refuse to Die," Washington Post, March 15, 1998.*
https://www.washingtonpost.com/archive/politics/1998/03/15/cold-war-

Trei zile mai târziu (27 februarie 2022), Vladimir Putin a dat ordinul de a trece forțele nucleare strategice într-un regim special de alertă[51] iar șase luni mai târziu, la 21 septembrie 2022, anunțând mobilizarea parțială, președintele a dat asigurări că „cetățenii ruși pot fi siguri că integritatea teritorială a patriei noastre, independența și libertatea noastră vor fi asigurate, prin toate mijloacele" atenționând că "cei care încearcă să ne șantajeze cu arme nucleare ar trebui să știe că roza vânturilor se poate întoarce în direcția lor." (Vladimir Putin, Kremlin, 21 septembrie 2022)

De la acest anunț, Vladimir Putin și membrii guvernului său (în special Dmitri Medvedev) au făcut amenințări nucleare repetate, implicând o „linie roșie" pe care, dacă SUA și aliații săi ar ignora-o, Rusia ar putea răspunde cu arme nucleare. Există, de asemenea, indicii puternice că Rusia ar fi folosit amenințări nucleare și în comunicațiile bilaterale închise pentru a descuraja statele occidentale să ofere diverse forme de sprijin Ucrainei: furnizarea de arme cu rază lungă de acțiune, avioane și vehicule blindate de luptă.

Mai mult, pe fondul desfășurării Conferinței de revizuire a Tratatului de neproliferare a armelor nucleare /TNP (New York, 1 august 2022) [52], Vladimir Putin a reiterat principiul potrivit căruia „într-un război nuclear nu pot exista câștigători și nu ar trebui să fie declanșat niciodată"[53].

Principiul a fost adoptat pentru prima dată, în 1985, de liderii URSS și SUA, Mihail Gorbaciov și Ronald Reagan iar trei decenii mai târziu, în 2021, Vladimir Putin și cel de-al 46-lea

doctrines-refuse-to-die/c73be619-8d9d-4ab4-b23e-3764584e6439/ (accesat la 25 august 2024)

[51] *"Путин приказал привести силы сдерживания в особый режим боевого дежурства", https://www.rbc.ru/politics/27/02/2022/621b77959a79477dcca4c36f*

[52] *https://www.state.gov/translations/russian/конференция-по-рассмотрению-действи/*

[53] *https://www.rbc.ru/politics/01/08/2022/62e7f3459a7947e625a35a9f*

președinte american Joe Biden au confirmat acest lucru la Summit-ul de la Geneva[54] din 16 iunie 2021, urmând ca la 3 ianuarie 2022, și liderii celor „cinci state nucleare" - Marea Britanie, China, Rusia, SUA și Franța – să semneze o declarație comună privind prevenirea războiului nuclear și prevenirea cursei înarmărilor [55].

Ulterior, în noiembrie 2022, Ministerul rus de Externe a comunicat că Moscova se angajează să respecte această declarație. Partea rusă a subliniat că, deși urmărește o politică de descurajare nucleară, Moscova „este strict și consecvent ghidată de postulatul inadmisibilității războiului nuclear", reiterând caracterul „pur defensiv" al doctrinei nucleare ruse (MID, 2 noiembrie 2022)[56].

De-a lungul desfășurării conflictului, principala provocare a Rusiei însă a constat în a face aceste amenințări nucleare credibile. Descurajarea nucleară a părții ruse a funcționat, dar numai într-un mod limitat în timp, Occidentul declarând că va menține „opțiunile de pe masă" sau va amâna furnizarea de sisteme de arme critice Ucrainei. După perioada septembrie și octombrie 2022, Rusia și-a escaladat amenințările nucleare împotriva Kievului, susținând că Ucraina își dezvoltă propriile arme radiologice și declarând că rolul ei este de a apăra întreg teritoriul ucrainean.

În acest context, amenințările nucleare ale Rusiei au fost primite cu reținere, în primul rând pentru că Rusia a susținut că va folosi arme nucleare pentru a apăra teritoriul pe care nu îl ocupase încă dar, mai ales pentru că, în același timp, guvernele occidentale au lucrat pentru a crește costurile politice ale acestor

---

[54] *https://www.rbc.ru/politics/16/06/2021/60ca43689a79471ebf4e7cdc*

[55] *"Joint Statement of the Leaders of the Five Nuclear-Weapon States on Preventing Nuclear War and Avoiding Arms Races https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/03/p5-statement-on-preventing-nuclear-war-and-avoiding-arms-races/ (accesat la 28 august 2024)*

[56] *https://mid.ru/ru/foreign_policy/news/1836575/*

amenințări, persuadând proprii aliați și parteneri ai Rusiei să respingă amenințările Rusiei. De asemenea, partenerii Moscovei, China[57] și India[58] au dezaprobat public retorica nucleară rusă.

Drept urmare, semnalizarea nucleară a Rusiei a scăzut pentru o perioadă fiind limitată la declarații verbale ale experților la posturile de televiziune de la Moscova urmând ca dezbaterile ulterioare din spațiul public din Rusia cu privire la doctrina nucleară să fie deosebit de îngrijorătoare.

Semnificativ în acest sens este impactul mediatic pe care articolul publicat de Serghei Karaganov[59], șeful Consiliului pentru Politica Externă și de Apărare al Rusiei, în iunie 2023, în Rusia, în „Global Affairs", l-a avut atât în plan intern cât și extern. Serghei Karaganov a cerut impunerea de măsuri radicale pentru „restabilirea descurajării nucleare" cu Occidentul[60], reluarea testelor nucleare și creșterea pregătirii pentru luptă a forțelor strategice salutând "primii pași au fost deja făcuți prin anunțata desfășurare de arme nucleare în Belarus[61].

---

[57] Andreas Rinke and Eduardo Baptista, "Xi, Scholz warn against 'irresponsible' nuclear threats to Ukraine," Reuters, 4 November 2022, https://www.reuters.com/world/china/german-chancellor-scholz-lands-beijing-2022-11-04/

[58] "India's defense minister warns against nukes in call with Russian counterpart", Reuters, 26 October 2022, https://www.reuters.com/world/indias-defence-minister-warns-against-nuclear-weapons-call-with-russian-2022-10-26/

[59] Professor Emeritus National Research University–Higher School of Economics, Moscow, Russia, Faculty of World Economy and International Affairs Academic Supervisor; Council on Foreign and Defense Policy Honorary Chairman of the Presidium

[60] Serghei Karaganov, „A Difficult but Necessary Decision", Russia in Global Affairs, 13 iunie 2023, https://eng.globalaffairs.ru/articles/a-difficult-but-necessary-decision/ (accesat la 1 septembrie 2024)

[61] În 2023, Putin a spus că Rusia își va desfășura armele nucleare tactice în Belarus. Potrivit președintelui rus, vorbim de desfășurare, nu de transfer - la fel cum armele nucleare americane sunt desfășurate în țările NATO.

Recomandările sale au declanșat o dezbatere în cadrul comunității de experți din Rusia, culminând cu dezbaterea publică dintre acesta și președintele Vladimir Putin în marja participării la Sesiunea Clubului de Discuții Valdai din octombrie 2023[62].

În context, deși a respins posibilitatea unor atacuri nucleare directe asupra NATO, președintele Putin a anunțat că Rusia ”nu are motive pentru a-și revizui doctrina nucleară” dar a semnalat dorința de a reveni la testarea armelor nucleare sens în care a amintit efectuarea ultimului ”test de succes” al 9M730 Burevestnik[63] (în codificarea NATO - SSC-X-9 Skyfall) și finalizarea rachetei super-grea Sarmat (Vladimir Putin 5 octombrie 2023)[64].

Subsumat procesului de descurajare, Rusia și Belarus au început, la 16 iunie 2024, faza a doua a exercițiilor nucleare militare (demarate în luna mai a.c.) comandate de preşedintele Vladimir Putin, menite a desfăşura arme nucleare tactice.

Potrivit Ministerului rus al Apărării, scopul exercițiului militar a fost pregătirea armatelor ambelor țări pentru utilizarea în luptă a armelor nucleare tactice. Deși ministrul apărării din Belarus, general-locotenentul Viktor Khrenin, a precizat că ”este vorba despre disponibilitatea forței de muncă și a tehnologiei pentru utilizarea în luptă a armelor nucleare nestrategice ale Rusiei și Belarusului pentru a asigura suveranitatea necondiționată și integritatea teritorială a statului Uniunii”, unii experții au fost de părere că înarmarea nucleară a Belarusului face parte din strategia Moscovei de a ține în șah Polonia[65].

---

[62] *«Владимир Путин встретился с членами дискуссионного клуба «Валдай», стенограмма», Дискуссионный клуб «Валдай», 5 октября 2023 г. http://www.kremlin.ru/events/president/news/72444*

[63] O rachetă de croazieră cu rază globală de acțiune și cu sistem de propulsie nucleară

[64] *http://www.kremlin.ru/events/president/news/72444*

[65] *https://www.defenseromania.ro/moscova-a-inceput-a-doua-faza-a-manevrelor-nucleare-belarus-se-alatura-exercitiilor_628696.html*

În scenariul în care Armata Belarusului ar invada Lituania pentru a-și securiza zona din dreptul Coridorului Suwalki (profitând de un posibil context internațional în care NATO și SUA ar șovăi și nu ar aplica imediat Articolul 5) Polonia s-ar găsi într-o dilemă majoră: fie ajută militar statul baltic cu riscul ca dictatorul Lukașenko să lovească nuclear un oraș polonez, fie așteaptă decizia comună a Alianței, amânare care ar putea însemna pierderea frontierei comune cu Lituania.

Părerile experților sunt întărite și de declarațiile oficialului din Belarus, făcute în marja participăriil la ce-a de-a XI-a Conferință de la Moscova privind securitatea internațională, potrivit cărora ”Republica Belarus consideră returnarea armelor nucleare tactice pe teritoriul său ca un factor eficient de descurajare strategică” față de (Viktor Khrenin, Moscova, 15 august 2023) Occidentul colectiv care ”pentru a duce războaie prin procură, folosește jucătorii nestatali sub forma organizațiilor teroriste și criminale, mișcări religioase radicale și reprezentanți ai coloanei a cincea, uniți cu diasporele din străinătate”. Viktor Khrenin a indus idea că acești „jucători sunt cei care își intensifică încercările de a-și realiza interesele și de a câștiga un loc în ordinea mondială în curs de dezvoltare” și ”cu sprijinul Occidentului, își creează propriile formațiuni armate care pot fi folosite pentru a destabiliza statele țintă, pentru a ocupa o parte a teritoriului lor prin mijloace militare și pentru a crea noi entități quasi-statale pe acesta”[66].

În ceea ce privește poziția SUA, de-a lungul întregii perioade de desfășurare a conflictului din Ucraina, reprezentanții oficiali ai NATO și ai Statelor Unite au susținut periodic că nu văd schimbări în desfășurarea forțelor nucleare rusești și, prin urmare, nu este nevoie de măsuri de represalii în această zonă.

[66] *” Министр обороны Республики Беларусь генерал-лейтенант Виктор Хренин выступил на Московской конференции по международной безопасности” https://function.mil.ru/news_page/country/more.htm?id=12475984@egNews*

În iunie 2023, secretarul de stat al SUA Antony Blinken a declarat direct că Washingtonul nu va face modificări în configurația forțelor sale nucleare în legătură cu transferul armelor nucleare rusești în Belarus.

Publicarea de către Administrația americană a Nuclear Posture Review /NPR[67], în 2022, a evidențiat faptul că SUA se angajează pe deplin să implementeze programe care vor începe să pună pe teren sisteme modernizate mai târziu în acest deceniu[68].

În 2023, Rusia și Statele Unite au suspendat Tratatul privind măsurile pentru reducerea și limitarea în continuare a armelor strategice ofensive (START), semnat în 2010. Moscova și Washingtonul nu au mai efectuat inspecții și nu au mai facut schimb de informații, dar în același timp au promis că nu vor încălca acordul. În prezent, nu există negocieri pentru încheierea unui nou acord în această chestiune - odată cu izbucnirea unui conflict pe scară largă în Ucraina, acestea au fost înghețate de Statele Unite. Tot în 2023, Washington a invitat Moscova să revină la consultări, separându-le de tensiunile geopolitice generale, dar Moscova a refuzat, spunând că până când Statele Unite nu își abandonează cursul „pentru a provoca înfrângerea strategică Rusiei", astfel de contacte sunt imposibile[69].

La 20 august 2024, cotidianul American *The New York Times* a publicat însă un articol în care confirma că în luna martie 2024, președintele american Joe Biden a aprobat o nouă

---

[67] *La 27 octombrie 2022, administrația Biden a lansat în cele din urmă o versiune neclasificată a revizuirii Nuclear Posture Review (NPR) întârziată. NPR clasificat a fost aprobată de Congres în martie 2022, dar publicarea sa a fost întârziată substanțial – probabil din cauza invaziei Ucrainei de către Rusia. Nuclear Posture Review (NPR) este declarația principală a Pentagonului privind politica nucleară, produsă de ultimii patru președinți în primii lor ani de mandat.*

[68] *https://fas.org/publication/the-biden-administrations-nuclear-posture-review/*

[69] *https://www.rbc.ru/politics/02/12/2023/6569d9db9a7947e27de7dd2e*

„îndrumare privind ocuparea forței de muncă în domeniul nuclear", un document clasificat care subliniază modul în care SUA ar folosi armele nucleare într-un potențial conflict.

Conform articolului, documentul, actualizat la fiecare patru ani, reorientează strategia de descurajare nucleară a SUA pentru a face față extinderii masive a arsenalului nuclear al Chinei. Schimbarea strategiei este prezentată de Administrația Biden ca fiind bazată pe preocupările legate de „posibilele confruntări nucleare coordonate cu Rusia, China și Coreea de Nord" și extinderea stocului de arme nucleare chinezești[70].

Casa Albă a confirmat rapoartele din presă conform cărora președintele Statelor Unite ale Americii Joe Biden a aprobat un plan secret de reorientare a strategiei nucleare a SUA într-un mod mai agresiv. Purtătorul de cuvânt, Sean Savett, a spus că, deși „textul specific al ghidului este clasificat, existența acestuia nu este în niciun fel secretă" și că „nu a fost un răspuns la nicio singură entitate, țară sau amenințare"[71].

În iunie 2024, un director senior al Consiliului Național de Securitate, a declarat sub anonimat, că SUA se pregătește să-și schimbe strategia de la modernizarea armelor existente la extinderea arsenalul nuclear subliniind că SUA ar putea fi nevoite să desfășoare mai multe arme nucleare strategice în anii următori pentru a descuraja amenințările tot mai mari din partea Rusiei, Chinei și a altor adversari.

Declarațiile și deciziile Washington-ului au fost percepute cu neliniște de către China, Beijing-ul subliniind că "este o propunere falsă menită să servească și să mascheze amenințarea

---

[70] https://www.nytimes.com/2024/08/20/us/politics/biden-nuclear-china-russia.html

71 "Biden's Nuclear Employment Guidance is a stunning reversal of policy", https://thehill.com/opinion/national-security/4844624-biden-nuclear-policy-shift/

latentă în schimbarea strategiei SUA" și argumentând că „și după estimările SUA, arsenalul de arme nucleare al Chinei rămâne considerabil mai mic decât cel al SUA"[72].

În privința Rusiei, încă din iunie 2024, președintele rus Vladimir Putin a recunoscut că, dacă este necesar, doctrina nucleară internă ar putea fi schimbată. El a explicat că strategia este un „instrument viu", iar autoritățile ruse monitorizează îndeaproape situația din lume[73].

Acest lucru a fost văzut ca un răspuns la presiunile exercitate de adepții liniei dure din elita rusă, care consideră că Putin ar trebui să poată acționa mai rapid în cazul unei escaladări nucleare și să reducă limita de utilizare[74].

Liderul de la Kremlin este convins că Moscova ar trebui să acorde atenție dezvoltării „dispozitivelor nucleare explozive de putere ultra-scăzută", a căror utilizare în Occident este percepută drept „nimic greșit"[75].

Ulterior, ministrul adjunct de externe al Rusiei, Serghei Riabkov, a anunțat (1 septembrie 2024) că „procesul de ajustare fină" a modificărilor în doctrina nucleară a Rusiei este acum în curs și "există o direcție clară de a face o corectare, care se datorează și studiului și analizei experienței de dezvoltare a conflictelor din ultimii ani, inclusiv de tot ce ține de escaladarea

---

[72] *https://www.chinadailyhk.com/hk/article/591209*

[73] *Conform declarațiilor făcute la 20 iunie 2024, în timpul unei conferințe de presă după vizita sa în Vietnam*

[74] "*Путин увязал возможность изменения ядерной доктрины с решениями Запада", 20 iunie 2024, https://www.interfax.ru/russia/967397*

[75] "*Почему Путин заявил об обсуждении изменений в ядерной доктрине России", https://www.vedomosti.ru/politics/articles/2024/06/20/1045223-pochemu-putin-zayavil-ob-obsuzhdenii*

cursului oponenților noștri occidentali în legătură cu Districtul Militar de Nord”[76].

În opinia sa, situația din jurul operațiunii militare speciale din Ucraina a arătat că descurajarea nucleară nu mai este pe deplin eficientă. Totodată, a recunoscut că, în viitor, Rusia ar putea specifica în doctrina sa nucleară cum va răspunde la escaladarea în continuare a conflictului de către oponenții săi.

În paralel, în plan intern, cele mai multe publicații centrale au readus în atenție narative privind apartenența Rusiei la grupul celor trei țări care dețin triade nucleare (Rusia, SUA și China) și componentele deținute de Federația Rusă cu accent pe supremația sa militară.

Concluzii

Pe tot parcursul războiului său împotriva Ucrainei, Rusia a folosit strategic, cu succes retorica și semnalele nucleare pentru a încetini viteza livrărilor de arme, pentru a restricționa tipurile de arme livrate și pentru a preveni utilizarea acestora împotriva unor anumite tipuri de ținte.

Scopul principal al amenințărilor nucleare coercitive rusești a fost acela de a convinge factorii de decizie ai NATO că costurile potențiale ale rezistenței la obiectivele politice ale Rusiei ar putea duce la război nuclear și, prin urmare, depășesc cu mult beneficiile unei astfel de rezistențe.

Retorica nucleară rusă este orientată spre interiorul țării și poate fi destul de revelatoare despre ceea ce crede Rusia despre ea însăși, precum și despre amploarea și direcția dinamicii interne a puterii politice și militare ruse și o altă parte este direcționată spre extern, Statele Unite jucând un rol special în

76 ”Рябков: РФ изменит ядерную доктрину на основе анализа действий Запада в связи с СВО”, 1 septembrie 2024, https://tass.ru/politika/21738323

răspuns, deoarece multe dintre semnalele nucleare ale Rusiei destinate publicului extern sunt îndreptate către Washington, urmate de Regatul Unit și Franța care joacă, de asemenea, un rol special ca puteri nucleare și aliați NATO.

Schimbarea anunțată de către Washington în strategia sa nucleară a fost prezentată de Beijing și Moscova drept un demers care va influența negativ percepția comunității internaționale despre armele nucleare și va avea un impact asupra eforturilor de prevenire a răspândirii armelor nucleare în alte țări. De asemenea, Moscova susține că nu numai că va perturba echilibrul nuclear relativ de la sfârșitul Războiului Rece, dar va declanșa și o nouă rundă de reajustări în pozițiile nucleare ale țărilor aliate, deoarece va declanșa inevitabil o spirală de neliniște strategică sporită, iar SUA ar trebui să joace un rol cheie în eforturile globale pentru controlul armelor și neproliferarea nucleară.

Faptul că în discursul oficialilor de la Moscova și Beijing a apărut tot mai frecvent apelul adresat comunității internaționale, factorilor de decizie, experților și cetățenilor privind exprimarea de către aceștia a obiecțiilor față de „normalizarea de către SUA a posibilității de utilizare a armelor nucleare pentru a evita un alt moment Oppenheimer” poate fi interpretat drept o încercare a celor două părți de a obține o poziție avantajoasă în eventualitatea deschiderii unui proces de negociere.

Referințe

- *http://www.scrf.gov.ru/security/military/document129/*
- *https://www.rbc.ru/politics/02/12/2023/6569d9db9a7947e27de7dd2e*
- *https://www.nytimes.com/2024/08/20/us/politics/biden-nuclear-china-russia.html*

- *http://kremlin.ru/events/president/news/72444*
- *https://www.chinadailyhk.com/hk/article/591209*
- *https://www.interfax.ru/russia/967397*
- *https://tass.ru/politika/21738323*
- *https://www.defenseone.com/threats/2022/02/what-just-happened-putins-nuclear-forces-heres-what-experts-say/362501/*
- *https://www.washingtonpost.com/archive/politics/1998/03/15/cold-war-doctrines-refuse-to-die/c73be619-8d9d-4ab4-b23e-3764584e6439/*
- *https://www.rbc.ru/politics/27/02/2022/621b77959a79477dcca4c36f*
- *https://www.state.gov/translations/russian/конференция-по-рассмотрению-действи/*
- *https://www.rbc.ru/politics/01/08/2022/62e7f3459a7947e625a35a9f*
- *https://www.rbc.ru/politics/16/06/2021/60ca43689a79471ebf4e7cdc*
- *https://thehill.com/opinion/national-security/4844624-biden-nuclear-policy-shift/*
- *https://fas.org/publication/the-biden-administrations-nuclear-posture-review/*
- *https://www.rbc.ru/politics/02/12/2023/6569d9db9a7947e27de7dd2e*
- *https://www.nytimes.com/2024/08/20/us/politics/biden-nuclear-china-russia.html*

Evoluția și revoluția inteligenței artificiale

Lt. col. (r) Ing. fiz. Nicolae Sfetcu, MPhil[77*]
(Membru susținător al Asociației Ofițerilor în Rezervă din România și membru al Grupului de Lucru pentru Securitate și Apărare Cibernetică)

Rezumat

Călătoria inteligenței artificiale este marcată de repere semnificative, de la începuturile sale în anii 1950 la schimbarea de paradigmă a algoritmilor simbolici și dezvoltarea sistemelor expert în anii 1970, introducerea învățării automate în anii 1990 și algoritmii de învățare profundă din anii 2010. Fiecare fază a adus noi capabilități și provocări, propulsând IA de la sisteme rudimentare bazate pe reguli la entități complexe, autonome de luare a deciziilor. Privind în perspectivă, IA este gata să-și depășească limitările actuale, alimentată de creșterea exponențială a puterii de calcul, a disponibilității datelor și a sofisticării algoritmice.

Cuvinte cheie: inteligența artificială,, testul Turing, iarna inteligenței artificiale, perceptron, învățarea profundă, big data, rețele neuronale, ChatGPT

[*] Cercetător - Academia Română - Comitetul Român de Istoria și Filosofia Științei și Tehnicii (CRIFST) , Divizia de Istoria Științei (DIS), ORCID: 0000-0002-0162-9973

Introducere

Călătoria inteligenței artificiale este marcată de repere semnificative, de la începuturile sale în anii 1950 la schimbarea de paradigmă a algoritmilor simbolici și dezvoltarea sistemelor expert în anii 1970, introducerea învățării automate în anii 1990 și algoritmii de învățare profundă din anii 2010. Fiecare fază a adus noi capabilități și provocări, propulsând IA de la sisteme rudimentare bazate pe reguli la entități complexe, autonome de luare a deciziilor. Privind în perspectivă, IA este gata să-și depășească limitările actuale, alimentată de creșterea exponențială a puterii de calcul, a disponibilității datelor și a sofisticării algoritmice.

Pe parcursul evoluției IA au existat mai multe schimbări de paradigmă (AlgorithmWatch 2024), în care au fost puse bazele celor mai cunoscute metode și algoritmi IA, s-au dezvoltat algoritmii simbolici și sistemele expert (sisteme bazate pe cunoaștere), și învățarea automată și învățarea profundă prin disponibilitatea crescută a datelor digitale și puterea de calcul.

Semințele IA moderne au fost plantate de filozofi care au încercat să descrie procesul gândirii umane ca fiind manipularea mecanică a simbolurilor. Acest concept a culminat cu inventarea computerului digital programabil în anii 1940.

Apariția inteligenței artificiale (1941-1956)
Primele succese

Cibernetica lui Norbert Wiener a descris controlul și stabilitatea în rețelele electrice. Teoria informației a lui Claude Shannon a descris semnalele digitale (binare). Teoria de calcul a lui Alan Turing a arătat că orice formă de calcul poate fi descrisă digital. Relația strânsă dintre aceste idei a sugerat că ar putea fi posibilă construirea unui „creier electronic”.

În anii 1950, au apărut două viziuni despre dezvoltarea inteligenței artificiale. O abordare, sprijinită printre alții de Allen Newell, Herbert A. Simon și Marvin Minsky, a fost IA simbolică (GOFIA), apelând la o reprezentare simbolică a lumii și a sistemelor care ar putea raționa despre lume. Aceasta s-a bazat pe „căutarea euristică", care necesită explorarea unui spațiu de posibilități pentru răspunsuri. A doua abordare, susținută de Frank Rosenblatt, este cea conexionistă, care a încercat să obțină IA prin învățare, încercând să conecteze perceptronul (un algoritm de învățare supravegheată) în moduri inspirate de conexiunile neuronilor (Manyika 2022, 9).

Abordările simbolice au dominat căutările pentru inteligența artificială în această perioadă, favorizată de tradițiile intelectuale ale lui Descartes, Boole, Gottlob Frege, Bertrand Russell și alții. Abordările conexioniste au renăscut în ultimele decenii (Manyika 2022, 10).

Proiectele de cercetare IA au primit finanțări generoase în această perioadă.

1941: Alan Turing a publicat o lucrare despre inteligența mașinilor care ar putea fi cea mai veche lucrare din domeniul IA (E. by B. J. Copeland 2004).

1943: Walter Pitts și Warren McCulloch au analizat rețele de neuroni artificiali idealizați, și au arătat cum aceștia ar putea îndeplini funcții logice simple (McCulloch și Pitts 1943).

1950: Alan Turing a publicat lucrarea „Computing machinery and intelligence" (Turing 1950), luând în considerare întrebarea fundamentală „Pot mașinile să gândească?", în care a speculat cu privire la posibilitatea de a crea mașini care gândesc, incluzând conceptul său cunoscut sub numele de "testul Turing": Dacă testul Turing implică o mașină care ar purta o conversație care nu se poate distinge de o conversație cu o ființă umană, atunci este rezonabil să spunem că mașina este inteligentă. Testul Turing a fost primul experiment propus să măsoare inteligența mașinilor.

Au fost construiți primii roboți experimentali, precum țestoasele lui W. Gray Walter și Bestia Johns Hopkins, fiind controlați în întregime de circuite analogice (McCorduck 2004, 98).

1951: Christopher Strachey a scris un program de dame, iar Dietrich Prinz a scris unul pentru șah (J. Copeland 2000).

Marvin Minsky a construit prima mașină de rețea neuronală, SNARC (McCorduck 2004, 102).

1952: Primul program care a demonstrat că computerele pot învăța și nu doar să realizeze ceea ce sunt programați pentru a face, a fost în jocul de dame (Samuel 1960, 165–92).

1955: Allen Newell și Herbert A. Simon au creat „Logic Theorist", care a demonstrat 38 din primele 52 de teoreme din cartea *Principia Mathematica* (Whitehead și Russell 1927) a lui Russell și Whitehead și a găsit demonstrații noi și mai elegante pentru altele (McCorduck 2004, 123–25). Au introdus concepte critice în inteligența artificială, cum ar fi euristica, procesarea listelor, „raționamentul ca și căutare" etc. (Newell, Shaw, și Simon 1962) Simon considera că au „rezolvat venerabila problemă minte/corp, explicând modul în care un sistem compus din materie poate avea proprietățile minții." (Russell și Norvig 2016, 17)

1956: Atelierul de lucru de la Dartmouth a marcat începutul oficial al inteligenței artificiale ca disciplină academică (McCorduck 2004, 111–36). A fost organizat de Marvin Minsky, John McCarthy, Claude Shannon și Nathan Rochester, având ca obiectiv aprofundarea posibilităților de a crea mașini capabile să simuleze inteligența umană, testând afirmația potrivit căreia „fiecare aspect al învățării sau orice altă trăsătură a inteligenței poate fi descrisă atât de precis încât să poată fi făcută o mașină să o simuleze" (McCarthy et al. 2006). Termenul „inteligență artificială" a fost introdus oficial de John McCarthy la atelier, devenind numele domeniului științific Declarația principală a conferinței a fost: „Fiecare aspect al

oricărei altei caracteristici de învățare sau inteligență ar trebui să fie descris cu acuratețe, astfel încât mașina să o poată simula" (Russell și Norvig 2016).

În toamna anului 1956 a avut loc o întâlnire a Grupului de interes special în teoria informației de la Institutul de Tehnologie din Massachusetts care a fost începutul „revoluției cognitive", care folosește instrumente conexe diverselor domenii pentru a modela mintea. Abordarea cognitivă ia în considerare „obiecte mentale" (gânduri, planuri, scopuri, fapte sau amintiri), analizate folosind simboluri de nivel înalt în rețele funcționale.

Primele succese (1956-1974)

Între1960 și 1970 s-au dezvoltat abordările simbolice, ajutate și de predicțiile exagerate ale oamenilor de știință (Newquist 1994, 86).

IA simbolică (sau „GOFIA") (Haugeland 1985, 112–17) a simulat raționamentul uman în rezolvarea problemelor. În anii 1960, Newell și Simon au propus ipoteza sistemelor de simboluri fizice: „Un sistem de simboluri fizice are mijloacele necesare și suficiente de acțiune generală inteligentă." (Russell și Norvig 2016, 18) A avut mare succes la sarcini „inteligente", precum algebra sau testele de IQ, dar a eșuat în sarcini pe care oamenii le rezolvă cu ușurință, cum ar fi învățarea, recunoașterea unui obiect sau raționamentul de bun simț (paradoxul lui Moravec (M. Minsky 1986, 29)).

Hubert Dreyfus a susținut încă din anii 1960 că expertiza umană depinde mai degrabă de instinctul inconștient decât de manipularea conștientă a simbolurilor, și de a avea o „simțire" a situației, mai degrabă decât de cunoștințe simbolice explicite (Dreyfus și Dreyfus 1986).[169]

1957: Rosenblatt a descoperit perceptronul, prezis a fi „embrionul unui computer electronic care va fi capabil să meargă, să vorbească, să vadă, să scrie, să se reproducă și să fie conștient de existența sa", și odată cu el a apărut conexionismul,

fundația rețelelor neuronale și a învățării profunde (Rosenblatt 1962).

1961: Machine Educable Nougats And Crosses Engine (MENACE) a fost unul dintre primele programe capabile să învețe să joace un joc perfect de Tic-Tac-Toe (Michie 1963).

1965: ELIZA era un sistem de procesare a limbajului natural care imita un medic. ELIZA a răspuns la întrebări ca un psihoterapeut (Weizenbaum 1966).

1969: Shakey the Robot a fost primul robot mobil de uz general capabil să-și raționeze acțiunile. Acest proiect a integrat cercetarea în robotică cu viziunea computerizată și procesarea limbajului natural, fiind astfel primul proiect care a combinat raționamentul logic și acțiunea fizică (Raphael 1972).

Cartea „Perceptrons" a evidențiat limitele nerecunoscute ale structurii perceptronului în două straturi. Perceptronii marchează începutul iernii IA a anilor 1970 (M. Minsky și Papert 1988).

1970: MYCIN a fost un sistem expert specializat în diagnosticarea bolilor de sânge și prescrierea de medicamente. A adoptat un calcul al incertitudinii care părea să se potrivească bine cu evaluarea medicilor cu privire la diagnostic (Shortliffe et al. 1975).

1972: A fost dezvoltat Prolog, un limbaj de programare simbolic realizat de Alain Colmerauer împreună cu Philippe Roussel (Colmerauer și Roussel 1993).

Abordări ale IA

În primele decenii de după nașterea IA au existat multe programe de succes și noi direcții, precum:

- **Raționamentul ca o căutare**: Astfel de programe IA timpurii au mers pas cu pas spre obiectiv. Problema era numărul de căi posibile extrem de mare („explozie combinatorie"), reducerea acestora făcându-se folosind euristici sau „reguli

generale", cu riscul de a nu ajunge la o soluție (McCorduck 2004, 246–82).

- **Rețele neuronale**: Frank Rosenblatt a construit mașini perceptron (1957-1962) de până la patru straturi (Rosenblatt 1962). Bernard Widrow și Ted Hoff au folosit ponderi reglabile (Widrow și Lehr 1990). Charles A. Rosen și Alfred E. (Ted) Brain, cu finanțare de la U.S. Army Signal Corps, au folosit, de asemenea, greutăți reglabile (N. J. Nilsson 1984), putând clasifica simboluri pe hărțile armatei și recunoaște caracterele imprimate manual pe foile de codare Fortran. Sistemele construite în această perioadă foloseau hardware personalizat.
- **Limbajul natural**: Un obiectiv al cercetării IA a fost să permită computerelor să comunice în limbi naturale. În acest scop s-au folosit rețele semantice reprezentând concepte ca noduri, și relații între concepte ca legături între noduri. În acest fel a fost construit primul chatterbot, ELIZA al lui Joseph Weizenbaum, care putea desfășura conversații foarte realiste (Weizenbaum 1966).
- **Micro-lumi**: La finele anilor '60, Marvin Minsky și Seymour Papert au propus ca cercetarea IA să se concentreze pe situații simple artificiale cunoscute sub numele de micro-lumi (modele simplificate) (McCorduck 2004, 299–305).
- **Automate**: În Japonia a fost construit primul robot umanoid „inteligent" (android) la Universitatea Waseda (WABOT) în perioada 1967-1972 (Zeghloul, Laribi, și Gazeau 2016).

Prima iarnă a IA (1974–1980)

Prima iarnă a IA s-a prefigurat din anii 1970, din cauza promisiunilor neîndeplinite, a așteptărilor vaste și a dificultăților financiare. Deficiențele IA au fost explicate în două rapoarte: a) raportul Comitetului consultativ de procesare automată a limbajului (ALPAC) al Guvernului SUA (Committee 1966) și

b) raportul Lighthill (Science Research Council 1973) al guvernului britanic.

Optimismul foarte mare al cercetătorilor IA a ridicat așteptările publicului incredibil de mari, iar când rezultatele promise nu s-au materializat, au apărut criticile și finanțarea aproape a dispărut. Explorarea rețelelor neuronale artificiale a fost oprită parțial din cauza cărții lui Marvin Minsky care sublinia limitele perceptronilor (Crevier 1993, 100–144).

La începutul anilor șaptezeci, toate programele erau, într-un anumit sens, „jucării" (Crevier 1993, 146). Cercetătorii IA au început să se lovească de câteva limite fundamentale care nu au putut fi depășite în acea perioadă:

- *Putere limitată a computerului*: Memorie și viteză de procesare insuficiente. Hans Moravec a susținut în 1976 că computerele erau încă de milioane de ori prea slabe pentru a prezenta inteligență (Moravec, Stanford, și California 94305 1976).
- *Intractabilitate*: În 1972, Richard Karp a arătat că există multe probleme care pot fi rezolvate doar în timp exponențial (în dimensiunea intrărilor). Găsirea soluțiilor optime la aceste probleme necesită cantități inimaginabile de timp pe calculator (Russell și Norvig 2016, 9, 21–22).
- *Cunoștințe și raționament de bun simț*: Multe aplicații importante de inteligență artificială, cum ar fi viziunea sau limbajul natural, necesită pur și simplu cantități enorme de informații despre lume. Nimeni în 1970 nu putea construi o bază de date atât de mare și nimeni nu știa cum un program ar putea învăța atât de multe informații (McCorduck 2004, 300, 421).
- *Paradoxul lui Moravec*: Demonstrarea teoremelor și rezolvarea problemelor de geometrie este relativ ușoară pentru computere, dar o sarcină presupus simplă precum recunoașterea unei fețe. sau traversarea unei camere, este extrem de dificilă (McCorduck 2004, 456).

- *Problemele de cadru și de calificare*: Cercetătorii IA au descoperit că nu pot folosi logica pentru a reprezenta deducții obișnuite care implică planificare sau raționament implicit fără a aduce modificări structurii logicii în sine. Au fost dezvoltate noi logici (precum logica nemonotonă și logica modală) pentru a încerca să rezolve problemele (Crevier 1993, 117–19).

Unii filozofi au avut obiecții puternice față de afirmațiile făcute de cercetătorii IA. John Lucas, a susținut că teorema de incompletitudine a lui Gödel a arătat că un sistem formal (cum ar fi un program de calculator) nu poate vedea niciodată adevărul anumitor afirmații, în timp ce o ființă umană l-ar putea vedea (Crevier 1993, 22).

Hubert Dreyfus a ridiculizat promisiunile din anii 1960 și a criticat ipotezele IA, argumentând că raționamentul uman implică de fapt foarte puțină „prelucrare a simbolurilor" și o mare cantitate de „know how" întruchipat, instinctiv, inconștient (Dreyfus și Dreyfus 1986).

Argumentul camerei chinezești al lui John Searle, prezentat în 1980, a încercat să arate că nu se poate spune că un program „înțelege" simbolurile pe care le folosește (o calitate numită „intenționalitate"). Dacă simbolurile nu au nicio semnificație pentru mașină, a argumentat Searle, atunci mașina nu poate fi descrisă ca „gândire" (Russell și Norvig 2016, 958–60).

Minsky a spus despre Dreyfus și Searle că „înțeleg greșit și ar trebui ignorați." (Crevier 1993, 143)

Perceptronul (o formă de rețea neuronală introdusă în 1958 de Frank Rosenblatt) a fost finanțat de-a lungul anilor 1960, dar dezvoltarea sa s-a oprit brusc odată cu publicarea cărții din 1969 a lui Minsky care a sugerat că existau limitări severe și că predicțiile lui Frank Rosenblatt au fost exagerate. Competiția pentru finanțarea guvernamentală s-a încheiat cu victoria abordărilor simbolice ale inteligenței artificiale (Rodríguez 1991, cap. 2. 3).

Logica a fost introdusă în cercetarea IA încă din 1959, de către John McCarthy în *Advice Taker* (Russell și Norvig 2016, 19, 23). O abordare de succes a logicii, dezvoltată în anii 1970 de Robert Kowalski în colaborare cu cercetătorii francezi Alain Colmerauer și Philippe Roussel, a dus la crearea limbajului de programare logic Prolog, care folosește un subset de logică (clauzele Horn, strâns legate de „reguli" și „reguli de producție") care permit calculul tratabil (Crevier 1993, 145–149, 193–96, 258–263). Criticii abordării logice au remarcat că ființele umane folosesc rareori logica atunci când rezolvă probleme. McCarthy a răspuns că ceea ce fac oamenii este irelevant. El a susținut că ceea ce este cu adevărat necesar sunt mașini care pot rezolva probleme, nu mașini care gândesc așa cum fac oamenii (McCarthy 1979).

Marvin Minsky, Seymour Papert și Roger Schank încercau să rezolve probleme precum „înțelegerea poveștii" și „recunoașterea obiectelor" care necesitau ca o mașină să gândească ca o persoană. Gerald Sussman a observat că „folosirea unui limbaj precis pentru a descrie concepte esențial imprecise nu le face mai precise." (Crevier 1993, 168, 175) Schank a descris abordările lor „anti-logice" ca fiind „scruffy" (dezordonate), spre deosebire de paradigmele „îngrijite" folosite de McCarthy, Kowalski, Feigenbaum, Newell și Simon. În 1975, Minsky a apelat la seturi structurate de ipoteze denumite de el „cadre", sau .„scripte" în concepția lui Schank (Crevier 1993, 170–73).

Pat Hayes a susținut că „majoritatea „cadrelor" este doar o nouă sintaxă pentru părți ale logicii de ordinul întâi", dar „există unul sau două detalii aparent minore care dau, totuși, o mulțime de probleme, în special implicite" (Hayes 1981, 451–58). Ray Reiter a admis că „logicilor convenționale, cum ar fi logica de ordinul întâi, le lipsește puterea expresivă de a reprezenta în mod adecvat cunoștințele necesare raționamentului în mod implicit" (K. L. Clark 1978, 29–37). El a propus extinderea logicii de ordinul întâi cu o presupunere a lumii închise că o concluzie este

valabilă (în mod implicit) dacă contrariul nu poate fi demonstrat, care ar corespunde ipotezei de bun simț făcută în raționamentul cu cadre. Asumarea lumii închise, conform lui Reiter, „nu este o noțiune de ordinul întâi. (Este o noțiune meta.)" (K. L. Clark 1978, 29–37) La sfârșitul anilor 1970 și de-a lungul anilor 1980, au fost dezvoltate o varietate de logici și extensii ale logicii de ordinul întâi atât pentru negație, cât și pentru eșecul în programarea logică, și pentru raționamentul implicit mai general, incluse în conceptul de logici non-monotone.

Un efect negativ în recunoașterea progreselor în IA l-a avut așa-numitul „efect IA"., care se referă la tendința oamenilor de a minimiza succesele în IA atunci când un anumit comportament inteligent ajunge să fie utilizat în viața de zi cu zi a utilizatorilor.

Prima perioadă de avânt a IA (1980–1987)

În anii 1990 IA a obținut un mare succes comercial și respectabilitate academică concentrându-se pe sub-probleme specifice, folosind rețelele neuronale artificiale și învățarea automată statistică.

Sisteme expert

În anii 1980 s-a dezvoltat o nouă direcție în cercetare, IA simbolică și o formă de program IA numită „sisteme expert" sau „sisteme bazate pe cunoaștere". Aceste sisteme erau formate din două componente: 1) baza de cunoștințe (o colecție de fapte, reguli și relații pe un anumit domeniu); și 2) motorul de inferență (manipularea și combinarea aceste simboluri). Lisp și Prolog au fost principalele limbaje de programare simbolică. Companiile ofereau clienților pachete software numite „motoare de inferență" (Joint Research Centre (European Commission), Samoili, et al. 2020).

Guvernul japonez a finanțat computerele de generația a cincea. De asemenea conexionismul a renăscut prin lucrarea lui John Hopfield și David Rumelhart (Newquist 1994, 189–92).

Sistemele expert sunt programe care răspund la întrebări sau rezolvă probleme despre un anumit domeniu de cunoaștere, folosind reguli logice derivate din cunoștințele experților (McCorduck 2004, 327–35), evitând astfel problema cunoștințelor de bun simț.

Conform lui Huang și Smith (Huang și Smith 2006), sistemele expert modelează expertiza umană din domenii specifice de cunoaștere, implicând trei componente de bază: o bază de date; un motor de inferență; și o interfață pentru interacțiunile cu utilizatorul. K. S. Metaxiotis et al definește următoarele caracteristici specifice ale sistemelor expert: (Metaxiotis și Samouilidis 2000)

- utilizarea logicii simbolice mai degrabă decât calcule numerice;
- procesarea este bazată pe date;
- bază de date cu cunoștințe din anumite domenii de cunoaștere; și
- abilitatea de a interpreta concluziile pe înțelesul utilizatorului.

Sistemele expert au întâmpinat probleme tehnologice și limitări de performanță care au afectat dezvoltarea și implementarea lor: inexistența standardelor și interoperabilitatea, achiziția și analiza de cunoștințe, gestionarea situațiilor incerte (unele sisteme încorporează logica fuzzy ca soluție), integrarea sistemului (pentru sistemele bazate pe LISP, de ex.), validarea (nu există specificații clare în tehnicile de validare) (Huang și Smith 2006).

De asemenea, sistemele expert s-au confruntat cu provocări manageriale și organizaționale, precum alinierea tehnologiei și a strategiei de afaceri, costul de întreținere, erorile în abordările juridice, rezistența utilizatorilor (ocuparea locurilor de muncă),

aspecte legislative privind drepturile de autor și proprietatea intelectuală.

Cercetătorii au început să se îndoiască de posibilitățile abordării simbolice în IA, analizând abordările „subsimbolice" ale problemelor specifice ale IA (Nils J. Nilsson 1998, 7). Interesul pentru rețelele neuronale, sistemele fuzzy, teoria sistemului Gray, calculul evolutiv și multe instrumente extrase din statistică sau optimizare matematic, și „conexionism", a fost reînviat de Geoffrey Hinton, David. Rumelhart și alții la mijlocul anilor 1980 (Russell și Norvig 2016, 25).

Odată cu succesul rețelelor neuronale, al tehnologiei CASE și al altor tehnologii de ultimă generație, viitorul sistemelor expert pare strălucitor, în ciuda eșecurilor anterioare (Huang și Smith 2006).

Revoluția cunoașterii

„Cercetătorii IA au început să suspecteze – fără tragere de inimă, pentru că au încălcat canonul științific al parcimoniei – că inteligența s-ar putea foarte bine să se bazeze pe capacitatea de a folosi cantități mari de cunoștințe diverse în moduri diferite" (McCorduck 2004, 299). Sistemele bazate pe cunoaștere și ingineria cunoștințelor au devenit un obiectiv major al cercetării IA în anii 1980.

În anii 1980 s-a încercat pentru prima dată să se rezolve problema cunoștințelor de bun simț în mod direct, prin crearea unei baze de date masive. Așa au apărut programele de joc de șah care au învins maeștrii de șah în 1989 (Newquist 1994, 431–55).

Reînvierea rețelelor neuronale

În 1982, John Hopfield a demonstrat că o formă de rețea neuronală (denumită acum „rețea Hopfield") poate învăța și

procesa informații și converge după suficient timp în orice condiție fixă (Sejnowski 2018, 93–94).

Geoffrey Hinton și David Rumelhart au popularizat o metodă de antrenament a rețelelor neuronale numită „retropropagare", aplicată rețelelor neuronale de Paul Werbos, revigorând rețelele neuronale artificiale, utilizate în recunoașterea optică a caracterelor și recunoașterrea vorbirii (Russell și Norvig 2016, 25).

Realizări

1982: „Rețeaua Hopfield", o formă de rețea neuronală (Hopfield 1982) și „retropropagarea" (Rumelhart, Hinton, și Williams 1988) au reînviat domeniul IA.

1983: A fost dezvoltat ID3, un algoritm care generează un arbore de decizie dintr-un set de date, precursorul algoritmului C4.5 utilizat în învățarea automată și procesarea limbajului natural (Quinlan 1986, 93–94).

A doua iarnă a IA (1987–1993)

La sfârșitul anilor 1980, câțiva cercetători au susținut o abordare complet nouă a inteligenței artificiale, bazată pe robotică (McCorduck 2004, 454–62). În 1990, Rodney Brooks a atacat ipoteza sistemului de simboluri fizice, argumentând că simbolurile nu sunt întotdeauna necesare, deoarece „lumea este cel mai bun model al ei, exact la zi. Are întotdeauna fiecare detaliu care trebuie cunoscut. Trucul este să îl simți în mod adecvat și suficient de des." (Brooks 1990, 3) Mulți oameni de știință cognitivă au respins, de asemenea, modelul de procesare a simbolurilor a minții și au susținut că corpul era esențial pentru raționament, o teorie numită teza minții întrupate (Lakoff și Johnson 1999).

Primul indiciu al unui nou declin al cercetării IA a fost prăbușirea bruscă a pieței pentru hardware specializat în 1987,

precum mașinile Lisp produse de Symbolics și Prolog, considerate prea scumpe și costisitoare de întreținut, față de computerele Apple și IBM. Sistemele expert s-au dovedit utile, dar numai în câteva contexte speciale. Finanțarea IA a fost tăiată „profund și brutal" (McCorduck 2004, 430–31). Au fost închise sute de companii de inteligență artificială până la sfârșitul anului 1993 (Newquist 1994, 440). Mulți cercetători au continuat să lucreze folosind alte nume specifice disciplinei: sisteme cognitive, sisteme inteligente, reprezentare a cunoștințelor și raționament, pentru a avea acces la finanțare.

Realizări

1989: Citirea cifrelor scrise de mână folosind rețele neuronale convoluționale (Y. LeCun et al. 1989, 541–51).

Conceptul de Q-learning, care îmbunătățește învățarea prin întărire prin optimizare fără a modela probabilitățile de tranziție sau recompensele așteptate ale procesului de decizie Markov (Watkins 1989).

1993: „Învățarea foarte profundă", care necesita peste 1.000 de straturi în rețeaua neuronală recurentă (Joint Research Centre (European Commission), Samoili, et al. 2020).

A doua perioadă de avânt a IA (1993–2011)

La începutul secolului XX, IA a început să fie folosit cu succes, în parte datorită creșterii puterii computerului și prin concentrarea pe probleme izolate specifice. În perioada 1990-2010, IA a abordat probleme complexe, oferind soluții care s-au dovedit a fi utile în diferite domenii de aplicație, inclusiv extragerea datelor, robotică industrială, logistică, business intelligence, software bancar, diagnostic medical, sisteme de recomandare și motoare de căutare. Multe probleme de IA au fost abordate de către cercetători din domenii precum matematică,

economie sau cercetarea operațională. Astfel IA s-a fragmentat în subdomenii concurente axate pe probleme sau abordări particulare, uneori chiar sub denumiri noi, ferindu-se de numele compromis de „inteligența artificială” (McCorduck 2004, 424).

O nouă paradigmă numită „agenți inteligenți” s-a dezvoltat în anii 1990, percepând mediul și întreprinzând acțiuni care le maximizează șansele de succes. Astfel, paradigma agentului inteligent definește cercetarea IA ca „studiul agenților inteligenți”. Paradigma a permis studierea problemelor izolate și găsirea de soluții care erau atât verificabile, cât și utile, oferind un limbaj comun pentru a descrie problemele și a împărtăși soluțiile și cu alte domenii (McCorduck 2004).

Noile sisteme au început să apeleze la teoria probabilității și a deciziei, utilizând noi instrumente noi precum rețele bayesiene, modele Markov ascunse, teoria informației, modelarea stocastică și optimizarea clasică. Au fost dezvoltate descrieri matematice precise pentru paradigmele „inteligenței computaționale”, cum ar fi rețelele neuronale și algoritmii evolutivi (Russell și Norvig 2016, 25–26).

Inteligența artificială a rezolvat o mulțime de probleme foarte dificile, iar soluțiile lor s-au dovedit a fi utile în industria tehnologică, precum mineritul datelor, robotica industrială, logistica, recunoașterea vorbirii, software bancar, diagnostic medical și motorul de căutare Google. Dar multe dintre cele mai mari inovații ale inteligenței artificiale nu au fost considerate ca aparținând IA (Newquist 1994, 445). Nick Bostrom afirma că „O mulțime de IA de vârf s-au infiltrat în aplicații generale, adesea fără a fi numite IA, deoarece odată ce ceva devine suficient de util și suficient de comun, nu mai este etichetat IA.” (CNN 2006) De asemenea, mulți cercetători în inteligența artificială din anii 1990 și-au inclus în mod deliberat produsele în alte domenii (informatica, sisteme bazate pe cunoaștere, sisteme cognitive sau inteligență computațională), parțial datorită faptului că au considerat produsele lor ca fiind fundamental

diferite de IA, dar și pentru a ajuta la obținerea de finanțare ferindu-se de numele compromis de IA, după cum scria New York Times în 2005: „Oamenii de știință în informatică și inginerii de software au evitat termenul de inteligență artificială de teamă să nu fie priviți ca naivi. - visători cu ochii deschiși.” (Newquist 1994, 532)

Aceste succese nu s-au datorat unei noi paradigme, ci mai ales abilităților de inginerie și creșterii extraordinare a vitezei și capacității computerului în anii 90.

Realizări

1995: Mașinile vectoriale suport, aplicate textului pentru categorisire, recunoașterea caracterelor scrise de mână și clasificarea imaginilor (Cortes și Vapnik 1995, 273–97) (Cortes și Vapnik 1995).

O mașină semi-autonomă a condus 4.501 km de la coastă la coasta Statelor Unite cu direcție controlată de computer. Accelerația și frâna controlate de șofer uman.

1996: Campionul mondial de șah, Garry Kasparov este învins pentru prima dată de un sistem IA de joc de șah, Deep Blue, o versiune cadru produs de IBM capabil să proceseze cca 200.000.000 de mișcări pe secundă (McCorduck 2004, 480–83).

1997: Arhitectura memoriei pe termen lung (LSTM) a îmbunătățit atât eficiența, cât și caracterul practic al rețelelor neuronale recurente prin eliminarea dependenței pe termen lung (Hochreiter și Schmidhuber 1997).

1998: Învățarea bazată pe gradient a fost îmbunătățită prin combinarea algoritmului de coborâre a gradientului stocastic cu algoritmul de retropropagare (Lecun et al. 1998).

2002: TD-Gammon pentru jocul de table a combinat rețelele neuronale și învățarea prin întărire (RL) cu metoda de auto-play (Tesauro 2002).

2005: Un robot Stanford a câștigat Marea Provocare DARPA conducând în mod autonom timp de 131 de mile de-a lungul unui traseu în deșert (DARPA 2007), iar doi ani mai târziu o echipă de la CMU a câștigat Provocarea Urbană DARPA navigând în mod autonom 55 de mile într-un mediu urban evitând pericolele din trafic și respectând toate legile rutiere.

2006: Fei-Fei Li a contribuit la o schimbare de paradigmă, plecând de la ipoteza că principala limitare IA este cantitatea de date.

2009: A fost publicat ImageNet care conține 3,2 milioane de imagini etichetate, separate în 5.247 de categorii, sortate în 12 subarbori (Deng et al. 2009).

2011: Watson de la IBM a câștigat un joc Jeopardy împotriva lui Ken Jennings și Brad Rutter (Ferrucci 2012).

Învățarea profundă, megadate (2011–2020)

În primele decenii ale secolului al XXI-lea, utilizarea tehnologiei megadatelor („big data”), computere mai ieftine și mai rapide și tehnici avansate de învățare automată au dus la o explozie a interesului pentru inteligența artificială (Lohr 2016). Aplicațiile big data (Becker Friedman Institute 2015), și învățarea profundă (în special rețelele neuronale convoluționale profunde și rețelele neuronale recurente) au permis procesarea imaginilor și video, analiza textului și chiar recunoașterea vorbirii (Yann LeCun, Bengio, și Hinton 2015).

Big data (megadatele, sau datele masive) nu pot fi capturate, gestionate și procesate de instrumente software convenționale într-un interval de timp suficient de mic, unde, în loc de analiză aleatorie (sondaj prin eșantion), toate datele sunt folosite pentru analiză.

Învățarea profundă modelează abstracții de nivel înalt în date utilizând un grafic profund cu multe straturi de procesare (Yann LeCun, Bengio, și Hinton 2015). Rețelele neuronale profunde

sunt capabile să genereze în mod realist modele mult mai complexe în comparație cu omologii lor mai puțin adânci. Dar învățarea profundă are propriile sale probleme, precum problema gradientului care dispare, atunci când gradienții trecuți între straturi se micșorează treptat și dispar literalmente pe măsură ce sunt rotunjiți la zero.

Realizări

2012: O rețea neuronală convoluțională, AlexNet, a atins o rată de eroare de clasificare de 16% (Krizhevsky, Sutskever, și Hinton 2017), care a scăzut apoi, în doi ani, la câteva procente, schimbând paradigma IA la învățare profundă (DL). DL a introdus o arhitectură de rețele neuronale cu mai multe straturi care învață reprezentări de date cu niveluri de abstractizare (Yann LeCun, Bengio, și Hinton 2015). Termenii IA sau ML (învățarea automată) înlocuiesc adesea DL, în special în știri și media. În paradigma ML, intrările includ date și răspunsuri, iar ML produce reguli din intrări. Sistemul ML este antrenat, mai degrabă decât programat în mod explicit.

Experimentul Cat a învățat să identifice și să recunoască pisicile din 10.000.000 de imagini neetichetate (Le et al. 2012).

2014: Generative Adversarial Networks (GAN), arhitecturi de rețele neuronale profunde compuse din două rețele, care se opun una cu cealaltă (deci „adversariale") (Goodfellow et al. 2014).

2015: DeepRL a dezvoltat o gamă diversă de jocuri Atari 2600 la un nivel supraomenesc, cu doar pixeli și scoruri brute ca intrări (Mnih et al. 2015).

2015 a fost un an de referință pentru inteligența artificială, numărul de proiecte software care utilizează IA în cadrul Google a crescut de la o „utilizare sporadică" în 2012 la peste 2.700 de proiecte (J. Clark 2015).Într-un sondaj din 2017, una din cinci companii a raportat că a „încorporat IA în unele oferte sau procese" (Ransbotham et al. 2017). Cantitatea de cercetare în

domeniul IA (măsurată prin totalul publicațiilor) a crescut cu 50% în anii 2015–2019 (UNESCO 2021).

2016: AlphaGo l-a învins pe Lee Sedol, jucătorul Go numărul unu din lume (Silver et al. 2016).

2017: Transformer, o arhitectură DL bazată pe un mecanism de auto-atenție folosită în modelarea limbajului, traducerea automată și răspunsul la întrebări (Vaswani et al. 2017).

Libratus a învins decisiv patru profesioniști umani de top în varianta de poker pentru doi jucători numită heads-up no-limit Texas hold'em (HUNL) (Brown și Sandholm 2017).

2018: OpenIA Five a învins o echipă de amatori umani la Dota 2, depășind inteligența umană într-un joc video complex (OpenAI 2018).

Yoshua Bengio, Geoffrey Hinton și Yann LeCun au primit Premiul Turing pentru descoperiri conceptuale și de inginerie care au făcut din DL o componentă critică a calculului.

2019: AlphaStar a învins un jucător profesionist de top în StarCraft II (AlphaStar 2019).

OpenIA l-a antrenat pe Dactyl4, o mână robot asemănătoare unui om, să manipuleze obiecte fizice cu o dexteritate fără precedent.

GPT-2.5, un model de limbaj nesupravegheat la scară largă care generează paragrafe coerente de text, cu performanțe în modelare lingvistică și înțelegerea lecturii, traducere automată, răspunsuri la întrebări și rezumate (Joint Research Centre (European Commission), Samoili, et al. 2020).

Evoluția IA a fost accelerată de codurile în acces deschis, cadre, seturi de date, publicații științifice și partajarea generală a cunoștințelor. Cercetările actuale implică IA statistică, și tehnici precum învățarea profundă, apărând o subdiviziune a IA, inteligența artificiala generală, cu multe instituții bine finanțate până în anii 2010.

Probleme

Învățarea profundă are mai multe probleme care trebuie abordate, inclusiv atacuri adverse, generarea de conținut deepfake, corectitudine, responsabilitate, transparență și alte considerații etice. (Joint Research Centre (European Commission), Samoili, et al. 2020)

- *Atacurile adverse*: Învățarea automată adversă încearcă să păcălească modelele prin furnizarea de date înșelătoare (Papernot et al. 2017).
- *Deepfake*: IA reduce costul generării de conținut fals și permite desfășurarea de campanii de dezinformare, prin:
    - uzurparea identității altora online,
    - generarea de imagini și știri false,
    - automatizarea producției de conținut fals postat adesea pe rețelele sociale,
    - automatizarea creării de conținut spam/phishing.

Succesul fără precedent al învățării automate statistice în anii 2010, în mare parte sub-simbolică, a eclipsat toate celelalte abordări (atât de mult încât unele surse, în special din lumea afacerilor, folosesc termenul „inteligență artificială" ca însemnând „învățare automată cu rețele neuronale"). Dar raționamentul subsimbolic poate face multe dintre aceleași greșeli pe care le face intuiția umană, cum ar fi părtinirea algoritmică. Critici precum Noam Chomsky susțin că continuarea cercetării în IA simbolică va fi în continuare necesară pentru inteligența generală (Langley 2011), în special pentru că IA sub-simbolică este o îndepărtare de IA explicabilă. Domeniul emergent al inteligenței artificiale neurosimbolice încearcă să întindă o punte între cele două abordări.

Modele mari de limbaj (2020-prezent)

Era modernă IA începe cu dezvoltarea unor modele la scară în limbaj mare, cum ar fi ChatGPT (Marr 2023), și cu dezvoltarea inițială a arhitecturilor și algoritmilor cheie, precum arhitectura transformatorului, în 2017, care a condus la scalarea și dezvoltarea unor modele de limbaj mari care prezintă trăsături asemănătoare omului de raționament, cogniție, atenție și creativitate. Arhitectura transformatorului a fost propusă de cercetătorii Google, mai târziu fiind utilizată pe scară largă în modelele mari de limbaj (Murgia 2023).

2020: Modele precum GPT-3 lansat de OpenIA, și

2022: Gato lansat de DeepMind, au fost descrise drept realizări importante ale învățării automate.

2023: Microsoft Research a testat modelul de limbaj mare GPT-4 cu o mare varietate de sarcini și a concluzionat că „ar putea fi privit în mod rezonabil ca o versiune timpurie (dar încă incompletă) a unui sistem de inteligență artificială generală (AGI)" (Bubeck et al. 2023).

2024: Pe 15 februarie 2024, Google lansează Gemini 1.5 în versiune beta limitată, capabil să aibă o lungime de context de până la 1 milion de jetoane.

15 februarie 2024: OpenIA anunță public Sora, un model text-to-video pentru generarea de videoclipuri de până la un minut.

22 februarie: StabilityIA anunță Stable Diffusion 3, folosind o arhitectură similară cu Sora.

În prezent, OpenIA dezvoltă ChatGPT 5 care va fi un model de limbaj de ultimă generație, a cincea iterație a modelului de limbaj GPT (Generative Pre-training Transformer), un salt masiv în domeniul procesării limbajului natural.

Allen Newell abordează istoria inteligenței artificiale în termeni de probleme intelectuale (opoziții dihotomice): "Cadrul standard pentru istoria științei este în termeni de evenimente și

descoperiri științifice importante, legate de oamenii de știință care au fost responsabili pentru acestea." (Newell 1982) Cadrele de aplicabilitate generală sunt teoriile propuse și metodologiile de cercetare, dar acestea nu sunt utile pentru IA. De asemenea, nici paradigmele lui Kuhn (Kuhn 1996) sau programele de cercetare ale lui Lakatos (Lakatos 1978) nu furnizează, din punctul lui de vedere, o istorie prea corectă, IA dezvoltând și menținând cel mult două paradigme pe durata ei de viață, și a dezvoltat puține programe de cercetare. În aceste condiții, cadrele surprind mai bine analiza istorică a IA.

Problemele intelectuale sunt de obicei prezentate ca dihotomii, fiind diferite de problemele din lumea reală a acțiunii, având un statut îndoielnic din punct de vedere științific, dar joacă un rol euristic în activitatea științifică. Newell consideră că deși domeniul IA a început oficial la mijlocul anilor 1950, problemele intelectuale relevante se întind cu mult mai devreme.

Concluzii

Spre deosebire de narațiunile distopice, viitorul IA nu este unul al învechirii umane, ci mai degrabă al simbiozei. Colaborarea om-IA deține cheia pentru a debloca întregul potențial al IA, păstrând în același timp agenția umană și creativitatea. Folosind inteligența artificială ca instrument de creștere și nu de înlocuire, putem amplifica ingeniozitatea umană și putem aborda probleme complexe la scară. În plus, cultivarea abilităților interdisciplinare care reduc decalajul dintre IA și diverse domenii va fi crucială în valorificarea puterii de transformare a IA pentru binele colectiv.

Privind în perspectivă, evoluția IA va continua probabil într-un ritm accelerat, determinată de progresele în puterea de calcul, inovația algoritmică și disponibilitatea în creștere a datelor mari. Tendințele emergente includ integrarea IA cu alte tehnologii de ultimă oră, cum ar fi calculul cuantic și Internetul lucrurilor

(IoT), care ar putea debloca noi niveluri de performanță și eficiență.

Cu toate acestea, viitorul IA depinde și de abordarea provocărilor etice pe care le prezintă. Asigurarea faptului că dezvoltarea IA este aliniată cu valorile umane și cu normele societale este esențială. Aceasta include crearea de sisteme IA transparente care pot fi de încredere și înțelese de către public, precum și stabilirea unor cadre solide de guvernanță pentru a ghida cercetarea și aplicarea etică a IA.

Pe măsură ce inteligența artificială continuă să avanseze, ne aflăm în pragul unor posibilități și dileme etice fără precedent. Integrarea IA în dispozitivele de zi cu zi, de la smartphone la case inteligente, estompează granițele dintre inteligența umană și cea a mașinilor, ridicând întrebări despre autonomie, confidențialitate și responsabilitate. Mai mult, apariția inteligenței generale artificiale (AGI), un sistem IA ipotetic capabil să depășească oamenii într-o gamă largă de sarcini cognitive, prezintă riscuri existențiale și dificultăți filozofice.

Dincolo de orizontul AGI se află tărâmul simbiozei om-mașină, unde inteligența artificială mărește și îmbunătățește capacitățile umane în moduri fără precedent. De la interfețele creier-calculator care permit comunicarea directă între creier și mașini până la creativitatea asistată de IA și luarea deciziilor, convergența inteligenței umane și artificiale deține promisiunea să deblocheze noi frontiere ale inovației și înțelegerii.

Bibliografie

- AlgorithmWatch. 2024. „AI Ethics Guidelines Global Inventory". AlgorithmWatch. 2024. https://algorithmwatch.org/en/ai-ethics-guidelines-global-inventory/.
- AlphaStar. 2019. „AlphaStar: Mastering the Real-Time Strategy Game StarCraft II". Google DeepMind. 24 ianuarie 2019. https://deepmind.google/discover/blog/alphastar-mastering-the-real-time-strategy-game-starcraft-ii/.
- Becker Friedman Institute. 2015. „How Big Data is Changing Economies". 2015. https://web.archive.org/web/20180618102343/https://bfi.uchicago.edu/events/how-big-data-changing-economies.
- Brooks, Rodney A. 1990. „Elephants don't play chess". *Robotics and Autonomous Systems*, Designing Autonomous Agents, 6 (1): 3–15. https://doi.org/10.1016/S0921-8890(05)80025-9.
- Brown, Noam, și Tuomas Sandholm. 2017. „Superhuman AI for heads-up no-limit poker: Libratus beats top professionals". *Science* 359 (decembrie):eaao1733. https://doi.org/10.1126/science.aao1733.
- Bubeck, Sébastien, Varun Chandrasekaran, Ronen Eldan, Johannes Gehrke, Eric Horvitz, Ece Kamar, Peter Lee, et al. 2023. „Sparks of Artificial General Intelligence: Early experiments with GPT-4". arXiv. https://doi.org/10.48550/arXiv.2303.12712.
- Clark, Jack. 2015. „Why 2015 Was a Breakthrough Year in Artificial Intelligence". *Bloomberg.Com*, 8 decembrie 2015. https://www.bloomberg.com/news/articles/2015-12-08/why-2015-was-a-breakthrough-year-in-artificial-intelligence.

- Clark, Keith L. 1978. „Negation as Failure”. În *Logic and Data Bases*, ediție de Hervé Gallaire și Jack Minker, 293–322. Boston, MA: Springer US. https://doi.org/10.1007/978-1-4684-3384-5_11.
- CNN. 2006. „AI set to exceed human brain power”. 2006. https://edition.cnn.com/2006/TECH/science/07/24/ai.bostrom/.
- Colmerauer, Alain, și Philippe Roussel. 1993. „The birth of Prolog”. *ACM SIGPLAN Notices* 28 (3): 37–52. https://doi.org/10.1145/155360.155362.
- Committee, National Research Council (U S.) Automatic Language Processing Advisory. 1966. *Language and Machines: Computers in Translation and Linguistics; a Report*. National Academies Press.
- Copeland, Edited by B. Jack, ed. 2004. *The Essential Turing: Seminal Writings in Computing, Logic, Philosophy, Artificial Intelligence, and Artificial Life plus The Secrets of Enigma*. Oxford, New York: Oxford University Press.
- Copeland, Jack. 2000. „A Brief History of Computing”. 2000. https://www.alanturing.net/turing_archive/pages/Reference%20Articles/BriefHistofComp.html.
- Cortes, Corinna, și Vladimir Vapnik. 1995. „Support-Vector Networks”. *Machine Learning* 20 (3): 273–97. https://doi.org/10.1007/BF00994018.
- Crevier, Daniel. 1993. *AI: The Tumultuous History of the Search for Artificial Intelligence*.
- DARPA. 2007. „The Grand Challenge”. 2007. https://www.darpa.mil/about-us/timeline/-grand-challenge-for-autonomous-vehicles.

- Deng, Jia, Wei Dong, Richard Socher, Li-Jia Li, Kai Li, și Li Fei-Fei. 2009. „ImageNet: A large-scale hierarchical image database”. În *2009 IEEE Conference on Computer Vision and Pattern Recognition*, 248–55. https://doi.org/10.1109/CVPR.2009.5206848.
- Dreyfus, Hubert L., și Stuart E. Dreyfus. 1986. *Mind Over Machine: The Power of Human Intuition and Expertise in the Era of the Computer*. Free Press.
- Ferrucci, D. A. 2012. „Introduction to “This is Watson””. *IBM Journal of Research and Development* 56 (3.4): 1:1-1:15. https://doi.org/10.1147/JRD.2012.2184356.
- Goodfellow, Ian, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville, și Y. Bengio. 2014. „Generative Adversarial Networks”. *Advances in Neural Information Processing Systems* 3 (iunie). https://doi.org/10.1145/3422622.
- Haugeland, John. 1985. *Artificial Intelligence: The Very Idea*. Cambridge: MIT Press.
- Hayes, P. J. 1981. „The Logic of Frames”. În *Readings in Artificial Intelligence*, ediție de Bonnie Lynn Webber și Nils J. Nilsson, 451–58. Morgan Kaufmann. https://doi.org/10.1016/B978-0-934613-03-3.50034-9.
- Hochreiter, Sepp, și Jürgen Schmidhuber. 1997. „Long Short-term Memory”. *Neural computation* 9 (decembrie):1735–80. https://doi.org/10.1162/neco.1997.9.8.1735.
- Hopfield, J J. 1982. „Neural networks and physical systems with emergent collective computational abilities.” *Proceedings of the National Academy of Sciences* 79 (8): 2554–58. https://doi.org/10.1073/pnas.79.8.2554.
- Huang, Ting, și Christopher Smith. 2006. „The History of Artificial Intelligence”. În .

https://www.semanticscholar.org/paper/The-History-of-Artificial-Intelligence-Huang-Smith/085599650ebfcfba0dcb434bc50b7c7c54fdbf05.

- Joint Research Centre (European Commission), S. Samoili, M. López Cobo, E. Gómez, G. De Prato, F. Martínez-Plumed, și B. Delipetrev. 2020. *AI Watch: Defining Artificial Intelligence : Towards an Operational Definition and Taxonomy of Artificial Intelligence*. Publications Office of the European Union. https://data.europa.eu/doi/10.2760/382730.
- Krizhevsky, Alex, Ilya Sutskever, și Geoffrey E. Hinton. 2017. „ImageNet classification with deep convolutional neural networks". *Communications of the ACM* 60 (6): 84–90. https://doi.org/10.1145/3065386.
- Kuhn, Thomas S. 1996. *The Structure of Scientific Revolutions* (versiunea 3rd edition). 3rd edition. Chicago, IL: University of Chicago Press.
- Lakatos, Imre. 1978. „The Methodology of Scientific Research Programmes". Cambridge Core. 1978. https://doi.org/10.1017/CBO9780511621123.
- Lakoff, George, și Mark Johnson. 1999. *Philosophy In The Flesh: The Embodied Mind And Its Challenge To Western Thought*. Basic Books.
- Langley, Pat. 2011. „The Changing Science of Machine Learning". *Machine Learning* 82 (3): 275–79. https://doi.org/10.1007/s10994-011-5242-y.
- Le, Quoc V., Marc'Aurelio Ranzato, Rajat Monga, Matthieu Devin, Kai Chen, Greg S. Corrado, Jeff Dean, și Andrew Y. Ng. 2012. „Building high-level features using large scale unsupervised learning". arXiv. https://doi.org/10.48550/arXiv.1112.6209.

- LeCun, Y., B. Boser, J. S. Denker, D. Henderson, R. E. Howard, W. Hubbard, și L. D. Jackel. 1989. „Backpropagation Applied to Handwritten Zip Code Recognition”. *Neural Computation* 1 (4): 541–51. https://doi.org/10.1162/neco.1989.1.4.541.
- Lecun, Y., L. Bottou, Y. Bengio, și P. Haffner. 1998. „Gradient-based learning applied to document recognition”. *Proceedings of the IEEE* 86 (11): 2278–2324. https://doi.org/10.1109/5.726791.
- LeCun, Yann, Yoshua Bengio, și Geoffrey Hinton. 2015. „Deep Learning”. *Nature* 521 (7553): 436–44. https://doi.org/10.1038/nature14539.
- Lohr, Steve. 2016. „IBM Is Counting on Its Bet on Watson, and Paying Big Money for It”. *The New York Times*, 17 octombrie 2016, sec. Technology. https://www.nytimes.com/2016/10/17/technology/ibm-is-counting-on-its-bet-on-watson-and-paying-big-money-for-it.html.
- Manyika, James. 2022. „Getting AI Right: Introductory Notes on AI & Society”. *Daedalus* 151 (2): 5–27. https://doi.org/10.1162/daed_e_01897.
- Marr, Bernard. 2023. „Beyond The Hype: What You Really Need To Know About AI In 2023”. Forbes. 2023. https://www.forbes.com/sites/bernardmarr/2023/03/20/beyond-the-hype-what-you-really-need-to-know-about-ai-in-2023/.
- McCarthy, John. 1979. „Ascribing Mental Qualities to Machines”. În *Philosophical Perspectives in Artificial Intelligence*, ediție de Martin Ringle. Humanities Press.
- McCarthy, John, Marvin L. Minsky, Nathaniel Rochester, și Claude E. Shannon. 2006. „A Proposal for the Dartmouth Summer Research Project on Artificial

Intelligence, August 31, 1955". *AI Magazine* 27 (4): 12–12. https://doi.org/10.1609/aimag.v27i4.1904.

- McCorduck, Pamela. 2004. *Machines Who Think: A Personal Inquiry Into the History and Prospects of Artificial Intelligence*. Taylor & Francis.
- McCulloch, Warren S., și Walter Pitts. 1943. „A Logical Calculus of the Ideas Immanent in Nervous Activity". *The Bulletin of Mathematical Biophysics* 5 (4): 115–33. https://doi.org/10.1007/BF02478259.
- Metaxiotis, Kostas, și J-E Samouilidis. 2000. „Expert Systems in Medicine: Academic Illusion or Real Power?" *Information Management & Computer Security* 8 (mai):75–79. https://doi.org/10.1108/09685220010694017.
- Michie, Donald. 1963. „Experiments on the Mechanization of Game-Learning Part I. Characterization of the Model and its parameters". *The Computer Journal* 6 (3): 232–36. https://doi.org/10.1093/comjnl/6.3.232.
- Minsky, Marvin. 1986. *The Society of Mind*. Simon and Schuster.
- Minsky, Marvin, și Seymour Papert. 1988. *Perceptrons: An Introduction to Computational Geometry*. Cambridge.
- Mnih, Volodymyr, Koray Kavukcuoglu, David Silver, Andrei A. Rusu, Joel Veness, Marc G. Bellemare, Alex Graves, et al. 2015. „Human-Level Control through Deep Reinforcement Learning". *Nature* 518 (7540): 529–33. https://doi.org/10.1038/nature14236.
- Moravec, Hans P., Stanford, și California 94305. 1976. „The Role of Raw Power in Intelligence". The History of Artificial Intelligence - Spotlight at Stanford. 1976. https://exhibits.stanford.edu/ai/catalog/ws563sd6050.
- Murgia, Madhumita. 2023. „Transformers: the Google scientists who pioneered an AI revolution". 2023.

https://www.ft.com/content/37bb01af-ee46-4483-982f-ef3921436a50.

- Newell, Allen. 1982. „Intellectual Issues in the History of Artificial Intelligence”: În . Fort Belvoir, VA: Defense Technical Information Center. https://doi.org/10.21236/ADA125318.
- Newell, Allen, J. C. Shaw, și Herbert A. Simon. 1962. „The processes of creative thinking”. În *Contemporary approaches to creative thinking: A symposium held at the University of Colorado*, 63–119. The Atherton Press behavioral science series. New York, NY, US: Atherton Press. https://doi.org/10.1037/13117-003.
- Newquist, Harvey P. 1994. *The Brain Makers*. Sams Pub.
- Nilsson, N. J. 1984. „The SRI Artificial Intelligence Center: A Brief History”. *SRI* (blog). 1 ianuarie 1984. https://www.sri.com/publication/artificial-intelligence-pubs/the-sri-artificial-intelligence-center-a-brief-history/.
- Nilsson, Nils J. 1998. *Artificial Intelligence: A New Synthesis*. Morgan Kaufmann.
- OpenAI. 2018. „OpenAI Five”. 2018. https://openai.com/research/openai-five.
- Papernot, Nicolas, Patrick McDaniel, Ian Goodfellow, Somesh Jha, Z. Berkay Celik, și Ananthram Swami. 2017. „Practical Black-Box Attacks against Machine Learning”. arXiv. https://doi.org/10.48550/arXiv.1602.02697.
- Quinlan, J. R. 1986. „Induction of Decision Trees”. *Machine Learning* 1 (1): 81–106. https://doi.org/10.1007/BF00116251.
- Ransbotham, Sam, David Kiron, Philipp Gerbert, și Martin Reeves. 2017. „Reshaping Business With Artificial Intelligence”. *MIT Sloan Management Review*, septembrie.

https://sloanreview.mit.edu/projects/reshaping-business-with-artificial-intelligence/.

- Raphael, Bertram. 1972. *Robot Research at Stanford Research Institute*. PN.
- Rodríguez, José Miguel Olazaran. 1991. *A Historical Sociology of Neural Network Research*. University of Edinburgh.
- Rosenblatt, Frank. 1962. *Principles of Neurodynamics: Perceptrons and the Theory of Brain Mechanisms*. Spartan Books.
- Rumelhart, D.E., G.E. Hinton, și R.J. Williams. 1988. „Learning Internal Representations by Error Propagation". În , 399–421. Elsevier. https://doi.org/10.1016/B978-1-4832-1446-7.50035-2.
- Russell, Stuart, și Peter Norvig. 2016. „Artificial Intelligence: A Modern Approach, 4th US ed." 2016. https://aima.cs.berkeley.edu/.
- Samuel, Arthur L. 1960. „Programming Computers to Play Games". În *Advances in Computers*, ediție de Franz L. Alt, 1:165–92. Elsevier. https://doi.org/10.1016/S0065-2458(08)60608-7.
- Science Research Council. 1973. *Artificial Intelligence; a Paper Symposium*. Science Research Council.
- Sejnowski, Terrence J. 2018. *The Deep Learning Revolution*. MIT Press.
- Shortliffe, Edward H., Randall Davis, Stanton G. Axline, Bruce G. Buchanan, C. Cordell Green, și Stanley N. Cohen. 1975. „Computer-based consultations in clinical therapeutics: Explanation and rule acquisition capabilities of the MYCIN system". *Computers and Biomedical Research* 8 (4): 303–20. https://doi.org/10.1016/0010-4809(75)90009-9.

- Silver, David, Aja Huang, Chris J. Maddison, Arthur Guez, Laurent Sifre, George van den Driessche, Julian Schrittwieser, et al. 2016. „Mastering the Game of Go with Deep Neural Networks and Tree Search”. *Nature* 529 (7587): 484–89. https://doi.org/10.1038/nature16961.
- Tesauro, Gerald. 2002. „Programming backgammon using self-teaching neural nets”. *Artificial Intelligence* 134 (1): 181–99. https://doi.org/10.1016/S0004-3702(01)00110-2.
- Turing, A. M. 1950. „Computing Machinery and Intelligence”. *Mind* LIX (236): 433–60. https://doi.org/10.1093/mind/LIX.236.433.
- UNESCO. 2021. „The Race against Time for Smarter Development | 2021 Science Report”. 2021. https://www.unesco.org/reports/science/2021/en.
- Vaswani, Ashish, Noam Shazeer, Niki Parmar, Jakob Uszkoreit, Llion Jones, Aidan N Gomez, Ł ukasz Kaiser, și Illia Polosukhin. 2017. „Attention is All you Need”. În *Advances in Neural Information Processing Systems*. Vol. 30. Curran Associates, Inc. https://papers.nips.cc/paper_files/paper/2017/hash/3f5ee243547dee91fbd053c1c4a845aa-Abstract.html.
- Watkins, Christopher. 1989. „Learning From Delayed Rewards”, ianuarie.
- Weizenbaum, Joseph. 1966. „ELIZA—a computer program for the study of natural language communication between man and machine”. *Communications of the ACM* 9 (1): 36–45. https://doi.org/10.1145/365153.365168.
- Whitehead, Alfred North, și Bertrand Russell. 1927. *Principia Mathematica*. Cambridge University Press.
- Widrow, B., și M.A. Lehr. 1990. „30 years of adaptive neural networks: perceptron, Madaline, and

backpropagation". *Proceedings of the IEEE* 78 (9): 1415–42. https://doi.org/10.1109/5.58323.

- Zeghloul, Saïd, med amine Laribi, și Jean-Pierre Gazeau. 2016. *Robotics and Mechatronics: Proceedings of the 4th IFToMM International Symposium on Robotics and Mechatronics*. Vol. 37. https://doi.org/10.1007/978-3-319-22368-1.

Analiză comparativă între India și China din perspectivă economică, militară și a capabilităților de apărare cibernetică

Alexia-Gabriela Szabo
(Voluntară la Grupul de Lucru pentru Securitate și Apărare Cibernetică și membru susținător al AORR)

Introducere

Această analiză comparativă își propune să ofere o evaluare riguroasă și detaliată a asemănărilor și a diferențelor dintre India și China, având în vedere dimensiunile geografice, economice, demografice, politice și militare. Obiectivele specifice includ: identificarea și evidențierea principalelor caracteristici ale fiecărei țări, compararea performanțelor economice, resurselor naturale și infrastructurii dintre India și China și examinarea structurii demografice și a impactului acesteia asupra dezvoltării economice și sociale. De asemenea, analiza își stabilește ca obiectiv să evalueze capabilitățile militare, inclusiv capabilitățile cibernetice și tehnologiile militare de ultimă generație și să determine implicațiile strategice ale acestei comparații pentru relațiile internaționale și securitatea globală.

Compararea între India și China este esențială din multiple perspective. Din punct de vedere economic, ambele state reprezintă economii emergente de prim rang, cu rate de creștere rapide și impact semnificativ asupra economiei globale. Înțelegerea asemănărilor și diferențelor economice oferă perspective valoroase asupra evoluțiilor economice viitoare. În contextul demografic, India și China sunt cele mai populate țări din lume, iar structurile lor demografice influențează profund dezvoltarea economică, socială și politică. Din perspectiva

politică, fiecare țară are un sistem politic distinct, cu influențe majore asupra politicii globale și relațiilor internaționale. Din punct de vedere militar, India și China sunt puteri militare regionale și globale, cu capacități cibernetice și tehnologii avansate. Compararea acestor capabilități ajută la înțelegerea echilibrului de putere și a potențialelor riscuri de securitate. Totodată, relațiile dintre India și China au implicații majore pentru stabilitatea regională și globală. Înțelegerea punctelor forte și a vulnerabilităților fiecărei țări contribuie la formularea de strategii politice și economice eficiente.

Pentru realizarea studiului, a fost utilizată o abordare metodologică mixtă, integrând surse primare și secundare. Datele statistice sunt obținute din informații oficiale furnizate de guvernele celor două țări, precum și din date de la organizații internaționale, cum ar fi Banca Mondială. Studii și rapoarte relevante sunt preluate din analize publicate de instituții de cercetare, publicații academice și literatură de specialitate. Analiza comparativă se bazează și pe utilizarea tabelelor, graficelor și schemelor pentru vizualizarea și compararea datelor colectate, facilitând înțelegerea.

Analiza Caracteristicilor Geomorfologice, Climatice și Resurselor Naturale ale Indiei și Chinei

Caracteristici	India	China
Locație	Asia de Sud, care se învecinează cu Marea Arabiei și Golful Bengal, între Birmania și Pakistan	Asia de Est, la granița cu Marea Chinei de Est, Golful Coreea, Marea Galbenă și Marea Chinei de Sud, între Coreea de Nord și Vietnam
Suprafață	**Total:** 3.287.263 km² **Teren:** 2.973.193 km² **Apă:** 314.070 km²	**Total:** 9.596.960 km² **Teren:** 9.326.410 km² **Apă:** 270.550 km²

Frontiere terestre	**Total:** 13.888 km **Țări de frontieră (6):** Bangladesh 4.142 km; Bhutan 659 km; Birmania 1.468 km; China 2.659 km; Nepal 1.770 km; Pakistan 3.190 km	**Total:** 22.457 km **Țări de frontieră (14):** Afganistan 91 km; Bhutan 477 km; Birmania 2.129 km; India 2.659 km; Kazahstan 1.765 km; Coreea de Nord 1.352 km; Kârgâzstan 1.063 km; Laos 475 km; Mongolia 4.630 km; Nepal 1.389 km; Pakistan 438 km; Rusia (nord-est) 4.133 km și Rusia (nord-vest) 46 km; Tadjikistan 477 km; Vietnam 1.297 km
Clima	Variază de la climatul musonic tropical în sud la cel temperat în nord.	Extrem de diversă; tropicală în sud până la subarctică în nord.
Relief	Câmpie înaltă (Platoul Deccan) în sud, câmpie plată până la ondulată de-a lungul Gangelui, deșerturi în vest, Himalaya în nord	Preponderent munți, platouri înalte, deșerturi în vest; câmpii, delte și coline în est
Altitudine	**Cel mai înalt punct:** Kanchenjunga, 8.586 m **Cel mai jos punct:** Oceanul Indian, 0 m **Altitudine medie:** 160 m	**Cel mai înalt punct:** Muntele Everest (cel mai înalt vârf din Asia și cel mai înalt punct de pe Pământ deasupra nivelului mării), 8.849 m **Cel mai jos punct:** Turpan Pendi, -154 m **Altitudine medie:** 1.840 m
Resurse naturale	Cărbune (a patra cea mai mare rezervă din lume), antimoniu, minereu de fier, plumb, mangan,	Cărbune, minereu de fier, heliu, petrol, gaze naturale, arsen, bismut, cobalt, cadmiu,

	mica, bauxită, elemente rare, minereu de titan, cromit, gaze naturale, diamante, petrol, calcar, terenuri arabile	ferosiliciu, galiu, germaniu, hafniu, indiu, litiu, mercur, tantal, telur, staniu, titan, tungsten, antimoniu, mangan, magneziu, molibden, seleniu, stronțiu, vanadiu, magnetit, aluminiu, plumb, zinc, elemente rare, uraniu, potențial hidroenergetic (cel mai mare din lume), terenuri arabile
Populației	1.409.128.296	1.416.043.270
Distribuția populației	Cu excepția notabilă a deșerturilor din nord-vest, inclusiv Deșertul Thar, și a zonei montane din nord, densitatea populației este foarte mare în majoritatea țării; nucleul populației se află în nord, de-a lungul malurilor Gangelui, iar alte văi de râuri și zonele de coastă din sud au, de asemenea, concentrații mari de populație	Majoritatea populației se află în jumătatea estică a țării; vestul, cu vastitatea sa montană și zonele deșertice, rămâne slab populat; deși clasificată pe primul loc în lume în ceea ce privește populația totală, densitatea generală este mai mică decât în multe alte țări din Asia și Europa; densitatea mare a populației se găsește de-a lungul văilor râurilor Yangtze și Galben, delta râului Xi Jiang, Bazinul Sichuan (în jurul orașului Chengdu), în și în jurul Beijingului, și în zona industrială din jurul orașului Shenyang
Acorduri internaționale	Protecția Mediului în Antarctica, Resursele	Protecția Mediului în Antarctica, Resursele

	Marine din Antarctica, Tratatul Antarctic, Biodiversitate, Schimbări Climatice, Protocolul de la Kyoto privind Schimbările Climatice, Acordul de la Paris privind Schimbările Climatice, Deșertificare, Specii Pe cale de dispariție, Modificarea Mediului, Deșeuri Periculoase, Dreptul Mării, Interzicerea Testelor Nucleare, Protecția Stratului de Ozon, Poluarea Navelor, Lemn Tropical 2006, Zone Umede, Vânătoarea de balene Semnate, dar neratificate: niciunul dintre acordurile selectate	Marine din Antarctica, Tratatul Antarctic, Biodiversitate, Schimbări Climatice, Protocolul de la Kyoto privind Schimbările Climatice, Acordul de la Paris privind Schimbările Climatice, Deșertificare, Specii pe cale de dispariție, Modificarea Mediului, Deșeuri Periculoase, Dreptul Mării, Depozitarea Marină - Convenția de la Londra, Depozitarea Marină - Protocolul de la Londra, Protecția Stratului de Ozon, Poluarea Navelor, Lemn Tropical 2006, Zone Umede, Vânătoarea de balene Semnate, dar neratificate: Tratatul de Interzicere Completă a Testelor Nucleare

(The World Factbook)

Analiza Economiilor din India și China: PIB, Putere Economică, Resurse de Subsol și Resurse Minerale

India și China sunt două dintre cele mai mari economii emergente ale lumii, având un impact semnificativ asupra economiei globale. Ambele țări au înregistrat creșteri economice

remarcabile în ultimele decenii și sunt considerate puteri economice majore.

Caracteristici	**India**	**China**
PIB nominal – anul 2023	3,5 trilioane USD	17,8 trilioane USD
PIB nominal – anul 2024	3,41 trilioane USD	14,7 trilioane USD
PIB-ul pe cap de locuitor – anul 2023	2.500 USD	12.500 USD
Rată de creștere – anul 2023	8%	5%
Exporturi – anul 2023	774 miliarde de dolari	3,6 trilioane de dolari
Exporturi – parteneri – anul 2022	SUA: 18%, UAE: 7%, Țările de Jos: 4%, China: 3%, Bangladesh: 3%	SUA: 15%, Hong Kong: 7%, Japonia: 5%, Germania: 4%, Coreea de Sud: 4%
Exporturi – mărfuri – anul 2022	Petrol rafinat, diamante, medicamente ambalate, îmbrăcăminte, bijuterii	Echipamente de radiodifuziune, circuite integrate, computere, îmbrăcăminte, piese de mașini
Importuri – anul 2023	850 miliarde de dolari	3,1 trilioane de dolari
Importuri – parteneri – anul 2022	China 15%, UAE 7%, SUA 7%, Arabia Saudită 6%, Rusia 6%	SUA 7%, Coreea de Sud 7%, Japonia 6%, Australia 6%, China 6%
Importuri – mărfuri – anul 2022	Petrol brut, cărbune, aur, gaz natural, diamante	Petrol brut, circuite integrate, minereu de fier, gaz natural, aur
Rata inflației – anul 2023	5.65%	0.23%
Produse agricole – anul 2022	Trestie de zahăr, orez, lapte, grâu, lapte de bizon, cartofi, legume, banane, porumb, ceapă	Porumb, orez, legume, grâu, trestie de zahăr, cartofi, castraveți, roșii, pepeni verzi, carne de porc

Industrii	Textile, produse chimice, procesarea alimentelor, oțel, echipamente de transport, ciment, minerit, petrol, utilaje, software, produse farmaceutice	Minerit și prelucrarea minereurilor, fier, oțel, aluminiu și alte metale, cărbune; construcții de mașini; armament; textile; petrol; ciment; produse chimice; îngrășăminte; produse de consum; procesarea alimentelor; echipamente de transport, inclusiv automobile, vagoane și locomotive, nave, aeronave; echipamente de telecomunicații, vehicule comerciale de lansare spațială, sateliți
Forța de muncă – anul 2023	593,729 milioane	779.246 milioane
Rezerve de valută străină și aur – anul 2023	627,793 miliarde de dolari	3,45 trilioane de dolari
Datorie externă – anul 2019	555,388 miliarde de dolari	2.028 trilioane de dolari
Buget	Venituri: 495,007 miliarde de dolari (anul 2020) Cheltuieli: 818,94 miliarde de dolari (anul 2020)	Venituri: 3,983 trilioane de dolari (anul 2019) Cheltuieli: 4,893 trilioane de dolari (anul 2019)

(World Bank, 2023)
(The World Factbook)

În ultimele două decenii, China a înregistrat o creștere economică extraordinară, devenind a doua cea mai mare economie din

lume. India, pe de altă parte, este a cincea cea mai mare economie a lumii (Prarthana, 2024). Coontrastul între ratele de creștere a celor două țări reflectă tranziția Chinei către o economie mai matură, în timp ce India este încă în faza de expansiune rapidă datorită populației sale tinere și în creștere (World Bank, 2023).

Puterea economică implică examinarea mai multor aspecte, precum creșterea economică, structura economică și comerțul.

India dispune de rezerve semnificative de minerale esențiale pentru dezvoltarea sa economică. Printre acestea se numără fierul, cu unele dintre cele mai mari rezerve din lume, fiind un element cheie. Cărbunele este, de asemenea, o resursă majoră, India fiind unul dintre cei mai mari producători și consumatori de cărbune, utilizat predominant pentru generarea de energie electrică și în procesele industriale. Bauxita, necesară pentru producția de aluminiu, este abundentă în India, iar manganul, care este important pentru industria metalurgică, are rezerve semnificative. În plus, statul este un mare producător de sare, cu resurse extinse în diferite regiuni ale țării. În ceea ce privește resursele de subsol, India dispune de rezerve moderate de petrol și gaze naturale. Deși aceste resurse nu sunt la fel de mari ca în alte regiuni ale lumii, ele sunt esențiale pentru securitatea energetică a țării. Apa subterană reprezintă o resursă vitală pentru India, fiind crucială atât pentru agricultură, cât și pentru aprovizionarea cu apă potabilă, mai ales în regiunile aride (Sanat Pai Raikar, Philip B. Calkins, 2024).

China este cunoscută pentru resursele sale minerale extrem de variate și abundente. Țara are rezerve semnificative de minerale și rezerve de subsol, ceea ce o face unul dintre cei mai mari producători și consumatori de minerale din lume. China are cele mai mari rezerve de cărbune din lume și este cel mai mare producător și consumator de cărbune. Cărbunele este o sursă majoră de energie pentru țară și este folosit pe scară largă în producția de energie electrică și industrie. Este un lider mondial

în producția de metale de bază, inclusiv fier, aluminiu, cupru și zinc. De asemenea, țara dispune de rezerve mari de minerale utilizate în industria construcțiilor și fabricarea de bunuri. Statul deține rezerve considerabile de metale rare, inclusiv litiu, neodim și alte elemente esențiale pentru tehnologia avansată, cum ar fi electronicele și bateriile. Statul explorează și dezvoltă resurse geotermale ca parte a eforturilor de diversificare a surselor de energie și reducere a dependenței de cărbune. China dispune de rezerve de petrol și gaze naturale, dar acestea sunt relativ mai limitate comparativ cu alte resurse. Exploatarea și dezvoltarea acestor resurse sunt importante pentru asigurarea securității energetice a țării (David N. Keightley, Kenneth G. Lieberthal, 2024).

China și India au resurse minerale și de subsol esențiale pentru economiile lor, dar există diferențe notabile în tipurile și volumele acestor resurse. India are rezerve importante de minerale precum fierul, bauxita și manganul, și un accent deosebit pe gestionarea apei subterane, având rezerve mai moderate de petrol și gaze naturale. China se remarcă prin resursele sale abundente de cărbune, metale de bază și metale rare, având un accent semnificativ pe dezvoltarea resurselor geotermale și reducerea dependenței de cărbune. Aceste diferențe reflectă strategiile de dezvoltare economică ale fiecărei țări și influențează modul în care fiecare națiune abordează provocările legate de resurse și securitatea energetică.

În viitor, India are potențialul de a-și accelera creșterea economică prin reforme structurale, îmbunătățirea infrastructurii și atragerea de investiții străine directe. De asemenea, sectorul tehnologic al Indiei, deja puternic, poate continua să crească și să contribuie semnificativ la PIB-ul național. Investițiile continue în tehnologie și inovație, precum și inițiativele strategice cum ar fi ,,Belt and Road Initiative'', pot menține China ca o putere economică globală. Inițiativa solicită contribuții comune și are un focus clar, care este de a promova construcția de infrastructură

și conectivitatea, de a întări coordonarea în politicile economice, de a spori complementaritatea strategiilor de dezvoltare și de a stimula dezvoltarea interconectată pentru a atinge prosperitatea comună (Xinhua, 2017).

Analiza Comparativă a Demografiei Chinei și Indiei: Tendințe, Provocări și Politici

Analiza demografică a Indiei și a Chinei relevă diferențe esențiale în structura și dinamica populațiilor acestor două națiuni majore. Studiul demografic este crucial pentru înțelegerea impactului asupra economiei, societății și politicii fiecărei țări.

Caracteristici	India	China
Structura de vârstă	**0-14 ani:** 24.5% **15-64 ani:** 68.7% **65 ani și peste:** 6.8%	**0-14 ani:** 16.3% **15-64 ani:** 69.3% **65 ani și peste:** 14.4%
Rata de creștere a populației	0.72%	0.23%
Rata natalității	16.2 nașteri la 1.000 de locuitori	10.2 nașteri la 1.000 de locuitori
Rata mortalității	9.1 decese la 1.000 de locuitori	7.7 decese la 1.000 de locuitori
Rata netă de migrație	0.1 migrant(i) la 1.000 de locuitori	-0.1 migrant(i) la 1.000 de locuitori
Urbanizare	36.4% din populația totală	64.6% din populația totală
Raportul de gen	48.42% femei 51.58% bărbați	49.06% femei 50.94% bărbați

(The World Factbook)
(United Nations)

Structura populației din India și China prezintă diferențe notabile. India are o structură demografică mai tânără, în timp ce China se confruntă cu o populație îmbătrânită. India continuă să aibă o rată de creștere a populației mai ridicată, cu o natalitate semnificativ mai mare decât în China. În contrast, rata de

creștere a populației în China a scăzut considerabil din cauza politicilor de control al natalității, cu o natalitate în scădere și o stagnare previzionată a populației în viitorul apropiat.

Migrarea internă și urbanizarea sunt aspecte importante în ambele țări. India, deși a accelerat urbanizarea, se confruntă cu provocări semnificative în gestionarea migrației interne și dezvoltarea infrastructurii urbane necesare pentru a susține creșterea populației urbane China a avut un proces rapid de urbanizare, cu orașe mari precum Shanghai și Beijing devenind centre economice majore. (United Nations Development Programme, 2024).

Istoricul demografic al Indiei și Chinei reflectă evoluții distincte. China a implementat politici stricte de control al populației, precum politica unui singur copil, urmată de politica a doi copii, care a avut un impact semnificativ asupra structurii populației sale. În contrast, India a optat pentru o abordare mai puțin restrictivă, concentrându-se pe educația și sănătatea publică pentru a controla creșterea populației. Aceste politici au influențat considerabil structurile demografice și economice ale ambelor țări (World Bank, 2023).

Analiza Comparativă a Sistemelor Politice din India și China: Structuri, Stabilitate și Perspective Viitoare

India și China prezintă diferențe marcante în privința structurii și funcționării sistemelor lor politice.

Caracteristici	India	China
Numele țării	Republica India	Republica Populară Chineză
Tip de guvernare	Republică federală parlamentară	Stat condus de partidul comunist
Capitala	New Delhi	Beijing
Diviziuni administrative	**8 state**: Andhra Pradesh, Arunachal Pradesh, Assam,	**23 provincii**: Anhui, Fujian, Gansu, Guangdong, Guizhou,

	Bihar, Chhattisgarh, Goa, Gujarat, Haryana, Himachal Pradesh, Jammu și Kashmir, Jharkhand, Karnataka, Kerala, Madhya Pradesh, Maharashtra, Manipur, Meghalaya, Mizoram, Nagaland, Odisha, Punjab, Rajasthan, Sikkim, Tamil Nadu, Telangana, Tripura, Uttar Pradesh, Uttarakhand, West Bengal **8 teritorii unionale**: Andaman și Nicobar, Chandigarh, Dadra și Nagar Haveli și Daman și Diu, Delhi, Ladakh, Lakshadweep, Puducherry	Hainan, Hebei, Heilongjiang, Henan, Hubei, Hunan, Jiangsu, Jiangxi, Jilin, Liaoning, Qinghai, Shaanxi, Shandong, Shanxi, Sichuan, Yunnan, Zhejiang; **5 regiuni autonome**: Guangxi, Nei Mongol (Mongolia Interioară), Ningxia, Xinjiang Uyghur, Xizang (Tibet) **4 municipalități**: Beijing, Chongqing, Shanghai, Tianjin **2 regiuni administrative speciale**: Hong Kong, Macau
Independență	15 august 1947 (independența față de Regatul Unit)	1 octombrie 1949 (înființarea Republicii Populare Chineze)
Sistem juridic	Sistem de drept comun bazat pe modelul englez; coduri legale personale separate se aplică musulmanilor, creștinilor și hindușilor; revizuirea judiciară a actelor legislative	Drept civil influențat de sistemele de drept civil sovietic și european continental; legislația păstrează puterea de a interpreta statutele

(The World Factbook)

India, cea mai mare democrație din lume, se caracterizează printr-un sistem politic federal și parlamentar, stabilit prin Constituția sa din 1950. Structura politică a Indiei este complexă, reflectând diversitatea etnică, religioasă și culturală a țării. Sistemul este bazat pe principiile democrației reprezentative, cu alegeri libere și corecte care joacă un rol crucial în funcționarea sa (Habermas, 2000, pg. 151-155). Este o republică federală cu un sistem parlamentar unicameral. Președintele Republicii India este șeful de stat, însă rolul său este în mare parte ceremonial. Funcția executivă este deținută de prim-ministru, liderul partidului majoritar în Lok Sabha, camera inferioară a Parlamentului Indian. Parlamentul este structurat în două camere, Lok Sabha și Rajya Sabha, dar puterea legislativă efectivă este concentrată în Lok Sabha (Habermas, 2000, pg. 151-155).

Partidele politice din India sunt diverse, reflectând structura socio-culturală a țării. Acest pluralism permite o reprezentare extinsă a diferitelor interese regionale și naționale.

Politica externă a Indiei este caracterizată de o abordare strategică, orientată spre consolidarea influenței regionale și globale. India își dezvoltă relațiile internaționale prin parteneriate strategice cu puteri mondiale, inclusiv Statele Unite și Uniunea Europeană, și prin implicarea activă în organizații internaționale precum Națiunile Unite și ASEAN (Habermas, 2000, pg. 159-164). În contextul rivalității regionale, India caută să îmbunătățească relațiile cu țările vecine, în special cu Pakistanul și China, în timp ce promovează stabilitatea și dezvoltarea economică în Asia de Sud. Politica externă a Indiei include și inițiative pentru combaterea terorismului, promovarea comerțului și abordarea problemelor globale, precum schimbările climatice (Habermas, 2000, pg. 159-164).

China este organizată ca o republică socialistă sub conducerea unui sistem unipartidist dominat de Partidul Comunist Chinez (PCC). Această structură politică reflectă un model de centralizare

extremă a puterii, cu un control riguros asupra tuturor aspectelor vieții politice și sociale. Liderul PCC, care simultan îndeplinește funcțiile de președinte al Republicii Populare Chineze și președinte al Comisiei Militare Centrale, deține o autoritate considerabilă asupra guvernului și forțelor armate (Dickson, 2016, pg. 25-50). Acest sistem de concentrare a puterii asigură o coordonare eficientă a politicii și strategiei naționale, dar limitează în mod semnificativ participarea publicului și pluralismul politic. PCC este structurat ierarhic, cu două organe principale de conducere: Politburo-ul și Comitetul Permanent al Politburo-ului. Politburo-ul, format dintr-un număr mai mare de membri, se ocupă de definirea direcțiilor strategice și politice, în timp ce Comitetul Permanent, constituit dintr-un grup restrâns de lideri, ia deciziile fundamentale și de mare importanță pentru partid și stat (Dickson, 2016, pg. 25-50). Deciziile critice sunt luate în cadrul acestor grupuri, în cadrul unui proces intern de consultare și deliberare. Sistemul electoral din China este restrictiv și nu permite o competiție deschisă pentru poziții de conducere. Schimbările de lideri sunt planificate și coordonate în mod intern de către PCC, fără alegeri directe care să implice votul publicului. Acest mecanism asigură o continuitate în leadership și o stabilitate politică relativă, dar se bazează pe limitarea libertăților civile și a pluralismului politic, iar lipsa de transparență și controlul asupra mass-media pot contribui la o acumulare de tensiuni interne (Dickson, 2016, pg. 75-100).

În ceea ce privește politica externă, China adopta o abordare pro activă și ambițioasă, cu scopul de a-și extinde influența globală. Strategii precum inițiativa „Belt and Road" reflectă obiectivele Beijingului de a construi și consolida legături economice și strategice cu alte țări, având ca țintă promovarea intereselor economice și creșterea influenței geopolitice (Dickson, 2016, pg. 150-180). Această agresivitate în politica externă a generat tensiuni cu vecinii, inclusiv India, și a atras critici internaționale, în special în contextul disputelor teritoriale din

Marea Chinei de Sud și al preocupărilor legate de drepturile omului (Dickson, 2016, pg. 150-180).

În perspectiva viitorului politic, India și China se află pe traiectorii distincte, fiecare confruntându-se cu provocări și oportunități proprii, influențate de structura lor politică și contextul internațional. Viitorul politic al celor două țări va fi determinat de modul în care fiecare țară gestionează provocările interne și externe. India va continua să navigheze complexitatea diversității interne și să dezvolte relații externe strategice pentru a sprijini creșterea economică și stabilitatea regională, în timp ce China se va concentra pe menținerea unui control autoritar și pe extinderea influenței internaționale. Ambele state vor trebui să abordeze eficient provocările interne și să valorifice oportunitățile externe pentru a-și consolida pozițiile pe scena globală.

Analiza Comparativă a Puterii Militare între India și China: Capacități Cibernetice, Tehnologii Avansate și Proiecția Forței

În contextul geopolitic global actual, India și China se conturează ca actori militari majori, având impact semnificativ asupra echilibrului de putere în Asia și nu numai. Ambele națiuni, cu economii în creștere rapidă și populații uriașe, investesc substanțial în dezvoltarea și modernizarea forțelor lor armate. Această competiție militară reflectă nu doar ambițiile lor regionale, ci și intențiile de a proiecta influență pe scena globală.

India se dovedește a fi un jucător militar important în Asia și în afara ei. Forțele Armate Indiene sunt structurate și echipate pentru a răspunde provocărilor regionale și pentru a susține obiectivele naționale în contextul unei competiții internaționale crescânde.

China, ca o putere emergentă și ascendentă pe scena globală, și-a consolidat poziția de lider militar printr-o combinație strategică de resurse financiare, tehnologice și umane. În

ultimele decenii, țara a investit masiv în modernizarea și extinderea forțelor sale armate, acoperind toate dimensiunile esențiale ale puterii militare.

Caracteristici	**India**	**China**
Cheltuieli militare – anul 2023	2,3% din PIB	1,5% din PIB
Inventar și achiziții de echipamente militare	**Inventar:** O mare parte din inventarul militar constă în echipamente de origine rusă și sovietică; există o proporție mai mică, dar în creștere, de armament occidental și produs intern. **Achiziții:** Rusia continuă să fie principalul furnizor de arme pentru India, deși în ultimii ani India a crescut achizițiile de la alți furnizori, inclusiv Franța, Israel și SUA. India este unul dintre cei mai mari importatori de arme din lume. **Industria de apărare:** India are capacitatea de a produce o gamă variată de sisteme de armament	**Echipamente:** PLA (Armata Populară de Eliberare) dispune de un mix de sisteme mai vechi și un număr crescând de sisteme moderne, în mare parte produse intern, influențate semnificativ de tehnologia provenită din alte țări. Rusia a fost principalul furnizor de echipamente militare străine în ultimii ani. **Industria de apărare:** China are unul dintre cele mai mari sectoare de apărare-industrială din lume și este capabilă să producă sisteme de arme avansate în toate domeniile militare (anul 2024)

	pentru aer, teren, rachete și nave, atât pentru uz intern, cât și pentru export. De asemenea, produce sisteme de arme sub licență (anul 2023)	
Vârsta și obligația serviciului militar	Între 16,5 și 27 de ani pentru serviciul militar voluntar pentru bărbați și femei	**Bărbați:** 18-22 ani pentru serviciul militar selectiv obligatoriu, cu o obligație de serviciu de 2 ani **Femei:** 18-19 ani, care sunt absolvente de liceu și îndeplinesc cerințele pentru anumite locuri de muncă în armată, sunt supuse conscripției
Dezvoltări militare – anul 2024	**1,800:** Republica Democratică Congo (MONUSCO) **200:** Înălțimile Golan (UNDOF) **890:** Liban (UNIFIL) **2,350:** Sudanul de Sud (UNMISS) **590:** Sudan (UNISFA) (2024) India are peste 6.000 de personal militar și de poliție desfășurat în misiuni ale ONU	**400:** Liban (UNIFIL) **1,030:** Sudanul de Sud (UNMISS) **150:** Sudan/Sudanul de Sud (UNISFA) **Până la 2,000:** Djibouti

(The World Factbook)

Puterea cibernetică și capabilități cibernetice ofensive

India investește semnificativ în infrastructura cibernetică și tehnologică, ceea ce constituie fundamentul puterii sale cibernetice. Guvernul indian a lansat și implementat inițiative majore pentru dezvoltarea infrastructurii IT și a rețelelor cibernetice. Aceste investiții nu doar că facilitează procesarea și stocarea datelor, dar asigură și o capacitate sporită de răspuns și de protecție împotriva amenințărilor cibernetice.

Capacitățile de apărare și atac cibernetic ale Indiei sunt bine dezvoltate și coordonate printr-o serie de organizații și agenții guvernamentale. Capacitățile ofensive ale Indiei includ dezvoltarea de tehnici avansate de atac cibernetic, care sunt utilizate în scopuri strategice și pentru descurajare. India dispune de structuri precum Computer Emergency Response Team – India (CERT-IN), care coordonează răspunsul național la incidentele cibernetice și dezvoltă strategii de protecție. Unități precum „Cyber Agency" din cadrul Direcției Generale a Sistemelor de Informații (DGIS) sunt responsabile pentru protecția infrastructurii critice și pentru efectuarea de operațiuni cibernetice. În plus, India a dezvoltat și unități speciale în cadrul Forțelor Aeriene Indiene care se ocupă cu războiul electronic, având ca scop atât protejarea propriilor resurse, cât și desfășurarea de atacuri cibernetice asupra inamicilor (Cherian Samuel, 2024).

Capacitățile de spionaj cibernetic și de colectare de informații sunt și ele parte integrantă a puterii cibernetice a Indiei. India utilizează tehnici avansate pentru a aduna informații strategice și pentru a efectua operațiuni de recunoaștere în spațiul cibernetic. Acest lucru implică nu doar colectarea de date sensibile, dar și monitorizarea și analizarea activităților cibernetice internaționale pentru a anticipa și a preveni potențiale amenințări. Resursele umane și expertiza sunt esențiale pentru succesul în domeniul cibernetic, iar India investește constant în formarea și dezvoltarea profesională a specialiștilor săi în securitate cibernetică. Instituțiile

educaționale din India oferă programe de pregătire avansate în domeniul tehnologiei informației și securității cibernetice, contribuind la crearea unei forțe de muncă bine pregătite și specializate.

Parteneriatele internaționale și cooperarea globală sunt aspecte importante ale puterii cibernetice a Indiei. Țara colaborează cu diverse state și organizații internaționale pentru a dezvolta standarde comune de securitate cibernetică și pentru a coordona răspunsurile la amenințările cibernetice globale. Aceste parteneriate contribuie la întărirea poziției țării ca actor global în securitatea cibernetică și facilitează accesul la informații și tehnologii avansate (Hannes Ebert, 2020).

Ascensiunea Chinei ca putere globală nu se limitează doar la domeniile tradiționale ale forței militare și economice, ci se extinde semnificativ și în domeniul războiului cibernetic. Lucrarea *China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence* explorează puterea cibernetică a Chinei, analizând obiectivele sale strategice, capacitățile și implicațiile pentru securitatea globală.

În centrul strategiei cibernetice a țării se află integrarea capacităților cibernetice în cadrul mai larg al militarismului și al geopoliticii. Guvernul chinez consideră puterea cibernetică ca un element crucial al strategiei naționale, folosind-o atât ca instrument de descurajare strategică, cât și ca mijloc de obținere a avantajelor asimetrice față de posibilii adversari. Această abordare este caracterizată de o combinație de operațiuni cibernetice ofensive și defensive, menite să îmbunătățească poziția Chinei pe scena internațională, protejând în același timp interesele sale naționale. Puterea cibernetică a Chinei reflectă de asemenea eforturile sale de a construi o infrastructură cuprinzătoare de apărare cibernetică. Recunoscând vulnerabilitățile inerente în spațiul cibernetic, China a înființat diverse organizații și unități dedicate securității cibernetice. Acestea includ Administrația Spațială Cibernetică a Chinei (CSAC) și Forța Strategică de

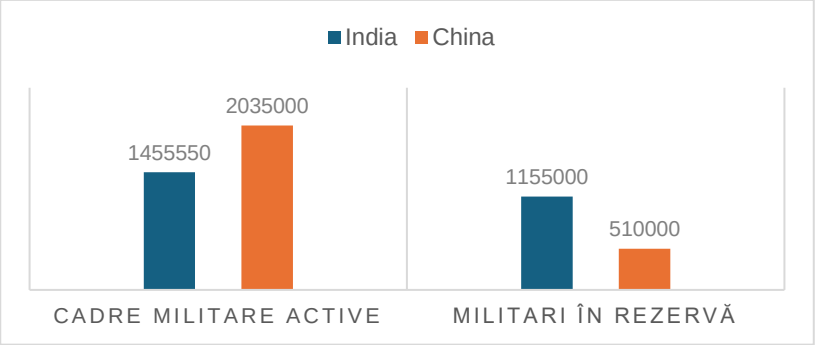
Suport a Armatei Populare de Eliberare (PLA), care sunt responsabile pentru protejarea infrastructurii cibernetice a Chinei împotriva amenințărilor externe și asigurarea rezilienței sistemelor sale digitale.

Un aspect esențial al puterii cibernetice a Chinei este accentul pus pe spionajul cibernetic. Operațiunile cibernetice chineze au fost utilizate sistematic pentru a aduna informații, a fura date de proprietate și a compromite infrastructura critică a altor națiuni. Spionajul cibernetic chinez este adesea realizat prin malware sofisticat, atacuri de phishing și alte intruziuni cibernetice, vizând atât entitățile guvernamentale, cât și cele din sectorul privat.

China a creat, de-a lungul timpului, o rețea complexă de unități și agenții specializate în război cibernetic și electronic. Una dintre cele mai notabile structuri este „Unitatea de Război Cibernetic a Armatei de Eliberare a Poporului". Această unitate este implicată în activități de spionaj cibernetic și atacuri cibernetice îndreptate împotriva unor obiective internaționale, inclusiv companii și organizații guvernamentale (Mark A. Stokes, Jenny Lin, L.C. Russell Hsiao, 2011, pg. 3-5).

Prin utilizarea instrumentelor cibernetice pentru a exercita presiune și a perturba adversarii, China urmărește să obțină avantaje strategice fără a se angaja în conflicte militare convenționale (Magnus Hjortdal, 2011).

Cadre militare active și militari în rezervă



(Global Firepower, 2024)

Forțe aeriene, terestre, navale și forțe speciale

Forțe aeriene

Caracteristici	India	China
Numărul total de aeronave	2296	3304
Avioane de vânătoare și interceptoare	606	1207
Avioane de atac la sol	130	371
Aeronave de transport	264	289
Avioane de antrenament	351	402
Avioane pentru misiuni speciale	70	112
Avioane pentru realimentare în zbor	6	10
Elicoptere	869	913
Elicoptere de atac	40	281

(Global Firepower, 2024)

Forțe terestre

Caracteristici	India	China
Tancuri	4614	5000
Vehicule blindate	151248	174300
Artilerie autopropulsată	140	3850
Artilerie tractată	3243	1434
Lansatoare de rachete multiple/proiectile reactive	702	3180

(Global Firepower, 2024)

Forțe navale

Caracteristici	India	China
Puterea flotei	294	730
Portavioane	2	2
Portelicoptere	0	3
Submarine	18	61
Distrugătoare	12	49
Fregate	12	42
Corvete	18	72
Nave de patrulare	137	150

(Global Firepower, 2024)

Articolul „Special Forces of India” analizează structura, misiunile și capabilitățile unităților de forțe speciale ale Indiei, subliniind importanța acestora în strategia de apărare națională. Forțele speciale indiene sunt organizate în cadrul diferitelor ramuri ale forțelor armate și organizații paramilitare, inclusiv Regimentul de Parașutiști (Para SF), Garda Națională de Securitate (NSG), Comando Marine (MARCOS) și Forțele de

Comando ale Armatei (Ghatak Force). Aceste unități sunt pregătite să desfășoare misiuni complexe de combatere a terorismului, salvare a ostaticilor, război de gherilă și operațiuni speciale în medii diverse, inclusiv urbane, montane și maritime (PC Katoch, 2011).

Articolul „Chinese Special Forces: Dragons of the East" oferă o analiză detaliată a forțelor speciale ale Chinei, subliniind structura și capabilitățile acestora. Aceste unități de elită, integrate în cadrul Armatei Populare de Eliberare (PLA), includ Forțele Speciale de Operațiuni (SOF), Forțele Speciale ale Marinei (PLANMC) și Forțele Speciale ale Forței Aeriene (PLAAF). Fiecare unitate este specializată în misiuni complexe, care variază de la atacuri directe și operațiuni de recunoaștere până la salvarea ostaticilor și combaterea terorismului (Maxwell Goldstein, 2024).

Tehnologie militară și robotică

În contextul tehnologiei militare de ultimă generație, India a făcut progrese semnificative în ultimele decenii, axându-se pe dezvoltarea și implementarea unor soluții avansate pentru a-și întări capacitățile de apărare. India a investit masiv în cercetarea și dezvoltarea tehnologiilor avansate, inclusiv în domeniul rachetelor, al sistemelor de apărare antiaeriană și al inteligenței artificiale. Conform declarațiilor recente ale șefului Statului Major al Armatei, generalul Manoj Pande, anul 2024 va fi dedicat absorbției tehnologice, marcând o tranziție de la angajamentul anterior din 2023 pentru „transformare". Această schimbare reflectă o adaptare la natura în continuă schimbare a războiului și a provocărilor de securitate. Armata Indiană va integra drone și sisteme anti-drone în batalioane de infanterie, artilerie și blindate, și va înființa aripi de suport pentru operațiuni cibernetice, subliniind angajamentul față de capacitățile cibernetice avansate (Ankit K, 2024).

Armata Indiană va integra în curând 25 de roboți câini MULE (Multi-Utility Legged Equipment) pentru supraveghere și transport pe terenuri dificile. Comanda pentru 100 de astfel de roboți a fost plasată în urgență în septembrie anul trecut. Dacă acești roboți se dovedesc eficienți, achizițiile vor fi extinse. Echipați cu camere termice și senzori avansați, roboții MULE pot realiza supravegherea în zone montane și ascunse, minimizând riscurile pentru soldați și transportând sarcini mici. Controlați de la distanță, aceștia îmbunătățesc conștientizarea situațională și oferă date în timp real (Analiza Pathak, 2024).

India se remarcă în mod considerabil pe scena internațională prin avansurile sale în domeniul tehnologiei informației și al securității cibernetice, domenii în care deține un număr semnificativ de specialiști și cercetători de renume. Această competență extinsă în tehnologia informației și securitatea cibernetică are un impact profund asupra capacităților cibernetice ale Forțelor Armate Indiene, demonstrând o integrare eficientă a acestor cunoștințe în strategia națională de apărare.

Expertiza avansată a specialiștilor și cercetătorilor din India în domeniul Informatică și Securitate Cibernetică are un impact semnificativ asupra capacităților Forțelor Armate Indiene, întărind securitatea națională și protejând infrastructura critică. Prin implementarea de soluții tehnologice avansate și prin formarea continuă a specialiștilor, India demonstrează o integrare eficientă a tehnologiei informației în apărarea națională, consolidându-și astfel poziția în domeniul securității cibernetice la nivel global.

În ultimele decenii, China a demonstrat o ascensiune remarcabilă în domeniul tehnologiilor de vârf, cu un accent deosebit pe inteligența artificială (IA). Studiile recente evidențiază faptul că statul nu doar că investește masiv în cercetare și dezvoltare, dar și că dezvoltă strategii sofisticate pentru a-și consolida poziția în această arie emergentă. Beijingul recunoaște IA ca fiind un factor esențial pentru modernizarea forțelor sale armate și pentru menținerea competitivității globale. Investițiile

chineze în IA se concentrează pe dezvoltarea unor tehnologii avansate, precum învățarea automată, procesarea limbajului natural și viziunea computerizată, care sunt integrate în diverse domenii, de la securitatea națională la aplicații civile. De asemenea, strategia de inovare chineză include colaborări între sectorul public și cel privat, precum și parteneriate internaționale pentru a accelera progresul tehnologic (Elsa B. Kania, 2019, pg. 1-20).

De asemenea, China a investit considerabil în cercetarea și dezvoltarea tehnologiilor robotice, concentrându-se pe două domenii principale: robotică industrială și robotică militară. Proiectele de robotică industrială sunt destinate să îmbunătățească eficiența și productivitatea în sectoare cheie precum manufacturarea și logistică, facilitând tranziția către o economie bazată pe tehnologii avansate. Această abordare este vizibilă prin implementarea de soluții robotice în linii de producție, unde robotii contribuie la automatizarea proceselor și la reducerea costurilor. Pe de altă parte, dezvoltarea roboticii militare în China a câștigat o importanță semnificativă în contextul strategiei naționale de apărare. Inovațiile în domeniul dronelor și al vehiculelor autonome sunt menite să întărească capabilitățile militare ale țării și să sprijine implementarea unor strategii avansate de apărare. Aceste tehnologii permit monitorizarea și intervenția în terenuri dificile, oferind un avantaj tactic considerabil (Jonathan Ray, Katie Atha, Edward Francis, Caleb Dependahl, Dr. James Mulvenon, Daniel Alderman, and Leigh Ann Ragland-Luce, 2016, pg. 26-29, 48-50).

Concluzii

Comparația între India și China subliniază diferențe fundamentale în abordarea și resursele fiecărei țări, ce au un impact profund asupra poziționării lor globale și capacităților lor de apărare.

Din perspectiva geografică și economică, . India, deși are o poziție strategică importantă și o economie în creștere, se confruntă cu limitări mai mari în ceea ce privește resursele naturale și dimensiunea economică. Acest lucru sugerează că India trebuie să valorifice în mod optim resursele sale existente și să investească în dezvoltarea economică și infrastructurală pentru a contrabalansa acest decalaj. China beneficiază de o amplasare extinsă și de resurse naturale semnificative care îi permit să mențină o putere economică robustă și o influență geopolitică extinsă.

Dintr-o perspectivă politică și demografică, diferențele de regim și structura populațională influențează profund modul în care cele două națiuni își gestionează politica internă și externă.

În domeniul militar, India are competențe remarcabile în domeniul securității cibernetice și își consolidează progresiv capabilitățile militare, dar trebuie să continue să investească în modernizarea echipamentelor și în dezvoltarea tehnologiilor avansate pentru a ține pasul cu China.

În ansamblu, fiecare țară are puncte forte distincte care îi influențează strategia națională și internațională. În timp ce India se remarcă prin expertiza sa în domeniul cibernetic și printr-o democrație dinamică, China beneficiază de o putere economică și militară considerabilă,.Ambele țări trebuie să își adapteze strategiile și să își optimizeze resursele pentru a-și menține și extinde influența în arena globală, reflectând complexitatea și diversitatea provocărilor și oportunităților pe care le întâmpină.

Bibliografie

1. CLIFF, ROGER, *China's Military Power: Assessing Current and Future Capabilities*, Cambridge University Press, 2015.
2. DICKSON, BRUCE J., *The Dictator's Dilemma: The Chinese Communist Party's Strategy for Survival*, Oxford University Press, 2016, pg. 25-50, 75-100, 150-180.
3. EBERT, HANNES, „Hacked IT superpower: how India secures its cyberspace as a rising digital democracy", *India Review*, vol. 19, nr. 4, 7 august 2020, pp. 376–413.
4. HJORTDAL, MAGNUS, „China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence", *Journal of Strategic Security*, vol. 4, nr. 2, iunie 2011, pp. 1–24.
5. KATOCH, PC, „Indian Special Forces: 2030", 2011.
6. PRARTHANA, „Top 15 Countries by GDP in 2024", *Global PEO Services*, https://globalpeoservices.com/top-15-countries-by-gdp-in-2024/, data accesării 7 august 2024.
7. RAY, JONATHAN; ATHA, KATIE; FRANCIS, EDWARD; DEPENDAHL, CALEB; MULVENON, DR JAMES; ALDERMAN, DANIEL; ET AL., „China's Industrial and Military Robotics Development", 2016, pg. 26-29, 48-50.
8. ROY, S. GUHA, „Demographic Trends in China and India", *China Report*, vol. 30, nr. 1, 1 februarie 1994, SAGE Publications India, pp. 1–18.
9. SAMUEL, CHERIAN, *India's International Cybersecurity Strategy*, Cybersecurity, S. Rajaratnam School of International Studies, 2014, https://www.jstor.org/stable/resrep05892.6, data accesării 15 august 2024.

10. STOKES, MARK A; LIN, JENNY; HSIAO, L C RUSSELL, „The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure", 2011, pg. 3-5.
11. XIA, LONGJI; LIU, YUN, „Electricity generation and China's GDP growth under dual control policy", *Energy Exploration & Exploitation*, vol. 42, nr. 4, 1 iulie 2024, SAGE Publications Ltd STM, pp. 1422–1431.
12. „Overview", *World Bank*, https://www.worldbank.org/en/country/china/overview, data accesării 14 august 2024.
13. „China", *The World Factbook*, https://www.cia.gov/the-world-factbook/countries/china/#people-and-society, data accesării 5 august 2024.
14. „China - Minerals, Resources, Mining | Britannica", https://www.britannica.com/place/China/Minerals, data accesării 14 august 2024.
15. „China's Economic Rise: History, Trends, Challenges, and Implications for the United States", https://www.everycrsreport.com/reports/RL33534.html#Content, data accesării 12 august 2024.
16. „Chinese Special Forces: Dragons of the East", *Grey Dynamics*, https://greydynamics.com/chinese-special-forces-dragons-of-the-east/, data accesării 15 august 2024.
17. „Comparison of India and China Military Strengths (2024)", https://www.globalfirepower.com/countries-comparison-detail.php?country1=india&country2=china, data accesării 15 august 2024.
18. „Full text of Chinese President Xi's address at APEC CEO Summit - Xinhua | English.news.cn",

http://www.xinhuanet.com/english/2017-11/11/c_136743492.htm, data accesării 14 august 2024.

19. „GDP (current US$) - India | Data”, https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=IN, data accesării 7 august 2024.
20. „GDP per capita (current US$) - China | Data”, https://data.worldbank.org/indicator/NY.GDP.PCAP.CD?locations=CN, data accesării 8 august 2024.
21. „Human Development Report 2023-24”, *UNDP*, https://www.undp.org/india/publications/human-development-report-2023-24-0, data accesării 15 august 2024.
22. „India”, *The World Factbook*, https://www.cia.gov/the-world-factbook/countries/india/#environment, data accesării 5 august 2024.
23. „Indian Army To Induct 25 Remote-Controlled MULE Robot Dogs; Know All About It Here”, https://www.india.com/news/india/all-about-remote-controlled-mule-robot-dogs-indian-armys-new-induction-to-its-squad-multi-utility-legged-equipment-7037949/, data accesării 15 august 2024.
24. „Indian Army’s year of technological advancement in 2024”, *orfonline.org*, https://www.orfonline.org/expert-speak/indian-army-s-year-of-technological-advancement-in-2024, data accesării 15 august 2024.
25. *Multiple modernities*, Daedalus 129.2000,1, American Academy of Arts and Sciences, Cambridge, Mass, 2000, pg. 151-164.
26. „‘Source of anxiety’: China’s new aircraft carrier pushes Asia to upgrade”, *South China Morning Post*, https://www.scmp.com/week-asia/politics/article/3264962/chinas-new-aircraft-carrier-pushes-india-japan-south-korea-boost-naval-

capabilities-source-anxiety, data accesării 15 august 2024.

27. „World Bank Open Data”, *World Bank Open Data*, https://data.worldbank.org, data accesării 7 august 2024.
28. Elsa B. Kania , ,,Chinese Military Innovation in Artificial Intelligence’’, 2019, pg. 1-20.
29. „World Population Prospects - Population Division - United Nations”, https://population.un.org/wpp/Download/Standard/Population/, data accesării 25 august 2024.

România prin lentila infracționalității cibernetice

Andreea Pop
(voluntară la Grupului de Lucru pentru Securitate și Apărare Cibernetică și membru susținător al Asociației Ofițerilor în Rezervă din România)

Abstract

Prăbușirea URSS a pus capăt epocii bipolare, făcând astfel loc unui sistem internațional multipolar. Interconectarea politică, economică și socială a actorilor sistemului internațional favorizează procesul de globalizare, însă pe de altă parte deschide scena riscurilor și amenințărilor hibride, precum cele ecologice sau cibernetice. Amenințările de natură cibernetică au devenit din ce în ce mai populare o dată cu evoluția tehnologică accelerată, iar formele pe care le preiau afectează atât sisteme informatice ale structurilor importante cât și cetățeni de rând. Această lucrare urmărește să exploreze atacurile cibernetice în România, căutând să răspundă la întrebarea: Cum se manifestă criminalitatea cibernetică în România? În prima parte, voi, prezenta o introducere a fenomenului de criminalitate cibernetică, în partea a doua voi identifica manifestarea acestuia în România, iar în final voi conclude cu analiza criminalității cibernetice ca și amenințare hibrid emergentă.

Introducere

Doar în iunie 2022 s-au înregistrat aproximativ 10 milioane de descărcări de programe malware.[78] Criminalitatea cibernetică este un rezultat al evoluției tehnologice și poate fi definită ca orice infracțiune comisă utilizând un sistem informatic. Fie că este vorba de furt de date sau infectarea unui program cu sisteme malițioase, criminalitatea cibernetică poate lua numeroase forme, de la atacuri de tip ransomware – în cadrul cărora infractorii preiau controlul unui sistem informatic și cer o răscumpărare pentru a putea fi revendicate de către ținte - până la dezinformare – atacuri menite să manipuleze opinia publică prin distribuirea de informații false. Acest fenomen se poate întinde chiar până la furtul de identitate, infracțiuni ce aparțin de sectorul economic și financiar, hărțuire și spionaj. Natura criminalității pe internet evoluează o dată cu mediul în care acesta a apărut. Prin urmare, cu cât spațiul cibernetic va fi mai evoluat, cu atât amenințările vor fi mai avansate.

În ultima perioadă, scena infracțiunilor cibernetice a fost pusă în lumină datorită atacurilor cibernetice lansate de Callisto Group, Star Blizzard și COLDRIVER, grupări de acțiuni cibernetice aparținând Serviciul Federal de Securitate rus, menite să spioneze SUA.[79] Doi acuzați principali au fost deconspirați, condamnați pentru rolul lor în acțiunile malițioase, iar Statele Unite au emis un aviz de securitate cibernetică în care au explicat detaliile atacului, semnale de alarmă dar și moduri în care securitatea rețelelor poate fi îmbunătățită astfel încât atacurile să fie prevenite. Nu în ultimul rând, Departamentul de

[78] „Principalele amenințări cibernetice în UE”, *Consilium*, https://www.consilium.europa.eu/ro/infographics/cyber-threats-eu/, data accesării 1 august 2024.
[79] „U.S. Takes Action to Further Disrupt Russian Cyber Activities”, *United States Department of State*, https://www.state.gov/u-s-takes-action-to-further-disrupt-russian-cyber-activities/, data accesării 2 august 2024.

Justiție al Statelor Unite ale Americii oferă o recompensă de 10 milioane de dolari pentru orice informație legată de cei doi deconspirați. [80]

criminalitatea cibernetică – dimensiuni

Datorită faptului că infracțiunile cibernetice pot lua variate forme, autori precum Gordon și Ford disting două categorii de infracțiuni cibernetice. Tipul I de infracțiune cibernetică se regăsește în atacurile de tip phishing, în cadrul cărora ținta accesează pagini care imită anumite servicii și fie permite accesul virușilor în dispozitiv, fie îi sunt compromise date personale stocate pe dispozitiv și devine astfel victima unui furt.[81] Acest tip de infracțiuni este cel mai răspândit în domeniul securității cibernetice, iar succesul acestora este influențat de vulnerabilitățile unui sistem informatic. Vulnerabilitățile reprezintă lacune în siguranța unei rețele, permițând entităților intruse să facă modificări în program și să exploateze sistemul informatic de pe care un utilizator accesează programul compromis.[82]

Al doilea tip de infracțiune cibernetică se regăsește în acțiuni de hărțuire, manipulare, șantaj, spionaj tehnologic sau chiar racolare de minori.[83] În cadrul acestor infracțiuni, elementul cibernetic este instrumentul și nu obiectul infracțiunii. În astfel de situații, un utilizator rău-intenționat alege și exploatează victima pe Internet. De pildă, rețelele de socializare sunt de multe ori canale prin care diferiți agresori hărțuiesc persoane, în cele mai multe cazuri, minori. Recent, Biroul Federal de Investigații alături de Departamentul de Poliție din Hartford,

[80] *Ibidem*.
[81] Sarah Gordon, Richard Ford, „On the definition and classification of cybercrime", *Journal in Computer Virology*, vol. 2, nr. 1, august 2006, p. 2.
[82] *Ibidem*.
[83] *Ibidem*, p. 3.

Connecticut, au anunțat arestarea unui individ pe fondul infracțiunii de corupere sexuală a unui minor, infracțiune realizată pe o platformă de socializare, Discord. S-a mai descoperit că inculpatul avea conversații cu victima și deținea imagini cu caracter explicit cu aceasta.[84] Tipul I de infracțiune, conform lui Gordon și Ford, este mult mai axat pe partea tehnică decât tipul II, care poate avea la bază alți factori determinanți.[85]

Criminalitatea cibernetică în România – prevenire și răspuns

Atacurile cibernetice nu ratează nici România. Datorită integrării europene, România are parte de ajutor în a confrunta acest tip de infracțiune prin intermediul colaborării cu statele partenere. Prin instituții precum INTERPOL, România reușește să combată amenințările cibernetice cu ajutorul schimbului de informații și platformelor securizate pentru cooperarea polițienească. De asemenea, EUROPOL desfășoară programul EC3 – European Cybercrime Centre – menit să dezvolte strategiile de combatere și prevenire a criminalității cibernetice, prin sprijinirea investigațiilor de criminalitate cibernetică, analize strategice asupra fenomenului, menținerea unei platforme de decriptare pentru a facilita investigațiile și colectarea de informații atât din sectorul public cât și din cel privat.[86]

---

[84] „District of Connecticut | Hartford Man Charged with Receiving Sexually Explicit Images of Minor Girl He Communicated with on Discord | United States Department of Justice", https://www.justice.gov/usao-ct/pr/hartford-man-charged-receiving-sexually-explicit-images-minor-girl-he-communicated, data accesării 2 august 2024.

[85] Sarah Gordon, Richard Ford, „On the definition and classification of cybercrime", p. 2.

[86] „EC3 Programme Board | Europol", https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/ec3-programme-board, data accesării 3 august 2024.

În aceeași ordine de idei, România a obținut un sprijin în ceea ce privește securitatea cibernetică din partea Statelor Unite. În urma parteneriatului strategic dintre România și Statele Unite, s-a decis constituirea unor Grupuri de Lucru sectoriale pentru problemele politice și militare, securitate cibernetică și afaceri digitale. În august 2019, a fost stabilită o Declarație Comună între cele două state și s-au introdus două noi domenii de colaborare, unul din acestea fiind securitatea rețelelor 5G.[87] A cincea generație a rețelelor wireless a fost implementată în România în urmă cu puțin timp, iar în ciuda controverselor create, se răspândește accelerat. Cadrul legislativ referitor la infrastructurile informatice și implementarea rețelelor 5G are ca scop autorizarea producătorilor de tehnologii și echipamente infromatice 5G în vederea prevenirii și eliminării riscurilor și amenințărilor la adresa securității naționale.[88]

La data de 14.03.2023, a fost adoptată legea 58/2023 privind organizarea și desfășurarea activităților din domeniile securitate și apărare cibernetică, mecanisme de cooperare și atribuțiile instituțiilor de securitate și apărare cibernetică.[89] Legea privind securitatea și apărarea cibernetică a României are în vedere asigurarea rezilienței statului la amenințări cibernetice în termeni de prevenție, răspuns și protecție, în concordanță cu prevederile legislației UE. [90] Astfel, au fost aduse modificări legii 51/1991 privind securitatea națională a României, adăugând

[87] „Parteneriatul strategic România – SUA | Ministry of Foreign Affairs", https://www.mae.ro/node/4944, data accesării 3 august 2024.
[88] „LEGE 163 11/06/2021 - Portal Legislativ", 1, https://legislatie.just.ro/Public/DetaliiDocumentAfis/243213, data accesării 6 august 2024.
[89] „LEGE 58 14/03/2023 - Portal Legislativ", 1, https://legislatie.just.ro/Public/DetaliiDocument/265677, data accesării 8 august 2024.
[90] „buletin-cyber-sem-1-2023-rom-online.pdf", p. 9, https://www.sri.ro/assets/files/publicatii/buletin-cyber-sem-1-2023-rom-online.pdf, data accesării 8 august 2024.

trei noi amenințări: atacuri cibernetice asupra infrastrcturii informatice și de comunicații de interes național, acțiuni cu consecințe asupra infrastructurilor menționate și acțiuni derulate de entități statale sau nonstatale prin realizarea în spațiul cibernetic a unor campanii de propagandă și dezinformare.[91]

În anul 2021, Poliția Română alături de Directoratul Național de Securitate Cibernetică și Asociația Română a Băncilor au lansat campania #SiguranțaOnline pentru informarea și protejarea cetățenilor cu privire la criminalitatea cibernetică prin atacurile de tip phishing.[92] Abordarea acestui proiect a avut în vedere distribuirea în online a mai multor bannere cu mesaje de tip phishing precum câștiguri sigure. A fost analizată ușurința cu care oamenii accesează astfel de mesaje, astfel că în 6 zile de la campanie, au fost înregistrate 6700 de accesări.[93] În anul 2022, această campanie s-a concentrat pe prevenirea atacurilor de tip malware, în baza analizei Criminalitatea Informatică- Atacurile Malware – Forme și Tendințe realizată de Institutul de Cercetare și Prevenire a Criminalității. Abordarea proiectului are în vedere distribuirea de mesaje printr-un spot TV informativ alături de un ghid de educație digitală.[94]

Atacuri cibernetice în România – manifestarea criminalității cibernetice

Centrul Național de Răspuns la Incidente de Securitate Cibernetică CERT-RO a concretizat în 2018 o analiză cu evoluția amenințărilor cibernetice în România. În urma procesului de colectare și prelucrare a informațiilor, s-a constatat că atacurile

[91] *Ibidem*.
[92] „Poliția Română - Campania Siguranța online”, https://www.politiaromana.ro/ro/prevenire/prevenirea-criminalitatii-informatice/campania-siguranta-online, data accesării 3 august 2024.
[93] *Ibidem*.
[94] *Ibidem*.

cibernetice țintite asupra României s-au triplat față de anul 2017.[95] Statistic, criminalitatea cibernetică în România este variată. În anul 2018 s-a înregistrat o creștere în atacurile de tip cryptojacking, în cadrul cărora infractorii folosesc sistemul informatic al victimei pentru a investi în valută de tip crypto. În România au fost identificate astfel de atacuri cu aplicații malițioase precum CoinMiner sau BitcoinMiner.[96] De asemenea, au fost identificate noi amenințări malware, printre care VPNFliter. Peste 500.00 de routere și dispozitive de stocare au fost identificate de hackeri în 54 de țări. În ceea ce privește România, au fost identificate adrese IP implicate atât în atacuri, cât și victime.[97]

În România, atacurile cibernetice evoluează cu pași repezi și pot lua diferite forme. Cele mai răspândite forme rămân atacurile de tip phishing – datorită subtilității și flexibilității – și atacurile de tip cryptojacking. Cele două sunt adesea întâlnite pe platfomrele rețelelor de socializare, datorită faptului că pot fi propagate ușor. Un sistem malițios, după ce compromite un utilizator, va folosi platforma victimei pentru a răspândi atacul. Acest tip de atacuri se soldează cel mai des cu date personale compromise, ceea ce înseamnă că există vulnerabilități în privința sistemelor informatice. Cu ajutorul unui protocol de securitate, precum autentificarea cu doi factori se poate diminua riscul pierderii datelor de autentificare sau datelor personale stocate într-un sistem informatic.

Odată cu izbucnirea conflictului dintre Rusia și Ucraina s-au înregistrat creșteri substanțiale în atacurile cibernetice țintite asupra României. Cele mai vizate ținte românești sunt instituțiile și firmele private. În 2022, Directoratul Național pentru Securitate Cibernetică (DNSC) a înregistrat un atac cibernetic de tip phishing

[95] „Documente”, p. 2, https://dnsc.ro/doc/raport, data accesării 1 august 2024.
[96] *Ibidem*, p. 6.
[97] *Ibidem*.

produs pe mail. Utilizând un link infectat, atacatorii au reușit să invadeze calculatoarele câtorva instituții publice și firme private ce lucrează cu publicul. În urma accesării linkului, a reușit să se instaleze un program malițios care să colecteze date personale, de card sau de autentificare sau date care pot fi compromise în așa fel încât să genereze noi atacuri.[98] Un alt atac din 2022, identificat de DNSC, imita o strângere de fonduri pentru refugiații Ucrainei, inițiativă supranumită „Ukraine Crisis Relief Fund". Metoda de transmitere a banilor era un portofel Bitcoin, iar textul e-mail-ului prezenta greșeli gramaticale. La final era semnat de Amin Awad, în realitate coordonator al crizelor pentru Ucraina, însă fără legătură cu Ukraine Crisis Relief Fund. [99] Atacurile de tip phishing deseori imită situații din realitate pentru a oferi un grad de credibilitate. De aceea, este important ca utilizatorii să nu acceseze linkuri suspicioase pentru a nu deveni victimele unui atac cibernetic.

România a căzut pradă și atacurilor de tip DDoS. Atacurile de tip Distributed-Denial-of-Service constă în blocarea unui sistem infromatic pe o perioadă de timp, făcând-ul astfel indisponibil pentru utilizatorii săi. La data de 29 Aprilie 2022, o serie de site-uri aparținând unor autorități naționale și instituții bancare au fost atacate cu acest sistem. Prin exploatarea unor vulenrabilități și a unor lacune în măsurile de securitate cibernetică, atacatorii au preluat controlul site-urilor și le-au indisponibilizat pentru o perioadă de timp. Gruparea KILLNET a fost responsabilă pentru acest atac țintit asupra României.[100]

---

[98] Oana Despa, „Atacurile cibernetice în România au crescut de 100 de ori în primele zile de război în Ucraina", 1–4, *Europa Liberă România*, 08:29:09Z, https://romania.europalibera.org/a/atacuri-cibernetice-masive/31781260.html, data accesării 3 august 2024.

[99] „DNSC", https://dnsc.ro/citeste/alerta-frauda-donatii-ucraina, data accesării 7 august 2024.

[100] „Atacuri cibernetice asupra site-urilor unor instituții publice și financiar-bancare", *Serviciul Român de Informații*, https://www.sri.ro/articole/atacuri-

Atacurile de tip ransomware și-au pus amprenta asupra României prin aplicația malițioasă HIVE. HIVE este un o aplicație malware folosită împotriva mai multor platforme software. La nivel național, ransomware-ul HIVE a fost utilizat în cadrul unui atac cibernetic asupra unei importante companii de carburanți. Atacatorii au criptat elemente de infrastructură IT&C, cerând răscumpărare suma de 2 milioane de dolari.[101] Atacatorii folosesc de asemenea email-uri de tip phishing pentru a asigura accesul inițial al malware-ului HIVE.[102] La finalul lunii Ianurarie 2024 innfrastructura infromatică aparținând Camerei Deputaților din Parlamentul României a fost compromisă datorită unui atac cibernetic ransomware. Malware-ul a fost dezvoltat de gruparea KNIGHT și comercializat pe darkweb.[103] De asemenea, în Februarie 2024 a avut loc un alt atac ransomware asupra sistemului informatic care gestionează platforma Hipocrate, utilizate de mai multe spitale din țară. Răspândirea atacului a dus la sisteme compromise a 26 de spitale, afectând activitatea acestora. Malware-ul utilizat este din familia PHOBOS, care a vizat în perioada 2019-2021 exclusiv sectorul medical din România.[104]

Cel mai recent atac cibernetic din România este compromiterea contului de Facebook a Universității de Medicină și Farmacie „Carol Davila". La data de 29.07.2024, Directoratul Național de Securitate Cibernetică a primit o sesizare de la reprezentanții universității cu privire la activități suspicioase și postări

---

cibernetice-asupra-site-urilor-unor-institutii-publice-si-financiar-bancare, data accesării 8 august 2024.

[101] „buletin-cyber-sem-2-2022-RO.pdf", p. 7, https://www.sri.ro/assets/files/publicatii/buletin-cyber-sem-2-2022-RO.pdf, data accesării 8 august 2024.

[102] *Ibidem*.

[103] „buletin-cyber-sem-1-2024.pdf", p. 7, https://www.sri.ro/assets/files/publicatii/buletin-cyber-sem-1-2024.pdf, data accesării 6 august 2024.

[104] *Ibidem*.

neautorizate. Experții DNSC au oferit sprijin pentru raportarea acțiunii către compania Meta, care este în deplin control și poate interveni asupra activităților pe Facebook. De asemenea, au recomandat implementarea unor măsuri de siguranță pentru a evita viitoare compromiteri ale contului.[105] La ora actuală atacul este în plină desfășurare, distribuind materiale inadecvate pe pagina universității, până când echipa de ajutor tehnic a Facebook va remedia problema.

Revenind la atacurile cibernetice de tip phishing și la dimensiunile criminalității cibernetice, ne îndreptăm atenția asupra unui atac identificat de Direcția de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism (DIICOT) la data de 07.08.2024. Împreună cu autoritățile din Republica Moldova, procurorii DIICOT au efectuat activități de urmărire penală într-o cauză privind săvârșirea de infracțiuni precum constituirea unui grup infracțional organizat, înșelăciune, accees fără drept la un sistem informatic, fals informatic și șantaj.[106] Din cercetările derulate până acum, s-a dovedit că în cursul anului 2022 s-a constituit un grup infracțional organizat al cărui membrii au creat și distribuit pe internet atacuri de tip phishing deghizate în reclame ce promiteau câștiguri consistente și rapide în schimbul unor investuții minime în criptomonede. În urma accesării linkurilor, utilizatorii erau redirecționați pe pagini false ce imitau platforme de investiții și conțineau fotografii ale unor persoane de încredere sau chiar sigle ale unor unități bancare și posturi de televiziune pentru credibilitate, unde li se cereau date personale. În urma furnizării datelor menționate, victimele erau contactate de atacatori sub identitatea de expertți financiar sau

[105] „DNSC", https://dnsc.ro/citeste/comunicat-de-presa-referitor-la-compromiterea-contului-de-facebook-al-universitaii-de-medicina-si-farmacie-carol-davila, data accesării 6 august 2024.

[106] „Direcţia de Investigare a Infracţiunilor de Criminalitate Organizată şi Terorism - Comunicat de presa 3 08.08.2024", https://www.diicot.ro/mass-media/4982-comunicat-de-presa-3-08-08-2024, data accesării 8 august 2024.

ofițeri de securitate cibernetică și li se solicitau fotografii ale cardului bancar și actului de identitate[107]. Ulterior, victimele erau manipulate să își instaleze programe ce permiteau controlul dispozitivului la distanță iar astfel au căzut pradă unei înșelăciuni și unui furt de date.[108] Atunci când victimele refuzau să coopereze, atacatorii recurgeau chiar și la amenințări. Prejudiciul înregistrat de victime ajunge la aproximativ 15 milioane de lei.[109]

Dimensiunile criminalității cibernetice se pot îmbina, crescând astfel nivelul de gravitate a unei infracțiuni. Rețelele de socializare sunt de multe ori un instrument prin care criminalitatea cibernetică se poate transforma. Latura tehnică a atacurilor de phishing se poate împleti cu latura „umană" a infracțiunilor, menită să manipuleze emoțional victima. DIICOT a mai identificat un caz de pornografie infantilă. În perioada 2022-2023, 3 inculpați au procurat și distribuit pe rețele sociale peste 3000 de materiale explicite cu persoane minore. [110] Criminalitatea informatică poate fi atât adresată lacunelor de securitate cibernetică cât și vulnerabilităților emoționale ale oamenilor.

Criminalitatea cibernetică – amenințare hibridă

Infracționalitatea cibernetică evoluează în tandem cu tehnologia. Criminalitatea informatică îmbină atacuri de phishing sau ransomware cu tehnici tradiționale de intimidare precum șantaj, fraudă sau exploatare. Țintele acestor infracțiuni sunt atât cetățenii de rând cât și instituțiile publice sau firmele private, entități care dețin infrastructuri importante sau furnizează

[107] *Ibidem*.
[108] *Ibidem*.
[109] *Ibidem*.
[110] „Direcția de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism - Comunicat de presa 4 08.08.2024", https://www.diicot.ro/mass-media/4983-comunicat-de-presa-4-08-08-2024, data accesării 8 august 2024.

servicii pentru sectorul medical sau politic. Motivele pentru care astfel de criminalitate există pot fi de natură politică, financiară sau ideologică. Cel mai des, acest fel de atacuri sunt lansate de grupuri, astfel atacatorii care acționează în grup pot fi numiți grup infracțional organizat. În ceea ce privește legislația României, legea 286/2009 definește grupul infracțional organizat ca *„grupul structurat, format din trei sau mai multe persoane, constituit pentru o anumită perioadă de timp şi pentru a acţiona în mod coordonat în scopul comiterii uneia sau mai multor infracţiuni*."[111] Criminalitatea informatică este subtilă, iar atacatorii pot exploata vulnerabilitatea victimelor mult mai ușor în mediul virtual.

Un raport concretizat de DIICOT pentru anul 2023 a scos în evidență ultimele tendințe în ceea ce privește infracționalitatea cibernetică în România. Pe lângă creșterea atacurilor de tip phishing care vizează furtul de date, s-a identificat noi cauze de fraude financiare prin utilizarea unor pagini false aparținând instituțiilor bancare. [112] Victimele, astfel, au căzut pradă unor furturi din aplicațiile de online banking. De asemenea, au fost identificate noi moduri de operare pentru realizarea acestor atacuri, precum SIM Swap (Clonarea cartelei SIM). Atacatorii clonau SIM-ul și preluau controlul asupra numărului de telefon al victimei, astfel obținând date și coduri de acces asupra diferitor platforme.[113] Mai mult, s-a sesizat o creștere în infracțiuni de pornografie infanitlă și fenomenul de „grooming", în care persoane minore sunt racolate pe internet cu scopul de a fi supuse abuzurilor sexuale.[114]

---

[111] „LEGE 286 17/07/2009 - Portal Legislativ", 6, https://legislatie.just.ro/Public/DetaliiDocumentAfis/109854, data accesării 8 august 2024.

[112] „Direcţia de Investigare a Infracţiunilor de Criminalitate Organizată şi Terorism - Raport de activitate", p. 35, https://www.diicot.ro/informatii-de-interes-public/raport-de-activitate, data accesării 8 august 2024.

[113] *Ibidem,* p. 34.

[114] *Ibidem,* p. 35.

În încheiere, caracterul hibrid al criminalității ciberentice constă în flexibilitatea acesteia de a fi simultan o formă de exploatare a sistemelor informatice și emoțiilor umane. Datorită acestui caracter bidimensional, criminalitatea informatică rămâne o amenințare emergentă care necesită nu numai strategii de prevenire și răspuns, ci și studiu continuu. Colaborarea internațională strânsă și campanii de informare destinate educației digitale sunt pași esențiali în a proteja infrastructura informatică de astfel de amenințări și riscuri emergente.

Bibliografie

- DESPA, OANA, „Atacurile cibernetice în România au crescut de 100 de ori în primele zile de război în Ucraina”, *Europa Liberă România*, 08:29:09Z, https://romania.europalibera.org/a/atacuri-cibernetice-masive/31781260.html, data accesării 3 august 2024.
- GORDON, SARAH; FORD, RICHARD, „On the definition and classification of cybercrime”, *Journal in Computer Virology*, vol. 2, nr. 1, august 2006, pp. 13–20.
- „Principalele amenințări cibernetice în UE”, *Consilium*, https://www.consilium.europa.eu/ro/infographics/cyber-threats-eu/, data accesării 1 august 2024.
- „U.S. Takes Action to Further Disrupt Russian Cyber Activities”, *United States Department of State*, https://www.state.gov/u-s-takes-action-to-further-disrupt-russian-cyber-activities/, data accesării 2 august 2024.
- „District of Connecticut | Hartford Man Charged with Receiving Sexually Explicit Images of Minor Girl He Communicated with on Discord | United States Department of Justice”, https://www.justice.gov/usao-

ct/pr/hartford-man-charged-receiving-sexually-explicit-images-minor-girl-he-communicated, data accesării 2 august 2024.

- „EC3 Programme Board | Europol”, https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/ec3-programme-board, data accesării 3 august 2024.
- „Parteneriatul strategic România – SUA | Ministry of Foreign Affairs”, https://www.mae.ro/node/4944, data accesării 3 august 2024.
- „LEGE 163 11/06/2021 - Portal Legislativ”, https://legislatie.just.ro/Public/DetaliiDocumentAfis/243213, data accesării 6 august 2024.
- „LEGE 58 14/03/2023 - Portal Legislativ”, https://legislatie.just.ro/Public/DetaliiDocument/265677, data accesării 8 august 2024.
- „buletin-cyber-sem-1-2023-rom-online.pdf”, https://www.sri.ro/assets/files/publicatii/buletin-cyber-sem-1-2023-rom-online.pdf, data accesării 8 august 2024.
- „Poliția Română - Campania Siguranța online”, https://www.politiaromana.ro/ro/prevenire/prevenirea-criminalitatii-informatice/campania-siguranta-online, data accesării 3 august 2024.
- „Documente”, https://dnsc.ro/doc/raport, data accesării 1 august 2024.
- „DNSC”, https://dnsc.ro/citeste/alerta-frauda-donatii-ucraina, data accesării 7 august 2024.
- „Atacuri cibernetice asupra site-urilor unor instituții publice și financiar-bancare”, *Serviciul Român de Informații*, https://www.sri.ro/articole/atacuri-cibernetice-asupra-site-urilor-unor-institutii-publice-si-financiar-bancare, data accesării 8 august 2024.

- „buletin-cyber-sem-2-2022-RO.pdf”, https://www.sri.ro/assets/files/publicatii/buletin-cyber-sem-2-2022-RO.pdf, data accesării 8 august 2024.
- „buletin-cyber-sem-1-2024.pdf”, https://www.sri.ro/assets/files/publicatii/buletin-cyber-sem-1-2024.pdf, data accesării 6 august 2024.
- „DNSC”, https://dnsc.ro/citeste/comunicat-de-presa-referitor-la-compromiterea-contului-de-facebook-al-universitaii-de-medicina-si-farmacie-carol-davila, data accesării 6 august 2024.
- „Direcţia de Investigare a Infracţiunilor de Criminalitate Organizată şi Terorism - Comunicat de presa 3 08.08.2024”, https://www.diicot.ro/mass-media/4982-comunicat-de-presa-3-08-08-2024, data accesării 8 august 2024.
- „Direcţia de Investigare a Infracţiunilor de Criminalitate Organizată şi Terorism - Comunicat de presa 4 08.08.2024”, https://www.diicot.ro/mass-media/4983-comunicat-de-presa-4-08-08-2024, data accesării 8 august 2024.
- „LEGE 286 17/07/2009 - Portal Legislativ”, https://legislatie.just.ro/Public/DetaliiDocumentAfis/109854, data accesării 8 august 2024.
- „Direcţia de Investigare a Infracţiunilor de Criminalitate Organizată şi Terorism - Raport de activitate”, https://www.diicot.ro/informatii-de-interes-public/raport-de-activitate, data accesării 8 august 2024.

Evoluția atacurilor cibernetice de tip troian în România

Alexia Oprea
(Membru susținător al Asociației Ofițerilor în Rezervă din România și voluntar la Grupul de Lucru pentru Securitate și Apărare Cibernetică)

Abstract

Această lucrare examinează evoluția atacurilor cibernetice de tip troian în România, accentuând caracteristicile și impactul lor asupra diferitelor sisteme de operare. În contextul securității cibernetice din România, sunt prezentate statistici privind atacurile de tip troian în România în perioada 2021-2024, evidențiind o creștere semnificativă în 2023, posibil influențată de tehnologii emergente precum ChatGPT. În final, este subliniată necesitatea unor strategii și măsuri de securitate cibernetică actualizate.

Cuvinte cheie: troian, malware, securitate cibernetică, inteligență artificială, ChatGPT, atacuri cibernetice.

Introducere

Atacurile cibernetice nu mai reprezintă de mult timp o noutate pe scena internațională, evoluând constant în complexitate și impact de-a lungul anilor. Este esențial să analizăm atât tipurile specifice de atacuri, cât și frecvența acestora, pentru a înțelege mai bine peisajul actual al securității cibernetice și pentru a dezvolta strategii eficiente de apărare. Un astfel de tip de atac este troianul, un malware periculos ascuns în programe aparent

legitime, care poate cauza daune semnificative sistemelor informatice. Pornind de la această perspectivă, se resimte necesitatea dezvoltării culturii de securitate cibernetică a utilizatorilor sistemelor informatice şi de comunicaţii, adesea insuficient informaţi în legătură cu potenţialele riscuri, dar şi cu soluţiile de contracarare ale acestora.

Definiție

Un troian este un tip de malware, denumit după calul de lemn folosit de greci pentru a se infiltra în Troia, care la prima vedere pare legitim. Utilizatorii sunt adeseea păcăliți să îl ruleze pe sistemele lor, însă odată ce este activat, acesta poate efectua un număr infinit de atacuri asupra gazdei. (CISCO, 2018)

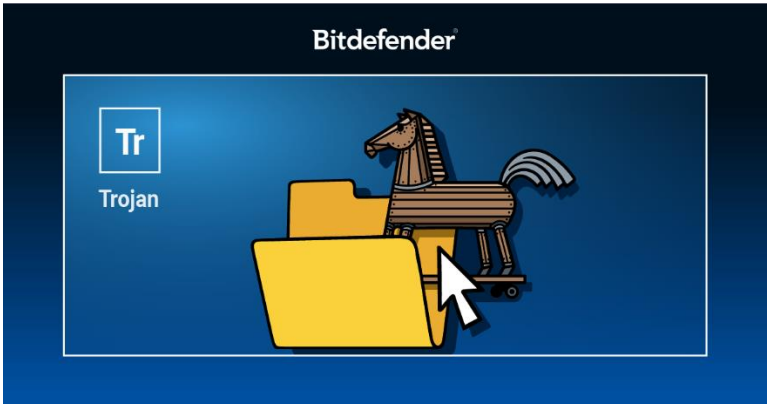


Figura 1 - (Bitdefender, 2022)

De exemplu, un operator de troieni ar putea încerca să păcălească utilizatorul care încearcă să acceseze conținut video (descărcat, de obicei, prin rețele de tip P2P), determinându-l să instaleze un „codec special” care se dovedește ulterior a fi o poartă de access pentru malware. (Bitdefender, 2022)

Spre deosebire de viruși și/sau viermi, troienii nu se reproduc prin infectarea altor fișiere și nici nu se multiplică. Troienii se

răspândesc prin activitatea utilizatorului, cum ar fi deschiderea atașamentului unui e-mail compromis sau descărcarea și rularea unui fișier de pe internet, fără verificarea legitimității acestuia în prealabil. (CISCO, 2018)

Sisteme de operare diferite, un dușman comun

Troienii sunt utilizați pe scară largă pentru a ataca ținte de profil înalt pe sistemele Windows și rămân pe harta celor mai importante amenințări la adresa punctelor terminale Windows la nivel global. În 2021, în ciuda eforturilor internaționale de a elimina troieni de renume precum Trickbot, Emotet, Dridex și AgentTesla, infractorii cibernetici au continuat să utilizeze această familie de malware.

Pe sistemele de operare Mac, multe infecții cu troieni provin de pe site-uri warez, care distribuie descărcări piratate. Troienii reprezintă cea mai mare amenințare pentru Mac-uri, iar majoritatea acestor tentative de atac au fost identificate în SUA, care au înregistrat 36% din activitatea troienilor ce vizează MacOS la nivel global în 2021.

În timp ce troienii care trimit SMS-uri sunt, de obicei, destul de populari, mai ales pentru că prezintă o modalitate ușoară de a face bani, troienii de root sunt printre cele mai periculoase amenințări. Aceștia sunt concepuți pentru a prelua controlul total de la distanță asupra unui dispozitiv, permițând atacatorului să acceseze orice tip de informații stocate, ca și cum ar deține efectiv dispozitivul. (Bitdefender, 2022)

Studiu de caz: Securitatea cibernetică în România

România, în calitate de membru cu drepturi depline al NATO și al UE, joacă un rol din ce în ce mai important în securitatea și apărarea cibernetică, atât la nivel regional, cât și la nivel internațional. România promovează o piață națională a tehnologiilor

informației și comunicațiilor deschisă și competitivă, care lucrează în strânsă legătură cu structurile publice de securitate cibernetică. Poziția sa geopolitică, în prima linie a conflictelor din jurul Mării Negre, generează un sentiment crescut de insecuritate la nivel național, care reflectă poziția actuală a țării în materie de securitate și apărare cibernetică, precum și cooperarea și angajamentele sale internaționale în creștere, în special cu UE și NATO. (Crelier, 2020, p. 4)

Din această perspectivă, se resimte necesitatea dezvoltării culturii de securitate cibernetică a utilizatorilor sistemelor informatice şi de comunicaţii, adesea insuficient informaţi în legătură cu potenţialele riscuri, dar şi cu soluţiile de contracarare ale acestora.

În sprijinul situațiilor neprevăzute în acest sens, a fost concepută Strategia de Securitate Cibernetică a României. Prin aceasta, se urmărește adaptarea cadrului normativ și instituțional la dinamica amenințărilor, respectiv creșterea culturii de securitate a populației, prin conștientizarea față de vulnerabilitățile, riscurile și amenințările provenite din spațiul cibernetic, realizată simultan cu propunerea ideii de promovare și dezvoltare a cooperării în plan național și internațional.(*Strategia de Securitate Cibernetică pentru perioada 2022-2027. Care [...]*, 2022)

Cu toate acestea, pentru ca o strategie să acopere în întregime realitatea amenințărilor pentru care a fost concepută, este esențială o analiză detaliată a tipurilor de amenințări actuale, însoțită de o perspectivă proactivă asupra potențialelor amenințări viitoare. În consecință, în rândurile următoare va fi analizată o categorie particulară a acestor amenințări, respectiv atacurile de tip troian în România, din perioada 2021-2024.

Statistici ale atacurilor de tip troian în România: 2021-2024

În anul 2021, conform alertelor emise de sistemul Țițeica, aplicațiile malware de tip infostealer și troian au fost cele mai frecvent utilizate de atacatorii cibernetici în încercările de a compromite infrastructurile IT&C critice pentru securitatea națională a României. Acest comportament sugerează intenția atacatorilor de a sustrage date în vederea comercializării acestora pe forumuri de criminalitate cibernetică, respectiv pentru a facilita potențiale atacuri viitoare.

Privind situația din punct de vedere procentual, 27,95% din totalul atacurilor desfășurate în acest an avut la bază folosirea unui malware de tip troian. (Serviciul Român de Informații, 2022, p. 16) Comparativ cu anul precedent, marcat de „starea de incertitudine prezentă în rândul cetățenilor și cantitatea mare de informații referitoare la pandemia COVID-19 și efectele acesteia", se poate observa o creștere semnificativă a procentului din sistem, în anul 2020 înregistrându-se un total de 10,45% atacuri de tip troian. (Serviciul Român de Informații, 2021, p. 11)

În anul 2022, au fost raportate 197927 de aplicații malware, din care 45398 au fost de tip troian. Un calcul rapid al proporției din totalul acestor aplicații, ne indică faptul că au fost înregistrate ≈22,94% atacuri de tip troian.(Serviciul Român de Informații, 2023, p. 13) Deși acest procent a scăzut cu 5,01% față de anul precedent, importanța lor ca amenințare cibernetică nu poate fi ignorată. Dacă această analiză ar fi fost limitată la anul 2022, concluziile ar fi sugerat o situație favorabilă, indicând o posibilă scădere a propagării acestui tip de atac cibernetic. Totuși, deoarece discuția nu se sfârșește în acest punct, anul 2023 urmează să distrugă orice speranță în această direcție.

În anul 2023, conform alertelor generate de Sistemul National de Protecție a Infrastructurilor IT&C de interes national împotriva amenințărilor provenite din spațiul cibernetic (Țițeica), au fost

înregistrate 170383 de aplicații malware, din care 82923 de tip troian. Procentul atacurilor cibernetice a crescut exponential în acest an, fiind plasat pe primul loc ca aplicație malware utilizată cel mai des de atacatorii cibernetici, cu un procent de ≈48,67%. (Serviciul Român de Informații, 2024, p. 21)

O posibilă explicație pentru această creștere considerabilă a frecvenței atacurilor de tip troian ar putea fi introducerea popularei tehnologii ChatGPT. Acest instrument, ChatGPT (Chat Generative Pre-Trained Transformer), este „un program de Inteligență Artificială bazat pe un model complex de machine learning, care poate genera răspunsuri ”umane”, comprehensibile, la întrebările utilizatorilor.” Din momentul lansării, la finalul lui noiembrie 2022, și până în ianuarie 2023, ChatGPT a adunat peste 100 de milioane de utilizatori.

De ce a declanșat ChatGPT un semnal de alarmă în cadrul securității cibernetice?

Un exemplu relevant în acest sens, este faptul că, în ianuarie 2023, ChatGPT a fost utilizat ca instrument de fabricare a mai multor tipuri de malware, prin capacitatea sa de a genera acțiuni și răspunsuri consistente, repetitive și de a ascunde cod malware în fișiere. Prin urmare, oricine ar fi apelat la ajutorul acestei tehnologii, ar fi putut dezvolta un astfel de cod fără a avea cunoștințele tehnice necesare. Totodată, utilizarea ChatGPT-ului de către actori cibernetici rău intenționați, va conduce inevitabil situația către o „înmulțire cantitativă și calitativă a amenințărilor din ecosistemul cibernetic”. (Serviciul Român de Informații, 2023, p. 15)

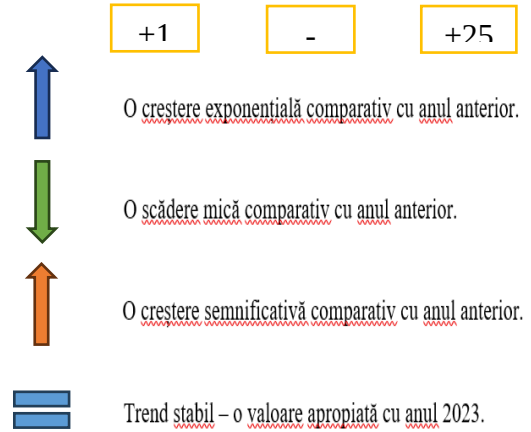
Deși nu dispunem încă de o analiză completă a anului curent, în prima jumătate a anului curent, în data de 21 mai 2024 a fost publicată o analiză privind apariția unui malware numit Ov3r_Stealer, specializat în furtul de informații personale și sensibile de pe computerele infectate. Acesta poate fi clasificat

drept troian, deoarece se ascunde în spatele unor programe sau fișiere aparent legitime, dar în același timp colectează și transmite date fără consimțământul utilizatorului. (DNSC, 2024, p. 3)

În continuare, contrar faptului că am observat o creștere constantă a atacurilor cibernetice de tip troian în ultimii ani, cu un ușor declin în 2022 și un record maxim atins în 2023, ne putem aștepta la o nouă creștere a procentului în acest an. Aplicarea directivei NIS 2 (2022/2555) la sfârșitul acestui an ar putea contribui la reducerea procentului de atacuri. Directiva NIS urmărește îmbunătățirea capabilităților naționale, consolidarea cooperării la nivelul UE și promovarea unei culturi a gestionării riscurilor și a raportării incidentelor în rândul principalilor actori economici care furnizează servicii esențiale și servicii digitale.

Pentru a ilustra clar evoluția atacurilor de tip troian în România, am compilat date statistice relevante pentru perioada 2021-2024. Tabelul de mai jos evidențiază fluctuațiile acestui trend, oferind o imagine detaliată asupra frecvenței acestor atacuri.

Atacul cibernetic	Anul 2021	Anul 2022	Anul 2023	Anul 2024
Troian				



Măsuri de protecție

Evitați să accesați site-uri suspecte, să urmați linkuri necunoscute sau să descărcați jocuri, muzică sau filme piratate din surse nesigure.

Instalarea aplicațiilor din surse de încredere reduce riscul de a instala accidental troieni de root sau alte tipuri de amenințări. Totuși, chiar și Google Play nu este complet imun la troieni, deoarece unii au reușit să se infiltreze.

Este recomandat să actualizați periodic sistemul de operare cu cele mai recente patch-uri de securitate, astfel încât atacatorii să nu poată exploata vulnerabilitățile cunoscute. Având în vedere că smartphone-urile stochează adesea la fel de multe, dacă nu mai multe, date personale decât PC-urile, este esențial să aveți instalată o soluție de securitate mobilă, care poate identifica aplicațiile malițioase atât pe piețele oficiale, cât și pe cele terțe.

O soluție de securitate poate identifica rapid orice aplicație malițioasă care utilizează capabilități de root, deoarece acesta nu este un comportament legitim. Astfel, utilizatorii sunt protejați de atacatorii care încearcă să preia controlul dispozitivului de la distanță. Indiferent dacă aplicația este descărcată de pe piețe terțe sau livrată printr-un URL malițios, o soluție de securitate poate bloca atât URL-ul care furnizează malware, cât și aplicația în sine înainte de instalare, protejând astfel dispozitivul și datele de o gamă largă de vectori de atac. (Bitdefender, 2022)

Concluzii

În urma acestei analize, se subliniază necesitatea dezvoltării unei abordări integrate și coordonate între toate instituțiile implicate în planul de securitate cibernetică al țării, precum și îmbunătățirea capacităților de detecție și reacție la incidente cibernetice, atât ale echipelor specializate, cât și ale cetățenilor.

Similar oricărui tip de incident de securitate cibernetică, utilizatorii trebuie să fie vigilenți și să adopte practici stricte de securitate, precum utilizarea de soluții de securitate actualizate, evitarea descărcărilor din surse nesigure și actualizarea periodică a sistemelor de operare. Doar printr-o abordare proactivă și bine informată putem reduce impactul troienilor și asigura o protecție mai eficientă a infrastructurilor digitale din România.

Bibliografie

- Bitdefender (2022) *Ce este un Troian? Prevenire și Eliminare* -. Available at: https://www.bitdefender.ro/consumer/support/answer/76459/ (Accessed: 30 July 2024).
- CISCO (2018) *What Is the Difference: Viruses, Worms, Trojans, and Bots?* Available at: https://sec.cloudapps.cisco.com/security/center/resources/virus_differences#5 (Accessed: 30 July 2024).
- Crelier, A. (2020) *Romania's National Cybersecurity and Defense Posture: Policy and Organizations, CSS Cyberdefense Reports*. Report. ETH Zurich. Available at: https://doi.org/10.3929/ethz-b-000445557.
- DNSC (2024) 'Analiza Ov3r_Stealer și impactul său asupra securității cibernetice'. Available at: https://dnsc.ro/vezi/document/analiza-malware-ului-ov3r-stealer-si-impactul-sau-asupra-securitatii-cibernetice.
- Serviciul Român de Informații (2021) 'Buletin CYBERINT Semestrul 1_2021'. Available at: https://sri.ro/assets/files/publicatii/buletin-cyber-sem-1-2021.pdf.
- Serviciul Român de Informații (2022) 'Buletin CYBERINT Semestrul 1_2022'. Available at:

https://sri.ro/assets/files/publicatii/buletin-cyber-sem-1-2022-RO.pdf.

- Serviciul Român de Informații (2023) 'Buletin CYBERINT Semestrul 1_2023'. Available at: https://sri.ro/assets/files/publicatii/buletin-cyber-sem-1-2023-rom-online.pdf.
- Serviciul Român de Informații (2024) 'Buletin CYBERINT Semestrul 1_2024'. Available at: https://sri.ro/assets/files/publicatii/buletin-cyber-sem-1-2024.pdf.
- *Strategia de Securitate Cibernetică pentru perioada 2022-2027. Care [...]* (2022) *Monitorul Apărării și Securității*. Available at: https://monitorulapararii.ro/strategia-de-securitate-cibernetica-pentru-perioada-2022-2027-care-sunt-obiectivele-romaniei-in-domeniul-securitatii-cibernetice-1-40152 (Accessed: 3 August 2024).

ONG-urile ca partener al statului Indonezia în gestionarea problemelor de securitate internă

Oana-Melisa Țolea
(Membru susținător al Asociației Ofițerilor în Rezervă din România și voluntară la Grupul de Lucru pentru Securitate și Apărare Cibernetică)

Introducere

Într-o lume tot mai dinamică și interconectată, colaborarea dintre guvern și societatea civilă în domeniul securității este crucială pentru abordarea amenințărilor actuale și a riscurilor neconvenționale, precum și pentru asigurarea stabilității și dezvoltării durabile a unei națiuni. Subiectul general a acestei lucrări constă în analiza colaborării între statul indonezian și organizațiile neguvernamentale (ONG-uri) în contextul securității. Argumentul principal este că Indonezia reprezintă un caz puțin studiat în ceea ce privește implicarea societății civile și a activității ONG-urilor. Deși există cercetări ample referitoare la societatea civilă și activitatea ONG-urilor din Indonezia, cum ar fi studiile realizate de Nyman Mikaela în lucrarea sa "Democratizarea Indoneziei: Provocările societății civile în era Reformasi"[115] sau de Fuad Muhammad în "Societatea civilă în Indonezia: potențial și limite ale Muhammadiyah"[116], precum și lucrările lui Beittinger-Lee Verena despre "(Ne)civil society and

[115] Nyman, Mikaela, „Democratising Indonesia: The Challenges of Civil Society in the Era of Reformasi", *Südostasien aktuell : Journal of current Southeast Asian affairs,* vol.26, nr.6, 2007, pp. 99-101.
[116] Fuad, Muhammad, „Civil Society in Indonesia: The Potential and Limits of Muhammadiyah*", Journal of Social Issues in Southeast Asia,* vol.17, 2002, pp. 133-163.

political change in Indonesia: o arenă contestată"[117], există o lipsă semnificativă de cercetare specializată privind colaborarea specifică dintre stat și ONG-uri în domeniul securității.

Indonezia, o țară din regiunea Asiei de Sud-Est, are o istorie îndelungată și diversificată. Compusă din peste 17.000 de insule, Indonezia găzduiește una dintre cele mai mari populații din lume, cu peste 270 de milioane de locuitori[118]. Istoria sa este marcată de influențe culturale, politice și economice variate din regiuni precum India, China, Arabia și Europa[119]. Primele comunități umane din zona ce constituie astăzi Indonezia datează de acum peste 1.2 milioane de ani, iar primele regate și state hinduse și budiste au apărut în această regiune în primul mileniu d.Hr[120]. Comerțul maritim a cunoscut o perioadă prosperă, iar influențele culturale străine au contribuit la modelarea societăților locale[121].

În secolul al XIII-lea Islamul a fost introdus în Indonezia prin intermediul comercianților și misionarilor, câștigând statutul de religie majoritară[122]. În decursul secolelor următoare diverse regate și imperii islamice au exercitat dominația asupra zonei, inclusiv Imperiul Majapahit care s-a numărat printre cele mai mari și puternice puteri ale Asiei de Sud-Est[123]. În secolul al XVI-lea colonialismul european a adus schimbarea majoră în Indonezia. Portughezii, olandezii, spaniolii și britanicii s-au

117 Verena Beittinger-Lee, (Un) Civil Society and Political Change in Indonesia. A Contested Arena, Routledge, 2010, p.5.
118 The World Factbook, Indonesia, accesat la 23.04.2024, disponibil online la https://www.cia.gov/the-world-factbook/countries/indonesia/#geography.
119 Steven Drakeley, *The History of Indonesia,* Greenwood Publishing Group, 2005, p.14
120 *Ibidem*, p.16.
121 *Ibidem.*
122 Carool Kersten, *A History of Islam in Indonesia. Unity in diversity*, Edinburgh University Press, 2017, p.7.
123 The World Factbook, Indonesia, accesat la 23.04.2024, disponibil online la https://www.cia.gov/the-world-factbook/countries/indonesia/#geography

stabilit în colonii în diferite părţi ale arhipelagului[124]. Olandezii au avut cel mai mare control asupra regiunii și Indonezia a fost cunoscută sub numele de Indiile Olandeze[125]. Controlul olandez asupra regiunii a durat până în mijlocul secolului al XX-lea, când a început un lung proces de luptă pentru independență[126].

După cel de-al Doilea Război Mondial, liderul naționalist indonezian Sukarno a proclamat independența țării în 1945[127]. Au urmat ani de confruntare împotriva stăpânirii coloniale olandeze, până când Olanda a recunoscut oficial independența Indoneziei în 1949[128]. De atunci, Indonezia s-a transformat într-o republică federală și a fost martora unor diverse schimbări politice și economice. A cunoscut perioade de dictatură, dar s-a remarcat prin diversitatea culturală, resursele naturale bogate și creșterea economică[129]. În prezent, Indonezia este una dintre cele mai mari economii globale și un actor important pe scena internațională[130].

Până în prezent, studiile de specialitate s-au concentrat pe impactul și rolul societății civile în Indonezia, cu o atenție deosebită acordată aspectelor politice, sociale și economice. Cu toate acestea, există o lacună semnificativă în înțelegerea modului în care guvernul indonezian colaborează cu aceste organizații în domeniul securității și factorii care influențează această colaborare între cele două entități. Este esenţial să examinăm motivul și modalitatea prin care se desfășoară această colaborare între stat și organizațiile neguvernamentale în domeniul securității din Indonezia. Ce determină acest tip de colaborare și care sunt

[124] Ricklefs Merle Calvin , *O istorie a Indoneziei moderne începând cu c. 1200*, MacMillan, Londra, 1993, p.25.
[125] *Ibidem.*
[126] *Ibidem.*
[127] The World Factbook, *op.cit.*
[128] Ricklefs Merle Calvin, op.cit, p.289.
[129] *Ibidem.*
[130] The World Factbook, *op.cit.*

consecințele sale asupra securității naționale și a comunităților locale? Ce proiecte sau inițiative sunt dezvoltate ca parte a acestui parteneriat și cum sunt ele puse în practică? Acestea sunt întrebările esențiale care necesită o analiză detaliată și reprezintă nucleul cercetării mele.

Prin investigarea acestor aspecte, îmi doresc să contribui la extinderea cunoștințelor academice referitoare la acest subiect specific și să ofer o perspectivă cuprinzătoare asupra relaţiei dintre guvernul indonezian și societatea civilă în ceea ce privește securitatea și evoluția acesteia. Prin intermediul lucrării mele, intenționez să subliniez și să analizez un elementul substanțial al guvernanței și cooperării într-un mediu complex și în continuă schimbare.

Scopul acestei lucrări este să identifice, analizeze și să explice motivele și contextele care stau la baza colaborării dintre statul indonezian și organizațiile neguvernamentale (ONG-uri) în domeniul securității. Într-un context socio-politic complex, caracterizat de o diversitate etno-religioasă accentuată, este esențial să înțelegem de ce și cum statul recurge la diverse ONG-uri pentru a gestiona anumite situații legate de securitatea națională. Un studiu relevant, care evidențiază complexitatea etno-religioasa în Indonezia, este cel al lui Arnaout Van der Meer, "Performing power: cultural hegemony, identity, and resistance in colonial Indonesia". Indonezia are aproximativ 300 de grupuri etnice native distincte, cu javanezii fiind cei mai numeroși[131]. Majoritatea acestor grupuri vorbesc propriile lor limbi. Uneori, unele grupuri etnice individuale nu sunt recunoscute de guvern, ceea ce complică implicarea politică a membrilor lor[132]. Guvernul indonezian recunoaște oficial doar

[131] Arnaout Van der Meer, *Performing power: cultural hegemony, identity, and resistance in colonial Indonesia*, Cornell University Press, 2020, p.180-184.
[132] *Ibidem.*.

cinci religii: islamul, protestantismul, catolicismul, hinduismul și budismul[133]. Toți indonezienii sunt înregistrați la naștere ca fiind parte a uneia dintre aceste religii, ceea ce a dus la discriminarea celor care nu se identifică cu niciuna dintre ele[134]. De exemplu, mulți indigeni din Papua de Vest și South Maluku nu sunt oficial recunoscuți ca membri ai vreunei religii și se confruntă astfel cu dificultăți în obținerea locurilor de muncă, accesarea educației și exercitarea dreptului la vot[135].

Prin urmare, întrebarea de cercetare de la care pornesc este: Cum se explică colaborarea stat-ONG-uri religioase în domeniul securității în Indonezia? Această întrebare îmi ghidează eforturile de a identifica și explica modul în care statul indonezian cooperează cu ONG-urile în abordarea amenințărilor și provocările legate de securitate într-un mediu caracterizat prin diversitate etnică și pluralism religios. Răspunsul la această întrebare ne va oferi o mai bună înțelegere a relațiilor dintre stat și societatea civilă din Indonezia, contribuind astfel la evaluarea modului în care colaborarea dintre stat și ONG-uri poate influența securitatea națională și stabilitatea într-un context cu o diversitate atât de accentuată.

În ceea ce privește aspectele metodologice ale acestei lucrări, am decis să mă concentrez pe situația din Indonezia în analiza relației dintre stat și organizațiile neguvernamentale, considerând colaborarea dintre aceste entități drept un exemplu de caz de tip singular reprezentativ. Optând pentru un caz de tip singular reprezentativ, se facilitează o investigație detaliată și cuprinzătoare a unui anumit aspect central de interes. Metodele de colectare a datelor calitative oferă flexibilitate și profunzime în explorarea complexității experiențelor umane, oferind cercetătorilor informații valoroase pe care metodele cantitative ar putea să nu le furnizeze.

---

[133] *Ibidem.*
[134] *Ibidem.*
[135] *Ibidem.*

Pentru colectarea datelor se vor examina documente relevante, incluzând acte legislative oficiale, rapoarte ale agențiilor guvernamentale și ONG-urilor, precum și articole din mass-media. Având în vedere particularitățile cazului specific selectat, studiul va adopta o metodologie bazată pe analiza studiului de caz pentru a explora detaliile specifice ale colaborării dintre stat și ONG-uri din Indonezia. Lucrarea mea va urma un cadru analitic fundamentat pe analiza narativă, concentrându-se asupra elementelor cheie cum ar fi capacitarea și expertiza ONG-urilor, mobilizarea resurselor și legitimitatea statului în contextul activității ONG-urilor pentru a orienta analiza studiului de caz.

Importanța studiului meu constă în analizarea colaborării dintre statul indonezian și organizațiile neguvernamentale (ONG-uri), cu accent pe aspectele securității, într-un context socio-politic complex și divers din punct de vedere etno-religios. Această cercetare aduce o contribuție semnificativă la înțelegerea modului în care guvernul indonezian interacționează și cooperează cu ONG-urile, mai ales cele cu orientare religioasă, pentru a gestiona situațiile de criză și a preveni conflictele.

Analiza informațiilor și datelor relevante indică faptul că statul indonezian se bazează pe colaborarea cu ONG-urile pentru a aborda amenințările la adresa securității, recunoscând legitimitatea, capacitățile și resursele acestora ca un complement la eforturile guvernamentale. Cercetarea evidențiază că într-un mediu multicultural complicat, ONG-urile nu concurează pentru influența politică, ci pot lucra eficient împreună cu statul în scopul asigurării securității și stabilității societății în timp de criză.

Prin implicarea lor activă în gestionarea situațiilor critice și prevenirea conflictelor, organizațiile neguvernamentale devin actori importanți ai procesului de asigurare a securității din Indonezia. Acestea contribuie semnificativ la promovarea unei abordări mai complexe și contextualizate privind relaţiile dintre

actorii implicaţi în domeniul securității și dezvoltarea conceptelor referitoare la interacțiunea dintre stat și societatea civilă în contextul siguranței publice și al securității naţionale.

Implicațiile empirice ale cercetării vizează o mai bună înţelegere a modului în care organizațiile neguvernamentale religioase pot fi implicate activ în gestionarea situațiilor critice și prevenirea conflictelor din Indonezia. Este important să se ia în considerare specificitățile culturale și religioase atunci când se analizează relațiile dintre stat și organizațiile neguvernamentale. Aceste aspecte sunt cruciale pentru elaborarea politicilor și strategiilor care să încurajeze și să sprijine colaborarea între guvern și societatea civilă în astfel de contexte.

Din punct de vedere teoretic, acest studiu aduce contribuții semnificative la dezvoltarea conceptelor privind relațiile dintre stat și ONG-uri în domeniul securității, furnizând un cadru conceptual mai cuprinzător și mai relevant pentru înțelegerea și abordarea provocărilor de securitate din lumea contemporană. Prin analiza detaliată a interacțiunii dintre stat și societatea civilă, acest studiu completează lacunele anterioare din literatura de specialitate și oferă o perspectivă nouă asupra modului în care acești actori devin vectori ai securității și influențează securitatea la nivel global.

Articolul este structurat în patru părţi distincte. În prima parte a lucrării, se afla introducerea care are rolul de a prezenta subiectul articolului, de a explica scopul pentru care a fost scris si pentru a evidenţia relevanța acestuia.

În a doua parte va fi prezentată teoria utilizată, revizuirea literaturii de specialitate si principalele concepte utilizate. Tot în această secțiune am detaliat abordarea metodologică utilizată în cercetare, unde am discutat despre procesul de selecție a cazurilor, justificând alegerea unui caz specific și prezentând motivele din spatele acestei decizii. Apoi, am detaliat tehnicile și strategiile folosite pentru colectarea datelor necesare pentru analiză, punând accent pe importanța datelor calitative și

explicând cum acestea pot fi utilizate eficient. Totodată, am prezentat metoda utilizată pentru analiza datelor, evidențiind modul în care voi interpreta și extrage sensuri din datele colectate.

A treia parte se concentrează pe analiza relației complexe dintre guvernul indonezian și societatea civilă, cu accent pe implicarea organizațiilor neguvernamentale religioase în soluționarea problemelor de securitate la nivel local și sintetizează rezultatele printr-o discuție cuprinzătoare ce integrează perspective teoretice relevante. A patra parte va fi alocată concluziilor unde se vor relua principalele puncte cheie ale articolului, se vor prezenta limitele cercetării si viitoarea agendă de cercetare.

Teoria si metodologia utilizate

În această sub-secțiune a articolului sunt prezentate principalele abordări conceptuale relevante pentru subiectul pe care doresc să-l analizez. Pentru o înțelegere aprofundată a conceptelor, am ales să lucrez pe diferite seturi de literatură. Astfel, pentru cadrul conceptual al acestei lucrări, principalele concepte le-am extras din literatura pe minorități și literatura pe Organizații Non-Guvernamentale în particular la care am adăugat și literatura pe relații internaționale și studii de securitate ca și corpusuri de literatură generale relevante în contextul cercetării alese.

Concepte din literatura pe minoritati

Grup minoritar

Conceptul de „minoritate” poate fi definit în diferite moduri în funcție de context, iar cercetătorii din diferite discipline pot aborda termenul din perspective diferite. În general, un grup minoritar se referă la o categorie de oameni care sunt depășiți

numeric sau au mai puțină putere si influenta într-o anumită societate în comparație cu grupul dominant[136].

Sociologii definesc adesea grupurile minoritare în termeni de putere socială, privilegii și acces la resurse. Potrivit sociologului Louis Wirth, un grup minoritar este „un grup de oameni care, din cauza caracteristicilor lor fizice sau culturale, sunt deosebiți de ceilalți din societatea în care trăiesc printr-un tratament diferențiat și inegal și care, prin urmare, se consideră obiecte ale discriminării colective[137]". Din punct de vedere *juridic*, statutul de minoritate poate fi determinat de factori precum rasa, etnia, religia sau limba. Definițiile legale joacă adesea un rol crucial în protecția drepturilor minorităților[138]. De exemplu, dreptul internațional recunoaște drepturile grupurilor minoritare de a-și păstra identitatea culturală[139].

Perspectiva psihologică se poate concentra pe experiența subiectivă de a fi o minoritate, inclusiv pe impactul discriminării, amenințarea stereotipului și dezvoltarea identității minorității[140]. Psihologii analizează, de asemenea, procesele prin care indivizii și grupurile fac față statutului de minoritate.

Grup etnic

Conceptul de *grupuri etnice* este complex și variază în funcție de discipline precum sociologia, antropologia și știința politică. Cercetătorii pot folosi definiții ușor diferite în funcție de perspectivele și domeniile lor de interes. Un grup etnic este o comunitate sau o populație care împărtășește o moștenire

---

[136] Karmela Liebkind, „The identity of a minority", Journal of Multilingual and Multicultural Development, vol.10, nr.1, 1989, p.48.

[137] Louis Wirth, "The Problem of Minority Groups", *American Sociological Review*, vol.10, nr.4, 1945, p.332.

138 Patrick Thornberry, International Law and the Rights of Minorities, Clarendon Press, 1993, p.57.

[139] *Ibidem.*

[140] J.S Phinney, "The Multigroup Ethnic Identity Measure: A New Scale for Use with Diverse Groups." *Journal of Adolescent Research*, vol.7, nr.2, 1992, p. 160.

culturală comună, inclusiv limba, tradițiile, obiceiurile și adesea un sentiment de istorie comună[141]. Unele definiții subliniază caracteristicile biologice sau rasiale ca si componente esențiale ale identității etnice[142]. Această perspectivă se concentrează adesea pe trăsăturile fizice comune.

Grupurile etnice sunt definite prin organizarea socială și instituțiile care le deosebesc de alte grupuri, cum ar fi structuri familiale specifice, practici religioase sau sisteme economice[143]. Grupurile etnice pot fi definite din punct de vedere politic, mai ales în contextul statelor-națiune, unde anumite grupuri sunt recunoscute și clasificate în scopuri administrative sau politice[144].

Unele definiții combină mai multe elemente, cum ar fi o combinație de factori culturali, istorici și ancestrali, pentru a oferi o înțelegere mai cuprinzătoare a identității etnice[145]. Este important de menționat că aceste definiții nu se exclud reciproc, iar identitatea etnică este un concept cu mai multe fațete care poate fi înțeles din diferite perspective. În plus, dezbaterile și discuțiile despre etnie sunt în desfășurare, iar definițiile pot evolua în timp.

Politici etnice

Politicile etnice se referă în general la acțiunile și strategiile guvernamentale menite să abordeze problemele legate de

[141] Cuartero, Izaskun Álvarez. "The concept of ethnicity and ethnic genealogy." *The Routledge Handbook to the History and Society of the Americas* ,2019, p.8

[142] Carter Bob, *Realism, and racism: Concepts of race in sociological research*, Routledge, 2002, p.10.

[143] Eriksen, Thomas Hylland, "The epistemological status of the concept of ethnicity.", *Anthropological Notebooks*, vol.25, nr.1, 2019, p.4.

[144] Cuartero, Izaskun Álvarez. "The concept of ethnicity and ethnic genealogy." *The Routledge Handbook to the History and Society of the Americas* ,2019, p.8

[145] Ibidem.

diversitatea etnică într-o anumită societate[146]. Aceste politici pot implica eforturi de gestionare a relațiilor între grupuri, de promovare a coeziunii sociale și de asigurare a șanselor egale pentru diferite grupuri etnice. Multe țări adoptă politici multiculturale pentru a recunoaște diversitatea populațiilor lor. Multiculturalismul urmărește să promoveze un sentiment de incluziune pentru diferite grupuri etnice, permițându-le să-și mențină și să-și exprime identitățile distincte, contribuind în același timp la cultura națională generală[147]. De asemenea, guvernele pot implementa politici pentru a aborda inegalitățile istorice și pentru a promova participarea grupurilor etnice subreprezentate în diferite domenii, cum ar fi educația și reprezentarea politică[148]. Politicile etnice pot pune accent pe protecția și promovarea drepturilor culturale, asigurând că grupurile minoritare au dreptul de a-și menține, dezvolta și exprima identitatea culturală fără a se confrunta cu discriminarea[149].

Unele țări implementează politici lingvistice pentru a proteja și promova limbile diferitelor grupuri etnice. Aceasta poate include măsuri precum educația bilingvă sau recunoașterea oficială a mai multor limbi[150]. Cadrele legale care interzic discriminarea pe criterii etnice sau rasă sunt componente esențiale ale politicilor etnice. Aceste legi urmăresc să asigure tratament și șanse egale pentru toți indivizii, indiferent de originea lor etnică[151].

---

[146] Will Kymlicka, Keith Banting, *Multiculturalism and the Welfare State: Recognition and Redistribution in Contemporary Democracies,* Oxford University Press, 2007, p. 120.

[147] *Ibidem,* p.125.

148 D. Pearson, The Politics of Ethnicity in Settler Societies: States of Unease, Palgrave Macmillan, 2001, p.40.

[149] *Ibidem,* p.45.

[150] *Ibidem.*

[151] Balasubramaniam Vejai, "Ethnic Politics and Multicultural Societies." *International Studies Review,* vol. 12, nr.1, 2010, p.106.

Mai mult, politicile etnice abordează adesea problemele reprezentării politice pentru a se asigura că diversele grupuri etnice sunt reprezentate adecvat în instituțiile guvernamentale și în procesele de luare a deciziilor[152].

Concepte din literatura despre organizațiile non-guvernamentale

ONG (Organizație Non-Guvernamentală)

Este important de menționat că termenul „ONG" cuprinde o mare varietate de organizații cu misiuni, structuri și abordări diferite. Diversitatea ONG-urilor reflectă complexitatea provocărilor globale pe care intenționează să le abordeze. În literatura de specialitate, abordările cu privire la definirea conceptului sunt extrem de variate. ONU definește ONG-urile ca fiind „organizații private care desfășoară activități pentru ameliorarea suferinței, promovarea intereselor celor săraci, protejarea mediului, furnizarea de servicii sociale de bază sau dezvoltarea comunității"[153]. Uniunea Europeană definește ONG-urile ca fiind „o organizație non-profit, independentă de guvern, care este organizată la nivel local, național sau internațional pentru a aborda probleme în sprijinul binelui public[154]".

Potrivit Mișcării Internaționale de Cruce Roșie și Semilună Roșie, ONG-urile sunt adesea descrise ca „organizații voluntare, de obicei non-profit și uneori organizate la nivel comunitar, care

152 Judith G. Kelley, Ethnic Politics in Europe: The Power of Norms and Incentives, Princeton University Press, 2004, pp.90-91.

153 United Nations, UN, and Civil Society, accesat la data de 10.11.2023, disponibil online la https://www.un.org/en/get-involved/un-and-civil-society.

154 European Institute for Gender Equality, Non-governmental organizations(NGOS), accesat la data de 08.11.2023, disponibil online la https://eige.europa.eu/publications-resources/thesaurus/terms/1087?language_content_entity=en.

sunt angajate în activități de ajutorare și dezvoltare”[155]. ONG-urile sunt adesea considerate parte a societății civile și sunt definite ca „organizații care nu fac parte din guvern și nu sunt afaceri convenționale cu scop lucrativ[156]”.

ONG-urile pot fi, de asemenea, definite prin prisma funcțiilor lor, cum ar fi ONG-urile umanitare care oferă ajutor în perioadele de criză, ONG-urile de advocacy care lucrează pentru a influența politica și creșterea gradului de conștientizare și ONG-urile de dezvoltare care se concentrează pe dezvoltarea socială și economică pe termen lung[157]. Operațional, ONG-urile se caracterizează prin independența lor față de controlul guvernamental, natura voluntară, statutul non-profit și un accent pe servirea binelui public[158]. ONG-urile sunt adesea clasificate în funcție de faptul că se angajează în principal în advocacy (promovarea unor cauze specifice, schimbări de politică etc.) sau furnizarea de servicii (furnizarea directă a serviciilor, cum ar fi asistența medicală, educația etc.)[159]. Definiția pe care o voi folosi în cadrul cercetării mele, va fi cea oferită de Uniunea Europeană, fiind cea mai comprehensivă.

---

[155] Code of Conduct for the International Red Cross and Red Crescent Movement and Non-Governmental Organizations (NGOs) in Disaster Relief, accesat la data de 30.10.2023, disponibil online la https://www.ifrc.org/our-promise/do-good/code-conduct-movement-ngos.

[156] Teegen Hildy, Jonathan P. Doh, Sushil Vachani, "The importance of nongovernmental organizations (NGOs) in global governance and value creation: An international business research agenda", *Journal of international business studies,* vol.35, 2004, p.466.

[157] Raustiala Kal, "States, NGOs, and international environmental institutions." *International Studies Quarterly, vol.*41, nr.4, 1997, p.725.

[158] *Ibidem.*

[159] Teegen Hildy, Jonathan P. Doh, Sushil Vachani, "The importance of nongovernmental organizations (NGOs) in global governance and value creation: An international business research agenda", *Journal of international business studies,* vol.35, 2004, p.467.

ONG religios

ONG-urile religioase sau organizațiile neguvernamentale sunt organizații care funcționează independent de entitățile guvernamentale și sunt de obicei conduse de motivații religioase sau bazate pe credință. Aceste organizații se angajează în diferite activități pentru a promova obiective sociale, umanitare și de dezvoltare, adesea bazate pe principiile și învățăturile unei anumite religii. Literatura de specialitate înțelege acest concept prin prisma unor perspective diferite. Un ONG religios este o organizație care este motivată de principii religioase sau bazate pe credință și lucrează pentru binele comun, dreptatea socială și bunăstarea indivizilor și comunităților[160]. Aceste ONG-uri se inspiră din învățăturile și valorile religioase pentru a-și ghida activitățile.

Organizațiile bazate pe credință sunt entități care sunt asociate cu o anumită religie sau tradiție de credință[161]. Aceste organizații pot include ONG-uri religioase, dar termenul este mai larg și poate include instituții religioase precum biserici, moschei, temple și alte organisme religioase implicate în activități sociale și umanitare[162]. Unele ONG-uri religioase lucrează în diferite tradiții de credință și sunt cunoscute ca ONG-uri interreligioase. Aceste organizații își propun să încurajeze înțelegerea, cooperarea și colaborarea între oameni de diverse medii religioase pentru binele comun[163]. În islam, termenul „Dawah" se referă la predicarea sau răspândirea învățăturilor

[160] Beinlich, Ann-Kristin, Clara Braungart, "Religious NGOs at the UN: A quantitative overview.", *Religious NGOs at the United Nations,* 2018, p.28.
[161] Berger, Julia, "Religious nongovernmental organizations: An exploratory analysis.", Voluntas*: International Journal of Voluntary and Nonprofit Organizations*, vol.14,2003, p.20.
[162] *Ibidem*.
[163] Beinlich, Ann-Kristin, Clara Braungart, "Religious NGOs at the UN: A quantitative overview.", *Religious NGOs at the United Nations,* 2018, p.28.

islamice[164]. Unele ONG-uri islamice se angajează în activități Dawah împreună cu activități umanitare și de dezvoltare. Ca și alte ONG-uri, ONG-urile religioase se pot confrunta cu provocări, cum ar fi echilibrarea identității lor religioase cu nevoia de incluziune si potențialul de acuzații de prozelitism[165].

Societatea civilă

UNDP definește societatea civilă ca fiind „arena din afara familiei, a statului și a pieței în care oamenii se asociază pentru a promova interese comune".

Include o gamă largă de organizații neguvernamentale (ONG-uri), grupuri comunitare, fundații și grupuri de experți[166]. Teoreticianul politic John Keane subliniază importanța societății civile ca spațiu în care cetățenii se reunesc pentru a delibera, a discuta și a se angaja în activități care contribuie la binele public[167]. El vede societatea civilă ca o componentă cheie a guvernării democratice. Michael Edwards, un cercetător în studii de dezvoltare, definește societatea civilă ca „o sferă de interacțiune socială între familie și stat care se manifestă în normele de cooperare comunitară, structuri de asociere voluntară și rețele de comunicare publică"[168].

[164] Mubarak Hafiz, "THE TECHNOLOGICAL REVOLUTION AND THE DYNAMICS OF ISLAMIC DA'WAH.", *At-Tajdid: Jurnal Pendidikan dan Pemikiran Islam*, vol.6, nr.1, 2022, p. 45.

[165] Berger, Julia, "Religious nongovernmental organizations: An exploratory analysis.", *Voluntas: International Journal of Voluntary and Nonprofit Organizations*, vol.14,2003, p.21.

[166] United Nations Development Programme, accesat la data de 25.11.2023, disponibil online la: https://www.undp.org/.

[167] John Keane, *Civil Society: Old Images, New Visions*, Stanford University Press, 1998, p. 90.

[168] Michael Edwards, *Civil Society*, John Wiley and Sons, 2013, p.35.

Concepte din literatura pe relatii internationale si studii de securitate

Stat-națiune

Conceptul de stat-națiune a fost influent în modelarea structurilor politice moderne și servește ca un cadru cheie pentru înțelegerea organizării statelor și a populațiilor acestora. O națiune se referă la un grup de oameni care împărtășesc o identitate comună, inclusiv caracteristici culturale, lingvistice, istorice și uneori etnice sau religioase[169]. Această identitate comună creează adesea un sentiment de apartenență și solidaritate între membrii națiunii. Națiunile pot fi definite printr-o limbă comună, istorie, teritoriu și alte atribute culturale[170]. Un stat este o entitate politică suverană cu granițe geografice definite, o populație permanentă, un sistem de guvernare și capacitatea de a intra în relații cu alte state[171]. Un stat are de obicei un guvern care exercită autoritate asupra teritoriului și populației sale, aplică legile și reprezintă statul în afacerile internaționale[172].

Un stat-națiune este forma idealizată de organizare politică în care granițele statului coincid cu granițele unei singure națiuni[173]. Cu alte cuvinte, un stat-națiune este un stat suveran care cuprinde un grup cultural și etnic omogen[174]. Conceptul de stat-națiune sugerează o aliniere puternică între identitățile

---

[169] Marx, Anthony W., "The Nation-State and Its Exclusions." *Political Science Quarterly*, vol. 117, nr. 1, 2002, p.105.
[170] *Ibidem*.
[171] Roeder, Philip G., Where *Nation-States Come From: Institutional Change in the Age of Nationalism*, Princeton: Princeton University Press, 2007, p.3.
[172] *Ibidem*.
[173] Wimmer, Andreas, Nina Glick Schiller, "Methodological nationalism and beyond: nation–state building, migration and the social sciences." *Global networks*, vol.2, nr.4, 2002, p. 312.
[174] *Ibidem*.

politice și culturale ale unei populații dintr-un anumit teritoriu geografic.

Naționalismul este o ideologie care subliniază importanța unei identități naționale comune și promovarea intereselor, culturii și bunăstării unei anumite națiuni[175]. Ea joacă adesea un rol semnificativ în formarea și coeziunea statelor naționale.

Securitate societală

În lucrarea fundamentală, ” Security: A New Framework for Analysis”, Barry Buzan și coautorii săi introduc conceptul de *securitate societală* ca unul dintre cele patru sectoare de securitate, alături de securitatea militară, politică și economică. Ei susțin că securitatea societală implică protejarea valorilor și instituțiilor de bază ale unei societăți[176]. Mary Kaldor discută despre securitatea umană, care se aseamănă cu securitatea societală, punând accent pe protecția împotriva unei game largi de amenințări, inclusiv instabilitatea economică, degradarea mediului și încălcările drepturilor omului[177]. Munca lui Booth contribuie la înțelegerea securității dincolo de perspectiva tradițională centrată pe stat. El subliniază importanța securității societale în abordarea provocărilor globale și pledează pentru o abordare mai largă și mai incluzivă a securității[178].

Grup religios

Un grup religios se referă la o comunitate sau organizație legată de credințe, practici și valori religioase comune. În literatura de specialitate exista mai multe abordări cu privire la definirea conceptului. Din punct de vedere sociologic, un grup

[175] *Idem*, p.314.

176 Barry Buzan, Ole Waever, Jaap De Wilde, Security: A New Framework for Analysis, Lynne Rienner Publishers, 1997, p.119-120.

[177] Mary Kaldor, *Human Security*, Polity, 2007, p.85.

[178] Booth K, *Theory of World Security*, Cambridge University Press, 2007, pp.95-96.

religios este o entitate socială caracterizată printr-un sistem comun de credințe, simboluri, ritualuri și practici[179]. Oferă un sentiment de identitate și apartenență membrilor săi. Din punct de vedere antropologic, un grup religios este un fenomen cultural în care indivizii se reunesc pe baza credințelor religioase comune și se angajează în ritualuri, ceremonii și tradiții care sunt semnificative pentru viziunea lor spirituală asupra lumii[180]. În dialogul interreligios, un grup religios poate fi înțeles ca o comunitate care reprezintă o tradiție religioasă specifică, favorizând comunicarea și înțelegerea între oameni de diferite credințe[181].

Din punct de vedere istoric, un grup religios poate fi definit ca „o comunitate de indivizi legați de o istorie religioasă comună, inclusiv dezvoltarea unor doctrine, practici și instituții religioase specifice[182]". Din punct de vedere filozofic, un grup religios este format din indivizi care împărtășesc un set de credințe fundamentale despre existență, scop, moralitate și divin[183].

În această sub-secțiune al articolului am realizat o revizuire a literaturii de specialitate, utilizând lucrări si cercetări esențiale pentru cercetarea mea. În acest sens, am încercat pe baza textelor existente, să identific posibile explicații pentru care statele aleg să lucreze împreună cu ONG-urile si explicații pentru existența

[179] Schilbrack Kevin, "The Concept of Religion", *The Stanford Encyclopedia of Philosophy* ,2022, p.6
[180] Wibisono Susilo, Winnifred R. Louis, Jolanda Jetten, "A multidimensional analysis of religious extremism." *Frontiers in psychology*, vol.10, 2019, p.5.
[181] Ibidem.
[182] Schilbrack Kevin, "The Concept of Religion", *The Stanford Encyclopedia of Philosophy* ,2022, p.6
[183] Héliot YingFei, "Religious identity in the workplace: A systematic review, research agenda, and practical implications." *Human resource management*, vol.59, nr.2, 2020, p.160.

acestor parteneriate în gestionarea conflictelor etnice sau a conflictelor dintre grupurile religioase.

Articolul lui Yelena Vladimirovna Kuntz și Vladimir Golubovskiy din 2015, „The Legal Nature of Ethnic and Religious Conflicts", prezintă o perspectivă semnificativă asupra naturii juridice a conflictelor etnice și religioase. Ei subliniază importanța tot mai mare a reglementării legale în abordarea acestor conflicte, în special datorită proceselor de migrație care afectează națiunile de pe tot globul. Autorii subliniază că legislația viciată și lipsa unui cadru adecvat au facilitat activitățile organizațiilor extremiste care promovează supremația rasială și xenofobia[184]. În general, această lucrare evidențiază cât de esențială este abordarea conflictelor etno-religioase dintr-o perspectivă juridică și sugerează că este necesară o abordare globală pentru a aborda această problemă în mod eficient.

Dintr-o altă perspectivă, „Boko Haram: Retorici și realități ale gestionării conflictelor etno-religioase în Nigeria", de B. Nwankwo examinează retorica versus realitate în gestionarea conflictelor etno-religioase din Nigeria. Fiind o țară multietnică cu peste 250 de grupuri etnice și două religii dominante (islam și creștinism), Nigeria s-a confruntat cu provocări continue în controlul unor astfel de conflicte de la obținerea independenței în 1960[185]. Articolul explorează diverse manifestări ale acestor conflicte, inclusiv revolte, sabotaj, lupte armate și campanii de secesiune ale milițiilor precum Congresul Poporului Oodua (OPC) și Boko Haram[186]. Utilizează o abordare de studiu de caz care combină surse primare și secundare, inclusiv baze de date

[184] Yelena Vladimirovna Kuntz, Vladimir Yurjevich Golubovskiy, "The Legal Nature of Ethnic and Religious Conflicts", *Indian Journal of Science and Technology,* vol.8, nr.10, 2015, p.5.
[185] Nwankwo Beloveth Odochi, "Rhethorics and Realities of Managing Ethno-Religious Conflicts: The Nigerian Experience.", American *Journal of Educational Research,* vol. 3, 2015, p.293.
[186] *Idem,* p.294.

care documentează morți violente, articole, ziare și cărți relevante. Lucrarea susține necesitatea descurajării sentimentelor etnice și religioase în rândul grupurilor și subliniază importanța mecanismelor de management eficiente[187]. Ea subliniază complexitatea conflictelor etno-religioase din Nigeria și subliniază importanța abordării acestor probleme din mai multe perspective.

În același timp „Diversitate, turism și dezvoltare economică: o perspectivă globală", de Saqib Amin explorează relația dintre diversitatea etnică și religioasă, turismul internațional și dezvoltarea economică. Studiul investighează modul în care diversitatea existentă influențează turismul și creșterea economică la scară globală. Cercetarea relevă că diversitatea etnică și religioasă poate avea un impact negativ semnificativ asupra turismului internațional și dezvoltării economice. Neînțelegerile culturale care decurg din polarizare și conflicte pot descuraja turiștii și pot slăbi sectorul turismului în diverse țări[188]. Prin urmare, sugerează că promovarea egalității de șanse pentru toate grupurile și promovarea coeziunii sociale sunt esențiale în reducerea la minimum a consecințelor negative ale diversității[189]. Această lucrare evidențiază importanța luării în considerare a implicațiilor diversității etnice și religioase asupra turismului internațional și dezvoltării economice. Ea solicită strategii care să favorizeze incluziunea și coexistența pașnică pentru a spori rezultatele pozitive asociate cu diversitatea culturală[190].

Articolul lui Kemal Yıldırım din 2016 explorează conflictele etnice și religioase dintre musulmani și hinduși din India. Yıldırım subliniază că ipotezele ideologice despre evenimentele istorice, mai degrabă decât interpretările exacte, au alimentat o

[187] *Idem*, p.296.
188 Amin Saqib, „Diversity, Tourism, and Economic Development: A Global Perspective", Tourism Analysis, vol.25, nr.1, 2020, p.26.
[189] *Ibidem*.
[190] *Idem*, p.28.

mare parte a conflictului religios din India de astăzi[191]. Se sugerează că liderii laici joacă un rol crucial în reintroducerea preocupărilor socioeconomice în politica democratică pentru a aborda aceste probleme în mod eficient[192]. Articolul subliniază că un lider puternic este necesar la nivel politic pentru a rezolva provocările de lungă durată cu care se confruntă regiunea. Reconstrucția politică însoțită de decizii obligatorii este esențială pentru asigurarea regiunii și pentru promovarea armoniei între diversele grupuri etnice ale Indiei[193]. Prin aceste articole este prezentată o analiză cuprinzătoare a conflictelor etnice și religioase în diferite contexte. În general, aceste articole contribuie la înțelegerea conflictelor etnice și religioase, oferind diferite perspective asupra cauzelor, implicațiilor și potențialelor strategii de soluționare a acestora.

Un alt set de literatură pe care l-am studiat surprinde evoluțiile etno-religioase din Indonesia în particular. Ristanti examinează un conflict interreligios care a avut loc în orașul Poso, Sulawesi Central, Indonezia. După perioada reformei din 1998, Indonezia a cunoscut instabilitate politică, ceea ce a dus la diverse conflicte, inclusiv confruntări de grupuri etnice și religioase[194]. În orașul Poso, în special, au izbucnit ciocniri violente între grupuri creștine și musulmane. Conflictul a fost rezolvat în cele din urmă prin dialoguri facilitate de personalități religioase respectate și mediate de oficiali guvernamentali[195]. Au fost implementate măsuri specifice, cum ar fi Declarația Malino,

---

[191] Kemal Yildirim, Ethnic and Religious Conflicts in India between Muslims and Hindus: Ethnic and Religious Conflicts, Lambert Academic Publishing, 2016, p. 71.
[192] *Ibidem*.
[193] *Idem*, p.73.
[194] D.N Ristanti , "Interreligious Violent Conflict Resolution: Discoursing Communal Violence between Christians and Moslems in Poso City, Indonesia", *Hasanuddin Journal of Strategic and International Studies (HJSIS)*, vol. 1, 2022, p. 33.
[195] *Idem*, p.34.

pentru a pune capăt conflictului, în timp ce intervenția militară a menținut pacea în timpul procesului de soluționare[196].

În cadrul lucrării mele, am ales să mă concentrez pe cazul Indoneziei în analiza relației dintre stat și ONG-uri în ultimele două decenii. Colaborarea dintre stat-ONG-uri în Indonezia reprezintă un caz de tip singular reprezentativ pentru democrațiile din Asia de Sud-Est. Utilizarea unui caz de tip singular permite o examinare amănunțită si comprehensivă a unui anumit punct de interes. Cu toate acestea, necesită o abordare meticuloasă pentru a evita denaturarea cercetării. Gerring și Seawright descurajează o selecție aleatorie a cazurilor, argumentând că ar reprezenta o inadecvare și o lipsă a acurateței cercetării[197]. În schimb, aceștia pledează pentru o metodă de selecție a unui caz de tip singular concepută cu scopul de a explora în mod eficient un caz[198].

Relația dintre Indonezia și organizațiile neguvernamentale (ONG-uri) poate fi utilizat ca un studiu de caz concludent datorită complexității și gamei diverse de probleme pe care le cuprinde. Acest parteneriat reprezintă o reflexie a dinamicii globale dintre guverne și societatea civilă, oferind perspective valoroase asupra provocărilor și oportunităților inerente unor astfel de colaborări.

În cadrul lucrării mele, vor fi analizate documentele relevante, documentele legislative oficiale și rapoartele agențiilor guvernamentale și ONG-urilor, dar si texte din mass-media. În ceea ce privește documentele legislative, am identificat două hotărâri legislative emise de guvernul indonezian. Prima hotărâre legislativă este reprezentată de legea 16/2001, lege adoptată cu scopul de a promova transparența și responsabilitatea în cadrul

[196] *Ibidem*.
[197] *Idem*, p.295.
[198] *Ibidem.*

sectorului societății civile, mai exact de a reglementa activitățile ONG-urilor. Celălalt document legislativ, se referă la regulamentul prezidențial numărul 16/2018 privind achizițiile publice, prin care ONG-urilor le-a fost oferită posibilitatea de a accesa fonduri guvernamentale pentru desfășurarea activităților specifice. Ambele documente legislative au fost obținute de pe platforma online oficială a guvernului indonezian[199]. Aceste documente legislative oferă o perspectivă nuanțată asupra evoluției istorice a relației dintre statul indonezian și ONG-uri, identificând schimbările cheie de politică și perspectivă a statului indonezian în ceea ce privește activitățile întreprinse de ONG-uri.

De asemenea, au fost folosite rapoarte oficiale ale unor ONG-uri din Indonezia. Aceste rapoarte au fost colectate de pe platformele oficiale ale anumitor ONG-uri indoneziene, precum MAMPU[200] și Muhammadiyah[201]. Un astfel de raport selectat relevant pentru a observa dinamica dintre relația stat-ONG și diversele perspective, a fost cel elaborat de ONG-ul MAMPU în 2018, intitulat „ The Experience of Parliamentary Engagement by MAMPU and Its Partners: Lessons learnt and openings for the future[202].” Aceste rapoarte sunt extrem de valoroase deoarece oferă o sursa de date primara privind relația dintre stat-ONG. ONG-urile colaborează adesea cu statul în diverse inițiative. Examinarea platformelor lor poate oferi informații

[199] Camera Reprezentanților a Republicii Indonezia, accesat la data de 23.12.2023, disponibil online la https://www.dpr.go.id/en/berita/index/category/bksap.

[200] *MAMPU* – The *Australia-Indonesia* Partnership for Gender Equality and Women's Empowerment, accesat la data de 23.12.2023, disponibil online la http://mampu.bappenas.go.id/en/category/knowledge/research/page/2/.

[201] *Muhammadiyah, accesat la 22.12.2023, disponibil online la* https://muhammadiyah.or.id/.

[202] *MAMPU* – The *Australia-Indonesia* Partnership for Gender Equality and Women's Empowerment, accesat la data de 23.12.2023, disponibil online http://mampu.bappenas.go.id/en/knowledge/research/the-experience-of-parliamentary-engagement-by-mampu-and-its-partners-lessons-learnt-and-openings-for-the-future-2018/.

despre aceste colaborări, inclusiv obiectivele, provocările și rezultatele acestora. Înțelegerea parteneriatelor dintre ONG-uri și stat este crucială pentru o analiză comprehensivă. De asemenea, platformele ONG-urilor pot reflecta percepțiile și discursul publicului asupra problemelor legate de stat.

Având în vedere caracteristicile unice ale cazului de tip singular ales pentru lucrarea mea și datele disponibile cu privire la subiectul relației dintre statul Indonezian și ONG-uri, studiul va folosi o analiză a unui studiu de caz. Această abordare analitică permite o examinare amănunțită a cazului statului indonezian, luând în considerare detaliile sale specifice. Lucrarea actuală va adopta metoda analizei narative, care implică un spectru larg de procese și explicații. În acest sens, lucrarea mea va urma un cadru analitic care se va concentra pe elemente cheie precum capacitatea și expertiza ONG-urilor, mobilizarea resurselor de către stat înspre ONG-uri și de către ONG-uri, precum și legitimitatea statului în raport cu activitatea ONG-urilor, toate acestea cu scopul de a ghida analiza studiului de caz

Pornind de la caracteristicile metodei de analiza selectate, factorii contextuali în raport cu subiectul acestei lucrări se bazează pe înțelegerea contextului socio-politic, economic și cultural în care funcționează relația stat-ONG. Aceasta implică examinarea factorilor istorici, a structurilor de putere și a normelor societale. Dinamica puterii se concentrează pe analiza distribuției puterii între stat și ONG-uri. Aceasta include investigarea modului în care dezechilibrele de putere influențează luarea deciziilor, alocarea resurselor și dinamica generală a colaborării sau a tensiunii dintre cele doua entități. Mediul politic și de reglementare examinează politicile și cadrele de reglementare care guvernează interacțiunea dintre stat și ONG-uri. Acesta implică evaluarea impactului structurilor juridice asupra autonomiei și eficacității ONG-urilor. Examinarea interacțiunilor financiare dintre stat și ONG-uri, include analiza

surselor de finanțare, a mecanismelor de plăți și a impactului sprijinului financiar asupra activităților și independenței ONG-urilor. Implicarea comunității se referă la evaluarea rolului comunităților în relația stat-ONG, precum si înțelegerea modului în care nevoile și aspirațiile comunității sunt luate în considerare și măsura în care ONG-urile acționează ca intermediari sau susținători pentru populațiile locale

ONG-urile ca vector de securitate în Indonezia

Evoluția organizațiilor neguvernamentale (ONG-uri) din Indonezia poate fi urmărită încă din epoca pre-independență, unde existau diferite forme de grupuri societale pentru a aborda problemele sociale și a susține schimbarea politică[203]. Însă, din punct de vedere istoric căderea președintelui Suharto în 1998 a marcat un punct de cotitură semnificativ pentru ONG-urile din Indonezia. Epoca Reformei a dus la libertăți politice extinse și reforme democratice, conducând la un mediu favorabil pentru societatea civilă[204]. Cadrul legal a devenit mai favorabil odată cu introducerea unor legi care au recunoscut rolul ONG-urilor în societate și le-au oferit un statut mai clar. Această perioadă a cunoscut o creștere exponențială a numărului și a varietății de ONG-uri, reflectând dinamica socială și politică complexă a țării. În anii 2000, guvernul indonezian a adoptat mai multe legi pentru a defini și reglementa în continuare ONG-urile. Legea cu privire la organizațiile societale (Legea nr. 8/1985), înlocuită cu Legea nr. 17/2013, a stabilit direcțiile principale pentru înființarea, activitățile și finanțarea externă a ONG-urilor[205].

[203] Mukhamad Shokheh, Mansoureh Ebrahimi, Kamaruzaman Yusoff: The Role of Indonesian and Egyptians' NGOs in Democratization", *Geopolitics Quarterly*, Vol.17, Nr. 4, 2022, p.290.
[204] *Ibidem*.
[205] Hans Antlöv, Rustam Ibrahim, Peter van Tuijl, *NGO GOVERNANCE AND ACCOUNTABILITY IN INDONESIA: CHALLENGES IN A NEWLY DEMOCRATIZING COUNTRY*, Routledge, 2006, p.6

Statul și societatea civilă sunt conectate, dar nu sunt la fel. Se crede că prin implicarea în societatea civilă, statul ar putea să realizeze și să mențină o dezvoltare economică durabilă cu politici mai eficiente și, de asemenea, sprijin public. Pe de altă parte, societatea civilă urmărește, de asemenea, să consolideze practicile democratice în care justiția socială, drepturile omului și responsabilitatea publică ar putea fi materializate. Relația dintre stat și societatea civilă este un aspect important și interesant de explorat deoarece, la fel ca în majoritatea țărilor în curs de dezvoltare, societatea civilă din Indonezia a crescut din ce în ce mai mult în ceea ce privește numărul de grupuri sau organizații și numărul de membri[206]. În plus, societatea civilă a fost, de asemenea, recunoscută ca o posibilitate pentru schimbări sociale și politice și o forță semnificativă de a capta cerințele și interesul publicului. Acest lucru se datorează faptului că societatea civilă a fost implicată activ în diferite inițiative de dezvoltare, colaborând cu organele de conducere, precum și cu organismele de implementare[207].

În Indonezia, există două tipuri de entități juridice pentru organizațiile non-profit: fundații (yayasan) și asociații (perkumpulan). Yayasan a fost recunoscut pentru prima dată ca entitate juridică în timpul epocii coloniale olandeze in 1870[208]. Cealaltă formă de entitate juridică este perkumpulan (asociația), care este înființată de un număr de persoane pentru a servi interesele membrilor săi sau ale publicului. Spre deosebire de yayasan, care este o organizație care nu se bazează pe apartenenta, perkumpulan se înființează pe baza apartenențelor[209]. În contextul specific indonezian, societatea civilă implică cetățenii, atât indivizi, cât și membri ai unor grupuri organizate, care participă la dezvoltarea

[206] Marcus Mietzner, „Sources of resistance to democratic decline: Indonesian civil society and its trials", *Democratization*, 2020, p.4.
[207] *Idem*, p.6.
[208] Hans Antlöv, Rustam Ibrahim, *op.cit.*,, p.5
[209] *Ibidem*.

și implementarea politicilor publice[210]. Aceste grupuri organizate pot fi sub forma unor organizații neguvernamentale (ONG-uri), asociații profesionale, grupuri religioase sau partide politice.[211] Totodată, una dintre caracteristicile societății civile indoneziene este reprezentată de organizațiile religioase non-islamice. Spre deosebire de ceea ce ar putea crede mulți, Indonezia nu este doar o țară musulmană, iar câteva alte religii și credințe sunt practicate în mod liber, inclusiv protestantismul, catolicismul, hinduismul și budismul. Aceste organizații religioase non-islamice sunt de obicei mai incluzive și mai democratice în operațiunile lor, exprimând adesea sentimente pro-seculare. De fapt, multe organizații democratice și pro-seculare ale societății civile non-islamice din Indonezia se angajează adesea în inițiative de construire a coaliților și de sensibilizare a comunității, străduindu-se să promoveze valorile armoniei religioase, acceptării și păcii în rândul cetățenilor și rezidenților indonezieni[212]. Numărul organizațiilor creștine care oferă sprijin social și pentru dezvoltarea comunității a crescut după tsunami-ul din Aceh din 2004[213].

Istoria Indoneziei a fost modelată de resursele sale naturale, cum ar fi mirodeniile prețioase, și de sosirea comercianților străini. De-a lungul timpului, olandezii au apărut ca putere colonială dominantă. În 1602, Compania Olandeză a Indiilor de Est sau Vereenigde Oost-Indische Compagnie (VOC), a fost înființată cu scopul de a crea un monopol comercial în Indiile de Est. În 1619, VOC a stabilit Batavia (acum Jakarta) ca sediu al VOC, iar prezența olandeză în Indonezia a continuat să se

[210]Sylvia Yazid, Aknolt K. Pakpahan, „Democratization in Indonesia: Strong State and Vibrant Civil Society*" Asian Affairs: An American Review*, p.12.
[211] *Ibidem.*
[212] Minako Sakai, „Building a partnership for social service delivery in Indonesia: state and faith-based organisations" , *Australian Journal of Social Issues*, vol 47, nr.3, 2012, p.381.
[213] *Ibidem*.

extindă[214]. Drept urmare, olandezii au început să controleze întreaga Indonezie până în secolul al XIX-lea. Cu toate acestea, secolul dominației coloniale olandeze a întărit sentimentul identității naționale indoneziene, deoarece exploatarea și opresiunea de către conducătorii olandezi aprinseseră spiritul naționalismului. În 1928, mișcarea de tineret indoneziană, numită Boedi Oetomo, a cerut independența prin Proclamarea Independenței Indoneziei. În cele din urmă, Indonezia și-a declarat independența față de olandezi pe 17 august 1945, iar Soekarno și Hatta au devenit primul președinte și vicepreședinte. Lupta Indoneziei împotriva stăpânirii olandeze și acordarea independenței în 1949 semnifică apariția celui mai mare stat arhipelag din lume în secolul al XX-lea. Olandezii lăsaseră o structură administrativă complexă bazată pe diviziunea rasială indonezienei. Olandezii i-au clasificat pe indonezieni și i-au plasat în diferite grupuri. De exemplu, olandezii au împărțit nativii în „Volk", adică oameni de origine indoneziană și parțial olandeză, și o categorie de clasă inferioară numită „Inlander"[215]. Între timp, chinezii, care intraseră în Indonezia în timpul erei coloniale olandeze, erau puși în „Vreemde Oostersche", care înseamnă oriental străin[216]. Sistemul juridic a fost menit să favorizeze olandezii și indo-europenii, dar nu si indonezieni. Drept urmare, olandezii au început să ofere „certificate de bună conduită" grupurilor privilegiate în schimbul sprijinului pentru stăpânirea olandeză[217]. O astfel de diviziune și politică discriminatorie a aprins tensiuni etnice și a servit drept unul dintre factorii care contribuie la conflictele etno-religioase care au avut loc în Indonezia.

---

[214] Arnaout Van der Meer, *Performing power: cultural hegemony, identity, and resistance in colonial Indonesia*, Cornell University Press, 2020, p.3.
[215] *Idem*, pp. 9-15.
[216] *Ibidem*.
[217] Luttikhui Bart, Arnout HC van der Meer, „1913 in Indonesian history: Demanding equality, changing mentality.", *TRaNS: Trans-Regional and-National Studies of Southeast Asia, vol.* 8, nr. 2, 2020, pp.5-7.

Indonezia are aproximativ 300 de grupuri etnice native distincte. Javanezii sunt cele mai populate dintre aceste grupuri și multe dintre aceste grupuri au propria lor limbă[218]. Uneori, grupurile etnice individuale nu sunt recunoscute de guvern, ceea ce îngreunează exprimarea politică pentru membrii acestor grupuri. Guvernul indonezian recunoaște oficial doar 5 credințe: islam, protestantism, catolicism, hinduism și budism[219]. Toți indonezienii sunt înregistrați ca adepți ai uneia dintre aceste credințe la naștere, ceea ce a condus la discriminarea celor care nu dețin una dintre aceste credințe. De exemplu, mulți indigeni din Papua de Vest și South Maluku nu sunt recunoscuți oficial ca adepți ai unei credințe și astfel se luptă pentru a avea acces la locuri de muncă, educație și drepturi de vot[220]. Există, de asemenea, o mare migrație istorică din insulele dens populate Java, Bali și Madura, care a provocat tensiuni cu populațiile indigene ale altor insule mai mici. Această migrație s-a datorat parțial stăpânirii coloniale, în care guvernul Indiilor de Est olandeze a folosit programul „transmigrasi" pentru a muta javanezii în alte insule pentru a reduce presiunile populației asupra Java[221]. Această politică a fost continuată de guvernul indonezian după independență și este încă practicată în unele zone sub pretextul reducerii sărăciei și dezvoltării infrastructurii. Acest lucru a provocat conflicte, deoarece populațiile indigene se simt marginalizate din punct de vedere politic și economic și sub presiunea influenței culturii Java. De exemplu, în Aceh și Papua de Vest, există mișcări separatiste de lungă durată care vizează stabilirea independenței față de Indonezia. Aceste mișcări au fost alimentate

[218] Steven Drakeley, *The History of Indonesia,* Greenwood Publishing Group, 2005, p.14.

219 James Joseph Errington, Other Indonesians: Nationalism in an Unnative Language, Oxford University Press, 2022, pp.49-52.

[220] *Ibidem*.

[221] Arnaout Van der Meer, *Performing power: cultural hegemony, identity, and resistance in colonial Indonesia*, Cornell University Press, 2020, p.180-184.

inițial de încercarea guvernului central de a impune cultura națională și au interzis exprimarea publică a culturii regionale[222]. Deși aceste interdicții au fost abrogate de atunci, au lăsat o moștenire de resentimente și politici discriminatorii care contribuie și astăzi la conflict

Diferențele religioase sunt principalele surse de conflict în Indonezia. În 2022, peste 87% dintre indonezieni s-au declarat musulmani, urmați de 7,43% care erau creștini, 1,69 erau hinduși, iar 0,73 budiști.[223] Deși Indonezia este un stat majoritar musulman, distribuția lor in teritoriu este inegala. De exemplu, creștinii și animiștii formează majoritatea în Sulawesi de Nord, Kepulauan Riau, Papua și East Nusa Tenggara, dar sunt minoritari în alte zone[224]. În orașul Kupang, Timorul de Vest, există o majoritate catolică, în timp ce în restul provinciei, în special pe Flores, protestanții sunt majoritatea. În insulele Sangihe Talaud din nordul Sulawesi, unde 90% din populație este creștină[225]. Creșterea grupurilor politice islamice și a grupurilor islamice în general ar putea avea implicații grave asupra stabilității regiunii. Cel mai bun exemplu in acest sens este conflict de la Ambon, între creștini si musulmani, în care au murit cel puțin 5.000 de oameni, 7 biserici au fost distruse și 2.500 de persoane au fost rănite[226]. Diviziunile din societatea

[222] *Ibidem*.

223 Statista, Share of population Indonesia 2022 by religion, accesat la 20.02.2024, disponibil online la https://www.statista.com/statistics/1113891/indonesia-share-of-population-by-religion/.

[224] Statista, Breakdown of Indonesian population who live in provinces where the majority of the population is not Muslim in 2010, by religion, accesat la 20.02.2024, disponibil online la https://www.statista.com/statistics/1260420/indonesia-population-breakdown-of-provinces-with-least-muslims-by-religion/.

[225] *Ibidem*.

[226] Hasudungan, Anju Nofarof. "Muslim and Christian relations in the field of education after The Ambon-Maluku conflict (The Biggest Religious

indoneziană sunt adânc înrădăcinate, iar diferențele religioase vor continua să fie principala sursă de conflict pentru viitorul apropiat. Conflictul etnic are rădăcini istorice adânci în Indonezia, dar a fost alimentat de factori politici, economici și sociali contemporani. Acești factori includ concentrarea puterii politice în mâinile javanezilor, marginalizarea relativă a altor grupuri de la luarea deciziilor politice și economice și exploatarea identităților comunale de către conducătorii autoritari[227].

Colaborarea dintre guvern și organizațiile neguvernamentale religioase din Indonezia este extrem de importantă în gestionarea crizelor și a tensiunilor etno-religioase. ONG-urile religioase aduc o contribuție valoroasă în această colaborare deoarece au capacitatea de a acționa dincolo de constrângerile politice și de a oferi abordări bazate pe valorile religioase comune și pe înțelegerea sensibilităților culturale[228]. Prin intermediul dimensiunii religioase, aceste organizații pot câștiga încrederea și acceptarea comunităților afectate, având acces mai ușor la informațiile necesare și la resursele specifice pentru acțiuni eficiente și rapide în situațiile de criză[229]. Colaborarea între guvern și organizațiile neguvernamentale religioase pentru gestionarea crizelor și tensiunilor etno-religioase are o importanță crucială în Indonezia. Ele sunt adesea parte integrantă a sistemului de răspuns la dezastre și joacă un rol esențial în asigurarea asistenței umanitare și reconstrucției după calamități

Conflict in Indonesia)." *Journal of Educafion, Society & Mulficulturalism* vol.1, nr.3, 2021, p. 46.

[227] Sylvia Yazid, Aknolt K. Pakpahan, „Democratization in Indonesia: Strong State and Vibrant Civil Society*" Asian Affairs: An American Review*, p.5.

[228] Muhammad Indrawan Jatmika, Palupi Anggraheni, „Civil Society's Role in Indonesia's Humanitarian Diplomacy: Study of Indonesian Religious Organizations' Humanitarian Aid in the Crisis in Myanmar's Rakhine State Region (2012- 2018)", *Jurnal Pemikiran Politik Islam,* vol.4, nr.2, 2021, p.8.

[229] *Ibidem.*

naturale sau conflicte[230]. Aceste entități sunt capabile să mobilizeze rapid resurse umane si materiale, având acces la comunitățile afectate si la cunoștințele necesare pentru a oferi sprijin acolo unde este mare nevoie[231]. De asemenea, ele pot promova dialogul inter-religios si pot reprezenta un canal eficient de comunicare între diferitele grupuri etno-religioase afectate de criză.

Într-un articol din Revista Internațională a Crucii Roșii din 2005, Elizabeth Ferris a evidențiat avantajele distincte ale organizațiilor neguvernamentale religioase în comparație cu cele laice. Acestea sunt: organizațiile neguvernamentale religioase au un rol important în influențarea și reconfigurarea normelor, ceea ce le face să fie mai susceptibile să treacă de la concentrarea pe politici și comportamente la aspecte mai profunde; motivația organizațiilor neguvernamentale religioase provine din credința lor; pentru credincioși, este o datorie morală să răspundă nevoilor celor defavorizați, deși diferite tradiții religioase pot influența modul în care își manifestă credința prin acțiuni, toate evidențiază faptul că această motivație este o sursă puternică pentru desfășurarea activităților umanitare; organizațiile neguvernamentale religioase sunt adânc înrădăcinate în societate și au o relație stabilă de încredere și familiaritate cu comunitățile locale în care activează; datorită rețelei sale globale, organizațiile neguvernamentale religioase pot juca roluri semnificative în furnizarea de servicii, mobilizarea comunitară, promovarea unor cauze sociale importante, medierea conflictelor dintre diferite grupuri sociale și strângerea de informații și resurse la nivel mondial[232]. Aceste avantaje ale ONG-urilor religioase, facilitează colaborarea acestora cu statul.

---

[230] Michael Bodakowski, *Faith-Inspired Organizations and Global Development Policy: A Background Review "Mapping" Social and Economic Development Work in Southeast Asia,* Berkley Center for Religion, Peace, and World Affairs, 2010, p.27.

[231] *Ibidem.*

[232] Elizabeth Ferris, „Faith-based and secular humanitarian organizations", *International Review of the Red Cross,* vol.87, nr. 858, 2005, pp. 316-320.

Religia atinge cel mai profund aspect al identității cuiva și poate fi folosită pentru a mobiliza oamenii în scopuri atât de luptă, cât și de negociere pașnică. În diverse regiuni ale lumii, religia poate determina oamenii să recurgă la acțiuni violente. De-a lungul istoriei umanității, religia a reprezentat adesea o sursă de intoleranță, abuz și violență[233]. Cu toate acestea, conform multor cercetători religia poate fi și o sursă de transformare non-violentă, promovare a drepturilor omului, integritate în afaceri și guvernare și societate pașnică[234]. Indonezia este o țară cu diverse religii. Există șase religii recunoscute oficial în țară: islamul, protestantismul, catolicismul, hinduismul, budismul și confucianismul[235]. Alte practici religioase, locale sau globale, pot exista și pot fi urmate, însă nu sunt sprijinite de guvern. La o zi după obținerea independenței în data de 18 august 1945, autoritățile au adoptat Pancasila ca fundament al identității indoneziene. Pancasila reprezintă un concept care cuprinde cinci principii: credința într-un singur Dumnezeu; o societate echitabilă și civilizată; unitatea Indoneziei; democrația sub îndrumarea consultanței reprezentative; justiția socială pentru toți cetățenii indonezieni[236].

Prezența organizațiilor neguvernamentale religioase în Indonezia nu este un element nou. O creștere semnificativă a avut loc între anii 1985 și 1997, când numărul organizațiilor sociale implicate în activități religioase a crescut cu 66,7%[237]. În această perioadă,

---

[233] Hariawan Adji, „The Role of Religious Institutions in Promoting Social Welfare in Indonesia", *Mozaik Humaniora,* vol.21, nr.2, 2021, p.172.
[234] *Ibidem.*
[235] Michael Bodakowski, *Faith-Inspired Organizations and Global Development Policy: A Background Review "Mapping" Social and Economic Development Work in Southeast Asia,* Berkley Center for Religion, Peace, and World Affairs, 2010, p.25.
[236] Hariawan Adji, „The Role of Religious Institutions in Promoting Social Welfare in Indonesia", *Mozaik Humaniora,* vol.21, nr.2, 2021, p.172.
[237] Caroline Hartnell, *PHILANTHROPY IN INDONESIA. A working paper.,* Philanthropy for Social Justice and Peace, 2020, pp. 3-5.

activitățile religioase au devenit mai democratizate și au câștigat teren datorită unei mai mari libertăți acordate de guvern. Acest lucru poate fi observat prin schimbarea tiparelor în ceea ce privește practicile religioase din societate. Inițial societatea indoneziană a limitat conceptul și practica religiei la ritualuri pentru a conserva identitatea de grup, mai ales în mediile rurale[238]. Cu toate acestea, rolul religiei ca forță socială este în expansiune și aceasta a transformat credințele într-un bun al unei economii politice care face parte din procesul de modernizare al Indoneziei[239]. Această tendință a fost alimentată de evenimente critice care au testat unitatea și hotărârea comunităților religioase. În contextul unor astfel de evenimente, organizațiile neguvernamentale cu caracter religios devin tot mai importante în gestionarea tensiunilor etno-religioase din Indonezia. Printre conflictele menționate se includ disputele dintre Gereja Masehi Injili di Minahasa/GMI (Biserica Creștin-Evanghelic din Minahasa) și Gereja Protestan Indonesia di Minahasa/GPIM (Biserica Protestantă din Sulawesi) din anul 1999, confruntările interreligioase dintre creștini și musulmani în Maluku, Poso, Sulawesi Central, în perioada 1999-2001[240].

Organizațiile neguvernamentale religioase joacă un rol activ în abordarea conflictelor și a tensiunilor comunitare. Participarea lor în regiunile afectate de conflicte ar putea contribui la reducerea tensiunilor și a numărului de victime. Deși uneori poziționate împotriva guvernului sau a autorităților locale din cauza diferitelor abordări, agende și viziuni, ele sunt în mare

[238] Hariawan Adji, „The Role of Religious Institutions in Promoting Social Welfare in Indonesia", *Mozaik Humaniora,* vol.21, nr.2, 2021, p.172.
[239] *Ibidem.*
[240] Angel Damayanti, Sri Yunanto, „From Evangelization to Worship Restrictions: The Changing Characteristics of Threat Perception between Muslims and Christians in Indonesia", *Islam and Christian–Muslim Relations,* vol.33, nr.4, 2022, pp.338-340.

parte considerate mediatori raționali[241]. Cunoștințele lor despre cultura locală au adus anumite beneficii în gestionarea conflictelor. În contextul acesta, organizațiile neguvernamentale religioase din Indonezia au avut un rol semnificativ în prevenirea, reducerea și contracararea conflictelor și violenței sectare. Pentru a evita escaladarea conflictului în diverse locuri, aceste organizații religioase își asumă responsabilitatea de a gestiona crizele prin intermediul unui set de acțiuni[242]. Aceste acțiuni includ furnizarea de ajutor umanitar, crearea rețelelor de răspuns rapid în situațiile de urgență și colaborarea cu autoritățile guvernamentale[243].

Deși există multe dezbateri cu privire la beneficiile oferite de implicarea organizațiilor non-guvernamentale religioase în managementul crizei, unele dintre acestea sunt succese care determină guvernul să fie deschis colaborării. Indonezia este o țară predispusă la dezastre și este adesea afectată de cutremure, inundații, alunecări de teren și erupții vulcanice[244]. Această situație a determinat guvernul să pună bazele Platformei Naționale pentru Reducerea Riscului de Dezastre în 2008. Această inițiativă a guvernului a creat oportunitatea pentru organizațiile neguvernamentale religioase de a se implica în gestionarea dezastrelor. Conform Legii gestionării dezastrelor nr. 24/2007, guvernul, prin intermediul Agenției Naționale pentru Managementul Dezastrelor, a implicat anumite organizații neguvernamentale religioase în elaborarea hărților tematice, în

---

[241] Michael Bodakowski, *Faith-Inspired Organizations and Global Development Policy: A Background Review "Mapping" Social and Economic Development Work in Southeast Asia,* Berkley Center for Religion, Peace, and World Affairs, 2010, p.27.

[242] Hariawan Adji, „The Role of Religious Institutions in Promoting Social Welfare in Indonesia", *Mozaik Humaniora,* vol.21, nr.2, 2021, p.174.

[243] *Ibidem.*

[244] Janiscus Pieter Tanesab, „Institutional Effectiveness and Inclusions: Public Perceptions on Indonesia's Disaster Management Authorities", *International Journal of Disaster Management,* vol.3, nr.2, 2020, p.3.

gestionarea dezastrelor, pregătirea comunităților pentru situații de urgențe, și reabilitarea infrastructurii[245]. Această implicare a fost consolidată prin semnarea unui Decret comun între Ministerul Afacerilor Interne, Ministerul Cultelor și Ministerul Cercetării și Tehnologiei. Prin acest Decret comun s-a legalizat implicarea organizațiilor neguvernamentale religioase în gestionarea dezastrelor[246]. În cazurile cutremurului și tsunami-ului din Aceh care au dus la moartea a peste 200.000 de persoane, participarea organizațiilor neguvernamentale religioase în gestionarea dezastrelor s-a dovedit benefică[247]. Aceh a fost primul loc unde s-a desfășurat un efort de gestionare a dezastrelor la nivel internațional. O inițiativă creată de anumite organizații neguvernamentale islamice și alte comunități islamice a declanșat o mișcare de solidaritate cunoscută sub numele de „mobilizarea a 1000 de mubaligh" (predicatori) pentru Aceh[248]. De asemenea, studii precum cel referitor la erupțiile vulcanice Merapi și Sinabung au arătat importanța implicării liderilor religioși și a comunitatilor în reducerea riscului provocat de dezastre naturale, subliniind astfel necesitatea implicării organizațiilor religioase neguvernamentale în gestionarea acestor situații dificile[249].

Astfel, organizațiile religioase și grupurile au un rol important în gestionarea riscului de dezastru în comunitățile lor. Ele pot accesa zone la care autoritățile civile nu pot ajunge sau nu la fel

---

[245] *Idem, p.4.*
[246] *Ibidem.*
[247] Sufri S., Dwirahmadi F., Phung D. , „Enhancing community engagement in disaster early warning system in Aceh, Indonesia: opportunities and challenges.", *Nat Hazards,* vol.103, 2020, p.2692.
[248] *Ibidem.*
[249] UNDRR, ,,Does Community Managed Risk Reduction Work? Experiences with the Eruption of Mount Merapi in Indonesia", accesat online la 14.03.2024, disponibil online la https://www.unisdr.org/files/17341_17341cmdrrbeforeandduringtheeruptio.pdf.

de ușor, având voluntari bine pregătiți care cunosc în profunzime zonele și locuitorii lor[250]. Prin urmare, au capacitatea de a interveni în zonele afectate fără un interes ascuns și pot obține informații directe de la locuitori. Datorită rețelelor deja existente, organizațiile religioase par să implementeze aceste acțiuni mai eficient decât alți participanți, iar fiind organizații neguvernamentale, persoanele afectate le acordă mai multă încredere și sunt mai deschise să împărtășească problemele cu ele[251]. Totodată, în comunitățile musulmane precum Indonezia, difuzoarele moscheii pot fi folosite ca mijloc de avertizare imediat înainte de dezastre și pot, de asemenea, să servească drept canal de comunicare cu locuitorii după producerea unui dezastru pentru a coordona operațiunile de ajutor, salvare și recuperare[252]. Acest lucru se datorează faptului că unele moschei mari sunt echipate cu generatoare și pot folosi sistemul lor de difuzoare chiar și în situații în care apare o pană de curent. De asemenea, Biserica Catolică din Indonezia si ONG-urile catolice, au un rol important în susținerea Obiectivelor de Dezvoltare Durabilă la nivel local[253]. Episcopii catolici din Indonezia (KWI/Konferensi Waligereja Indonesia) s-au întâlnit pentru a discuta despre sprijinul acordat de biserica catolică indoneziană și implicarea activă în atingerea ODD-urilor[254]. Ei consideră că guvernul, pe cont propriu, nu poate gestiona toate provocările doar prin intermediul politicilor și planurilor sale detaliate[255].

---

[250] Rahim Ali Sheikhi, Hesam Seyedin, Ghader Qanizadeh, Katayoun Jahangiri, „Role of Religious Institutions in Disaster Risk Management: A Systematic Review", *Disaster Medicine and Public Health Preparedness,* 2020, p.7.

[251] *Ibidem.*

[252] *Ibidem.*

[253] Hariawan Adji, „The Role of Religious Institutions in Promoting Social Welfare in Indonesia", *Mozaik Humaniora,* vol.21, nr.2, 2021, p.174.

[254] *Ibidem.*

[255] *Ibidem.*

Este necesar să fie sprijinit de societatea civilă și alte instituții sociale.

În ceea ce privește problema conflictelor etnico-religioase, ONG-urile cu orientare religioasă adoptă diverse abordări și strategii pentru a gestiona tensiunile etnice și religioase. Voi evidenția câteva dintre acestea aici. O metodă semnificativă prin care organizațiile neguvernamentale religioase își propun să promoveze înțelegerea interreligioasă și pacea este prin intermediul educației[256]. În acest sens, ONG-urile islamice au un impact semnificativ. Din perspectiva islamică, fiecare musulman are datoria de a-și ajuta semenii, de a lupta împotriva sărăciei, de a consolida legăturile dintre oameni și de a menține coeziunea comunitară[257]. În Indonezia, două organizații musulmane dominante în domeniul activităților sociale și caritabile sunt Muhammadiyah, cu 30 de milioane de membri preponderent moderniști, și Nahdlatul Ulama, cu 40 de milioane de membri preponderent tradiționaliști[258]. Membrii Muhammadiyah sunt concentrați mai ales în zonele urbane ale Javei, Sumatrei si insulelor externe din Indonezia, în timp ce membrii Nahdlatul Ulama se regasesc in principal in zonele rurale ale Javei[259]. Ambele organizații desfășoară programe extinse de dezvoltare sociala, concentrându-se în special pe implicarea și susținerea instituțiilor educaționale. Muhammadiyah administrează peste 12.000 de școli în întreaga ţară pentru aproximativ un milion de

[256] Hilman Latief, *Philanthropy in the Muslim World*, Monograph Book, 2023, p.315.
[257] Smith C. Q., WilliamsS. G. ,"Why Indonesia Adopted 'Quiet Diplomacy' over R2P in the Rohingya Crisis: The Roles of Islamic Humanitarianism, Civil–Military Relations, and ASEAN.", *Global Responsibility to Protect*, vol.*13, nr.2* , p. 164.
[258] Michael Bodakowski, *Faith-Inspired Organizations and Global Development Policy: A Background Review "Mapping" Social and Economic Development Work in Southeast Asia,* Berkley Center for Religion, Peace, and World Affairs, 2010, p.28.
[259] *Ibidem.*

elevi musulmani şi non-musulmani[260]. Sistemul educațional al Muhammadiyah cuprinde două tipuri diferite de școli: cele predominant laice care urmează un curriculum secular şi pesantrens religios care includ curriculum religios[261]. Atât școlile laice, cât și cele religioase sunt implicate: 8.522 de grădinițe, 197 de școli primare; 3.861 de școli primare islamice; 378 de școli gimnaziale, 733 de scoli gimnaziale islamice, 211 licee, precum și 212 licee islamice, 44 universități și 23 academii/colegii[262]. De asemenea, au o implicare indirectă în majoritatea internatelor islamice din Indonezia. Având în vedere că doar între 1 și 2% din PIB-ul național este alocat educației, rolul ambelor organizații este evident esențial[263]. În plus față de contribuția lor semnificativă în domeniul educației, ambele oferă suport grupurilor de femei și mișcărilor de tineret și administrează centre medicale[264].

Un alt rol al organizațiilor neguvernamentale religioase în rezolvarea conflictelor etnice religioase este promovarea dialogului interconfesional. Atât NU, cât și Muhammadiyah subliniază importanța pluralismului și a toleranței religioase[265]. Figuri importante din ambele organizații au colaborat pentru a încuraja cooperarea interconfesională în proiecte de dezvoltare. În 2003, fostul lider al Muhammadiyah, Ahmad Syafi'i Maarif, a înființat Institutul Maarif pentru Cultură și Umanitate cu misiunea principală de a promova dialogul interconfesional[266]. Similar, în 2004, Abdurrahman Wahid, fost președinte al Indoneziei și al NU, a fondat Institutul Wahid, care își propune printre alte obiective să dezvolte dialogul între liderii spirituali și politici din lumea occidentală și societățile musulmane[267]. Un exemplu de

[260] *Ibidem.*
[261] *Idem, p.29.*
[262] *Ibidem.*
[263] *Ibidem.*
[264] *Ibidem.*
[265] *Idem, p.28.*
[266] *Ibidem.*
[267] *Ibidem.*

succes al organizațiilor neguvernamentale religioase în acest sens, este „Rețeaua de tineret interreligios pentru pace" (Interfaith Youth Network for Peace). Rețeaua de tineret interreligios pentru pace a fost inițiată de două organizații neguvernamentale religioase, Conferința Indoneziană pentru Religie și Pace și Institutul Wahid (RYWP), în urma violenței din Poso și Maluku[268]. Ambele organizații consideră că implicarea tinerilor din Indonezia este esențială în consolidarea păcii. RYWP își propune să implice tinerii în activități și discuții care promovează înțelegerea reciprocă, empatia și cooperarea între tineri de diferite religii[269]. RYWP și Institutul Wahid speră că acest proiect va aduce direct implicarea tinerilor din Poso și Maluku. Scopul acestei inițiative este să creeze o rețea de tineri care să promoveze pacea în comunitate[270]. Se consideră că succesul păcii pe termen lung în Maluku constă în dezvoltarea unei noi generații de lideri din diferite religii angajați să mențină pacea în comunitatea lor.

Rolul Mănăstirilor Forestiere Budiste în Securitatea din Indonezia

Mănăstirile forestiere budiste au jucat un rol crucial în menținerea securității sociale și ecologice în Indonezia. Acestea au funcționat ca bastioane de protecție a mediului, centre de educație spirituală și piloni ai păcii comunitare. Articolul analizează importanța mănăstirilor forestiere budiste din perspectiva conservării pădurilor, promovării armoniei sociale și întăririi securității naționale. Indonezia, cu vastitatea sa ecologică și diversitatea culturală, a găzduit de-a lungul secolelor numeroase tradiții spirituale și religioase. Mănăstirile forestiere

[268] Asia & the Pacific Interfaith Youth Network, accesat la 16.03.2024, disponibil online la https://rfpasia.org/apiyn/.
[269] *Ibidem.*
[270] *Ibidem.*

budiste, deși mai puțin cunoscute în contextul predo-minant musulman al țării, au avut un impact semnificativ asupra men-ținerii echilibrului ecologic și social. Aceste mănăstiri, situate în zone izolate de pădure, oferă nu doar refugiu spiritual, ci și contribuții esențiale la securitatea națională prin conservarea biodiversității și stabilizarea comunităților locale[271].

Mănăstirile forestiere budiste sunt în mod tradițional situate în zone împădurite, unde călugării trăiesc în armonie cu natura. Această coexistență pașnică promovează conservarea pădurilor tropicale, care sunt cruciale pentru stabilitatea climatică globală și biodiversitatea regională[272]. Pădurile tropicale din Indonezia sunt printre cele mai diverse din lume, găzduind mii de specii de plante și animale. Prin practicile lor de meditație și agricultură sustenabilă, mănăstirile budiste contribuie la prevenirea defrișărilor ilegale și a degradării mediului[273].

Acestea funcționează și ca centre de educație și conștientizare ecologică. Călugării și adepții lor promovează valori de respect și protecție a naturii prin învățături și exemple practice[274]. În acest fel, mănăstirile influențează comunitățile locale, încurajând practici agricole durabile și protejarea resurselor naturale[275]. Educația oferită de mănăstiri are un efect pe termen lung asupra mentalității comunității, contribuind la crearea unei generații mai conștiente și mai responsabile față de mediul înconjurător. Pe lângă rolul lor ecologic, mănăstirile forestiere budiste sunt esențiale în promovarea armoniei sociale. Ele servesc ca spații neutre unde comunitățile se pot reuni pentru a rezolva conflicte și a discuta probleme comune[276]. Prin intermediul valorilor

[271] Gombrich R., *Theravada Buddhism: A Social History from Ancient Benares to Modern Colombo*, Routledge, 2009, p.30.
[272] *Ibidem.*
[273] *Ibidem.*
[274] Winters Dennis A., "The first Buddhist monasteries." *The Tibet Journal*, vol.13, nr.2, 1988, pp.12-14.
[275] *Ibidem.*
[276] *Ibidem.*

budiste de compasiune, non-violență și cooperare, mănăstirile contribuie la reducerea tensiunilor sociale și la crearea unui mediu de pace și stabilitate[277].

Contribuțiile ecologice și sociale ale mănăstirilor forestiere budiste au implicații directe pentru securitatea națională a Indoneziei. Prin protejarea pădurilor, aceste mănăstiri ajută la prevenirea dezastrelor naturale, cum ar fi inundațiile și alunecările de teren, care pot avea efecte devastatoare asupra comunităților și infrastructurii naționale[278]. De asemenea, prin promovarea păcii și stabilității sociale, mănăstirile contribuie la reducerea riscurilor de conflicte interne și la întărirea coeziunii naționale[279].

În partea ce urmează, vor fi prezentate exemple concrete de implicare a mănăstirilor forestiere budiste în dinamica securității din Indonezia. Mănăstirea Wat Suan Mokkh din Java de Vest este cunoscută pentru programele sale educaționale de conștientizare ecologică. Aceasta organizează seminarii și ateliere pentru comunitățile locale, învățându-le tehnici de agricultură durabilă și metode de conservare a resurselor naturale[280]. Programul "Eco-Monk" a avut un succes deosebit, formând tineri lideri ecologiști care lucrează acum pentru protecția mediului în diverse regiuni din Indonezia[281].

O altă inițiativă importantă, situată în regiunea montană din Bali, unde mănăstirea Wat Doi Inthanon colaborează cu organizații non-guvernamentale pentru a proteja sursele de apă potabilă. Proiectul lor de conservare a apei include construirea

---

[277] Rizzo Roberto, Buddhism *in Indonesia: A Study of Multiple Revivals*. Taylor & Francis, 2024, pp.95-96.

[278] Ministry of Environment and Forestry of Indonesia, The State of Indonesia's forests(2020), accesat la 17.05.2024, disponibil online la https://indonesianembassy.de/wp-content/uploads/2020/12/Lowres2-SOFO-2020-B5_ENG-12.24.2_compressed.pdf.

[279] *Ibidem.*

[280] Wat Suan Mokkh International Dharma Hermitage, accesat la 17.05.2024, disponibil online la https://www.suanmokkh-idh.org/.

[281] *Ibidem.*

de baraje mici și terasarea versanților pentru a preveni eroziunea solului și a menține calitatea apei[282]. Aceste măsuri au îmbunătățit siguranța aprovizionării cu apă pentru zeci de sate din zonă[283]. Totodată, mănăstirea Wat Phra Dhammakaya din Jakarta a dezvoltat un program de mediere a conflictelor comunitare, folosind principiile budiste de compasiune și non-violență[284]. Acest program a ajutat la rezolvarea disputelor teritoriale și a tensiunilor etnice în diverse comunități, contribuind astfel la menținerea păcii și stabilității sociale.

Concluzii

Colaborarea dintre organizațiile non-guvernamentale (ONG-uri) și autoritățile din Indonezia în ceea ce privește securitatea a fost determinată de expertiza distinctivă, resursele semnificative și legitimitatea pe care aceste organizații le au în comunități. ONG-urile au adus o expertiză specializată în diferite domenii relevante pentru securitate, precum gestionarea riscurilor naturale, prevenirea conflictelor și reconstrucția post-conflict. De-a lungul timpului, aceste organizații au dezvoltat capacități solide în analizarea și intervenția în situațiile de criză, oferind soluții inovatoare și flexibile pentru provocările specifice ale mediului indonezian.

Pe lângă cunoștințele lor specializate, ONG-urile au pus la dispoziție resurse semnificative, inclusiv finanțare, echipamente și personal calificat. Aceste resurse au fost esențiale pentru

[282] Doi Inthanon, accesat la 17.05.2024, disponibil online la https://www.thainationalparks.com/doi-inthanon-national-park.
[283] The ordination of 500 Indonesian ordinands at Borobudur-Indonesia, accesat la 17.05.2024, disponibil online la https://en.dhammakaya.net/the-ordination-of-500-indonesian-ordinands-at-borobudur-indonesia/.
[284] *Ibidem.*

sprijinirea eforturilor guvernamentale în gestionarea situațiilor de urgență și implementarea proiectelor de securitate pe termen lung. În plus, legitimitatea și încrederea câștigate de ONG-urile în rândul comunităților locale au avut un rol crucial în succesul colaborării. Fiind organizații independente orientate către nevoile populației locale, aceste ONG-uri au putut mobiliza și implica comunitatea în eforturile de securitate, consolidând astfel coeziunea socială și susținând implementarea eficientă a inițiativelor guvernamentale. Acest parteneriat contribuie la abordarea holistică și eficientă a provocărilor legate de securitate.

În principal, cercetarea mea a evidențiat motivația statului indonezian și modalitatea în care statul indonezian colaborează cu ONG-urile, mai ales cu cele de factură religioasă, în gestionarea situațiilor de criză, aceasta fiind o perspectivă puțin studiată în literatura relațiilor internaționale și a studiilor de securitate. Analiza mea a relevat că, într-un mediu multicultural complex precum Indonezia, ONG-urile religioase nu se află într-o competiție pentru influență, ci pot colabora eficient cu statul pentru a asigura securitatea și stabilitatea societății pe durata crizelor. Această descoperire reprezintă o contribuție semnificativă la înțelegerea modului în care relația dintre stat și ONG-uri poate funcționa în contexte variate și poate influența abordările privind securitatea.

Implicațiile empirice ale cercetării mele sunt, prin urmare, multiple și profunde. În primul rând, ele oferă o mai bună înțelegere a modului în care organizațiile non-guvernamentale religioase pot fi implicate în gestionarea crizelor și prevenirea conflictelor într-o țară precum Indonezia. Această înțelegere este crucială pentru dezvoltarea politicilor și strategiilor care să promoveze și să susțină colaborarea între guvern și societatea civilă în astfel de contexte. De asemenea, cercetarea mea subliniază importanța luării în considerare a specificităților culturale și religioase în analiza relațiilor dintre stat și ONG-uri,

deoarece aceste aspecte au capacitatea de a influența semnificativ dinamica colaborării și cooperării între acești actori.

Cercetarea mea empirică a relevat că, în situațiile de securitate, organizațiile neguvernamentale religioase și cele de dezvoltare sunt actorii principali care colaborează cu guvernul indonezian. Caracteristicile acestui parteneriat specific includ abilitatea acestor ONG-uri de a mobiliza resurse și comunități locale, precum și expertiza lor în domenii relevante pentru gestionarea crizelor, cum ar fi ajutorul umanitar, asistența medicală și educația. În plus, aceste ONG-uri demonstrează un nivel ridicat de încredere și legitimitate în ochii populației, ceea ce facilitează colaborarea lor cu autoritățile guvernamentale în situații de urgență. Prin urmare, aceste caracteristici distincte definesc parteneriatul complex dintre organizațiile neguvernamentale religioase și cele de dezvoltare și guvernul Indonezian în abordarea problemelor legate de securitate, conferindu-i o eficiență și relevanță sporite în contextul specific al țării.

În cercetarea mea, am investigat cum statul indonezian colaborează cu organizațiile neguvernamentale, în special cele de natură religioasă în contextul securității. Am folosit teoriile lui Buzan și agenda sa extinsă pentru a examina aceste relații. Am constatat că statul Indonezian se bazează pe colaborarea cu ONG-urile pentru a aborda amenințările la adresa securității, recunoscând capacitățile și resursele acestora în completarea eforturilor guvernamentale de gestionare a crizelor și prevenirea conflictelor. Acest parteneriat este esențial pentru asigurarea securității naționale și stabilitatea societății, iar înțelegerea acestei dinamici este crucială pentru elaborarea unor politici și strategii eficiente în domeniul securității.

Contribuțiile teoretice ale cercetării mele sunt multiple și fundamentale pentru înțelegerea relației dintre stat și organizațiile neguvernamentale (ONG-uri) în contextul securității, cu accent pe studiul de caz al Indoneziei. Prin analizarea dinamicii colaborării dintre stat și ONG-uri într-un cadru specific și mai

puțin explorat anterior, cercetarea mea aduce o contribuție semnificativă la extinderea cunoștințelor și cadrelor teoretice în domeniul securității și relațiilor internaționale. Studiul scoate în evidență importanța ONG-urilor religioase în peisajul multicultural al Indoneziei, subliniind necesitatea unei abordări mai complexe și contextualizate a relațiilor dintre actorii de securitate. De asemenea, cercetarea subliniază importanța ONG-urilor religioase în procesul de securitizare în situațiile de criză. Prin colaborarea lor strânsă cu statul, aceste organizații devin factori importanți ai procesului de asigurare a securității, contribuind la gestionarea şi rezolvarea diferitelor amenințări la adresa acesteia

Cercetarea mea, deși aduce contribuții semnificative în înțelegerea colaborării dintre stat și organizațiile neguvernamentale (ONG-uri) în contextul securității, este limitată de mai multe aspecte importante. Una dintre principalele limite ale studiului meu a fost accesul limitat la sursele de date în limba indoneziană. Din cauza lipsei cunoștințelor despre limba indoneziană, am fost limitata la sursele disponibile în limba engleză, ceea ce a redus capacitatea mea de a accesa informații, discursuri ale oficialilor guvernamentali, declarații și perspective care ar fi putut fi disponibile exclusiv în limba indoneziana. Această limita are capacitatea de a reduce înțelegerea mea a contextului cultural și socio-politic specific al Indoneziei și poate influența negativ interpretarea și analiza datelor existente.

Un alt aspect restrictiv al studiului meu a fost lipsa timpului și a resurselor necesare pentru analizarea datelor. Analiza datelor, mai ales într-un context complex și interdisciplinar precum cel al studiilor de securitate, necesită timp și resurse considerabile pentru a fi realizată corespunzător. În plus, metodele de colectare și analizare a datelor pot fi, de asemenea, restricționate de disponibilitatea resurselor și timpul dedicat cercetării. În situația mea, aceste constrângeri ar putea afecta în mod negativ profunzimea și exactitatea analizei mele și ar putea duce la subestimarea sau supraestimarea unor aspecte ale

colaborării dintre stat și organizațiile neguvernamentale în cadrul securității. Utilizarea unui studiu de caz, cum ar fi cel din Indonezia, implică anumite constrângeri metodologice. Deși studiile de caz oferă o înțelegere detaliată a contextului specific și a dinamicilor locale, ele pot fi greu de generalizat la nivel global sau chiar la alte contexte similare. Acest lucru înseamnă că rezultatele și concluziile cercetării mele pot avea aplicabilitate limitată în alte contexte geografice sau culturale.

Perspectiva viitoare a cercetării în colaborarea dintre guvern și organizațiile non-guvernamentale (ONG-uri) în contextul securității poate fi extinsă și diversificată pentru a analiza mai profund complexitatea dinamicii acestei relații. Exista mai multe direcții posibile pentru viitoarele cercetări în acest domeniu. O abordare viitoare ar putea să se concentreze exclusiv pe ONG-urile cu orientare religioasă și modul în care acestea interacționează cu statul în cadrul securității. Această perspectivă ar putea analiza detaliat rolul și impactul ONG-urilor religioase în gestionarea și soluționarea problemelor de securitate, precum și felul în care cooperează sau concurează cu alte tipuri de organizații din același domeniu.

Cercetările ulterioare ar putea să se axeze de asemenea, pe un anumit sector al securității, cum ar fi siguranța alimentară, siguranța energetică sau siguranța cibernetică, pentru a aprofunda cunoștințele despre modul în care statul și ONG-urile colaborează sau concurează în această sferă specifică. De exemplu, un astfel de studiu ar putea explora cum ONG-urile colaborează cu statul pentru a gestiona amenințările cibernetice sau cum își fac simțit prezențele în promovarea siguranței alimentare.

Bibliografie

- ADJI, Hariawan, "The Role of Religious Institutions in Promoting Social Welfare in Indonesia". *Mozaik Humaniora*, vol. 21, nr. 2, 2021.
- ÁLVAREZ CUARTERO, Izaskun, "The Concept of Ethnicity and Ethnic Genealogy." *The Routledge Handbook to the History and Society of the Americas*, 2019.
- ANTLÖV, Hans, IBRAHIM, Rustam, VAN TUIJL, Peter, *NGO Governance and Accountability in Indonesia: Challenges in a Newly Democratizing Country*, Routledge, 2006.
- Asia & the Pacific Interfaith Youth Network, disponibil online la https://rfpasia.org/apiyn/.
- BEINLICH, Ann-Kristin, BRAUNGART, Clara, "Religious NGOs at the UN: A Quantitative Overview.", *Religious NGOs at the United Nations*, 2018.
- BEITTINGER-LEE, Verena, *(Un) Civil Society and Political Change in Indonesia. A Contested Arena*, Routledge, 2010.
- BERGER, Julia, "Religious Nongovernmental Organizations: An Exploratory Analysis.", *Voluntas: International Journal of Voluntary and Nonprofit Organizations*, vol.14, 2003.
- BODAKOWSKI, Michael. "Faith-Inspired Organizations and Global Development Policy: A Background Review 'Mapping' Social and Economic Development Work in Southeast Asia". *Berkley Center for Religion, Peace, and World Affairs*, 2010.
- BOOTH, Ken, *Theory of World Security*, Cambridge University Press, 2007.

- BUZAN, Barry, WAEVER, Ole, DE WILDE, Jaap, *Security: A New Framework for Analysis*, Lynne Rienner Publishers, 1997.
- Camera Reprezentanților a Republicii Indonezia, disponibil online la https://www.dpr.go.id/en/berita/index/category/bksap.
- CARTER, Bob, *Realism, and Racism: Concepts of Race in Sociological Research*, Routledge, 2002.
- Code of Conduct for the International Red Cross and Red Crescent Movement and Non-Governmental Organizations (NGOs) in Disaster Relief, disponibil online la https://www.ifrc.org/our-promise/do-good/code-conduct-movement-ngos.
- DAMAYANTI, Angel, YUNANTO, Sri, "From Evangelization to Worship Restrictions: The Changing Characteristics of Threat Perception between Muslims and Christians in Indonesia", *Islam and Christian–Muslim Relations*, vol. 33, nr. 4, 2022.
- Doi Inthanon, disponibil online la https://www.thainationalparks.com/doi-inthanon-national-park.
- DRAKELEY, Steven, *The History of Indonesia*, Greenwood Publishing Group, 2005.
- EDWARDS, Michael, *Civil Society*, John Wiley and Sons, 2013.
- ERIKSEN, Thomas Hylland, "The Epistemological Status of the Concept of Ethnicity.", *Anthropological Notebooks*, vol.25, nr.1, 2019.
- ERRINGTON, James Joseph, *Other Indonesians: Nationalism in an Unnative Language*, Oxford University Press, 2022.

- European Institute for Gender Equality, Non-governmental organizations (NGOs), disponibil online la https://eige.europa.eu/publications-resources/thesaurus/terms/1087?language_content_entity=en.
- FERRIS, Elizabeth, "Faith-based and secular humanitarian organizations". *International Review of the Red Cross*, vol. 87, nr. 858, 2005.
- FUAD, Muhammad, „Civil Society in Indonesia: The Potential and Limits of Muhammadiyah", *Journal of Social Issues in Southeast Asia*, vol.17, 2002.
- GOMBRICH, *Theravada Buddhism: A Social History from Ancient Benares to Modern Colombo*, Routledge, 2009.
- HARTNELL,CAROLINE, *PHILANTHROPY IN INDONESIA. A working paper.*, Philanthropy for Social Justice and Peace, 2020.
- HASUDUNGAN, Anju Nofarof., "Muslim and Christian relations in the field of education after The Ambon-Maluku conflict (The Biggest Religious Conflict in Indonesia)". *Journal of Education, Society & Multiculturalism*, vol. 1, nr. 3, 2021.
- HÉLIOT, YingFei, "Religious Identity in the Workplace: A Systematic Review, Research Agenda, and Practical Implications." *Human Resource Management*, vol.59, nr.2, 2020.
- JATMIKA, Muhammad Indrawan, ANGGRAHENI, Palupi. "Civil Society's Role in Indonesia's Humanitarian Diplomacy: Study of Indonesian Religious Organizations' Humanitarian Aid in the Crisis in Myanmar's Rakhine State Region". *Jurnal Pemikiran Politik Islam*, vol. 4, nr. 2, 2021.
- KALDOR, Mary, *Human Security*, Polity, 2007.

- KEANE, John, *Civil Society: Old Images, New Visions*, Stanford University Press, 1998.
- KELLEY, Judith G., *Ethnic Politics in Europe: The Power of Norms and Incentives*, Princeton University Press, 2004.
- KERSTEN, Carool, *A History of Islam in Indonesia. Unity in diversity*, Edinburgh University Press, 2017.
- KUNTZ, Yelena Vladimirovna, GOLUBOVSKIY, Vladimir Yurjevich, "The Legal Nature of Ethnic and Religious Conflicts", *Indian Journal of Science and Technology*, vol.8, nr.10, 2015.
- KYMLICKA, Will, BANTING, Keith, *Multiculturalism and the Welfare State: Recognition and Redistribution in Contemporary Democracies*, Oxford University Press, 2007.
- LATIEF, Hilman, *Philanthropy in the Muslim World*, Monograph Book, 2023.
- LIEBKIND, Karmela, „The Identity of a Minority", *Journal of Multilingual and Multicultural Development*, vol.10, nr.1, 1989.
- LUTTIKHUI, Bart, și VAN DER MEER, Arnout HC. ,"1913 in Indonesian history: Demanding equality, changing mentality", *TRaNS: Trans-Regional and-National Studies of Southeast Asia*, vol. 8, nr. 2, 2020.
- MAMPU – The Australia-Indonesia Partnership for Gender Equality and Women's Empowerment, disponibil online la http://mampu.bappenas.go.id/en/category/knowledge/research/page/2/.
- MARX, Anthony W., "The Nation-State and Its Exclusions." *Political Science Quarterly*, vol. 117, nr. 1, 2002.

- MIETZNER, Marcus. "Sources of resistance to democratic decline: Indonesian civil society and its trials". *Democratization*, 2020.
- Ministry of Environment and Forestry of Indonesia, The State of Indonesia's forests(2020), disponibil online la https://indonesianembassy.de/wp-content/uploads/2020/12/Lowres2-SOFO-2020-B5_ENG-12.24.2_compressed.pdf.
- MUBARAK, Hafiz, "The Technological Revolution and the Dynamics of Islamic Da'wah.", *At-Tajdid: Jurnal Pendidikan dan Pemikiran Islam*, vol.6, nr.1, 2022.
- Muhammadiyah, disponibil online la https://muhammadiyah.or.id/.
- NWANKWO, Beloveth Odochi, "Rhethorics and Realities of Managing Ethno-Religious Conflicts: The Nigerian Experience.", *American Journal of Educational Research*, vol. 3, 2015.
- NYMAN, Mikaela, „Democratising Indonesia: The Challenges of Civil Society in the Era of Reformasi", *Südostasien aktuell: journal of current Southeast Asian affairs*, vol.26, nr.6, 2007.
- PEARSON, D., *The Politics of Ethnicity in Settler Societies: States of Unease*, Palgrave Macmillan, 2001.
- PHINNEY, J.S., "The Multigroup Ethnic Identity Measure: A New Scale for Use with Diverse Groups." *Journal of Adolescent Research*, vol.7, nr.2, 1992.
- RAUSTIALA, Kal, "States, NGOs, and International Environmental Institutions." *International Studies Quarterly*, vol.41, nr.4, 1997.
- RICKLEFS, Merle Calvin, *O istorie a Indoneziei moderne începând cu c. 1200*, MacMillan, Londra, 1993.

- RISTANTI, D.N., "Interreligious Violent Conflict Resolution: Discoursing Communal Violence between Christians and Moslems in Poso City, Indonesia", *Hasanuddin Journal of Strategic and International Studies (HJSIS)*, vol. 1, 2022.
- RIZZO, Roberto, Buddhism *in Indonesia: A Study of Multiple Revivals*. Taylor & Francis, 2024.
- ROEDER, Philip G., *Where Nation-States Come From: Institutional Change in the Age of Nationalism*, Princeton: Princeton University Press, 2007.
- S., Sufri, F., Dwirahmadi, și Phung, D, "Enhancing community engagement in disaster early warning system in Aceh, Indonesia: opportunities and challenges", *Nat Hazards*, vol. 103, 2020.
- SAKAI, Minako, "Building a partnership for social service delivery in Indonesia: state and faith-based organisations", *Australian Journal of Social Issues*, vol. 47, nr. 3, 2012.
- SAQIB, Amin, „Diversity, Tourism, and Economic Development: A Global Perspective", *Tourism Analysis*, vol.25, nr.1, 2020.
- SCHILBRACK, Kevin, *The Concept of Religion*, The Stanford Encyclopedia of Philosophy, 2022.
- SHEIKHI, Rahim Ali, SEYEDIN, Hesam, QANIZADEH, Ghader, și JAHANGIRI, Katayoun, "Role of Religious Institutions in Disaster Risk Management: A Systematic Review". *Disaster Medicine and Public Health Preparedness*, 2020.
- SHOKHEH, Mukhamad, EBRAHIMI, Mansoureh, YUSOFF, Kamaruzaman. "The Role of Indonesian and Egyptians' NGOs in Democratization", *Geopolitics Quarterly*, Vol.17, Nr. 4, 2022.

- SMITH, C. Q., și WILLIAMS, S. G., "Why Indonesia Adopted 'Quiet Diplomacy' over R2P in the Rohingya Crisis: The Roles of Islamic Humanitarianism, Civil–Military Relations, and ASEAN", *Global Responsibility to Protect*, vol. 13, nr. 2.
- Statista, Breakdown of Indonesian population who live in provinces where the majority of the population is not Muslim in 2010, by religion, accesat la 20.02.2024, disponibil online la https://www.statista.com/statistics/1260420/indonesia-population-breakdown-of-provinces-with-least-muslims-by-religion/.
- Statista, Share of population Indonesia 2022 by religion, accesat la 20.02.2024, disponibil online la https://www.statista.com/statistics/1113891/indonesia-share-of-population-by-religion/.
- TANESAB, Janiscus Pieter, "Institutional Effectiveness and Inclusions: Public Perceptions on Indonesia's Disaster Management Authorities". *International Journal of Disaster Management*, vol. 3, nr. 2, 2020.
- TEEGEN, Hildy, JONATHAN, P. Doh, VACHANI, Sushil, "The Importance of Nongovernmental Organizations (NGOs) in Global Governance and Value Creation: An International Business Research Agenda", *Journal of International Business Studies*, vol.35, 2004.
- The ordination of 500 Indonesian ordinands at Borobudur-Indonesia, disponibil online la https://en.dhammakaya.net/the-ordination-of-500-indonesian-ordinands-at-borobudur-indonesia/.
- The World Factbook, Indonesia, disponibil online la https://www.cia.gov/the-world-factbook/countries/indonesia/#geography.

- THORNBERRY, Patrick, *International Law and the Rights of Minorities*, Clarendon Press, 1993.
- UNDRR. "Does Community Managed Risk Reduction Work? Experiences with the Eruption of Mount Merapi in Indonesia", disponibil online la https://www.unisdr.org/files/17341_17341cmdrrbeforeanddduringtheeruptio.pdf.
- United Nations Development Programme, disponibil online la: https://www.undp.org/.
- United Nations, UN, and Civil Society, disponibil online la https://www.un.org/en/get-involved/un-and-civil-society.
- VAN DER MEER, Arnaout, *Performing Power: Cultural Hegemony, Identity, and Resistance in Colonial Indonesia*, Cornell University Press, 2020.
- VEJAI, Balasubramaniam, "Ethnic Politics and Multicultural Societies." *International Studies Review*, vol.12, nr.1, 2010.
- Wat Suan Mokkh International Dharma Hermitage, disponibil online la https://www.suanmokkh-idh.org/.
- WIBISONO, Susilo, LOUIS, Winnifred R., JETTEN, Jolanda, "A Multidimensional Analysis of Religious Extremism." *Frontiers in Psychology*, vol.10, 2019.
- WIMMER, Andreas, SCHILLER, Nina Glick, "Methodological Nationalism and Beyond: Nation–State Building, Migration and the Social Sciences." *Global Networks*, vol.2, nr.4, 2002.
- WINTERS, Dennis A., "The first Buddhist monasteries." *The Tibet Journal*, vol.13, nr.2, 1988.
- WIRTH, Louis, "The Problem of Minority Groups", *American Sociological Review*, vol.10, nr.4, 1945.

- YAZID, Sylvia, și PAKPAHAN, Aknolt K. "Democratization in Indonesia: Strong State and Vibrant Civil Society". *Asian Affairs: An American Review*, vol.47, nr.2, 2022.
- YILDIRIM, Kemal, *Ethnic and Religious Conflicts in India between Muslims and Hindus: Ethnic and Religious Conflicts*, Lambert Academic Publishing, 2016.