INTELLIGENCE ŞI CULTURA DE SECURITATE

CONFERINȚA ȘTIINȚIFICĂ STUDENȚEASCĂ

PROCEEDINGS

VOLUMUL 2
2023

Editura Academiei Naţionale de Informaţii „Mihai Viteazul”

INTELLIGENCE
ȘI CULTURA DE SECURITATE

nr. 2 – 2023

– Conferința Științifică Studențească –

Editura Academiei Naţionale de Informaţii „Mihai Viteazul”

Bucureşti, 2023

COLECTIVUL DE REDACŢÍE
Redactare şi tehnoredactare: Lucian COROI
Coperta: Lucian COROI

Apărut: decembrie 2023

	Editura Academiei Naţionale de Informaţii „Mihai Viteazul”
	© ANIMV
	Bucureşti, 2023
	Telefon: 0377720.000/1158
	Fax: 0377721.134; 0377721.125
	ISSN 2972 – 1350 ISSN-L 2971 – 8139

CUPRINS

STRATEGIA CÂȘTIGĂTOARE A ARMATEI CAUCAZIENE PENTRU CUCERIREA CETĂȚII ERZURUM (FEBRUARIE 1916)

Bogdan MORAR[*]

Abstract:

In the summer of 1914, the two great military-political camps - the West and the Central Powers – unleashed the First World War. In early November 1914, the Ottoman Empire chose to side with the Central Powers. This led to the opening of a secondary front in the Caucasus where Turkish troops were to clash with Russian troops. The Battle of Sarikamis (22 December 1914-17 January 1915) ended in a great Russian victory, but both sides remained on the sidelines unprepared to strike the decisive blow.

In 1915 the allies in Anatolia, notably Britain and France but without Russian participation, attempted to defeat Turkey by attacking the Dardanelles. The attack failed because the Ottomans concentrated significant troops near Constantinople. These troops were able to be withdrawn and redeployed after the Anglo-French withdrawal from the Turkish Straits. Intelligence warned Russia that the bulk of the Turkish troops were about to leave for the Caucasus. For this reason, the commander of the Caucasian Army, N.N. Yudenich was very anxious because he assumed that a resistance against them was very difficult. So he implemented a very bold plan. This article presents this plan and its results. To write the article I used written testimonies found in the RGVIA – Российский Государственный Военно-Исторический Архив (Russian State Historical-Military Archive) archive, including notes and positions sent by N.N. Yudenich to his superior, the viceroy of the Caucasus Nicholas Nikolaevich.

The conclusions of the article highlight the winning strategy devised by N.N. Yudenich argues the author's personal opinion that this strategy (which included the conquest of Erzurum) was one of the greatest military victories of Tsarist Russia in the First World War.

Keywords: *Caucasus, Russian Empire, Ottoman Empire, World War I, N.N. Yudenich.*

Abrevieri

RGVIA – Российский Государственный Военно-Исторический Архив (Arhiva Istorico-Militară de Stat a Rusiei).

[*] Bogdan Morar, PhD student of the Doctoral School of International Relations and Security Studies, Faculty of History, Babeș-Bolyai University of Cluj-Napoca, e-mail: bmorar2012@gmail.com

Termeni

Antanta sau **Tripla Înțelegere** – este o alianță încheiată între francezi, britanici și ruși, între anii 1904 și 1907, prin care cele trei țări au creat un bloc politico-militar îndreptat împotriva Triplei Alianţe;

Drujină – echipă (detașament), în textul prezent unitate de miliție;

Sotnie – unitate de cavalerie rusească (căzăcească) formată din 100 de călăreți.

Tripla Alianță – încheiată între Germania, Austro-Ungaria și Italia, la 20 mai 1882, pe o perioadă de 5 ani. Scopul acestei alianţe a fost izolarea diplomatică și militară a Franței.

1. Introducere

La începutul lunii august 1914, armatele Antantei şi Triplei Alianţe intrau în Primul Război Mondial. Principalele acţiuni militare au avut loc pe fronturile din vestul (unde s-au înfruntat anglo-franco-belgienii cu germanii) şi estul Europei (unde s-au înfruntat germano-austro-ungarii cu ruşii) şi în Balcani (unde s-au înfruntat austro-ungarii cu sârbii). La sfârşitul lunii octombrie 1914, Imperiul Otoman a ales să intre în război de partea Triplei Alianţe (semnase deja, în luna august, un tratat de alianţă cu Germania). Drept urmare, Turcia a atacat porturile ruseşti de la Marea Neagră (Sevastopol, Odessa, Feodosia, Novorosiisk), mobilizând armata pentru a înainta prin Caucaz şi pentru a-i elimina pe britanici din Egipt (ocupat de englezi din 1882). S-au deschis astfel, o serie de fronturi suplimentare: unul în Caucaz, unde otomanii, consiliaţi de germani, trebuiau să îi înfrunte pe ruşi şi alte două, unul în Mesopotamia (actualmente Irak) şi unul de-a lungul canalului Suez, unde turcii urmau să se înfrunte cu britanicii.

Primele lupte, de pe frontul din Caucaz, au avut loc la începutul lunii noiembrie 1914. Acest front a fost neglijat, în lucrările care au tratat istoria Primului Război Mondial. În opinia lui B.A. Șteifon, acest lucru s-a datorat interesului mult prea mare arătat de unii istorici, pentru fronturile deschise în vestul Europei sau în partea europeană a Rusiei. Aceiași istorici „au subestimat rolul acestui front, considerând că războiul a fost purtat în Caucaz cu tehnici învechite şi împotriva unei armate slabe (cu referire la cea otomană, n.a.)” (B.A. Șteifon, 1929, p. 49). Însă, lucrurile nu au stat deloc așa. Din punctul meu de vedere, faptele de arme ale armatei ruse din Caucaz pot rivaliza oricând, cu realizările celorlalte armate aliate din Antantă. Luptele aprige dintre ruși și turci au fost deosebit de importante, pentru avansul britanicilor în Imperiul Otoman și, în final, pentru victoria Antantei în război.

Conform istoricului I.I. Rostunov, la intrarea în război împotriva Turciei, trupele ţariste, din Caucaz, au însumat aproape 9 divizii de infanterie (care aveau în compunere 143 de batalioane), 211 sotnii şi peste 600 de tunuri (I.I. Rostunov, vol. I, 1975, p. 198). Acelaşi istoric a menţionat că, planul rusesc, în cazul unui război cu Imperiul Otoman, prevedea trei opţiuni: 1) un război doar între Rusia şi Turcia, 2) Turcia, încă de la începutul războiului, acţionează împreună cu o coaliţie ostilă Rusiei, 3) la începutul războiului, Turcia rămâne neutră şi apoi atacă Rusia în Caucaz. Principala sarcină atribuită armatei caucaziene a fost apărarea oraşelor Baku (principalul centru al industriei extractive a petrolului din Imperiul Ţarist) şi Tiflis (acum Tbilisi în Georgia, atunci capitala viceregatului caucazian). Încercarea otomanilor de a încercui armata ţaristă din Caucaz s-a transformat în marea înfrângere de la Sarikamiş (22 decembrie 1914 – 15 ianuarie 1915), în care armata a 3-a turcă a înregistrat aproape 60.000 de morţi, răniţi şi dispăruţi. Victoria ruşilor în această bătălie (generalul N.N. Iudenici având un rol important, fiind la comanda unei mari unităţi) a zdruncinat serios moralul otomanilor. La fel au stat lucrurile şi în anul 1915. Cu toate întăririle primite, inclusiv prin venirea unor consilieri militari germani, otomanii nu au putut obţine un succes în timpul luptelor de la Alaşkert (iulie 1915). În fapt, contraofensiva rusă, din luna august 1915, era gata să ducă la o încercuire a trupelor otomane. În acest timp, încercările Antantei de a forţa înfrângerea Turciei, odată cu bombardarea şi debarcarea din zona strâmtorii Dardanele (Gallipoli), au dat greş. Pornită în luna aprilie 1915, operaţiunea Gallipoli a fost sistată la sfârşitul aceluiaşi an. Respingerea trupelor anglo-franceze din zona strâmtorilor a fost considerată o mare victorie de către otomani. Aceştia şi-au îndreptat privirea, tot mai insistent, spre frontul caucazian, unde urmau să concentreze trupe tot mai numeroase. Istoricul David Martyrosian a confirmat şi el, că otomanii urmau să aducă din zona strâmtorilor tot mai multe trupe, pe măsură ce anglo-francezii se retrăgeau. Ca atare, pentru armata ţaristă din Caucaz, anul 1916 nu se anunţa a fi foarte bun (David Martyrosian, on-line, material consultat la data de 22 mai 2023). Stavka (Înaltul Comandament militar rus) era destul de bine informată şi a sesizat că, o serie de unităţi otomane au început să fie mutate de la Constantinopol pe frontul caucazian, încă din noiembrie 1915. Situaţia a devenit şi mai complicată după ce, în Mesopotamia, un atac englez înspre Bagdad fusese stopat la Kut el-Amara, iar britanicii, fiind înconjuraţi de armata turcă, nu aveau nici o şansă reală de a înainta sau de a se retrage. În faţa acestor noi provocări, conducerea armatei caucaziene a luat hotărârea de a ataca, imediat, armata a 3-a turcă din faţa sa, cu scopul de a-i provoca o

înfrângere majoră, pentru ca aceasta să nu mai poată beneficia de ajutorul trupelor ce veneau dinspre capitala Imperiului Otoman. Planul, gândit de generalul N.N. Iudenici, care asigura comanda directă a trupelor țariste de pe frontul caucazian, prevedea o acțiune inițială cu al doilea corp din Turkestan, în direcția orașului Olti (Oltu). Această ofensivă a fost planificată cu două zile înainte de ofensiva principală, care trebuia dată de corpul I armată caucazian, în direcția Erzurum. În același timp, unitățile grupului de șoc (forțe din rezerva armatei și din cele două corpuri, II Turkestan și I caucazian) vor lovi la joncțiunea acestor două corpuri, unde turcii nu se așteptau la apariția marilor forțe rusești, în condițiile unui teren inaccesibil. „Prin urmare, la consiliul militar ținut la Tiflis la 4/17 noiembrie 1915, generalul N.N. Iudenici a propus abandonarea acțiunilor defensive și începerea unei operațiuni ofensive în direcția Erzurum în vederea distrugerii armatei a 3-a otomane până la sosirea unor întăriri" (B.A. Șteifon, 1929, p. 50). La 12/25 ianuarie 1916, același general Iudenici îi cerea acordul Marelui Duce Nicolai Nicolaevici, viceregele Caucazului, pentru a începe asaltul cetății Erzurum (vezi Appendix 1-I). Viceregele a ezitat inițial să-și dea acordul (vezi Appendix 1-II). Iudenici nu a renunțat la cererea sa și a insistat pentru declanșarea operațiunii Erzurum. Generalul rus avea să primească un acord parțial din partea viceregelui, care i-a impus să sisteze atacul în cazul unei rezistențe încăpățânate a turcilor. În esență, planul rusesc de atac era destul de simplu. Așa cum aminteau istoricii William David Allen și Paul Muratoff, Iudenici a propus, ca o parte a trupelor ruse să treacă printr-un sector nedefinit al liniei turcești, nedefinit pentru că era considerat imposibil de trecut, din cauza dificultății naturale a terenului (munți înalți cu creste abrupte) și a iernii feroce. Acest sector era creasta Kargabazar, unde urmau să ajungă soldații diviziei a 4-a de pușcași caucazieni, comandată de generalul Vorobiev. În ajutorul lor, o altă grupare aflată sub comanda generalului Voloșinov-Petricenko a fost trimisă pe terenul, încă mai dificil, al crestei Kandil-dağ. Cele două grupări urmau să faciliteze înaintarea corpului II armată, din Turkestan, condus de generalul Prjevalski, care urma să treacă prin defileul Gürcü-bogaz, înainte de a pătrunde în câmpia din fața cetății Erzurum (William David Allen, Paul Muratoff, 2010, p. 355). Atacul propus de generalul Iudenici a fost privit, încă de la început, cu reticențe chiar de unii comandanți de mari unități. Accesul pe creasta Kargabazar era limitat, din cauza temperaturilor foarte scăzute, ridicarea și amplasarea tunurilor trebuind să fie făcute în nămeți, care ajungeau pe alocuri la 3 metri. Cu toate acestea, Iudenici a trecut peste obiecțiile tuturor și a cerut respectarea întocmai a planului de luptă.

2. Materiale şi metode folosite

Pentru realizarea prezentului studiu am folosit, în primul rând, materiale inedite. Totodată, din punct de vedere istoric, am considerat că, obiectivitatea este cea mai importantă. Din acest motiv, am ales să redau câteva pasaje din materialele de arhivă identificate, care sper, că vor ajuta la înţelegerea demersului meu.

3. Dezbaterea problemei în lucrările de până acum

Din păcate, lucrările de specialitate care au început să apară după terminarea Primului Război Mondial au ocolit evenimentele, care au avut loc între anii 1914 şi 1917, pe frontul caucazian. Marile lucrări de istorie militară s-au concentrat aproape exclusiv pe fronturile deschise în vestul Europei, în Rusia europeană şi apoi, în nordul Italiei. Practic, pentru o perioadă de timp, istoricii nu au avut acces la informaţii detaliate despre ce lupte sau acţiuni au avut loc, pe parcursul primei conflagraţii mondiale, în teatrul de război caucazian. Primii care au publicat lucrări, care au acoperit şi frontul turco-rus din Caucaz au fost: Maurice Larcher, La guerre turque dans la guerre mondiale, (Etienne Chiron-Berger-Levrault ed., Paris, 1926); Evgheni V. Maslovski, Мировая война на Кавказском фронте 1914-1917 г., Стратегический очерк (Războiul mondial pe frontul caucazian 1914-1917, Schiţă strategică, Editura Renaşterea, Paris, 1933) şi Nikolai G. Korsun, Эрзерумская операция (Operaţia Erzurum, Editura Comisariatului Apărării al U.R.S.S., Moscova, 1938). Primul autor s-a bazat, exclusiv, pe informaţii şi mărturii ale unor comandanţi otomani care au luptat în Caucaz. Celelalte două sunt lucrări ample, bine realizate ale unor ofiţeri ruși, de pe frontul caucazian, care au avut acces la multiple informaţii, o parte dintre acestea fiind prezentate în lucrările lor. Ulterior, a mai apărut cartea lui Nikolai G. Korsun, Первая мировая война на Кавказском фронте. Оперативно-стратегический очерк (Primul război mondial pe frontul caucazian 1914-1917, Schiţă strategică şi operaţională, Editura Militară a U.R.S.S., 1946), dar apoi interesul pentru evenimentele din Caucaz, din perioada 1914-1917, a scăzut. În ultima perioadă au apărut o serie de lucrări, care au înfăţişat amploarea acţiunilor militare care au avut loc în Primul Război Mondial, pe frontul caucazian: William David Allen, Paul Muratoff, Caucasian Battlefields, a history of the wars on turco-caucasian border, 1828-1921, Cambridge University Press, New York, 2010 (după ediţia din 1953); A.A. Kersnovski, История Русской армии (Istoria armatei ruse), vol. IV, Editura Golos, Moscova, 1994; Edward J. Erickson, Ordered

to die, a history of the Ottoman Army in the First World War, Greenwood Publishing, Westport, 2001; Roger Ford, Eden To Armageddon: World War I in The Middle East, Pegasus Books Llc., 2010.

4. Cuprins

La mijlocul lunii ianuarie 1916, chiar înainte de începerea operațiunii Erzurum, „armata rusă din Caucaz era formată din 126,5 batalioane de infanterie, 372 tunuri, 493 mitraliere, 208 sotnii de cavalerie, 21 companii de ingineri și 52 de drujini (detașamente) de miliție. Totalul trupelor era de 203.741 soldați și ofițeri (ofițeri – 4610, infanterie – 171.053, cavalerie – 28.078)" (RGVIA, fond 2003, opis 1, delo 544, p. 689, în Forțele armate ruse în Primul Război Mondial, vol. II, 2014, p. 205). În fața trupelor ruse, era desfășurată armata a 3-a otomană, care era condusă de Mahmut Kâmil Pașa, avându-l pe colonelul german Felix Guse ca șef de stat major. Cu toate că, armata turcă avea în compunere forțe impresionante (118 batalioane de infanterie, 180 de tunuri, 77 de mitraliere și 41 de escadroane de cavalerie, adică un total 101.294 soldați și ofițeri conform datelor furnizate de autorii lucrării Forțele armate ruse în Primul Război Mondial, vol. II, 2014, p. 206), în fapt, doar o parte a acesteia era aptă de luptă (este vorba de 50.539 soldați și ofițeri). Acest lucru s-a datorat bolilor, care au afectat tot mai serios trupele otomane din zona Erzurum și dezertărilor, care au sporit ca număr. Din acest motiv, pentru lansarea operațiunii Erzurum, generalul Iudenici a reușit să concentreze, la 1/14 ianuarie 1916, forțe care au depășit armata a 3-a otomană de peste două ori în infanterie, de trei ori în artileria de câmp și de cinci ori în cavalerie, adică aproape 76 de mii de infanteriști, aproximativ 10 mii de călăreți, 213 tunuri și 236 mitraliere (Forțele armate ruse în Primul Război Mondial, vol. II. 2014, p. 206). Pe lângă această superioritate în soldați, trebuie să menționăm metodele ingenioase folosite de generalul Iudenici, pentru a pregăti operațiunea Erzurum (vezi Appendix 1-III și 1-IV). Unii istorici au sugerat, că această pregătire ar trebui introdusă într-un manual de tactici militare.

Turcii nu se așteptau la nici un eveniment deosebit pe frontul caucazian. Știau că, pentru ruși, urmau Sărbătorile sfârșitului de an 1915. Ca atare, au considerat că frontul va rămâne liniștit în aceea perioadă.

La începutul anului 1916, armata caucaziană comandată de N.N. Iudenici era dispusă astfel: în zona orașului Olti (Oltu) corpul II armată din Turkestan, sub conducerea generalului Prjevalski, în zona orașului Sarikamiș corpul I armată caucazian, sub conducerea generalului Kalitin, iar în zona Erivan (Armenia) corpul IV armată caucazian, sub conducerea

generalului de Witt. Alte detaşamente ale armatei caucaziene acţionau în Azerbaidjanul persan şi în zona Batumi, de lângă Marea Neagră.

Operaţiunea Erzurum a constat din patru etape: 1) bătălia de la Köprüköy (28 decembrie 1915/10 ianuarie 1916 – 12/25 ianuarie, 1916); 2) pregătirea pentru asaltul asupra cetăţii Erzurum; 3) asaltul Erzerumului (30 ianuarie/10 februarie – 3/16 februarie 1916); 4) urmărirea turcilor. În zona cetăţii Erzurum „întreaga poziţie fortificată de turci avea o lungime de până la 40 km. Cel mai slab punct al fortificaţiilor a fost porţiunea de 10 km dintre forturile Tafta şi Çoban-dede; în faţa acesteia se afla creasta accidentată Kargabazar, neocupată de turci. În total, pentru asalt ruşii au pregătit 78 de batalioane de infanterie, 12 drujini, 180 de tunuri (din care 12 arme de asediu aduse din cetatea Kars), 54 ½ sotnii, 4 companii de săpători" (N.G. Korsun, 1946, p. 53, vezi şi Appendix 1-V). Apărarea cetăţii Erzurum a necesitat prezenţa unei garnizoane formată din mulţi soldaţi. Cu toate acestea, „comandamentul turc credea că forţele în retragere ale corpurilor IX, X şi XI ale armatei a 3-a erau suficiente pentru a apăra Erzurum" (N.G. Korsun, 1946, p. 53), mai ales că, datorită dotării cu un număr mare de tunuri Krupp, cetatea Erzurum era socotită, în aceea vreme, de necucerit.

Debutul operaţiunii Erzurum s-a produs prin atacul asupra localităţii turce Köprüköy unde, la 5/18 ianuarie 1916, divizia 39 infanterie rusă a înfrânt trupele otomane, care apărau acel oraş. Cu toate că, acţiunile ofensive ruseşti arătau că ceva se întâmplă pe front, Înaltul Comandament otoman de la Constantinopol, care sărbătorea încă respingerea debarcării anglo-franceze, din zona strâmtorilor, a catalogat aceste acţiuni drept „atacuri de ochii lumii" (Birinci Dünya Harbinde Türk Harbi Kafkas Cephesi, vol. II, 1993, p. 18). Ministrul turc de război, Enver Paşa, a adăugat că, armata rusă din Caucaz nu a primit întăriri de pe frontul european şi nu se poate presupune că le va primi. Greşind şi mai mult, el a ordonat armatei a 3-a turce să trimită forţe în Irak şi Iran pentru a se bate cu britanicii. Acest lucru arată, cât de departe de realitate era comandamentul otoman. Încă de la începutul operaţiunii Erzurum, turcii au fost păcăliţi de atacurile surpriză date de ruşi. „Aceştia au considerat că acţiunile încăpăţânate ale trupelor ruse în valea Passin erau o dovada că acolo este dată lovitura principală, iar pentru respingerea acesteia şi-au concentrat în acest sector toate rezervele" (Forţele armate ruse în Primul Război Mondial, vol. II, 2014, p. 207). După ce a observat că turcii sunt păcăliţi de atacul din valea Passin, generalul Iudenici a ordonat corpului I caucazian, la 1/14 ianuarie 1916, să atace decisiv, pe direcţiile Olti şi Erzurum. Luptele au fost deosebit de

grele, soldații ambelor tabere trebuind să înfrunte furtunile de zăpadă și temperaturile scăzute (vezi Appendix I-VI).

Comandantul armatei a 3-a otomane, Mahmud Kâmil Paşa, care fusese plecat la Constantinopol, s-a întors, în sfârşit, la 29 ianuarie 1916. El a observant că, Erzurumul era sub amenințarea directă, astfel că, și-a dispus trupele în poziții defensive mai avantajoase. După ce a primit o serie de întăriri a reuşit să stabilizeze frontul. Nu se aştepta la un atac asupra Erzurumului și a fost surprins când acesta a început, pe 11 februarie 1916. Conform lui A.A. Kernovski, în acea zi, conform ordinelor primite de la generalul N.N. Iudenici, corpul II armată din Turkestan (32 de batalioane, 75 de tunuri și 21 de sotnii), de pe aripa dreaptă a frontului rus, a trebuit să ocolească poziția puternică Deve-Boyun. În centru, divizia a 4-a de puşcaşi caucazieni a ţintit spre platoul Kargabazar. Pe flancul stâng, corpul I armată caucazian (42 de batalioane, 12 drujini de miliție, 128 de tunuri și 28 de sotnii) a primit onoarea unui atac frontal asupra poziției Deve-boyun și platoului Palanteken. Divizia 66 infanterie a format rezerva. Pentru acțiunea împotriva fortului Çoban-dede, unul din punctele cheie a liniei de rezistență a otomanilor, „a fost trimisă divizia a 39-a, cea mai puternică ca număr și curajoasă în spirit" (B.A. Șteifon, 1929, p. 61). În total, pentru cucerirea cetății Erzurum, generalul Iudenici a trimis la atac forțe care au însumat 100 ½ batalioane de infanterie, 12 drujini de miliție, 237 de tunuri și 86 de sotnii. Trebuie menționat că, onoarea de a începe atacul a fost acordată unui batalion de sub comanda colonelului armean Pirumov (Pirumyan). Unitatea acestuia a atacat fortul Dalan-göz unde, „după o luptă surdă, o companie rusă a escaladat zidul și a pătruns în fort. Restul trupelor au urmat-o. Au fost câteva ore de luptă la baionetă în interiorul fortului, dar în zorii zilei de 12 februarie, Dalan-göz a intrat în mâinile rușilor"(W.E.D. Allen, Paul Muratoff, 2010, p. 358). Turcii, disperați, au încercat să recucerească fortul, dar toate încercările lor au fost respinse (vezi Appendix 1-VII). La 14 februarie, rușii au capturat fortul Tafta (luând 1500 de prizonieri și 20 de tunuri) și au deschis accesul spre câmpia Erzurum din nord. Cea de-a 4-a divizie de puşcaşi caucazieni, care a străpuns frontul turcilor la nord de fortul Çoban-Dede, a coborât, de asemenea, înspre câmpia Erzurum. Turcii au început să înțeleagă planul rușilor, de abia după patru zile. Acest lucru a întârziat un răspuns din partea lor și a pecetluit soarta cetății Erzurum. După ce, în 15 februarie 1916, cade și fortul Çoban-dede, „care a fost abandonat de turci după o rezistență serioasă" (W.E.D. Allen, Paul Muratoff, 2010, p. 362), întreaga linie de rezistență a otomanilor din fața Erzurumului s-a prăbuşit. În dimineața zilei următoare, trupele ruse

pătrund în oraş, care fusese părăsit în grabă de turci (vezi şi Appendix I-VIII). Veştile despre succesul de la Erzurum ajung aproape instantaneu la Tiflis, capitala Caucazului rusesc. Nicolai Nicolaevici, viceregele Caucazului, care iniţial nici nu a vrut să-l lase pe generalul N.N. Iudenici să pornească atacul, este impresionat de succes. Francis W. Halsey a notat într-o lucrare despre Primul Război Mondial:

<<Victoria lui Iudenici a fost atât de bruscă încât Marele Duce, ale cărui munci la sediul central fuseseră nepreţuite, nu a avut timp să vină şi să fie prezent la triumful final. A primit marea veste la palatul său din Tiflis, unde a fost aclamat cu entuziasm>> (Francis W. Halsey, vol. VIII, 1919, p. 144). Victoria contra turcilor era totală, cea mai importantă victorie a armatei ruse de pe toate fronturile Primului Război Mondial. Iar B.A. Şteifon a amintit că:

<<La trei zile după capturarea oraşului Erzurum generalul N.N. Iudenici a primit o telegramă din partea ţarului Nicolae al II-lea: Drept răsplată pentru marele curaj şi conducerea iscusită arătată de dumneavoastră în capturarea cetăţii Erzurum, vă ofer Ordinul Sf. Gheorghe, clasa a II-a. Guvernele Angliei şi Franţei, prin decoraţiile trimise generalului Iudenici, au subliniat importanţa capturării Erzurumului pentru victoria Antantei>> (B.A. Şteifon, 1929, p. 65).

Figura 1: Generalul Iudenici,comandantul armatei caucaziene în timpul asediului şi cuceririi fortăreţei Erzurum, fotografie publicată de periodicul «*Разведчик*» (*Cercetaşul*), nr. 1317 din 2/15 februarie 1916, p. 67.

5. Concluzii

Fără îndoială, că succesul de la Erzurum s-a datorat încăpățânării generalului N.N. Iudenici. Conform lui B.A. Șteifon, acesta era o persoană extrem de modestă, tăcută, care nu a avut nici un corespondent de război în jurul lui și nu i-a plăcut publicitatea. În schimb, s-a dedicat complet muncii sale, fiind un adevărat organizator (vezi și Appendix I-IX). În încheiere redau opinia istoricului scoțian John Buchan care a afirmat, că:

<<Cucerirea Erzerumului a fost unul dintre cele mai strălucite episoade strategice ale Primului Război Mondial. Iudenici adoptase un plan care presupunea o sincronizare atentă, în condițiile în care era aproape imposibil să se respecte un calendar [...] De asemenea, era un plan care punea la grea încercare devotamentul oamenilor săi. Să tragi tunuri peste vârfurile stâncoase înfundate de zăpadă, așa cum a făcut Prjevalsky înainte de a cuceri fortul Kara-göbek, a fost o ispravă care trebuie să se claseze pe o poziție ridicată printre realizările războiului purtat în munți>> (John Buchan, 1917, p. 96).

Appendix 1-I:

I. N.N. Iudenici a scris marelui Duce Nicolai Nicolaevici:

<<Cerând permisiunea Alteței Voastre Imperiale pentru a începe o operațiune ofensivă împotriva turcilor, raportez că această operațiune nu vizează nicio achiziție teritorială, ci urmărește doar o posibilă slăbire a armatei turce înainte de apropierea întăririlor de la Constantinopol. Această operațiune ar putea obține un rezultat mai mare decât s-ar putea aștepta, existând posibilitatea să cucerim cetatea Erzurum [...] Această cucerire va face inevitabilă distrugerea finală a întregii armate a 3-a otomane, din moment ce, slăbită de luptele recente, această armată va avea și sarcina de a apăra cetatea [...] Având în vedere acest lucru, am trecut la pregătirea operațiunilor împotriva Erzurumului, dar trebuie mai întâi să cer permisiunea Alteței Voastre Imperiale pentru a epuiza rezerva de muniții din cetatea Kars, în așteptarea sosirii proviziilor din Rusia europeană. Cât despre direcția atacului asupra cetății Erzurum, ținând cont de situația generală și de condițiile terenului, consider că este cel mai oportun să încep un atac decisiv simultan dinspre est – prin Deve-Boyun – și nord – până la trecătoarea Gürcü-bogaz, deoarece acest lucru îi va obliga pe turci să își întindă forțele lor la maximum; iar noi, după concentrarea tuturor forțelor [...] vom da o lovitură decisivă între forturile Çoban-dede și Tafta [...] Raportez cu cel mai mare devotament că eu împreună cu statul major luăm măsuri pentru pregătirea atentă și minuțioasă a planului pentru capturarea cetății Erzurum în cel mai scurt

timp posibil, ţinând cont că orice întârziere nu va face decât să complice asaltul, întrucât le va permite turcilor să-şi revină după înfrângerea suferită şi să beneficieze de întăriri. Generalul de infanterie Iudenici>> (RGVIA, fond 2100, opis 1, delo 590, pp. 5–6 reprodus în Forţele armate ruse în Primul Război Mondial, vol. II, 2014, pp. 641-642).

Appendix 1-II:

II. Răspunsul Marelui Duce a fost următorul:

<<Sunt destul de sigur că trupele care au dat dovadă de atâta vitejie (în bătăliile trecute, n.a.) [...] sunt capabile de cele mai înalte fapte eroice, dar sunt de acord cu tine că situaţia generală nu ne permite să trecem la asaltul Erzurumului fără o pregătire atentă şi având la îndemână toate mijloacele necesare pentru a face acest lucru. Pe lângă faptul că stăm prost cu muniţia, nu avem nici artileria adecvată pentru a lupta cu succes cu artileria grea turcească din forturi; iar bazele noastre de aprovizionare sunt îndepărtate. În faţa corpului al II-lea din Turkestan, judecând după rapoartele primite de la tine, turcii opun încă o rezistenţă serioasă [...] S-ar putea ca armata turcă să nu fie în măsură să reziste în teren, dar nu ştim de ce este capabilă pentru apărarea cetăţii, fiind susţinută de sute de tunuri. Având în vedere cele spuse, nu mă consider îndreptăţit să permit efectuarea acestei operaţiuni. Marele Duce Nicolai Romanov>> (A.V. Şişov, 2004, p. 235).

Appendix 1-III şi 1-IV:

III. Dintre măsurile propuse de generalul Iudenici, pentru desfăşurarea în bune condiţii a operaţiunii Erzurum, amintim:

<<Menţinerea în stare de funcţionare a şinelor de cale ferată de la Kars până la gara Sarikamiş şi a drumurilor. De la Kars la Merdenek şi apoi până la Olti din vara anului 1915 s-a dat în folosinţă o cale ferată cu ecartament îngust, vagoanele fiind trase de cai. Întrucât iarna din munţii din partea turcă a Armeniei era deosebit de grea, s-au format echipe speciale de deszăpezire pentru această perioadă. Acestea s-au luptat cu zăpada pentru a înlesni comunicaţiile armatei. Fiecare ocazie a fost folosită pentru a crea aspectul pregătirii trupelor caucaziene doar pentru iernare în munţi. Alte măsuri ordonate de generalul Iudenici au vizat: mutarea cartierului său general la Karaurgan, situat la doar 20 de kilometri de linia frontului pentru a fi în legătură permanentă cu trupele şi o grijă deosebită pentru asigurarea proviziilor necesare trupelor din prima linie (în acest sens s-au achiziţionat cămile din nordul Persiei). Totodată, liniile telegrafice au primit o protecţie sporită cu ajutorul

patrulelor de călăreţi cazaci şi a grănicerilor [...] Cerinţele pentru camuflajul militar au fost dure. Pentru ca observatorii inamici să nu poată detecta întăririle în marş, trecerile prin lanţurile muntoase din zona frontului au fost efectuate doar noaptea. Chiar şi fumatul în timpul mersului era interzis. O atenţie deosebită a fost acordată derutării inamicului pentru viitoarea ofensivă [...] Cu doar câteva zile înainte de începerea ofensivei, de la cartierul general al armatei ruse o telegramă urgentă necriptată a fost trimisă comandantului diviziei a 4-a de puşcaşi caucazieni [...] Totul a fost făcut în aşa fel încât conţinutul telegramei necriptate de o importanţă deosebită să devină cunoscut de foarte mulţi pe parcursul „circulației" acesteia>> (A.V. Şişov, 2014, pp. 227-228).

IV. B.A. Şteifon a scris că:

<<Nici una dintre armatele ţărilor care au luptat în Primul Război Mondial nu au dispus de un astfel de sistem original de comandă şi control al trupelor ca cel organizat de generalul Iudenici. Acesta, [...] fiind cu trupele mai tot timpul, a avut doar un aşa-numit sediu de teren compus din 4-5 ofiţeri ai Statului Major General şi din cei care asigurau comunicaţiile. Aceştia din urmă (datorită faptului că asigurau transmiterea rapidă a ordinelor către marile unităţi, n.a.) erau foarte importanţi pentru Iudenici şi au ajutat foarte mult la succesul operaţiei>> (B.A. Şteifon, 1929, pp. 51-52).

Appendix 1-V:

V. <<După ce a primit permisiunea pentru asalt, generalul N.N. Iudenici a adus din sectoarele secundare ale frontului tot ceea ce ar putea fi dus de acolo [...] Prin măsuri eroice, el a reuşit să ia din cetatea Kars artileria grea necesară asediului Erzurumului pe care a trimis-o pe flancul stâng al trupelor sale de atac. Toate rezervele care erau în spate, până şi brigăzile de miliţie, au fost atrase pe front>> (B.A. Şteifon, 1929, p. 61).

Appendix I-VI:

VI. La finalul primei etape a operaţiunii „pierderile trupelor ruseşti s-au ridicat la: ofiţeri uciși – 37, răniţi – 185; soldaţi uciși – 1332, răniţi – 7195. Armata otomană, conform unor date oficiale, a pierdut 22 de mii de soldaţi şi ofiţeri. Dintre aceştia, potrivit comunicărilor armatei caucaziene, 98 de ofiţeri şi 4753 de soldaţi au fost luaţi prizonieri" (Forţele armate ruse în Primul Război Mondial, vol. II, 2014, p. 209).

Appendix 1-VII:

VII. Istoricul A.V. Şişov a relatat că, infanteria turcă a plecat de opt ori la atac pentru a recupera fortul.

<<Ultimele două atacuri au fost respinse de ruşi cu baionetele, aceştia salvând ultimele cartuşe pentru a le folosi doar în cazuri extreme. Când a început al optulea atac, soldaţii ruşi din fort au primit ajutorul mult aşteptat: un soldat necunoscut pe un măgar a reuşit să livreze muniţie pentru puşti. Generalul Iudenici, după ce a aflat despre această ispravă, a ordonat să se găsească acel soldat pentru a fi recompensat, dar nimeni nu l-a putut găsi, spre mâhnirea comandantului>> (A.V. Şişov, 2004, p. 240).

Appendix I-VIII:

VIII. „La ora 7 dimineaţa, un regiment de cazaci din Terek a intrat în oraş, urmat de elemente ale regimentului 263 infanterie şi ale regimentului 5 de puşcaşi caucazieni. Turcii au fost alungaţi înapoi spre vest. Din cetate au fost luate 9 stindarde, 315 tunuri, stocuri mari de muniţie şi alimente, precum şi peste 8000 de prizonieri. Pierderile ruseşti pentru cucerirea Erzerumului: până la 950 ucişi, 7500 răniţi şi îngheţaţi" (N.G. Korsun, 1946, p. 54). În total, de la sfârşitul lunii ianuarie şi până la mijlocul lunii februarie 1916, ruşii au pierdut cca. 17.000 soldaţi morţi, răniţi sau îngheţaţi sau 10% din efective, în timp ce turcii au pierdut peste 60 % din totalul forţelor. A.A. Kernovski a menţionat că luptele din sectorul cetăţii Erzurum au durat până pe 9/22 februarie 1916. Astfel că, „pe lângă prizonierii şi trofeele capturate în timpul asaltului, ruşii au mai capturat alţi 80 de ofiţeri, 7500 de soldaţi şi 130 de tunuri în timpul urmăririi resturilor armatei a 3-a otomane" (A.A. Kernovski, 1994, p. 148).

Appendix I-IX:

IX. <<Informaţiile, pe care le obţinea de la prizonierii de război sau cu ajutorul avioanelor, i-au dat lui N.N. Iudenici o idee completă despre ce se întâmpla în prima linie a frontului. Acesta absorbea fără întrebări inutile toate informaţiile şi prin puterea talentului său le alegea pe cele mai importante. Toate aceste lucruri l-au ajutat să termine operaţiunea Erzurum cu o victorie răsunătoare>> (B.A. Şteifon, 1929, p. 53).

Bibliografie:

1. Birinci Dünya Harbinde Türk Harbi Kafkas Cephesi – 3 ncü ordu harekati, cilt II – Luptele la care au participat turcii în Primul Război Mondial – Frontul caucazian, operațiunea armatei a 3-a, 1993, vol. II, Imprimeria Statului Major General al Armatei Turce, Ankara.

2. Вооруженные силы России в Первой Мировой Войне 1914–1917 (Forțele armate ale Rusiei în Primul Război Mondial, 1914-1917), 2014, colectiv de autori, vol. II, Editura Magapolis, Moscova.

3. Allen, William David; Muratoff, Paul, 2010, Caucasian Battlefields, a history of the wars on turco-caucasian border, 1828-1921, Cambridge University Press, New York.

4. Bogdan, Morar, 2021, Un front uitat (Războiul ruso-turc din Caucaz 1914-1917), Editura Casa Cărții de Știință, Cluj-Napoca.

5. Bogdan, Morar, 2021, Cum a căzut fortăreața Erzurum cu 5 minute întârziere, în revista Magazin Istoric, nr. 9(654), pp. 58-62.

6. Buchan, John, 1917, Nelson's history of the war, vol. XIII, Thomas Nelson and son, Londra.

7. Coene, Frederik, 2009, The Caucasus: an introduction, Taylor & Francis e-Library.

8. Erickson, Edward J., 2001, Ordered to die, a history of the Ottoman Army in the First World War, Greenwood Publishing, Westport.

9. Halsey, Francis W., 1919, The literary digest, History of the world war, vol. VIII, Funk & Wagnalls, New York

10. Martyrosian, David, Эрзерумская операция (Operațiunea Erzurum), pe encyclopedia.mil.ru, material consultat în data de 22 mai 2023.

11. Kersnovski, Anton A., 1994, История Русской армии (Istoria armatei ruse), vol. IV, Editura „Golos", Moscova.

12. Korsun, Nikolai G., 1938, Эрзерумская операция (Operația Erzurum), Editura Comisariatului Apărării al U.R.S.S., Moscova.

13. Korsun, Nikolai G., 1946, Первая мировая война на Кавказском фронте. Оперативно-стратегический очерк (Primul război mondial pe frontul caucazian 1914-1917, Schiță strategică și operațională), Editura Militară a U.R.S.S.

14. Maslovski, Evgheni V., 1933, Мировая война на Кавказском фронте 1914-1917 г., Стратегический очерк (Războiul mondial pe frontul caucazian 1914-1917, Schiță strategică), Editura Renașterea, Paris.

15. Popa, Mircea N., 1979, Primul Război Mondial, Editura Științifică și Enciclopedică, București. 16. Rostunov, Ivan I., 1975, История Первой Мировой Войны 1914-1918 гг. (Istoria Primului Război Mondial 1914-1918), vol. I și II, Nauka, Moscova.

17. Șișov, A.V., 2004, Юденич, генерал Суворовской школы (Iudenici, general al școlii militare a lui Suvorov), Editura Vece, Moscova.

18. Şteifon, Boris A., 1929, Штурм Эрзерума (Cucerirea cetăţii Erzurum), în Военный сборник (Revista militară), nr. 10, Belgrad, pp. 49-66.

19. Tucker, Spencer C., 2014, World War I, The Definitive Encyclopedia and Document Collection, ABC-CLIO Llc, Santa Barbara, California.

20. Zaioncikovski, Andrei M., 2002, Первая Мировая Война 1914–1918 гг. (Primul Război Mondial 1914-1918), Editura „Poligon", Sankt Petersburg.

ANALIZĂ DE CONȚINUT A ARIILOR STRATEGICE DE SECURITATE CIBERNETICĂ – STATELE UNITE ALE AMERICII, MAREA BRITANIE, SPANIA ȘI ROMÂNIA

(CONTENT ANALYSIS OF STRATEGIC CYBER SECURITY FOCUS AREAS – UNITED STATES OF AMERICA, UNITED KINGDOM, SPAIN AND ROMANIA)

Cristian CONDRUȚ[*]

Abstract:

Nowadays cybersecurity is a topic that is more extensively addressed at a strategic level, both form a technical as well as form a non-technical perspective. In this context, the most important international organizations address cybersecurity by organizing international discussions aimed at keeping an open, free and secure cyberspace. These endeavours are usually taking the form a policy paper, a recommendation guide or a common initiative signed by multiple states. This kind of practice requires a correspondent in national strategic policy papers, the most important one being the national cybersecurity strategy. Taking into consideration that cybersecurity is not only a technical matter, multiple strategic areas are needed to be addressed. Thus, in this paper we aim to identify the most important cybersecurity strategic areas at a national level and their corelations. To achieve this research objective, we apply a content analysis and a frequency analysis methodology, using MAXQDA 20222 software. Our findings show that cybersecurity governance strategic area and preparedness and resilience strategic area are the most important ones at a national level, having multiple corelations with other strategic areas retrieved from the Guide to Developing a National Cybersecurity Strategy published by International Telecommunications Union in 2021.

Keywords: *cybersecurity, strategy, ITU, USA, UK, Spain, Romania*

Introducere

Am pornit cercetarea, de la premisa că securitatea cibernetică este un domeniu care a dobândit o importanță strategică, din ce în ce mai

[*] Asistent universitar, doctorand în cadrul Școlii Doctorale „Informații și Securitate Națională”, Academia Națională de Informații „Mihai Viteazul”, condrut.cristian@animv.eu

ridicată în ultimii ani, având în vedere preocupările statelor pentru elaborarea strategiilor naţionale de securitate cibernetică. Conform *International Telecommunications Union* (ITU), în *Global Cybersecurity Index 2020* (GCI 2020), 127 de state din 194 aveau în vigoare, în 2020, o strategie naţională de securitate cibernetică (i.e. 65%) (ITU Development Sector, 2021, p. p. 9). La nivelul Uniunii Europene (UE) şi *European Free Trade Association* (EFTA) toate cele 31 de state, 27 membre UE şi 4 membre ETFA, au în vigoare o strategie naţională de securitate cibernetică (ENISA, s.a.). De asemenea, tematicile existente în cadrul strategiilor naţionale de securitate cibernetică sunt extrem de diversificate, Agenţia Europeană de Securitate Cibernetică (ENISA) identificând 21 de categorii de obiective strategice de securitate cibernetică în cadrul acestor documente (ENISA, s.a.), iar ITU, în *Guide to Developing a National Cybersecurity Strategy*, 7 arii strategice de securitate cibernetică: guvernanţă; management al riscului; pregătire şi reziliență; infrastructuri critice şi servicii esenţiale; capabilitate, capacitate şi consolidarea conştientizării; legislaţie şi reglementare şi cooperare internaţională (ITU, 2021, pg. pp. 2-3).

Aceste aspecte ne determină să investigăm aprofundat strategii naţionale de securitate cibernetică, în scopul identificării modului în care securitatea cibernetică este reflectată la nivel strategic, ghidaţi de întrebarea: *Cum este reflectată securitatea cibernetică la nivel strategic prin raportare la ariile strategice prezentate în Guide to Developing a National Cybersecurity Strategy, elaborat de ITU?* Alegerea acestei lucrări drept referenţial este justificată, pe de o parte, de nivelul ridicat de autoritate al emitentului său – ITU este organism internaţional specializat în domeniul comunicaţiilor electronice, parte a Organizaţiei Naţiunilor Unite –, iar pe de altă parte, prin structura şi conţinutul ei, explicând detaliat modul în care statele ar trebui să elaboreze strategiile naţionale de securitate cibernetică.

Obiectivul de cercetare, pe care ni-l propunem, este identificarea celor mai importante arii strategice de securitate cibernetică şi a conexiunilor dintre acestea, în cadrul strategiilor naţionale de securitate cibernetică selectate. Modul în care, vom selecta strategiile naţionale de securitate cibernetică incluse în demersul de cercetare este explicat în secţiunea *metodologie*. Pentru a satisface obiectivul de cercetare, vom aplica metodele analizei calitative de conţinut şi analizei de frecvenţă şi vom utiliza aplicaţia software MAXQDA 2022. În această lucrare vom prezenta rezultatele cercetării noastre, prin respectarea următoarei structuri: *metodologie*, *rezultate*, *interpretări* şi *concluzii*.

Metodologie

Vom aplica metoda analizei calitative de conţinut în maniera etapizată descrisă de Denscombe în *The Good Research Guide*: eşantionare, alegerea unei unităţi de analiză, dezvoltarea unor categorii relevante pentru analizarea datelor, codarea unităţilor în acord cu categoriile alese, analizarea frecvenţei unităţilor de analiză şi a conexiunilor dintre acestea (Denscombe, 2010, pg. pp. 281-282).

Eşantionarea o vom realiza, prin aplicarea următoarelor criterii de selecţie, pentru strategiile naţionale de securitate cibernetică: 1) să aparţină statelor se află pe primele poziţii în clasamentul GCI 2020 şi să aparţină României; 2) să aparţină statelor membre NATO, având în vedere apartenenţa României la NATO; 3) să fi fost adoptate cu maxim 5 ani în urmă, faţă de perioada de derulare a cercetării[1]; 4) să fie în vigoare la momentul derulării cercetării; 5) să fie publicate în limbile engleză sau română.

Conform GCI 2020, primele 4 poziţii în clasamentul celor mai puternice state, din puncte de vedere al securităţii cibernetice, de la nivel global sunt ocupate de: Statele Unite ale Americii (prima poziţie); Marea Britanie şi Arabia Saudită (poziţia a doua); Estonia (poziţia a treia) şi Coreea de Sud, Singapore şi Spania (poziţia a patra). România ocupă poziţia 62 (ITU Development Sector, 2021, p. pp. 25). Am selectat câte o strategie naţională de securitate cibernetică, pentru fiecare dintre primele poziţii din clasamentul GCI 2020 (i.e. Statele Unite ale Americii, Marea Britanie şi Spania) şi le-am eliminat pe cele emise de state, care nu fac parte din NATO (i.e. Arabia Saudită, Coreea de Sud şi Singapore). Am eliminat şi strategia de securitate cibernetică a Estoniei, deoarece perioada de aplicare a acesteia a fost 2019 – 2022 (i.e. nu îndeplineşte criteriul 2) de selecţie) (MAEC Estonia, 2019, p. pp. 1). De asemenea, am inclus şi Strategia de Securitate Cibernetică a României pentru perioada 2022 – 2027, având în vedere că, pe parcursul cercetării ne-am propus inclusiv investigarea comparativă a aspectelor strategice de securitate cibernetică, de la nivel naţional, cu cele existente în Statele Unite ale Americii, Marea Britanie şi Spania. Am ales ca unitate de analiză paragraful din cadrul documentului de tip strategie naţională de securitate cibernetică, având în vedere că, o astfel de abordare ne-a

[1] Cercetarea a fost derulată în perioada februarie – mai 2023 şi face parte din programul individual de cercetare doctorală al autorului.

permis să identificăm conexiuni între ariile strategice de securitate cibernetică – aspecte prezentate în secțiunile *rezultate* și *interpretări*.

Am extras categoriile din literatura de specialitate, acestea fiind ariile strategice de securitate cibernetică, din cadrul *Guide to Developing a National Cybersecurity Strategy*, elaborat de ITU: guvernanță; management al riscului; pregătire și reziliență; infrastructuri critice și servicii esențiale; capabilitate, capacitate și consolidarea conștientizării; legislație și reglementare și cooperare internațională (2021, pg. pp. 2-3). Procesul de codare a fost realizat în acord cu cele 7 categorii alese și am utilizat funcțiile aplicației software MAXQDA 2022. Pentru analizarea frecvențelor categoriilor și a conexiunilor dintre acestea am utilizat funcția *Code Frequencies*[2], respectiv *Code Relations Browser*[3]. În ceea ce privește conexiunile, vom utiliza tipul de analiză de intersecție a codurilor (i.e. în cazul cercetării noastre – categoriilor) dintr-un segment (i.e. în cazul cercetării noastre – un paragraf). Acest tip de analiză este cel mai relevant pentru cercetarea noastră, având în vedere că, documentele strategice de securitate cibernetică tratează transversal arii strategice de la nivel național, conexându-le în cele mai multe situații în cadrul aceluiași paragraf.

Rezultate

În continuare vom prezenta rezultatele cercetării noastre după cum urmează: frecvența fiecăreia dintre cele 7 categorii în strategiile naționale de securitate cibernetică în *Figura 1* (vezi mai jos); frecvența tuturor corelațiilor dintre categorii în *Figura 2* (vezi mai jos); frecvența celor mai importante 10 corelații dintre categorii, în *Tabelul 1* (vezi mai jos).

[2]Mai multe informații referitoare la această funcție se regăsesc la https://www.maxqda.com/help-mx20/statistics-and-graphics-functions/code-frequencies, accesată la data de 12.05.2023.

[3] Mai multe informații referitoare la această funcție se regăsesc la https://www.maxqda.com/help-mx20/visual-tools/code-relations-browser-visualizing-overlapping-codes, accesată la data de 12.05.2023.

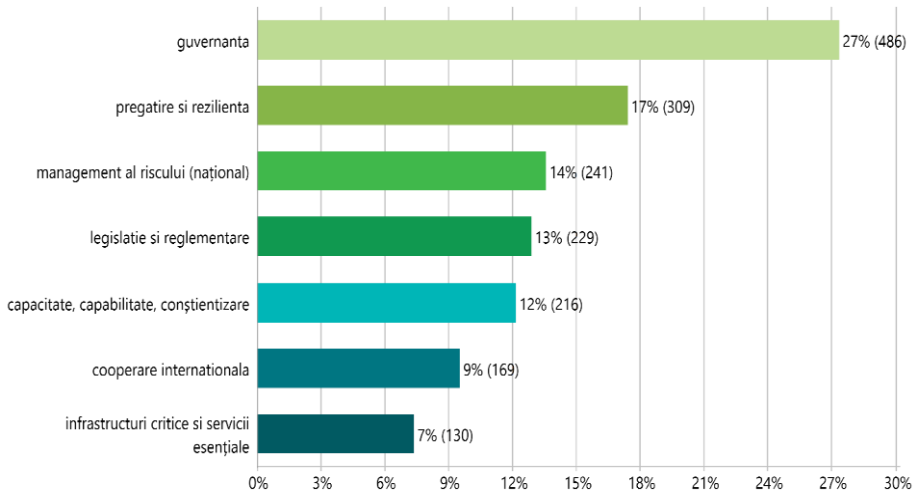

Figura 1: Frecvenţa categoriilor, exprimată procentual şi numeric. Figura a fost generată prin utilizarea funcţiei *code frequencies* a aplicaţiei software MAXQDA 2022.

Prin codarea celor patru strategii de securitate cibernetică alese (i.e. Statele Unite ale Americii, Marea Britanie, Spania şi România) şi analizarea frecvenţei de apariţie a categoriilor am obţinut o listă, ordonată descrescător, a ariilor strategice de securitate cibernetică, exprimată în valori procentuale şi numerice. Această clasificare furnizează o parte din răspunsul aşteptat pentru întrebarea de cercetare formulată, urmând ca, în secţiunea *Interpretări* să aprofundăm analiza rezultatului obţinut.

Guvernanţa de securitate cibernetică se clasează pe prima poziţie în graficul din *Figura 1* (vezi mai sus), această categorie fiind utilizată pentru a coda 486 de segmente sau 27% din totalitatea segmentelor codate, în cele 4 strategii naţionale de securitate cibernetică analizate. Pe cea de-a doua poziţie se clasează *pregătirea şi reziliența* cu 309 segmente codate sau 17% din totalitatea segmentelor codate. Următoarele rezultate pot fi grupate, din punct de vedere numeric, în două intervale, diferenţa dintre cele două capete ale intervalelor fiind de exact 2%:

Intervalul α – (12%; 14%) – este compus din categoriile de *management al riscului* de securitate cibernetică, 241 de segmente codate sau 14%, *legislaţie şi reglementare*, 229 de segmente codate sau 13% şi *capacitate, capabilitate şi conştientizare*, 216 segmente codate sau 12% din totalul segmentelor codate.

Intervalul β – (7%; 9%) – este compus din categoriile de *cooperare internațională*, 169 de segmente codate sau 9% și infrastructuri critice și servicii esențiale, 130 de segmente codate cu 7%.

Code System	guvern...	manag...	infrastr...	pregat...	capaci...	legisla...	coope...
guvernanta		137	67	183	120	128	87
management al riscului (național)	137		43	101	39	58	29
infrastructuri critice si servicii esențiale	67	43		66	20	50	16
pregatire si rezilienta	183	101	66		75	98	64
capacitate, capabilitate, conștientizare	120	39	20	75		43	36
legislatie si reglementare	128	58	50	98	43		54
cooperare internationala	87	29	16	64	36	54	
Σ SUM	722	407	262	587	333	431	286

Figura 2: Matricea de corelație a categoriilor, exprimată numeric. Figura a fost generată prin utilizarea funcției *code frequencies* a aplicației software MAXQDA 2022.

Rezultatele prezentate în *Figura 2* (vezi mai sus) completează răspunsul la întrebarea de cercetare având în vedere că reflectă modul în care ariile strategice de securitate cibernetice sunt corelate între ele în cadrul strategiilor naționale de securitate cibernetică. În ceea ce privește matricea de ocurență, aceasta este de tip simetric (i.e. o valoare aleasă arbitrar de pe linia *i* și coloana *j* este egală cu o valoare aleasă arbitrar de pe linia *j* și coloana *i*), ceea ce presupune că indiferent de modul în care alegem să citim un anumit rezultat (ex. corelația dintre *pregătire și reziliență* cu *legislație și reglementare* sau corelația dintre *legislație și reglementare* și *pregătire și reziliență*) acesta va fi același prin raportare la diagonala matricei. Pentru a facilita interpretările cu privire la cele mai importante corelații dintre categorii (i.e. ariile strategice de securitate cibernetică), vom prezenta cele mai frecvente 10 rezultatele din *Figura 2* în *Tabelul 1* (vezi mai jos).

Tabelul 1: Cele mai frecvente 10 corelaţii ale ariilor strategice extrase din *Figura 1*.

Nr.crt.	Intersecţie	Valoare
1.	guvernanţă – pregătire şi reziliență	183
2.	guvernanţă – management al riscului (național)	137
3.	guvernanţă – legislaţie şi reglementare	128
4.	guvernanţă – capacitate, capabilitate şi conştientizare	120
5.	management al riscului (național) – pregătire şi reziliență	101
6.	pregătire şi reziliență – legislaţie şi reglementare	98
7.	guvernanţă – cooperare internaţională	87
8.	pregătire şi reziliență – capacitate, capabilitate şi conştientizare	75
9.	guvernanţă – infrastructuri critice şi servicii esenţiale	67
10.	pregătire şi reziliență – infrastructuri critice şi servicii esenţiale	66

Interpretări

În continuare ne propunem să discutăm rezultatele prezentate în *Figura 1* (vezi mai sus) şi în *Tabelul 1* (vezi mai sus). Datele prezentate în *Figura 1*, frecvenţele exprimate procentual şi numeric ale ariilor strategice de securitate cibernetică, ne ajută să atingem o parte din obiectivul de cercetare pe care ni l-am propus – identificarea celor mai importante arii strategice de securitate cibernetică. Datele prezentate în *Tabelul 1*, cele mai frecvente corelaţii ale ariilor strategice de securitate cibernetică, ne ajută să atingem şi al doilea aspect al obiectivului de cercetare – identificarea conexiunilor dintre ariile strategice de securitate cibernetică. În cele ce urmează, vom discuta cele 7 arii strategice cuprinse în Ghidul ITU, în ordinea scorurilor frecvenţelor obţinute în cadrul cercetării noastre (vezi *Figura 1*).

Guvernanţă

Guvernanţa de securitate cibernetică face referire la modul în care, statul consolidează rezilienţa cibernetică şi reduce riscurile asociate, prin definirea de obiective strategice şi desemnarea de autorităţi responsabile (ITU, 2021, p. pp. 34). De asemenea, aria

strategică a guvernanței de securitate cibernetică include următoarele dimensiuni strategice: asigurarea celui mai ridicat nivel de suport; stabilirea unei autorități competente de securitate cibernetică; asigurarea cooperării intra-guvernamentale; asigurarea cooperării inter-sectoriale; alocarea de buget și resurse; dezvoltarea unui plan de implementare (ITU, 2021, pg. pp. 2-3). Guvernanța de securitate cibernetică a obținut cel mai ridicat scor în analiza noastră – 27% ,din totalitatea segmentelor codate. Semnificația acestui rezultat este că, cele 4 state analizate prioritizează, din punct de vedere strategic, modul în care este planificat domeniul securității cibernetice la nivel național. În toate cele 4 strategii analizate am putut să observăm, că strategia desemnează o autoritate de securitate cibernetică responsabilă cu implementarea strategiei – *Office of National Cyber Director* (ONCD) în SUA, *National Cyber Security Centre* (NCSC) în Marea Britanie, *National Cybersecurity Council* (NCC) în Spania și Directoratul Național de Securitate Cibernetică în România (DNSC). De asemenea, toate cele 4 state încurajează dezvoltarea unui plan de implementare și alocarea de resurse, pentru domeniul securității cibernetice, ceea ce relevă că, cele 4 țări planifică la nivel strategic implementarea de proiecte strategice în domeniu. Cooperarea inter-guvernamentală și cooperarea intra-guvernamentală sunt dimensiuni strategice regăsite de asemenea în toate cele 4 strategii, ceea ce înseamnă, pe de o parte, că responsabilitățile în domeniu sunt alocate unor instituții publice diferite, care trebuie să coopereze pentru a duce la îndeplinire obiectivele strategice, iar pe de altă parte, că îndeplinirea obiectivelor strategice de securitate cibernetică este dependentă de implicarea unui număr cât mai mare de actori societali. Singura strategie de securitate cibernetică, în care nu există o secțiune dedicată sprijinului oferit de un înalt oficial al statului, este cea a României. Strategiile SUA, Marea Britanie și Spania debutează cu o astfel de secțiune.

Importanța guvernanței de securitate cibernetică este reliefată și de rezultatele prezentate în *Tabelul 1,* având în vedere că, această arie strategică de securitate cibernetică se corelează puternic (i.e. 6 din primele 10 poziții ale corelațiilor), cu toate celelalte incluse în analiza noastră, pe pozițiile: 1 cu *pregătire și reziliență*; 2 cu *management al riscului;* 3 cu *legislație și reglementare;* 4 cu *capacitate, capabilitate și conștientizare*; 7 cu *cooperare internațională*; 9 cu *infrastructuri critice și servicii esențiale*.

Pregătire şi reziliență

Pregătirea şi reziliența de securitate cibernetică se referă la bune-practici necesar a fi implementate la nivel naţional, pentru stabilirea şi consolidarea unor capabilităţi eficiente de securitate cibernetică, necesare pentru pregătirea, prevenirea, detectarea, diminuarea efectelor şi răspunsul la incidente grave de securitate cibernetică (ITU, 2021, p. p. 39). Dimensiunile strategice asociate de ITU ariei pregătire şi reziliență sunt: stabilirea de capabilităţi de răspuns la incidente de securitate cibernetică, stabilirea de planuri de contingență şi management al crizelor, promovarea schimbului de informaţii, derularea de exerciţii de securitate cibernetică şi stabilirea impactului şi severităţii incidentelor de securitate cibernetică (ITU, 2021, pg. pp. 2-3). Singurul domeniu strategic, care nu îşi găseşte corespondent în toate cele 4 strategii analizate, este cel al exerciţiilor de securitate cibernetică, acesta fiind abordat de Marea Britanie, Spania şi România, ceea ce indică o omogenitate în abordarea statelor europene, din eşantionul nostru. Stabilirea capabilităţilor de răspuns la incidente de securitate cibernetică este tratată în toate cele 4 strategii analizate, având în vedere că, desemnează instituţii de tip *Computer Emergency Response Team* (CERT) responsabile de acest domeniu: SUA – *Cybersecurity & Infrastructure Security Agency* (CISA); Marea Britanie – *National Cyber Security Centre* (NCSC); România – Directoratul Naţional de Securitate Cibernetică (DNSC); Spania – Institutul Naţional de Securitate (INCIBE). Stabilirea de planuri de contingență şi management al crizelor îşi găseşte corespondent în toate cele 4 strategii, având în vedere necesitatea de reacţie post-incident de securitate cibernetică. Lipsa unei astfel de reacţii, poate conduce la amplificarea consecinţelor iniţiale ale unui incident de securitate cibernetică şi la diversificarea obiectelor de securitate afectate. Practica schimbului de informaţii este recunoscută ca fiind benefică, la nivelul tuturor celor 4 state, constatându-se ca fiind, în general, abordată prin referiri la operatori de infrastructuri critice şi servici esenţiale, la industria privată de securitate cibernetică şi la platforme naţionale, create special în acest scop. O altă practică inclusă în aria strategică *pregătire şi reziliență* este cea a stabilirii impactului şi severităţii incidentelor de securitate cibernetică, abordarea celor 4 state fiind asociată unor linii de acţiune clare, ce presupun reorganizarea unor autorităţi în domeniu sau realizarea unor metodologii de evaluare a incidentelor de securitate.

Corelaţiile cele mai frecvente ale ariei strategice *pregătire şi reziliență*, în conformitate cu *Tabelul 1*, sunt cu: *guvernanța*, pe poziţia 1;

management al riscului, pe poziția 5; *legislație și reglementare*, pe poziția 6; *capacitate, capabilitate și conștientizare*, pe poziția 8; *infrastructuri critice și servicii esențiale*, pe poziția 10. Astfel, 5 din primele 10 cele mai frecvente corelații între arii strategice de securitate cibernetică includ *pregătirea și reziliența*. Acest aspect relevă faptul că, cele 4 state sunt preocupate cu sprijinirea, din punct de vedere strategic, a demersurilor care vizează consolidarea rezilienței cibernetice naționale, fiind astfel, în acord cu o serie de documente elaborate la nivelul NATO, precum *Rezoluția 475/2022 privind dezvoltarea rezilienței cibernetice în societățile aliate*[4] sau cu *Cyber Defence Pledge*[5] adoptată la Summitul de la Varșovia în 2016. Reținem faptul că, cele 4 strategii corelează puternic *reziliența și pregătirea* cu *guvernanța* de securitate cibernetică, ceea ce înseamnă, că *pregătirea și reziliența* este tema prioritară pe agenda strategică a celor 4 state. De asemenea, *pregătirea și reziliența* este corelată puternic și cu *managementul riscului*, aspect care ne relevă, că măsurile de management al riscului cibernetic susțin capacitatea de reziliență cibernetică a statului și că, un management mai eficient al riscurilor de securitate cibernetică se realizează prin asumarea obiectivului de consolidare a rezilienței cibernetice de la nivel național.

Management al riscului

Aria strategică a *managementului riscului de securitate cibernetică* cuprinde bunele-practici necesar a fi implementate, pentru eficientizarea proceselor de management al riscului: realizarea de evaluări de securitate cibernetică, definirea unei abordări de management al riscului, identificarea unei metodologii comune de management al riscului, dezvoltarea unor profiluri de risc cibernetic sau stabilirea de politici de securitate cibernetică (ITU, 2021, pg. pp. 37-38). Singura practică de management al riscului, care nu este abordată în toate cele 4 strategii, este identificarea unei metodologii comune de management al riscului de securitate cibernetică, în strategia Spaniei neexistând referiri la aceasta. Practica evaluărilor de securitate cibernetică este încurajată de toate cele 4, preponderent, prin raportare la amenințările curente de securitate cibernetică (ex. spionajul cibernetic, sabotajul cibernetic,

[4] Disponibilă în 15.05.2023 pe https://www.nato-pa.int/download-file?filename=/sites/default/files/2022-11/RESOLUTION%20475%20%20ENHANCING%20THE%20CYBER%20RESILIENCE%20OF%20ALLIED%20SOCIETIES.pdf

[5] Disponibilă în 15.05.2023 pe https://www.nato.int/cps/en/natohq/official_texts_133177.htm

criminalitatea cibernetică, hacktivismul sau dezinformarea şi propaganda prin mijloace cibernetice). Definirea unei abordări de management al riscului se reflectă în cele 4 strategii analizate prin elemente, precum dezvoltarea de tehnologii pentru detectarea ameninţărilor de securitate cibernetică, dezvoltarea capabilităţilor de colectare şi analizare a informaţiilor de securitate cibernetică sau dezvoltarea parteneriatelor, între mediul public şi cel privat. Stabilirea profilurilor de risc este abordată în cele 4 strategii de securitate cibernetică, prin încurajarea realizării unor evaluări de risc de securitate cibernetică, pentru sectoarele de activitate ce administrează şi operează infrastructuri cibernetice critice. Politicile de securitate cibernetică trebuie să fie definite la toate nivelurile domeniului securităţii cibernetice (i.e. strategic, operaţional şi tactic) (ITU, 2021, p. p. 38). Toate cele 4 state analizate definesc sau încurajează demersuri menite să consolideze aplicarea de politici de securitate cibernetică, câteva exemple în acest sens fiind: crearea, diseminarea şi aplicarea de standarde de securitate cibernetică; acordarea de stimulente financiare companiilor care implementează standarde de securitate cibernetică; reconsiderarea politicii de resurse umane.

Corelaţiile ariei strategice *management al riscului de securitate cibernetică*, în conformitate cu *Tabelul 1* (vezi mai sus), sunt cu: *guvernanţa*, pe poziţia 2; *pregătirea şi reziliența*, pe poziţia 5. Astfel, managementul riscului de securitate cibernetică reprezintă o arie strategică, necesar a fi coordonată de la nivelul autorităţilor publice cu responsabilităţi de ordin tehnic (ex. organismele de tip CERT) sau de la nivelul celor cu responsabilităţi non-tehnice (ex. instituţii din domeniul afacerilor externe, servicii de informaţii), fiecare dintre aceste autorităţi contribuind, conform competenţelor legale, la definirea unui cadru naţional în materie. Menţinem concluziile referitoare la corelaţia cu aria strategică *pregătire şi reziliență*, în ceea ce priveşte modul în care cele două arii strategice se influenţează reciproc.

Legislaţie şi reglementare

Legislaţia şi reglementarea de securitate cibernetică se referă la modul în care, statele trebuie să îşi construiască elemente de cadru legislativ, în ceea ce priveşte protejarea societăţii împotriva criminalităţii cibernetice şi promovarea unui spaţiu cibernetic sigur (ITU, 2021, p. pp. 47). Domeniile strategice incluse în aria *legislaţie şi reglementare* sunt: stabilirea unui cadrul legislativ naţional de securitate cibernetică; stabilirea unui cadru legal naţional pentru criminalitate cibernetică şi

pentru dovezi digitale; recunoașterea și protejarea drepturilor și libertăților omului; crearea unor mecanisme de control; stabilirea de procese inter-organizaționale; sprijinirea cooperării internaționale pentru combaterea amenințărilor și criminalității cibernetice (ITU, 2021, pg. pp. 47-50). Toate cele 4 state abordează, în proporții variabile, fiecare domeniu strategic inclus în aria *legilsație și reglemetare*. Stabilirea unui cadru legal de securitate cibernetică este relaționată în cele 4 documente analizate, cu existența sau necesitatea de adoptare a unui cadru normativ, care să reglementeze responsabilitățile instituționale în domeniul securității cibernetice. De asemenea, la nivelul statelor europene analizate, sunt realizate referiri cu privire implementarea Directivei NIS – *nr. 1148 din 2016 privind măsurile pentru un nivel ridicat de securitate a rețelelor și sistemelor informatice din Uniune*[6]. În ceea ce privește stabilirea unui cadru legal de criminalitate cibernetică și dovezi digitale, cele 4 state fac referiri la elemente, precum: tragerea la răspundere a criminalilor cibernetici, prin adoptarea sau actualizarea unor elemente legislative judiciare (ex. în Marea Britanie se propune amendarea *Computer Misuse Act* și *Proceeds of Crime Act 2002*) și implementarea de standarde legale de combatere a utilizării în scopuri ilicite a criptomonedelor. În ceea ce privește protejarea drepturilor omului, toate cele 4 state recunosc importanța acestui demers și încurajează comportamentul responsabil al statelor în spațiul cibernetic și respectarea legislației internaționale. Domeniul mecanismelor de control este reliefat în cele 4 strategii, prin: necesitatea de adoptare a unor standarde de natură tehnică și non-tehnică; definirea de criterii de încredere pentru entitățile care furnizează echipamente IT&C; criterii de securitate cibernetică specifice fiecărui sector critic de activitate. Practica stabilirii proceselor inter-organizaționale este reliefată în strategiile analizate, prin elemente precum: crearea de mecanisme de cooperare interinstituțională, pentru afirmarea de poziții naționale și pentru consultanță în domeniul securității cibernetice; dezvoltarea unor proceduri de atribuire a atacurilor cibernetice; crearea de mecanisme de raportare a incidentelor de securitate cibernetică. Cooperarea internațională pentru combaterea criminalității cibernetice este un domeniu exprimat în cele 4 strategii analizate, preponderent, prin raportare la eforturile internaționale de diminuare a amenințărilor de criminalitate cibernetică (ex. acțiuni realizate în cooperare, de

[6] Disponibilă la https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016L1148, la data de 16 mai 2023.

organizaţiile de aplicare a legii; iniţiative internaţionale comune de combatere a unor fenomene, manifestate în spaţiul cibernetic).

Corelaţiile ariei strategice *legislaţie şi reglementare*, în conformitate cu *Tabelul 1* (vezi mai sus), sunt cu *guvernanţa*, la poziţia 3 şi cu *pregătirea şi reziliența,* la poziţia 6. Corelaţia puternică a ariei strategice *legislaţie şi reglementare* cu *guvernanţa* este explicată prin faptul că, statul este emitentul cadrului legislativ naţional pe orice subiect, nu doar pe cel de securitate cibernetică. De asemenea, având în vedere, că activităţile de criminalitate cibernetică intră sub incidenţa legislaţiei penale, în forme şi proporţii variate de definire, şi că pentru a combate aceste activităţi este necesară o bună cooperare intra-guvernamentală şi inter-sectorială (i.e. domenii strategice de guvernanţă), corelaţia puternică, dintre *guvernanţă* şi *legislaţie şi reglementare* este un rezultat normal. Intensitatea celei de-a doua corelaţii (i.e. *legislaţie şi reglementare* & *pregătire şi reziliență*) ne reliefează faptul că, pentru dezvoltarea rezilienţei cibernetice la nivel naţional, este nevoie de adoptarea unui cadru legislativ, care să ofere statului mecanisme rapide de acţiune, prin definirea de responsabilităţi instituţionale, stabilirea unor facilităţi fiscale şi sancţionarea, pe căi civile şi penale, a entităţilor care nu se supun legislaţiei în vigoare.

Capacitate, capabilitate şi conştientizare

Capacitatea, capabilitatea şi conştientizarea este o arie de securitate cibernetică ce tratează atât provocările asociate consolidării capacităţii şi capabilităţii tehnologice şi umane, cât şi provocările conexate creşterii nivelului de conştientizare a domeniului securităţii cibernetice în rândul entităţilor cheie, precum instituţii publice, cetăţeni şi organizaţii private (ITU, 2021, p. p. 44). Domeniile de interes din această arie strategică sunt: planificarea strategică; dezvoltarea *curriculei* de securitate cibernetică; stimularea dezvoltării capacităţii şi a formării profesionale; implementarea de programe coordonate de consolidare a conştientizării; consolidarea cercetării, inovării şi dezvoltării de securitate cibernetică; implementarea de programe pentru sectoarele şi grupurile vulnerabile (ITU, 2021, pg. pp. 44-48). Planificarea strategică nu a fost abordată în toate cele 4 strategii analizate, având în vedere, că Spania nu desemnează entităţi responsabile pentru această arie strategică. De asemenea, implementarea de programe pentru sectoarele şi categoriile vulnerabile este abordată doar în strategiile SUA, Marii Britanii şi Spaniei, fiind prezentate o serie de iniţiative deja existente în acest domeniu (ex.

dezvoltarea de competențe de securitate cibernetică pentru tineri; diversificarea incluziunii forței de muncă de securitate cibernetică pentru categorii, precum cea a imigranților și a persoanelor cu handicap) și necesitatea de implementare a unora noi. Domeniul dezvoltării unor cadre curriculare de securitate cibernetică este abordat în toate cele 4 strategii, fiind corelat cu măsuri, precum: acordarea de burse educaționale de securitate cibernetică; includerea în programele școlare și universitare a unor subiecte sau discipline de securitate cibernetică; organizarea de evenimente educaționale de securitate cibernetică (ex. tabere de pregătire). Stimularea capacității și formării profesionale de securitate cibernetică este reliefată prin măsuri, precum: organizarea de cursuri de specializare pentru profesioniștii în securitate cibernetică, inclusiv în parteneriat public-privat; dezvoltarea de centre de instruire naționale de securitate cibernetică; aplicarea unor cadre de competență de securitate cibernetică deja existente la nivel național. Domeniul conștientizării amenințării de securitate cibernetică este transpus în cele 4 strategii, prin necesitatea de informare a societății civile, derularea de programe educaționale, în scopul consolidării igienei de securitate cibernetică sau prin derularea de campanii specializate, pentru sectoarele critice de activitate. Consolidarea cercetării, inovării și dezvoltării de securitate cibernetică este percepută în cele 4 strategii, în raport cu reziliența cibernetică. Astfel, programele de cercetare în domeniul securității cibernetice trebuie să contribuie, pe de o parte la dezvoltarea tehnologiilor defensive de securitate cibernetică, iar pe de altă parte, să mențină avantajul competitiv al statului. De asemenea, cercetarea de securitate cibernetică este dependentă de o bună cooperare între mediul public, privat și academic, acest aspect fiind surprins în toate cele 4 strategii.

Corelațiile ariei strategice *capacitate, capabilitate și conștientizare*, în conformitate cu *Tabelul 1,* sunt cu: *guvernanță*, pe poziția 4 și *pregătire și reziliență*, pe poziția 8. Prima corelație (i.e. *guvernanță* & *capacitate, capabilitate și conștientizare*) se explică, prin implicarea autorităților publice în demersuri, care vizează dezvoltarea acestei arii strategice. Un domeniu extrem de important în acest context este cel al cooperării inter-sectoriale (i.e. inclus în aria strategică a *guvernanței*) având în vedere că, efectele consolidării capacității, capabilității și conștientizării de securitate cibernetică se resimt la nivelul întregii societăți. Spre exemplu, în ceea ce privește *dezvoltarea curriculei de securitate cibernetică*, este necesară implicarea autorităților publice, cu responsabilități în domeniul educațional și de securitate

cibernetică, pentru a asigura cadrul necesar formării viitorilor şi actualilor specialişti de securitate cibernetică. Efectele existenţei unui cadru coerent de educaţie de securitate cibernetică sunt resimţite la nivelul întregii societăţi, având în vedere că, specialiştii care au parcurs procese formative instituţionalizate, constituie masa critică de specialişti în domeniu, care îşi desfăşoară activitatea în diverse sectoare de activitate, indiferent dacă luăm în considerare mediul public, privat sau academic. Corelaţia dintre *capacitate, capabilitate şi conştientizare* & *pregătire şi rezilienţă* are un rol extrem de important în dezvoltarea domeniului securităţii cibernetice, pe termen mediu şi lung. Având în vedere că, ITU defineşte reziliența inclusiv prin raportare la pregătire (ITU, 2021, p. pp. 39), consolidarea capacităţii resursei umane, ce îşi desfăşoară activitatea în domeniul securităţii cibernetice, devine o misiune extrem de importantă pentru state. Cu toate acestea, putem identifica şi alte sinergii între cele două arii strategice, una dintre ele fiind cea a consolidării capacităţii de reacţie la incidente de securitate cibernetică (i.e. domeniu inclus în aria strategică *pregătire şi rezilienţă*) şi consolidarea cercetării, dezvoltării şi inovării (i.e. domeniu inclus în aria strategică interpretată în acest paragraf). Lipsa dezvoltării de tehnologii actuale de securitate cibernetică şi inacţiunea statului, pentru a valorifica aceste tehnologii, poate diminua capacitatea de răspuns la incidente, având în vedere creşterea complexităţii atacurilor cibernetice şi varietatea, din ce în ce mai ridicată, a instrumentelor utilizate de atacatori.

Cooperare internaţională

Aria strategică a cooperării internaţionale este caracterizată, prin angajamentele externe ale unui stat în domeniul securităţii cibernetice, atât la nivel regional, cât şi la nivel internaţional (ITU, 2021, p. pp. 50). Domeniile incluse în această arie strategică sunt: recunoaşterea securităţii cibernetice, ca o componentă a politicii externe; angajarea în discuţii internaţionale şi angajamentul pentru implementare; promovarea cooperării formale şi informale de securitate cibernetică; promovarea consolidării capacităţii de cooperare internaţională (ITU, 2021, pg. pp. 50-53). Securitatea cibernetică, percepută ca o componentă a politicii externe a statului, este o temă abordată în toate cele 4 strategii de securitate cibernetică, în relaţie cu rolul pe care fiecare dintre state doreşte să şi-l asume la nivel internaţional, în următorii ani: Marea Britanie – lider în domeniu şi putere cibernetică globală (HM Government , 2022, p. pp. 11); SUA – putere diplomatică activă, în

domeniul securității cibernetice (The White House, 2023, p. pp. 32); Spania – model de securitate cibernetică (DSN, 2019, p. pp.14); România – lider regional în domeniul securității cibernetice (Guvernul României, 2022, p. pp. 27). Angajarea în discuții internaționale este reliefată, în cele 4 strategii de securitate cibernetică, prin referiri la apartenența fiecăruia dintre state la diferite organizații (ex. ONU, NATO, UE, OSCE) și inițiative internaționale (ex. *Counter-Ransomware Initiative*) în domeniul securității cibernetice. Promovarea cooperării formale și informale, în domeniul securității cibernetice, este identificată în cele 4 strategii, prin referiri la: dezvoltarea de mecanisme de cooperare în cadrul organizațiilor internaționale; valorificarea prezenței globale a unor companii relevante de securitate cibernetică la nivel național; valorificarea prezenței unor organisme regionale și internaționale de securitate cibernetică la nivel național (ex. Centru European de Competențe de Securitate Cibernetică[7] are sediul în București); influențarea discuțiilor referitoare la standarde, asociate unor tehnologii cheie, din domeniul securității cibernetice (ex. 5G). Promovarea consolidării capacității de cooperare internațională este abordată, în relație cu dezvoltarea competențelor cibernetice de politică externă ale celor 4 state.

Singura corelație a ariei strategice *cooperare internațională*, conform *Tabelului 1*, este cu aria strategică a *guvernanței*, corelație aflată pe poziția a 7-a. Având în vedere, că aria strategică a *cooperării internaționale* de securitate cibernetică determină responsabilități doar pentru câteva tipuri de instituții publice (i.e. cele din domeniul afacerilor externe), nu este surprinzător faptul că, aceasta o obținut doar o singură corelație, în clasamentul primelor 10 (vezi *Tabelul 1*).

Infrastructuri critice și servicii esențiale

Aria strategică a *infrastructurilor critice și serviciilor esențiale* se referă la bunele-practici, asociate protejării acestor infrastructuri și a consolidării rezilienței acestora (ITU, 2021, p. pp. 41). Domeniile incluse în această arie strategică sunt: stabilirea unei abordări de management al riscului; adoptarea unui model de guvernanță; definirea unor standarde minime de securitate cibernetică; utilizarea pârghiilor de piață; stabilirea de parteneriate public private (ITU, 2021, pg. pp. 41-44). Domeniul stabilirii unei abordări de management al riscului este regăsit

[7] Disponibil la https://cybersecurity-centre.europa.eu/news/eccc-opens-its-doors-bucharest-2023-05-09_en, la data de 16.05.2023.

în toate cele 4 strategii analizate, fiind reliefat prin elemente, precum: elaborarea de proceduri de audit de securitate cibernetică, în conformitate cu cadrul legislativ în domeniu (i.e. pentru statele europene, legislaţia de transpunere a Directivei NIS, iar pentru SUA, *National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems* şi *Executive Order on Improving the Nation's Cybersecurity* (The White House, 2023, p. pp. 6)), consolidarea rezilienţei infrastructurilor critice printr-o abordare de tip *zero trust*[8] sau implementarea obligativităţii de raportare a incidentelor de securitate cibernetică. Domeniul adoptării unui model de guvernanţă pentru securitatea cibernetică a infrastructurilor critice şi serviciilor esenţiale se regăseşte în strategiile SUA, Marii Britanii şi Spaniei, prin elemente, precum: desemnarea de autorităţi publice naţionale în materie; stabilirea de mecanisme de cooperare intra-guvernamentală şi inter-sectorială, pentru rezolvarea incidentelor de securitate cibernetică. Definirea de standarde minimale de securitate cibernetică se regăseşte în toate cele 4 strategii analizate şi este reliefată prin elemente, precum: transpunerea în legislaţia naţională a Directivei NIS (i.e. pentru statele europene); adaptarea criteriilor în funcţie de sectorul de activitate; furnizarea de sprijin pentru administratorii infrastructurilor critice în implementarea standardelor, inclusiv prin elaborarea de proceduri şi ghiduri de bune-practici în domeniu. Domeniul utilizării pârghiilor de piaţă a fost abordat doar în strategiile Marii Britanii şi Spaniei, într-o manieră extrem de sumară, principalele referiri fiind la modalitatea în care, statul trebuie să valorifice relaţionarea cu principalii actori economici din piaţa de securitate cibernetică, pentru asigurarea securităţii cibernetice. Practica parteneriatelor public-private, pentru asigurarea securităţii cibernetice a infrastructurilor critice este încurajată doar în strategiile SUA şi Marii Britanii.

Corelaţiile ariei strategice *infrastructuri critice şi servicii esenţiale*, în conformitate cu *Tabelul 1* (vezi mai sus), se realizează cu: *guvernanţa*, la poziţia 9 şi cu *pregătirea şi reziliența* la poziţia 10. Niciuna, dintre cele două corelaţii, nu ocupă una dintre primele poziţii din *Tabelul 1.* Din punct de vedere cantitativ, acest aspect se poate explica, prin frecvenţa scăzută a segmentelor incluse în aria strategică *infrastructuri critice şi*

[8] Cadru de securitate cibernetică în care toţi utilizatorii unei reţele, indiferent de faptul că îşi desfăşoară activitatea în interiorul sau în afara ei, trebuie să fie validaţi din prin proceduri de autentificare, autorizare şi auditare de securitate. Mai multe informaţii despre *zero trust* se regăsesc la https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/, disponibil la data de 17.05.2023.

servicii esențiale (vezi *Figura 1*). Din punct de vedere calitativ, aria infrastructurilor critice și serviciilor esențiale desemnează doar o parte dintre infrastructurile cibernetice, existente la nivelul unui stat, existând totodată reglementări, metodologii și proceduri diferite pentru aceste tipuri de infrastructuri cibernetice. Aceste aspecte izolează aria strategică a *infrastructurilor critice și serviciilor esențiale*, de celelalte arii existente și determină, în consecință, un număr mai scăzut de corelații ale acesteia.

Concluzii

Pornind de la întrebarea de cercetare – *Cum este reflectată securitatea cibernetică la nivel strategic prin raportare la ariile strategice prezentate în Guide to Developing a National Cybersecurity Strategy, elaborat de ITU?* – considerăm că, am reușit să atingem obiectivul de cercetare pe care ni l-am propus: *identificarea celor mai importante arii strategice de securitate cibernetică și a conexiunilor dintre acestea, în cadrul strategiilor naționale de securitate cibernetică selectate*, respectiv, cele mai importante arii strategice de securitate cibernetică identificate de noi sunt *guvernanța*, cu 27% din totalitatea segmentelor codate și *pregătirea și reziliența*, cu 17% din totalitatea segmentelor codate. Acest aspect ne indică faptul că, statele acordă o importanță deosebită aspectelor ce țin de guvernanța de securitate cibernetică, statul fiind principalul actor relevant în domeniu, cu toate că, se constată la nivel strategic, necesitatea adoptării unei viziuni de tip *whole-of-society*. Cu toate acestea, pentru atingerea obiectivelor strategice de securitate cibernetică este necesară implicarea unei varietăți cât mai ridicate de actori de la nivelul societății, având în vedere că, guvernanța de securitate cibernetică include și domeniul cooperării inter-sectoriale. Un alt aspect important, de reținut, este dat de interpretarea rezultatului obținut de aria strategică *pregătire și reziliență*: statele conștientizează importanța adoptării de măsuri strategice, menită să consolideze reziliența cibernetică națională. În ceea ce privește corelațiile, constatăm că, *guvernanța* de securitate cibernetică realizează cele mai multe astfel de legături cu celelalte arii strategice, aspect care, completează concluziile ce rezultă din interpretarea rezultatelor, pe care fiecare arie de securitate cibernetică le-a obținut.

În ceea ce privește limitările, considerăm că, cercetarea prezentă ar fi putut obține o relevanță mult mai accentuată, în situația în care, am fi selectat un număr mai ridicat de strategii de securitate cibernetică, pentru a avea o reprezentativitate cât mai bună a documentelor de acest

fel. Astfel, considerăm că, o viitoare direcție de cercetare necesar a fi aprofundată este cea a realizării unui studiu, asupra unui număr reprezentativ de strategii de securitate cibernetică, prin aplicarea metodei analizei de conținut.

Bibliografie:

1. Denscombe, M. (2010). The Good Research Guide. Berkshire: Open University Press.

2. DSN. (2019). National Cybersecurity Strategy 2019. Preluat pe Aprilie 24, 2023, de pe DSN: https://www.dsn.gob.es/eu/file/2989/download?token=EuVy2lNr

3. ENISA. (fără an). National Cyber Security Strategies - Interactive Map. Preluat pe Mai 12, 2023, de pe https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map

4. Guvernul României. (2022, Ianuarie 3). E-monitor. Preluat pe Aprilie 18, 2023, de pe Monitorul Oficial: https://monitoruloficial.ro/Monitorul-Oficial--PI--2Bis--2022.html

5. HM Government. (2022). National Cyber Strategy 2022. Preluat pe Martie 16, 2023, de pe https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf

6. ITU. (2021). Guide to Devepoling a National Cybersecurity Strategy. Preluat pe martie 16, 2023, de pe United Nations: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2021-ncs-guide.pdf

7. ITU Development Sector. (2021). Global Cybersecurity Index 2020. Preluat pe Aprilie 6, 2023, de pe ITUPublications: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

8. MAEC Estonia. (2019). Cybersecurity Strategy. Republic of Estonia. Preluat pe Martie 16, 2023, de pe https://www.mkm.ee/media/703/download

9. The White House. (2023, Martie 2). FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy. Preluat pe Aprilie 24, 2023, de pe The White House: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

MODIFICAREA PEISAJULUI AMENINȚĂRILOR CIBERNETICE DATORITĂ IMPLICĂRII GRUPĂRILOR DE CYBERCRIME ÎN RĂZBOIUL RUSO-UCRAINEAN

Claudia-Alecsandra GABRIAN[*]

Abstract:

A year after the start of the Russia-Ukraine war, the threat landscape influenced by cybercrime groups has seen further changes, and while some groups have declared allegiance to the Russian government, others have split over ideological differences or remained apolitical, opting to capitalize on geopolitical instability for financial gain. Affiliates of these cybercrime groups are actively involved in operations targeting entities and critical infrastructures of Ukraine, as well as countries that have declared their support for Ukraine, posing a threat to supporting states.

This paper aims to highlight how financially motivated cybercrime actors capitalize on geopolitical instability and how they aid and abet Russian state interests, either by accident or on purpose. The objectives of the paper are to identify those cybercrime groups that use the ransomware attack or advanced persistent threat methods to carry out major cyber-attacks and how they changed their attack method after the outbreak of the conflict. The research methods used are qualitative, through document analysis and netnography, and the interpretation of the results is a justification of the involvement of cybercrime groups in this war. Netnography is used to analyse how these cybercrime groups discuss on public forums and groups, such as on Telegram, where they share all the information between members.

In the NIS Directive are mentioned 7 sectors of economic activity that should be insured a common high level of security of networks and IT systems. In the main results of this research, we identify that cybercriminals groups attack all these main sectors, such as energy, transport, banking, infrastructures, health, and digital infrastructures. There were identified changes in malware-as-a-service and ransomware-as-a-service attacks, as well as changes in cybercriminal tactics and methods to orchestrate an attack. Also, when we refer to ransomware, LockBit, and CL0P groups are currently the most important cybercrime groups that carry out major cyber-attacks on countries from Europe. The information used in the research comes from open sources, mainly oriented toward those originating from the Russian language and those found in the public groups of the affiliates of these groups.

Keywords: *cyber-attacks, cybercrime groups, cyber threats, ransomware, Telegram.*

[*] Student doctorand, Facultatea de Istorie și Filosofie, Universitatea Babeș Bolyai, domeniul de expertiză este relații internaționale și studii de securitate, date de contact: claudiaalecsandra@yahoo.com

Introducere

Transformarea digitală a condus la apariția de noi amenințări în spațiul cibernetic, iar războiul dintre Rusia și Ucraina a reprezentat un facilitator pentru grupările de criminalitate cibernetică, pentru a lansa noi tipuri de atacuri și pentru a obține câștiguri financiare, de pe urma acestui conflict. La începutul războiului, unii actorii sponsorizați de stat acționau în numele serviciilor din cadrul guvernului rus, iar unele grupări de *ransomware-as-a-service* (RaaS), motivate financiar, lucrau sub protecția guvernului rus și ulterior, și-au declarat public loialitatea pentru acesta. Aceste grupări s-au împărțit în tabere de susținere a beligeranților și s-au alăturat unor campanii masive de atacuri cibernetice, asupra țărilor care au sprijinit Ucraina.

Din 2022 și până în prezent, atacurile *ransomware* au continuat să reprezinte principalele amenințări cibernetice, care au crescut atât în intensitate, cât și prin câștigurile financiare obținute. Grupările de criminalitate cibernetică folosesc platforma Telegram drept un instrument cheie de comunicare, pentru a discuta despre viitoare atacuri cibernetice, prin crearea unor grupuri, din care fac parte persoane care se aliniază intereselor și obiectivelor lor.

Lucrarea prezintă o perspectivă asupra modificării peisajului amenințărilor cibernetice, care include studiul grupărilor de *cybercrime* și modul în care acestea sunt implicate în conflict, dar și rolul pe care îl are Federația Rusă, în lansarea de atacuri cibernetice. De asemenea, în cadrul lucrării vor fi prezentate date, care să justifice impactul pe care grupările de *cybercrime* l-au avut asupra operatorilor de servicii esențiale.

Scopul cercetării este de a evidenția modul în care, grupările de *cybercrime* și-au schimbat modul de operare și au realizat atacuri cibernetice, orientate asupra companiilor și organizațiilor din Europa. Obiectivele cercetării sunt: 1) identificarea grupărilor implicate în acest conflict; 2) evidențierea motivației acestora, în realizarea de atacuri de tip *ransomware* în contextul războiului. Întrebarea de cercetare este următoarea: Cum a influențat războiul dintre Rusia și Ucraina strategia grupărilor de criminalitate cibernetică, cu privire la selectarea viitoarelor victime?

Din punct de vedere metodologic, a fost utilizată analiza documentară, având la bază date statistice și rapoarte de la instituții (EUROPOL, CISA, Consiliul Uniunii Europene, FBI) și de la companii (Microsoft, Kaspersky, TrendMicro, IBM, SOCRadar), având ca temă criminalitatea cibernetică, iar documentele analizate conțin informații,

care evidenţiază modul în care aceste grupări de criminalitate cibernetică operează, cât şi traiectoria pe care o au, cu privire la modificarea strategiei lor de atac. O altă metodă folosită este netnografia, pentru analizarea discuţiilor de pe platforma de comunicare Telegram. Pe această platformă sunt regăsite grupuri şi canale, unde membrii grupărilor de *cybercrime* discută metode de atac, postează foarte detaliat atacurile pe care le realizează şi fac referire la datele pe care le obţin. Utilizarea netnografiei este relevantă în acest context, deoarece grupările de *cybercrime* şi-au transferat activitatea de pe *dark web*, pe canelele de Telegram, care în momentul actual este considerat un instrument specializat în criminalitatea cibernetică.

Principala limită a cercetării este legată de fluxul mare de informaţii regăsite pe canalele de Telegram, fiind necesară verificarea acestora, din surse alternative, pentru a evita riscul dezinformării. O altă limită este legată de literatura academică de specialitate, având în vedere, că există un număr limitat de lucrări pe subiectul cercetat.

Cybercrime

Potrivit unui raport Kaspersky, criminalitatea cibernetică reprezintă o activitate desfăşurată în mediul online, unde majoritatea celor care întreprind astfel de acţiuni sunt criminali cibernetici sau hackeri, care vizează sau folosesc un computer, o reţea de computere sau un dispozitiv în reţea, pentru a obţine câştiguri financiare, în urma atacurilor cibernetice pe care le realizează (Kaspersky, 2019a).

Criminalii cibernetici sunt persoane sau grupuri care utilizează programe *malware* şi alte tipuri de *software*, pentru a realiza activităţi rău intenţionate asupra anumitor sisteme sau reţele digitale, având scopul de a fura informaţii sensibile ale companiilor, care conţin chiar şi datele personale ale indivizilor, de pe urma cărora, să obţină profit. Criminalii cibernetici accesează pieţele subterane, cum ar fi cele de pe *dark web*, pentru a tranzacţiona bunuri şi servicii rău intenţionate, cum ar fi instrumente de hacking sau date furate (Trend Micro, 2019).

Cel mai important act legislativ referitor la criminalitatea cibernetică este Convenţia de la Budapesta, care reprezintă şi primul tratat internaţional, prin care sunt incriminate infracţiunile comise în mediul online. Importanţa acestuia reiese din faptul că, cele mai relevante state în domeniul securităţii cibernetice sunt semnatare a acestuia. În prezent, sunt 68 de semnatari ai acestei convenţii, state din UE şi NATO, 21 de state au semnat sau urmează să adere, iar Ucraina este unul dintre aceşti semnatari. Obiectivul principal este de a urmări o

politică penală comună, care vizează protecţia societăţii împotriva criminalităţii informatice, în special prin adoptarea unei legislaţii adecvate şi încurajarea cooperării internaţionale (Council of Europe, 2014).

În februarie 2022, când a început conflictul dinte Federaţia Rusă şi Ucraina, grupările de cybercrime erau active în spaţiul cibernetic, derulând activităţi, precum vânzarea de date, obţinute ca urmare a derulării de atacuri cibernetice tip *ransomware.* Ascensiunea platformei Telegram a fost observată începând de atunci, deoarece au fost create grupuri unde se discutau detalii despre război şi despre atacurile cibernetice realizate, în context, fiind relevante următoarele grupuri: *Donbass Devushka* (transcris din limba rusă), *Ria Novosti* (transcris din limba rusă), *POKOT* (transcris din limba rusă). Analizând discuţiile din cadrul acestor grupuri, am observat că, infractorii cibernetici au coordonat atacuri cibernetice împotriva adversarilor de pe această platformă, unde au şi postat date cu privire la atacurile cibernetice realizate.

Răspândirea grupărilor de *cybercrime* în mediul digital a facilitat promovarea mesajelor de susţinere a acestora, iar cel mai relevant exemplu este gruparea de *ransomware Conti*. Aceasta şi-a promovat sprijinul pentru armata rusă şi administraţia rusă, enunţând faptul că, „dacă cineva va organiza un atac cibernetic sau orice altă activitate împotriva Rusiei, vor folosi toate resursele disponibile pentru a ataca infrastructurile critice ale unui inamic" (Bleih Adi, 2023). Gruparea CONTI este un exemplu menţionat în această secţiune, deoarece a fost una dintre cele mai active grupări de ransomware până în primăvara lui 2022, când a fost desfiinţată. Datorită legăturii confirmate a acesteia cu guvernul rus, a cunoscut schimbări semnificative la nivel organizaţional, care ulterior, au dus la scurgeri mari de date interne şi ulterior, la închiderea definitivă a serverelor acesteia pe serverul TOR (Warminsky Joe, 2022)

Peisajul ameninţărilor a fost modificat de către grupările de *cybercrime*, deoarece acestea şi-au schimbat modul de atac, în contextul războiului dintre Rusia şi Ucraina şi s-a creat o divizare în rândul acestor grupări, unele au fost în tabăra pro-rusă, iar altele în cea pro-ucraineană. Grupările care au continuat colaborarea cu guvernul rus au fost susţinute atât direct, cât şi indirect, iar cele care şi-au recunoscut loialitatea faţă de guvern, au primit şi mai mult sprijin pentru a se implica activ în operaţiuni care vizau derularea de atacuri cibernetice asupra

infrastructurii critice a Ucrainei şi a ţărilor care şi-au oferit sprijinul pentru Ucraina (Insikt Group, 2023).

Grupările de cybercrime

Grupările de *cybercrime* îşi concentrează atacurile asupra acelor sectoare şi organizaţii care reprezintă pentru ei ţinte uşoare şi despre care ei cred, că vor genera cel mai mare flux de date. Aceste grupări folosesc ofertele lor de atac drept un serviciu pentru alte grupări de criminalitate cibernetică, care pot ajuta la creşterea numărului de atacuri cibernetice (Steer Jason, 2023).

Atacul de tip *ransomware* reprezintă un *malware*, care împiedică sau limitează utilizatorii să-şi acceseze sistemul, prin criptarea fişierelor utilizatorilor până când se plăteşte o răscumpărare (Microsoft, n.d.). Există două categorii principale de ransomware: *ransomware locker* şi *crypto ransomware*. R*ansomware locker* afectează funcţiile de bază ale computerului, iar *crypto ransomware* afectează doar anumite fişiere care sunt criptate, iar pentru reobţinerea datelor, membrii grupărilor de *cybercrime* solicită o răscumpărare, pentru a transmite o cheie de decriptare (Trend Micro, 2011). Primele atacuri de ransomware moderne au fost raportate în Rusia, în 2005, iar din acel moment, acest tip de atac cibernetic a fost răspândit şi în exteriorul teritoriului, unde au fost dezvoltate din ce în ce mai multe tipuri. La momentul actual reprezintă cele mai avantajoase tipuri de atacuri cibernetice, datorită câştigurilor obţinute. (Kaspersky, 2019b)

Din punctul de vedere al analizării grupărilor de *cybercrime* după modelul de atac *ransomware*, acestea se evidenţiază în fiecare lună, prin numărul de atacuri pe care le realizează asupra anumitor sectoare şi ţări, astfel, fiind identificate 5 grupări de *ransomware*, care sunt top 5 în acest moment: *LockBit*, *CL0P*, *BlackCat*, *Royal* şi *BlackBasta* (SOCRadar, 2023a). În continuare vom analiza activitatea grupărilor LockBit şi CL0P.

De la începutul războiului dintre Rusia şi Ucraina, gruparea LockBit este responsabilă pentru peste o treime din toate atacurile *ransomware*, din a doua jumătate a anului precedent şi până în prezent (SOCRadar, 2023b). Prezenţa grupării LockBit a fost identificată pentru prima dată, în septembrie 2019 şi a devenit cel mai activ grup de ransomware, din 2022 şi până acum, aspect facilitat şi de destructurarea grupării Conti, în primăvara lui 2022. Din punct de vedere financiar, pierderile cauzate companiilor care au fost ţintele acestei grupări pot ajunge până la miliarde de dolari (SOCRadar, 2023c).

În prezent, gruparea LockBit rulează o versiune actualizată a malware-ului din 2022, care se numește LockBit Black sau LockBit 3.0. Gruparea se bazează pe o abordare bazată pe afiliați, iar aceștia vizează companii și organizații din aria operatorilor de servicii esențiale. LockBit își realizează propria promovare pe forumurile de criminalitate cibernetică, prin anunțuri de recrutare și concursuri, iar aceste inițiative atrag numeroși afiliați (SOCRadar, 2023d).

Această grupare respectă un tipar identificat și la alte grupări de criminalitate cibernetică, folosind limba rusă pentru a realiza atacuri, sistemele vizate fiind infectate doar dacă, limba sistemului de operare nu este cea rusă sau orice altă limbă înrudită cu rusa sau cu limbile oficiale ale statelor aliate Federației Ruse, spre exemplu araba (Siria) și tătara (Rusia) (SOCRadar, 2023e). De asemenea, în anumite situații este folosită identificarea locației, prin utilizarea adresei IP, iar dacă țara de origine nu se potrivește cu niciuna dintre țările specificate de atacatori, în codul sursă al *malware*-ului, atacul cibernetic trece la etapa următoare de infectare. Deși, acest grup de ransomware susține că nu se implică în politică, multe dintre țintele sale sunt țările aliate NATO și Ucrainei (SOCRadar, 2023f). Potrivit raportului realizat de către DarkFeed, până în acest moment, LockBit a realizat în total 1875 de atacuri, 740 de atacuri au avut loc în 2022, iar 548 în 2023 (DarkFeed, 2023a). Ceea ce se poate evidenția este faptul că, atacurile acestei grupări sunt în continuă creștere, iar menținerea frecvenței actuale a acestora poate genera depășirea numărului din 2022, pentru anul 2023.

Interviurile realizate cu membrii acestor grupări sunt rare, iar un interviu relevant este al scriitorul Dmitry Smilyanets, din cadrul *Recorded Future*. Acesta i-a adresat întrebări unui membru din gruparea LockBit, pentru a obține informații cu privire la metoda de atac a acestei grupări. Acest membru menționează că, din perspectiva lor, nu contează atât de mult criptarea datelor, cât importanța informațiilor criptate, deoarece pentru nedezvăluirea acestora, compania va plăti mai mult decât pentru decriptarea lor (Smilyanets Dmitry, 2021a). Un alt aspect important este legat de faptul că, membrii grupării sunt încrezători în sistemul propriu de securitate, însă, pentru a avea un back-up, au realizat mai multe copii de siguranță ale datelor criptate pe mai multe servere din diferite părți ale lumii, precum și copii de rezervă separate fizic de Internet (Smilyanets Dmitry, 2021b). Din 2021, afiliații grupări LockBit folosesc *dubla extorcare*, care se referă la criptarea datelor victimelor combinată cu exfiltrarea acelor date și solicitarea unei răscumpărări pentru nu fi publicate (CISA, 2023). Potrivit unui raport IBM, în anul

2022, extorcarea a reprezentat principala abordare asociată atacului tip *ransomware*. Europa a fost cea mai vizată regiune, reprezentând 44% din cazurile de extorcare observate, deoarece infractorii cibernetici au exploatat tensiunile geopolitice (IBM, 2023a).

Infractorii cibernetici vizează adesea cele mai vulnerabile industrii, întreprinderi şi regiuni. Spre exemplu, industria manufacturieră a fost cea mai extorcată în 2022 şi a fost cea mai atacată industrie pentru al doilea an consecutiv (IBM, 2023b). Industria manufacturieră reprezintă o ţinţă pentru aceste grupări, deoarece acestea deţin proprietate intelectuală, iar datele acestea sunt valoroase pentru aceştia, iar dat fiind faptul că, scopul lor principal este producţia şi livrarea în timp a produselor, îi determină să plătească răscumpărarea, pentru a nu exista întreruperi (Exalens, 2022). De la începutul anului 2022, au fost folosite instrumente şi tehnici care să ajute atacatorii de ransomware, să evolueze şi să lanseze atacuri asupra operatorilor de servicii esenţiale, ceea ce a dus la o creştere de 63,2% a grupărilor de ransomware, în primul trimestru al anului 2022. Peste 50 de grupări de ransomware au vizat şi compromis peste 1.200 de organizaţii, în prima jumătate a anului 2022 (TRENDMicro, 2023).

Gruparea CL0P a fost identificată pentru prima dată, la începutul anului 2019 şi este asociată cu gruparea TA505, conform MITRE ATT&CK Framework. TA505 este activ din 2014 şi este cunoscut pentru schimbarea frecventă a malware-ului şi pentru campaniile de ransomware, care implică funcţia CL0P (MITRE, n.d.). Această grupare deşi a început să fie activă din ianuarie 2022, doar în anul 2023 a realizat atacuri cibernetice, pe care le-a derulat asupra operatorilor de servicii esenţiale din Europa. La fel ca gruparea LockBit, atacurile cibernetice ale acestei grupări nu sunt executate la adresa sistemelor care utilizează limba rusă şi limbile înrudite sau cele ale statelor aliate Federaţiei Ruse (SentinelOne, n.d.).

Informaţiile relevante, pentru analizarea grupărilor LockBit şi CL0P au fost identificate pe grupurile de Telegram *SecurityLab.ru*, *Russian OSINT* şi *SecAtor*, unde s-au postat mai multe mesaje referitoare la atacurile realizate de acestea. Gruparea CL0P a atras atenţia prin faptul că, a realizat 70 de atacuri într-o săptămână, dintre care 42 într-o singură zi. Potrivit paginii Twitter *DarkFeed*, în luna martie, gruparea a realizat 98 de atacuri fiind clasificată pe cel de-al doilea loc, după LockBit, care a derulat 99 de atacuri (Twitter, Ido_cohen2 n.d.a). De asemenea, ultima statistică pentru luna iunie, publicată tot pe pagina Twitter *DarkFeed,* evidenţiază faptul că, gruparea CL0P ocupă primul loc în clasamentul

pentru cele mai multe atacuri realizate de grupările de ransomware, adică 89, iar gruparea LockBit ocupă locul 2, cu doar 67 de atacuri (Twitter, Ido_cohen2 n.d.b). De asemenea, potrivit unei analize *DarkFeed*, gruparea CL0P a realizat până în prezent 393 de atacuri, dintre care, doar 19 atacuri în anul 2022, iar de la începutul anului 2023 și până în prezent a realizat 247 de atacuri, ceea ce reprezintă o creștere exponențială a activității acestei grupări (DarkFeed, 2023b). Aceste rezultate sunt importante pentru a justifica faptul că, grupările de ransomware sunt foarte active și pentru a prezenta faptul, că realizează din ce în ce mai multe atacuri cibernetice. Dat fiind faptul că, aceste date sunt postate în timp real, ajută la monitorizarea acestor grupări și la observarea tendințelor pe care le au în fiecare lună, cu impact major în anumite zile, de asemenea, aceste date justifică selectarea acestor două grupări pentru subiectul cercetat.

Cea mai mare atenție asupra grupării CL0P a fost alocată în urma celui mai recent și important atac cibernetic realizat de aceasta, care a fost derulat prin exploatarea vulnerabilităților instrumentului de transfer fișiere MOVEit, care este folosit la nivelul mediului privat, pentru a partaja fișiere. Acesta a determinat, ca sute de companii să fie compromise, fiindu-le criptate date sensibile, iar gruparea a luat legătura direct cu ele pentru a discuta ei înșiși despre răscumpărare. În urma analizării atacului de către CISA, aceștia au fost prezenți încă din 2021, în sistemul MOVEit, au testat metode de atac de mai multe ori pe parcursul a doi ani, realizând atacurile efective în perioada sărbătorilor (CISA, 2023). Prin această abordare, atacatorii au exploatat vulnerabilitatea umană a potențialelor victime, acestea acordând atenție redusă tentativelor de manipulare în perioadele festive ale anului (Abrams Lawrence, 2023).

Potrivit unui raport al companiei de securitate cibernetică Thales, pe tema războiului dintre Rusia și Ucraina, sunt prezentate date care justifică faptul că, la începutul conflictului majoritatea atacurilor au afectat doar Ucraina. A fost identificată o tendință începând cu vara anului 2022, deoarece în țările europene au avut loc aproape la fel de multe atacuri cibernetice, câte au fost în Ucraina până în acel moment. Pentru anul 2023, în primul trimestru, majoritatea atacurilor au avut loc în interiorul Uniunii Europene. Cele mai importante sectoare afectate au fost administrația publică europeană, sectorul financiar, sectorul transporturilor, sectorul comunicațiilor electronice, sectorul energetic, sectorul sănătății și sectorul educației (THALES, 2023).

Guvernul rus şi ameninţările cibernetice

Actualul război se desfăşoară cu implicarea grupărilor de *cybercrime,* inclusiv cele aliniate intereselor strategice ale Federaţiei Ruse, ceea ce denotă, că tehnologia cibernetică poate să fie utilizată concomitent cu operaţiunile militare. Un exemplu este cel al evenimentelor din 2014, când Rusia a invadat Crimeea, iar Ucraina a fost victima unor atacuri cibernetice semnificative[1]. În Rusia sunt prezente grupări sponsorizate de guvern, care pot să îşi folosească capabilităţile cibernetice pentru a lansa atacuri majore, deoarece primesc protecţie în schimbul oferirii serviciilor lor guvernului, fiind susţinute să realizeze operaţiuni cibernetice la scară largă, astfel, atacuri asupra Ucrainei sunt justificate de către aceste grupări, deoarece acţionează în numele statului rus, pentru a obţine avantaje strategice sau financiare. (Górka, 2022).

Serviciile secrete ruse sunt cunoscute pentru implicarea lor în realizarea de atacuri cibernetice de tip *Advanced Persistent Threat* (APT), orientate către ţinte de nivel înalt, cum ar fi statele şi marile corporaţii, cu scopul de a fura informaţii sensibile, pe o perioadă lungă de timp (Kaspersky 2020). Grupările APT sponsorizate de guvernul rus folosesc capabilităţi cibernetice avansate şi vizează, în special, infrastructura critică a adversarilor, menţinându-şi prezenta uneori nedetectabilă în mediile ţintă. Toată activitatea este coordonată de serviciile ruse de informaţii, pentru a se asigura că toate cerinţele sunt îndeplinite, iar în prezent sunt dezvoltate capabilităţi cibernetice, care să răspundă obiectivelor de politică internă şi externă pe care guvernul rus le are (Rosengren, 2023a).

Implicarea serviciilor secrete ruse în realizarea de atacuri cibernetice conexate cu grupările pe care le susţin, a fost pregătită înaintea începerii războiului în 2022, deoarece un grup afiliat statului rus, sub numele de Nobelium sau APT29*,* recunoscut pentru relaţia cu Serviciul Rus de Informaţii Externe (SVR), a fost identificat încă din luna mai a anului 2021, în realizarea de atacuri care au vizat Ucraina. Obiectivele acestei grupări sunt compromiterea sistemelor şi serviciilor ucrainene de comunicaţii, transport, energie şi apărare (Schulze Matthias, 2023.a). Potrivit The Record, Nobelium este recunoscut pentru acţiuni de spionaj asupra entităţilor diplomatice ale ţărilor care fac parte

[1] Se pot menţiona atacuri DDoS asupra reţelelor de comunicaţii ucrainene, iar grupurile pro-ruse au realizat o serie de atacuri cibernetice, pentru a manipula alegerile prezidenţiale din Ucraina.

din NATO și UE („Grupul de hacking susținut de Kremlin pune un accent nou pe furtul de acreditări", n.d.).

Pe 23 februarie 2022, Agenția Rusă de Informații Militare (GRU) a lansat mai multe atacuri cibernetice, prin gruparea APT28, care au avut drept obiectiv ștergerea datelor pe care guvernul ucrainean le avea despre război. Acest tip de atac este un exemplu, pentru a justifica interesul Federației Ruse de a utiliza atacuri cibernetice, care să reprezinte pentru ei un avantaj tactic (Schulze Matthias. 2023.b). De asemenea, atacul Rusiei, din 24 februarie 2022, asupra sistemului de comunicații prin satelit Viasat, a avut drept scop oprirea comunicațiilor prin satelit între Ucraina și Europa, însă, acest atac nu le-a oferit un avantaj operațional, deoarece nu a reușit să împiedice operațiunile de comandă și control ucrainene (Schulze Matthias. 2023.c).

Pe grupul de Telegram *Russian OSINT* s-au postat informații, cu privire la modul în care Federația Rusă se raportează la spațiul cibernetic. În Federația Rusă sunt necesare noi abordări, care să fie adaptate la schimbările tehnologice, iar astfel, guvernul rus a reconfigurat modul de raportare la controlul și supravegherea spațiului cibernetic. Din punct de vedere legislativ, Rusia a refuzat să semneze Convenția de la Budapesta, însă, face în momentul actual schimbări legislative și normative, cu privire la modul de raportare la atacurile cibernetice și modul în care, fondurile criminalilor cibernetici pot să fie utilizate. Federația Rusă oferă noi oportunități, pentru actorii sprijiniți de stat, pentru lansarea de atacuri cibernetice și pentru accesarea ilegală a sistemelor statelor (Gritsenko et al., 2020).

Cu toate acestea, chiar dacă Rusia are capacități de a ataca diverse ținte în mediul online, nu au fost identificate operațiuni cibernetice ofensive, care să ofere Federației Ruse avantajul strategic pe câmpul de luptă, observându-se chiar o limitare a acestora. O operațiune cibernetică necoordonată cu alte operațiuni cibernetice, nu este suficientă pentru a obține avantaje strategice pe terenul de luptă. Astfel, sunt necesare atacuri cibernetice de mai multe tipuri, care să fie realizate concomitent, pentru a bloca sisteme ale anumitor instituții sau organizații de importanță strategică. Grupările APT reprezintă o amenințare în continuă dezvoltare la nivel global, printre cele mai importante obiective regăsindu-se spionajul, dezinformarea și sabotajul cibernetic. Motivația strategică a Federației Ruse este evidențierea puterii și catalogarea țării drept o super putere cibernetică (Rosengren, 2023b).

Potrivit Statista, în ultimii ani, rușii s-au confruntat cu un număr tot mai mare de amenințări cibernetice, cum ar fi breșe de securitate,

atacuri malware şi frauda digitală (Statista, 2023). Cele mai multe breşe de securitate din ţară au implicat pierderi de date personale, cum ar fi nume, e-mailuri sau adrese, ceea ce denotă faptul că, şi Federaţia Rusă a fost atacată de către grupările pro-ucrainene (Lewis James Andrew, 2022a).

În Rusia sunt regăsite cele mai avansate grupări de criminali cibernetici din lume, pe care guvernul rus le protejează, le oferă imunitate, însă, câştigurile sunt folosite în avantajul statului rus. Regulile după care se ghidează membrii acestor grupări sunt simple, aceştia nu au permisiunea să atace site-urile ruseşti, nu trebuie să compromită confidenţialitatea legăturii cu serviciile de informaţii ruse şi trebuie să împartă ceea ce câştigă. Unele dintre grupările de ransomware active au echipe specializate, care sunt împărţite în funcţie de sarcina pe care trebuie să o realizeze, fiecare sarcină fiind specifică cu metoda de atac şi cu selectarea victimei (Lewis James Andrew, 2022b).

Concluzii

Ransomware-ul este utilizat de către grupările de cybercrime, pentru a exploata victimele şi a devenit o constantă în rândul ameninţărilor cibernetice, mai ales prin metoda dublei extorcări. Atacurile, care au fost realizate în urma izbucnirii conflictului dintre Rusia şi Ucraina, au vizat şi operatorii de servicii esenţiale din Europa, iar infractorii cibernetici şi-au dezvoltat noi tipuri de atac, pentru a indisponibiliza accesul la date. Având în vedere elementele prezentate, putem concluziona că, fenomenul criminalităţii cibernetice nu a fost afectat de către război, ci a fost potenţat, date fiind dezvoltarea tehnologică a acestora şi amploarea atacurilor derulate.

Prin cercetarea realizată am răspuns la întrebarea de cercetare, deoarece am identificat grupările LockBit şi CL0P drept cele mai active grupări de ransomware. Aceste grupări şi-au orientat atenţia înspre ţări care sprijină Ucraina, iar divizarea acestor grupări în două tabere, nu face altceva decât să demonstreze faptul că, strategia lor de atac şi modul în care acţionează, au fost influenţate de către acest război, iar grupările şi-au dezvoltat tehnica de atac. De asemenea, implicarea guvernului rus în atacuri cibernetice asupra Ucrainei, este justificată prin grupările APT, care sunt sponsorizate de către serviciile secrete, din cadrul guvernului rus. Motivaţia acestor grupări fiind de natură strategică şi financiară, în scopul perturbării în primul rând, al sistemelor de importanţă strategică a Ucrainei şi a ţărilor din Uniunea Europeană. Aceste aspecte ne-au permis atingerea obiectivelor de cercetare. Grupările de cybercrime au o

prezenţă constantă în mediul online şi se constată faptul că, acestea au folosit platforma Telegram drept un instrument cheie de comunicare între ei şi adepţii grupărilor, pentru a conduce operaţiuni care să se alinieze intereselor şi obiectivelor lor. Prin analiza documentară au fost identificate elementele specifice grupărilor de cybecrime, cum ar fi: tipologia lor, ţintele pe care le au şi modul de operare. De asemenea, documentele strategice identificate şi analizele statistice au reprezentat surse de documentare, bazate pe cercetări empirice relevante subiectului cercetat. Prin netnografie, s-au putut contura idei despre modul în care, grupările de cybercrime sunt prezente pe un canal public de socializare, cum este Telegram. Această sursă deschisă oferă o multitudine de perspective, cu privire la ceea ce se discută între membrii grupărilor, în limba lor nativă, cât şi evidenţierea modului în care, aceste grupări au făcut o tranziţie de la grupurile de pe dark web, pe o platformă unde oricine poate să aibă acces la conţinutul lor. Cu siguranţă, unele mesaje regăsite sunt criptate şi nu pot să fie citite doar de către cei care au cheia de decriptare, însă, acestea au fost puţine, comparativ cu datele publicate încă de la începutul războiului. Grupurile de Telegram menţionate în lucrare sunt active şi acum, pot să fie accesate de către oricine, iar mesajele transmise despre război şi atacurile cibernetice realizate sunt postate în fiecare zi, cu o medie de până la 1.000 de postări pe zi.

Direcţiile viitoare de cercetare propuse s-ar putea orienta înspre extinderea cercetării, o analiză a atacului de tip ransomware, pentru a se analiza dacă acesta va continua să reprezinte o ameninţare majoră, pentru ţările care au sprijint Ucraina şi în anul 2023. De asemenea, o analiză a modului în care, grupările de cybecrime vor rămâne active sau nu pe canelele de Telegram, cât şi modul în care, îşi vor coordona activităţile viitoare. Astfel, platforma Telegram ar putea să fie analizată din punct de vedere al atractivităţii, pentru grupările de cybercrime, în comparaţie cu reţeaua TOR sau din punct de vedere al modificării tipului de activitate la nivelul acesteia – ce se vehiculează la nivelul grupurilor, care încă sunt active şi dacă mesajele şi conţinutul postat pe aceste canale este schimbat sau nu. De asemenea, o altă direcţie de cercetare ar putea fi analiza cantitativă a atacurilor cibernetice asupra ţărilor care sprijină Ucraina, unul dintre nivelurile luate în considerare fiind cel al sectorului de proveniență al infrastructurii victimă.

Referințe bibliografice:

1. Abrams Lawrence. 2023. „*Clop ransomware claims responsibility for MOVEit extortion attacks*" BleepingComputer. Accesat la data de 19.04.2023 la https://www.bleepingcomputer.com/news/security/clop-ransomware-claims-responsibility-for-moveit-extortion-attacks/

2. Antoniuk Daryna. 2023. „*Kremlin-backed hacking group puts fresh emphasis on stealing credentials*" Therecord.media. Accesat la data de 07.05.2023 la https://therecord.media/nobelium-hacking-group-stealing-credentials

3. BleepingComputer. 2023. „*The Great Exodus to Telegram: A Tour of the New Cybercrime Underground*" Accesat la data de 11.07.2023 la https://www.bleepingcomputer.com/news/security/the-great-exodus-to-telegram-a-tour-of-the-new-cybercrime-underground/

4. Bleih Adi. Lerner Dov. 2023 „*How Telegram became the battlefront of the Russia-Ukraine cyberwar*" n.d. Cybersixgill. Accesat la data de 25.04.2023 la https://cybersixgill.com/news/articles/telegram-russia-ukraine-cyberwar.\

5. Braue David. 2023. "*How Geopolitics Affects Cybersecurity*". Cybercrime Magazine. Accesat la data de 20.04.2023 la https://cybersecurityventures.com/how-geopolitics-affects-cybersecurity/

6. CISA. 2023. "*#StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 Vulnerability*" Accesat la data de 17.07.2023 la https://www.cisa.gov/sites/default/files/2023-07/aa23-158a-stopransomware-cl0p-ransomware-gang-exploits-moveit-vulnerability_8.pdf

7. CISA. 2023. "*CISA and Partners Release Joint Advisory on Understanding Ransomware Threat Actors: LockBit*" Accesat la data de 11.05.2023 la https://www.cisa.gov/news-events/alerts/2023/06/14/cisa-and-partners-release-joint-advisory-understanding-ransomware-threat-actors-lockbit

8. CISA. 2023. „*Understanding Ransomware Threat Actors: LockBit*" Accesat la data de 07.05.2023 la https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a

9. CISA. n.d. „*Combatting Cyber Crime*". Accesat la data de 18.04.2023 la https://www.cisa.gov/combatting-cyber-crime

10. Council of Europe 2014. "*The Budapest Convention (ETS No. 185) and its Protocols*" Accesat la data de 14.05.2023 la https://www.coe.int/en/web/cybercrime/the-budapest-convention

11. DarkFeed. 2023 „*CLOP-Overview*" Accesat la data de 11.07.2023 la https://darkfeed.io/2023/04/27/clop-overview/

12. DarkFeed. 2023. „Lockbit-Overview". Accesat la data de 11.07.2023 la https://darkfeed.io/2023/04/27/lockbit-overview/

13. DNSC. n.d. "*Informații generale despre NIS*" Accesat la data de 13.07.203 la https://dnsc.ro/pagini/informatii-generale-despre-nis

14. Eurojust. n.d. „*Cybercrime*". Accesat la data de 18.04.2023 la https://www.eurojust.europa.eu/crime-types-and-cases/crime-types/cybercrime

15. Exalens. 2023. "*A Troubling Trend Continues: Why Manufacturing Remains the Top Target for Cyber Criminals*" Accesat la data de 17.07.2023 la https://www.exalens.com/post/a-troubling-trend-continues-why-manufacturing-remains-the-top-target-for-cyber-criminals

16. FBI. n.d. „*The cyber threat*" Accesat la data de 02.05.2023 la https://www.fbi.gov/investigate/cyber

17. Glover Claudia. 2023. „*Russia's invasion of Ukraine has changed cybercrime forever, says report*" Accesat la data de 16.05.2023 la https:// techmonitor.ai/technology/cybersecurity/how-russia-ukraine-war-changed-cybercrime

18. Górka Marek. 2022. „*A Definitional Framework for Cyber Warfare. The Ukrainian Aspect*" Polish Political Science Yearbook 51: 1–14. Accesat la data de 18.05.203 la https://doi.org/10.15804/ppsy202272

19. Gritsenko Daris. Kopotev, Mikhail. 2020. "*Digital Russia Studies: An Introduction*". The Palgrave Handbook of Digital Russia Studies. Accesat la data de 20.05.2023 la https://cris.maastrichtuniversity.nl/en/publications/digital-russia-studies-an-introduction

20. Huntley Shane. 2023. „*Fog of war: how the Ukraine conflict transformed the cyber threat landscape*". Google. Accesat la data de 19.05.2023 la https:// blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/

21. IBM. 2023. „*IBM Report: Ransomware Persisted Despite Improved Detection in 2022*" Accesat la data de 12.07.2023 la https://newsroom. ibm.com/2023-02-22-IBM-Report-Ransomware-Persisted-Despite-Improved-Detection-in-2022

22. Insikt Group. 2023. *„Dark Covenant 2.0: Cybercrime, the Russian State, and the War in Ukraine"*. Accesat la data de 16.07.2023 la https://www. recordedfuture.com/dark-covenant-2-cybercrime-russian-state-war-ukraine

23. Intel471. 2022. „*Why cybercriminals are flocking to Telegram*". Intel471. Accesat la data de 28.04.2023 la https://intel471.com/blog/why-cybercriminals-are-flocking-to-telegram

24. INTERPOL. d.d. „*Cybercrime*". Accesat la data de 18.04.2023 la https://www.interpol.int/Crimes/Cybercrime

25. Iyengar Rishi. 2023. „*How the Ukraine War Has Changed Russia's Cyberstrategy"* Accesat la data de 14.05.2023 la https://foreignpolicy.com/ 2023/02/24/russia-ukraine-war-cybercrime-strategy/

26. Kaspersky. 2019 "*What is Ransomware?*". Accesat la data de 15.04.2023 la https://www.kaspersky.com/resource-center/threats/ ransomware

27. Kaspersky. 2019. „*What is cybercrime? How to protect yourself from cybercrime*" Accesat la data de 16.04.2023 la https://www.kaspersky.com/ resource-center/threats/what-is-cybercrime

28. Kaspersky. 2020. „*What Is an Advanced Persistent Threat (APT)?*" Accesat la data de 12.07.2023. https://www.kaspersky.com/resource-center/ definitions/advanced-persistent-threats

29. KELA. 2023. „*Telegram: How a messenger turned into a cybercrime ecosystem by 2023*". Accesat la data de 10.05.2023 la https://ke-la.com/resource/telegram-how-a-messenger-turned-into-a-cybercrime-ecosystem-by-2023/

30. Lewis James Andrew. 2022. "*A Dangerous Moment for Russian Cybercrime May Get Worse*". Accesat la data de 11.07.2023 la https://www.barrons.com/articles/a-dangerous-moment-for-russian-cybercrime-may-get-worse-51644936090

31. Lewis James Andrew. 2022. "*Cyberwar and Ukraine*". CSIS. Accesat la data de 08.07.2023 la https://www.csis.org/analysis/cyber-war-and-ukraine

32. Martin Alexander. 2023. „*Ransomware group Clop issues extortion notice to 'hundreds' of victims*" Therecord.media. Accesat la data de 06.05.2023 la https://therecord.media/clop-extortion-hundreds-organizations-moveit-vulnerability

33. Microsoft. n.d. „*Ce este ransomware-ul?*" Accesat la data de 16.04.2023 la https://www.microsoft.com/ro-ro/security/business/security-101/what-is-ransomware

34. MITRE. n.d. „*TA505*". Accesat la data de 12.07.2023 la https://attack.mitre.org/groups/G0092/

35. Positive Technologies. 2022. "*Cybercriminal market in Telegram*". Accesat la data de 12.07.2023 la https://www.ptsecurity.com/ww-en/analytics/cybercriminal-market-in-telegram/

36. Rosengren Oscar. 2023. "*The Five Bears: Russia's Offensive Cyber Capabilities*" Accesat la data de 10.07.2023 la https://greydynamics.com/the-five-bears-russias-offensive-cyber-capabilities/

37. Schulze Matthias. 2023. "*Cyber Operations in Russia's War against Ukraine*". Accesat la data de 04.06.2023 la https://www.swp-berlin.org/10.18449/2023C23/

38. SentinelOne. n.d. "*CL0P*". Accesat pe 22.04.2023 la https://www.sentinelone.com/anthology/clop/

39. Smilyanets Dmitry. 2021. „*An interview with LockBit: The risk of being hacked ourselves is always present*" Therecord.media. Accesat pe 05.05.2023 la https://therecord.media/an-interview-with-lockbit-the-risk-of-being-hacked-ourselves-is-always-present

40. SOCRadar. 2023. „*Dark Web Profile: LockBit 3.0 Ransomware*" Accesat pe 27.04.2023 la https://socradar.io/dark-web-profile-lockbit-3-0-ransomware/

41. Statista. 2023. "*Information security and cyber crime in Russia - statistics & facts*" Accesat pe 08.05.2023 la https://www.statista.com/topics/7335/informatica-securitatea-si-crima-cibernetica-in-russia/#topicOverview23

42. Steer Jason. 2023. „*More DDoS, More Leaks: Where Ransomware is Headed in 2023*" Infosecurity magazine. Accesat pe 12.07.2023 la https://www.infosecurity-magazine.com/blogs/ddos-leaks-ransomware-2023/

43. THALES. 2023. „*FROM UKRAINE TO THE WHOLE OF EUROPE: THE CYBER CONFLICT ENTERS A NEW STAGE*” 2023. Thales Group. Accesat pe 11.07.2023 la https://www.thalesgroup.com/ro/hwl-alalm/security/press_release/din-ucraina-nivelul-intregii-europe-conflictul-cibernetic-intra

44. TRENDMicro. 2011. “*Ransomware Definition*” Accesat pe 16.05.2023 la https://www.trendmicro.com/vinfo/us/security/definition/ransomware

45. TRENDMicro. 2023. „*5 Types of Cyber Crime Groups*”. Accesat pe 14.05.2023 la https://www.trendmicro.com/en_us/ciso/23/e/cyber-crime-group-types.html

46. TRENDMicro. 2019. “Cybecriminals”. Accesat pe 29.04.2023 la https://www.trendmicro.com/vinfo/us/security/definition/cybercriminals.

47. Twitter – Dark Feed. 2023. “*Top active #ransomware groups june*” Accesat pe 10.07.2023 la https://twitter.com/ido_cohen2/status/1675905937524109325?S=20

48. Twitter - DarkFeed 2023. *„#Ransomware groups statistics March 2023*”. Accesat pe 10.07.2023 la https://twitter.com/ido_cohen2/status/1642218169765883907?s=20

49. Warminsky Joe. 2022. „*Notorious cybercrime gang Conti 'shuts down,' but its influence and talent are still out there*”. Therecord.media. Accesat la 05.05.2023 la https://therecord.media/conti-ransomware-gang-digital-infrastructure-shut-down

TERORISMUL ÎN AFRICA
ORGANIZAȚII TERORISTE PE TERITORIUL AFRICII

Alina (c. Tianu) IOVAN*

Abstract:

Africa has become a haven for jihadist terrorist organisations that run covers the whole range from local groups fighting to avenge political and economic grievances to splinter groups affiliated with the Islamic State in Iraq and Syria (ISIS) or al-Qaeda.

Jihadist groups that have moved out of Syria and into the Sahel region or Africa after ISIS was defeated have only increased the terrorist threat in the region.

Terrorists and violent extremists, including Da'esh, al-Qa'ida and their affiliates, have exploited instability and conflict to increase their activities and escalate attacks across the African continent.

The vast Sahel region has become home to some of the most active and deadly terrorist groups and it is essential to better understand the links between organised crime and terrorism.

Nearly half of the world's victims of terrorism are African, and organised crime is increasingly widespread.

In a hyper-connected world, the spread of terrorism in Africa is not just a concern for African Member States, but for all. Combating international terrorism requires effective multilateral efforts.

Keywords: *terrorism, Africa, islamic organisations.*

Introducere

În prezentul articol am abordat tema terorismului pe continentul african, precum şi a organizaţiilor teroriste care acţionează pe teritoriul Africii.

Obiectivele de cercetare au reieşit după formularea următoarelor întrebări de cercetare:

Care este intensitatea mişcărilor teroriste în această arie geografică? (2) Este Africa noul nucleu al grupărilor teroriste? (3) Ce este diferit la violenţa extremistă islamistă?

* Academia Națională de Informații „Mihai Viteazul”, Facultatea de Informații, masterand anul I –MICT, Bucureşti, email: iovan.alina@animv.eu

Instabilitatea economică și conflictele de pe teritoriul african (ex. marginalizarea grupurilor etnice de către stat, terorismul, crima organizată și extremismul violent, insecuritatea alimentară) au un impact major asupra securității mondiale prin efecte colaterale, cum ar fi migrația, criminalitatea transnațională și răspândirea actelor de terorism.

Africa a devenit un refugiu pentru organizații teroriste jihadiste, de la grupuri locale, care luptă pentru a răzbuna nemulțumiri politice și economice, până la grupări disidente afiliate cu Statul Islamic, în Irak și Siria (ISIS) sau al-Qaeda.

Grupările jihadiste, care au părăsit Siria și s-au mutat în regiunea Sahel sau în alte zone din Africa, după ce ISIS a fost învins, nu au făcut decât să sporească amenințarea teroristă în regiune.

Teroriștii și extremiștii violenți, inclusiv ISIS, al-Qaeda și afiliații acestora, au exploatat instabilitatea și conflictele pentru a-și spori activitățile și pentru a intensifica atacurile pe întreg continentul african.

Metodologia cercetării

În centrul metodologiei de cercetare utilizate stau analiza de conținut și sinteza**.**

Acest articol este adaptat, în principal, la o cercetare proprie, pe baza unor date interpretate în mod sistematic, cantitativ, cu o metodologie cât mai apropiată de cerințele științifice.

De asemenea, are ca fundament o analiză bazată pe literatura de specialitate, utilizând materiale din surse primare și secundare, cum ar fi articole, statistică și materiale video.

Metoda aleasă este potrivită, deoarece am urmărit descrierea comprehensivă a unor evenimente și analiza unor teorii de referință în domeniul ales, precum și determinarea cauzelor sau explicarea unor eventuale evoluții. Scopul selectării surselor utilizate în acest articol este, în primul rând, stabilirea unui context istoric și situațional detaliat, în ceea ce privește natura organizațiilor teroriste, care operează pe continentul african și în al doilea rând, explorarea modului în care, acestea au ajuns să se suprapună una cu cealaltă, de-a lungul unei perioade de timp.

Astfel, voi putea să ofer o relatare istorică a evoluției organizațiilor individuale, detaliind punctele-cheie, în care acestea au devenit afiliate și rezultatele ulterioare ale acestor decizii asupra organizațiilor lor.

În plus, am creat o imagine a reţelei de islamişti, inclusiv a militanţilor (seniori), a clericilor radicali, ideologi, simpatizanţi şi recrutori în estul, centrul şi sudul ţării.

Astfel, voi documenta profilul, activităţile şi legăturile acestor persoane, precum natura şi contextul relaţiei dintre ei şi alţi membri. Prin urmare, măsurile-cheie[1] ale analizei acestui articol vor fi relaţiile dintre actorii, din organizaţii, şi rolurile lor în influenţarea ideologiei şi strategiei organizaţiilor.

Astfel, scopul acestui articol nu este de a nega factorii locali care contribuie la creşterea insurgenţelor islamiste, ci acela de a explica ascensiunea bruscă a activităţilor grupărilor teroriste pe continentul african, ceea ce conduce la întrebări cu privire la măsura în care aceste insurgenţe au fost propulsate de factori transnaţionali.

Evoluţia francizei de terorism global: De la al-Qaeda la Statul Islamic

Conform Departamentului de Stat al SUA, 10 martie 2021, Statul Islamic, din Irak şi Siria (ISIS), a anunţat lansarea Provinciei Statului Islamic din Africa Centrală (ISCAP), în aprilie 2019, pentru a promova prezenţa elementelor asociate ISIS în cadrul Africii Centrale, de Est şi de Sud.

Potrivit studiului Global Terrorism Index 2023, regiunea Sahel din Africa Subsahariană este în prezent epicentrul terorismului, fiind zona cea mai afectată şi reprezentând 43% din decesele cauzate de terorism la nivel global, cu 7% mai mult decât în anul precedent.

Patru dintre cele zece ţări, cu cele mai mari creşteri ale numărului de decese cauzate de terorism au fost, de asemenea, din Africa Subsahariană: Niger, Mali, Republica Democrată Congo şi Burkina Faso.

[1] Cadrul conceptual, tehnica analitică, contextualizare.

							DESCRIPTION
1	COUNTRY	PAKISTAN	PROVINCE	BALOCHISTAN PROVINCE	DEATHS	195	Gunmen bombed and shot at two Frontier Corps buildings in a coordinated attack
	DATE	2/2/22	GROUP	BALOCHISTAN LIBERATION ARMY (BLA)			
2	COUNTRY	SYRIA	PROVINCE	AL-HASAKAH GOVERNORATE	DEATHS	154	At least 200 assailants attacked Al-Sina prison, driving two explosive-ladens truck bombs into the outside wall of the prison before gunmen then stormed the facility as a riot took place inside. The attack lasted ten days until the Syrian Democratic Forces (SFD) announced they had regained control of the prison. At least 154 SDF members were killed. Islamic State (IS) claimed responsibility for the attack.
	DATE	20/1/22	GROUP	ISLAMIC STATE (IS)			
3	COUNTRY	SOMALIA	REGION	BANAADIR REGION	DEATHS	120	Two car bombs killed at least 120 people and wounded 300 outside the education ministry building. Al-Shabaab claimed responsibility for the attack, saying that the ministry was responsible for a 'war on minds' that has removed Islam from schools and recruits students into militias.
	DATE	29/10/22	GROUP	AL-SHABAAB			
4	COUNTRY	BURKINA FASO	PROVINCE	SAHEL REGION	DEATHS	116	Gunmen killed at least 116 civilians in an attack on a village. No group had claimed responsibility at the time of writing, but jihadists operate in the area.
	DATE	12/6/22	GROUP	UNKNOWN - JIHADISTS			
5	COUNTRY	MALI	PROVINCE	MOPTI REGION	DEATHS	110	Gunmen killed at least 110 civilians in attacks on several villages. No group had claimed the attack at the time of writing, but jihadists operate in the region.
	DATE	19/6/22	GROUP	UNKNOWN - JIHADISTS			
6	COUNTRY	MALI	REGION	GAO REGION	DEATHS	100	Gunmen killed approximately 100 Jamaat Nusrat Al-Islam wal Muslimeen (JNIM) fighters in Gao region. The battle lasted for approximately 24 hours and local media outlets said that there were casualties on both sides. Islamic State (IS) claimed responsibility attributing the attack to its 'Sahel Province'.
	DATE	7/12/22	GROUP	ISLAMIC STATE (IS)			
7	COUNTRY	SOMALIA	REGION	HIRSHABELLE STATE	DEATHS	59	Gunmen killed an unspecified number of Burundian soldiers during an attack on an African Union. Al-Shabaab claimed responsibility for the attack, claiming to have killed 59 soldiers, but authorities had not released details on casualty numbers at the time of writing.
	DATE	3/5/22	GROUP	AL-SHABAAB			
8	COUNTRY	PAKISTAN	REGION	PAKHTUNKHWA PROVINCE	DEATHS	56	A suicide bombing killed at least 56 people and injured over 190 others in an attack on a Shia mosque. Islamic State - Khorasan Province (ISK) claimed responsibility.
	DATE	4/3/22	GROUP	ISLAMIC STATE - KHORASAN PROVINCE			
9	COUNTRY	AFGHANISTAN	PROVINCE	KABUL PROVINCE	DEATHS	50	A bomb killed more than 50 civilians and wounded an unspecified number of others at a mosque. No individual or group had claimed responsibility for the attack at the time of writing, but based on the target, tactic, and location, Islamic State - Khorasan Province (ISK) was probably responsible.
	DATE	29/4/22	GROUP	ISLAMIC STATE - KHORASAN PROVINCE			
10	COUNTRY	AFGHANISTAN	PROVINCE	BALKH PROVINCE	DEATHS	50	A bomb killed 50 civilians and wounded at least 100 more in an attack on a mosque during prayers. Islamic State - Khorasan province (ISK) claimed responsibility.
	DATE	21/4/22	GROUP	ISLAMIC STATE - KHORASAN PROVINCE			

							DESCRIPTION
11	COUNTRY	NIGERIA	PROVINCE	BORNO STATE	DEATHS	50	Gunmen killed at least 50 civilians after they accused them of informing on their movements to security forces. Islamic State West Africa (ISWA) claimed responsibility, saying it had targeted "spies".
	DATE	22/5/22	GROUP	ISLAMIC STATE WEST AFRICA (ISWA)			
12	COUNTRY	BURKINA FASO	REGION	KOMPIENGA PROVINCE	DEATHS	50	Gunmen killed at least 50 civilians in an armed attack. No group had claimed the attack at the time of writing but jihadists operate in the area.
	DATE	25/5/22	GROUP	UNKNOWN - JIHADISTS			
13	COUNTRY	MALI	REGION	GAO	DEATHS	42	Gunmen killed 42 soldiers and wounded 22 people in armed attack. No individual or group claimed the attack at the time of writing, but jihadists operate in the area
	DATE	7/8/22	GROUP	UNKNOWN - JIHADISTS			
14	COUNTRY	NIGERIA	REGION	BORNO	DEATHS	40	Gunmen killed at least 40 civilians in an armed attack. No group had claimed responsibility at the time of writing, but local media outlets said that Boko Haram was responsible.
	DATE	22/5/22	GROUP	BOKO HARAM			
15	COUNTRY	BURKINA FASO	CITY	SAHEL REGION	DEATHS	37	Gunmen killed 27 soldiers and ten civilians while they were travelling to a nearby town in a supply convoy. Jamaat Nusrat Al-Islam wal Muslimeen (JNIM) claimed responsibility.
	DATE	26/9/22	GROUP	JAMAAT NUSRAT AL-ISLAM WAL MUSLIMEEN (JNIM)			
16	COUNTRY	BURKINA FASO	REGION	CENTRE-NORD REGION	DEATHS	35	A roadside bomb killed 35 civilians and wounded 37 others in an attack on a supply convoy. No group had claimed responsibility at the time of writing, but jihadists operate in the area.
	DATE	5/9/22	GROUP	UNKNOWN - JIHADISTS			
17	COUNTRY	MALI	REGION	GAO REGION	DEATHS	70	Gunmen killed an unconfirmed number of civilians allegedly affiliated with Islamic State (IS) in coordinated attacks on villages in Gao reigon. No group had claimed responsibility at the time of writing but local media outlets said that Jamaat Nusrat Al-Islam wal Muslimeen (JNIM) was responsible.
	DATE	5/12/22	GROUP	JAMAAT NUSRAT AL-ISLAM WAL MUSLIMEEN (JNIM)			
18	COUNTRY	AFGHANISTAN	CITY	KABUL PROVINCE	DEATHS	30	At least seven gunmen and five suicide bombers mounted an attack on a Hindu festival in a Hindu temple. The attack lasted at least five hours when Taliban forces announced they had regained control of the temple. There were conflicting details about casualties but at least 30 civilians and Taliban fighters were killed and several others wounded. Islamic State - Khorasan Province claimed responsibility for the attack.
	DATE	18/6/22	GROUP	ISLAMIC STATE - KHORASAN PROVINCE			
19	COUNTRY	MALI	REGION	GAO REGION	DEATHS	30	Gunmen killed around 30 civilians in an armed attack. No group had claimed responsibility at the time of writing, but local media outlets said that Islamic State (IS) was probably responsible.
	DATE	9/9/22	GROUP	ISLAMIC STATE (IS)			
20	COUNTRY	NIGERIA	REGION	BORNO STATE	DEATHS	30	Gunmen killed at least 30 civilians and wounded six others in an armed attack. No group had claimed responsibility at the time of writing, but local media outlets said that Islamic State West Africa (ISWA) was responsible.
	DATE	21/5/22	GROUP	ISLAMIC STATE WEST AFRICA (ISWA)			

Figura 1: Incidente teroriste – 20 cele mai fatale atacuri teroriste în 2022 (sursa Global Terrorism Index 2023)

În anii care au urmat, au fost înfiinţate două organizaţii notabile de al-Qaeda: Uniunea Instanţelor Islamice (ICU), precursoarea organizaţiei al-Qaeda, al-Shabaab, în Somalia, în 2006, şi al-Qaeda în Maghrebul Islamic, în 2007, cu sediul în principal, între graniţele din sudul Algeriei şi nordul Mali.

Într-o perioadă scurtă de timp, ICU şi predecesori (inclusiv o insurgenţă islamică radicală, cunoscută sub numele de al-Itihaad al-Islamiyah, fondată în 1984) au reprezentat o ameninţare suficient de mare, astfel încât, să atragă Statele Unite ale Americii, Etiopia şi întreaga regiune, într-o intervenţie militară în Somalia.

Până în 2019, Africa Subsahariană a depăşit Africa de Nord şi Orientul Mijlociu, în ceea ce priveşte numărul de victime, ca urmare a atacurilor teroriste, comise de islamişti militanţi (Indicele Terorismului Global, 2022).

Această schimbare a coincis cu prăbuşirea califatului fizic al Statului Islamic, în Irak şi Siria, care a determinat gruparea să înceapă, să facă deschideri regionale în Africa.

Procedând astfel, Statul Islamic (SI) a trebuit să se confrunte cu membrii devotaţi al-Qaeda şi cu afiliaţii săi, ceea ce a dus la confruntări mortale, dar a reuşit, de asemenea, să capitalizeze pe facţiuni emergente, insurgenţi aspiranţi ai SI şi reţele extremiste.

Figura 2: Membri ai grupării SI în Africa (sursă foto: RFI)

Între 2015 şi 2019, SI a dobândit patru afiliaţi în regiunea subsahariană Africa şi Sahel: în Mali, Niger şi Burkina Faso, Statul Islamic în Marea Saharei; în Nigeria, Provincia Statului Islamic din Africa de Vest; în Somalia, Statul Islamic în Somalia (ISS); în Republica Democrată Congo (RDC) şi Mozambic, Statul Islamic Central African Province (ISCAP).

Ca urmare, începând din 2015, numărul de incidente care au implicat lupte cu forțele de securitate, explozii și violențe împotriva civililor au fost în continuă creștere, iar anul 2021 a fost cel mai mortal an în întreaga regiune Sahel, în vestul, centrul și estul Africii (Full dashbord results, 2020).

Somalia a fost, din punct de vedere istoric, punctul central al extremismului islamic în Africa de Est. De la prima rețea al-Qaeda, din anii 1990, până la al-Shabaab în prezent, Africa de Est și în special Somalia au fost esențiale pentru mișcarea jihadistă globală, cu precădere pentru al-Qaeda.

Pe fondul incursiunilor SI pe întreg continentul, Ayman al-Zawahiri a declarat în 2018:

Să stabilim în Africa de Est o fundație solidă pentru islam și jihad, pentru a sprijini Umma sa de pretutindeni și pentru a pedepsi pe cei care îi încalcă sanctuarele și îi atacă sfințeniile .... Frații mei, mujahedinii din Africa de Est! Trebuie să înțelegeți marea responsabilitate care se află pe umerii voștri. Voi nu duceți un război local, ci vă confruntați cu o campanie cruciată modernă și a aliatului său, Israel, care încearcă să cucerească controlul asupra Cornului Africii și a capului Nilului, și de a sufoca jihadul islamic în Africa de Est și în restul lumii (ICSR Report, 2021).

Figura 3: Ayman al-Zawahiri a fost cel mai important purtător de cuvânt și ideolog al al-Qaeda (sursă foto: BBC)

Cu toate acestea, declarația recentă de înființare a unei organizații oficiale a SI în Africa Centrală și de Est vine ca o surpriză, deoarece nici RDC și Mozambic nu au legături puternice cu grupările islamice tradiționale.

În scopul de a ajunge la o mai bună înţelegere a incursiunii SI în Africa subsahariană şi natura internaţională a militanţilor din regiune, am încercat, prin prezenta lucrare, să analizez ecosistemul islamist militant din estul Africii de Nord şi din estul, centrul şi sudul Africii de Sud.

Deslușind istoricul şi traiectoria ideologică a reţelelor militante transfrontaliere din regiune, articolul detaliază centralitatea Somaliei, ca bază al militantismului din regiune, de unde acesta s-a răspândit, din ţară în ţară.

Cazul principal, pentru studiul afilierilor teroriste globale înainte de apariţia Statului Islamic a fost al-Qaeda, care a fost considerată, pe scară largă, ca o organizaţie ierarhică, cu o conducere superioară foarte implicată în multe aspecte cheie ale organizaţiei, inclusiv în ceea ce priveşte filialele sale.

Studiile, care detaliază legăturile dintre al-Qaeda şi filialele sale africane, demonstrează măsura în care, conducerea superioară a al-Qaeda a modelat identităţile ideologice, capacităţile operaţionale şi structura de conducere a filialelor grupului (Wu, Cartleton, Davies, 2014, p. 57-73).

În acest fel, al-Qaeda a dezvoltat criterii şi procese de afiliere care, de obicei, necesitau ca grupurile subsidiare să îndeplinescă simultan următoarele condiţii:

1) să fie ierarhic structurate, cu o conducere formată din veterani, cu legături personale cu conducerea superioară a al-Qaeda;

2) grupul să aibă un lider stabilit şi acesta să încheie un angajament de credinţă faţă de al-Qaeda şi Osama bin Laden şi, ulterior, să primească un răspuns din partea lui al-Zawahiri sau bin Laden, care să recunoască angajamentul pentru a stabili o afiliere oficială;

3) să îşi însuşească marca al-Qaeda, pentru a instiga la atacuri împotriva Occidentului şi Europei, cunoscute şi sub numele de *inamicul îndepărtat*. Al-Qaeda s-a bazat, din ce în ce mai mult, pe abilităţile afiliaţilor săi de a instiga la atacuri împotriva ţintelor occidentale, pentru a-şi susţine prezenţa şi notorietatea la nivel global, mai ales că, a început să sufere pierderi majore după 11 septembrie 2001, după invazia americană din Afganistan şi Irak. Gruparea a trecut la o abordare de tip *organizată lejer, cu o conducere centrală*, care a supravegheat în mare parte afilierile globale autonome.

În mod similar, SI, în urma victoriei sale teritoriale califatul teritorial a optat pentru aceeaşi abordare organizatorică, asortată cu un interes, în creştere, pentru afilierea la marca jihadistă şi de notorietate

din partea facțiunilor și insurgenților lipsite de drepturi. În prezent, filialele africane ale SI joacă un rol-cheie în susținerea narațiunii de reziliență a grupului, în ciuda eșecurilor majore din Orientul Mijlociu.

Spre deosebire de al-Qaeda, care părea să aibă un proces de verificare riguros, inițial, SI părea dornic să sprijine orice afiliat aspirant. Ca urmare, saturația a necesitat un anumit nivel de compartimentare regională, pentru a conține multitudinea de actori ai SI, mai ales în astfel de regiuni care se suprapun, precum Africa de Vest și Sahel. Cu toate acestea, în ultimii ani, SI de asemenea, a avut nevoie de timp pentru a recunoaște promisiunile facțiunilor emergente, transformându-le, în esență, în *afiliați aspiranți.* Chiar dacă recunoașterea promisiunilor rămâne un criteriu fundamental pentru afilierea unui grup fie al-Qaeda, fie SI, este demn de remarcat faptul că, SI este o organizație distinctă, cu propriile sale procese de adoptare a afiliaților (Daniel Holbrook, 2013, p. 5-7).

Afiliații Al-Shabaab în Kenya și Tanzania

Al-Shabaab și-a manifestat, pentru prima dată, intenția de a-și extinde teroarea dincolo de Somalia, cu două atentate sinucigașe cu bombă din proiecție a Cupei Mondiale FIFA din Kampala, Uganda, în 2010. Atacul a fost instigat de către Batalionul Saleh Ali Saleh Nabhan, un grup militar, aripa militară a al-Shabaab, numită în onoarea liderului organizației al-Qaeda din estul Africii, Saleh Nabhan, un cetățean kenyan, care a promis pentru prima dată al-Qaeda, în numele al-Shabaab în 2008. Acest atac ar fi prima desfășurare a unui batalion într-o misiune externă, o operațiune care a provocat 74 de morți și 85 de răniți (ICSR Report, 2021).

Ulterior, al-Shabaab a căutat să găsească o modalitate de a-și susține prezența și expansiunea, în țările vecine cu unități de elită, afiliate, și rețele în Kenya și Tanzania. Ceea ce este unic, complex și totuși crucial de înțeles despre aceste structuri diferite este că, acestea sunt foarte fluide și se suprapun în diverse aspecte, ceea ce face ca dificil să se distingă natura legăturilor lor, una față de cealaltă și cu al-Shabaab. Acest lucru necesită o explorare în profunzime a vieții anumitor persoane, pentru a cartografia mișcarea inspirației ideologice prin Africa de Est și semnificația anumitor incidente, care au condus până la apariția ISCAP în RDC și Mozambic.

Al-Shabaab are două afiliate principale, în Kenya: al-Hijra şi Jaysh Ayman.

Figura 4: Hartă Kenya (sursă foto: Britannica)

Ambele joacă roluri distincte, în susţinerea al-Shabaab. Al-Hijra operează o reţea sofisticată de radicalizare şi recrutare, în timp ce, Jaysh Ayman instigă la atacuri teroriste în numele său, în colaborare cu militanţii al-Shabaab din Somalia. Al-Hijra şi Jaysh Ayman au jucat un rol crucial în extinderea ideologiei şi a operaţiunilor al-Shabaab dincolo de Somalia, asigurându-se, că atacurile ar putea avea loc în Kenya, chiar şi în timp ce ideologia a continuat să fie propagată şi mai la sud, în Tanzania.

Al-Hijra este o reţea de radicalizare şi recrutare cu sediul în Kenya şi în Tanzania. Unul dintre membrii fondatori şi liderii săi a fost Ahmad Iman Ali, un cleric de la moscheea Riyadha din Pumwani. Ali a fost un membru vechi şi lider de tineret al moscheii, care a finanţat şi contribuit atât la aceasta, cât şi la construirea altor moschei din Majengo (J. Stig Hansen, 2019, p. 128).

Până în 2007, Ali a acumulat suficient capital social pentru a înlătura conducerea existentă, ceea ce a deschis calea pentru Aboud Rogo şi Samir Khan, să ţină predici de promovare a jihadului la Riyadh, moscheea Riadyad. Rogo a fost foarte influent în alte câteva moschei, inclusiv Madrasa Sirajul Munir, din Mtwapa (Kenya) şi Masjid Musa şi Masjid Sakina din Mombasa. Schimbarea conducerii a fost percepută de comunitatea locală, ca un eşec al guvernului autorităţilor locale de a interveni, într-o schimbare către extremismul violent. Aceasta a fost privită, de asemenea, şi ca o ciocnire între generaţii, care a împins

conducerea mai veche să își înființeze propriile moschei moderate în Majengo.

În 2008, Ali a înființat ceea ce a fost cunoscut sub numele de Centrul Tineretului Musulman (MYC), care a devenit o platformă majoră de propagandă jihadistă, pentru radicalizarea și recrutarea de kenyeni, pentru a se alătura al-Shabaab în Somalia.

Abubakar Sheriff Ahmad, cunoscut și sub numele de Makaburi, a făcut parte din cercul de apropiați ai lui Ali și a devenit unul dintre principalii facilitatori de recrutare a kenyenilor pentru al-Shabaab. Ali însuși a părăsit Kenya pentru a se alătura al-Shabaab în 2009 (Cristopher Anzalone, 2012, p. 9-12).

Doi ani mai târziu, în octombrie 2011, guvernul kenyan a lansat Operațiunea Linda Nchi ("Protejați țara") în sudul Somaliei, împotriva incursiunilor al-Shabaab în țară. Operațiunea a dus la începerea unor atacuri de represalii pe teritoriul kenyan. Doar trei luni mai târziu, al-Shabaab a anunțat o fuziune oficială cu MYC, care a început în noul său nume: al-Hijra. Ca urmare, serviciile de securitate kenyene au lansat o campanie de represiune împotriva figurilor din al-Hijra, ceea ce a dus la o serie de asasinate, între 2012 și 2014: Rogo, în august 2012, octombrie 2013 și Makaburi în 2014.

Al-Hijra a început să facă incursiuni în Tanzania când a apărut pe Twitter, a pretins că operează din Tanga și Korogwe (ICSR Report, 2021).

Publicațiile au început, de asemenea, să prezinte comentarii despre politica tanzaniană și mențiuni despre al-Muhajiroun *(Emigranții din Africa de Est),* care a apărut ca o altă filială kenyană a al-Shabaab, dedicată creșterii amprentei sale ideologice de-a lungul coridorului Africii de Est. Al-Muhajiroun a apărut în ianuarie 2015, odată cu publicarea, în limba swahili, în revista Amka , în care Abu Salim al-Kenyi a jurat credință față de al-Qaeda și al-Shabaab. În luna noiembrie a aceluiași an, un al-Muhajiroun din Tanzania, Abu Khalid Abu Izz al-Din, a dezvăluit într-un interviu, că a fost rezident din Majengo și un student al lui Aboud Rogo, care a inspirat extinderea jihadului în toată Africa de Est. Al-Din a afirmat că, al-Muhajiroun opera în munții Mahenge, din centrul Tanzaniei și, făcând referire la prima declarație a grupului, a spus:

...trebuie să ne uităm la iubiții noștri cavaleri din Al-Shabaab. Ei ne-au făcut mândri. Cred că a fost în Amka când fratele Abu Salim al-Kenyi s-a referit la al-Shabaab ca fiind "pionieri". Eu cred că avea dreptate – al-Shabaab și al-Qaeda sunt inițiatorii jihadului în Africa de Est (Site Intelligence Group, 2015).

Aceasta a urmat unei declaraţii, din mai 2015, când al-Muhajiroun a ameninţat de a instiga la atacuri în Tanzania, Kenya şi Uganda, precum şi împotriva unor ţinte occidentale şi i-a avertizat pe musulmanii tanzanieni împotriva democraţiei.

Al-Muhajiroun părea, prin urmare, să fie o extensie a al-Hijra, o altă reţea ideologică, care să răspândească propaganda al-Shabaab la comunitatea musulmană tanzaniană. Propaganda Al-Hijra a avut deja creat un public familiarizat şi receptiv la ideologia sa. Astfel, al-Shabaab şi-a extins zona de influenţă la o a doua ţară de pe coasta Africii de Est: Tanzania.

Ca şi în Kenya, al-Shabaab avea două filiale în Tanzania: Ansar Muslim Youth Centre şi al-Muhajiroun. Prima este implicată în radicalizarea şi recrutarea de tineri tanzanieni, pentru a se alătura al-Shabaab în timp ce, cea de-a doua a susţinut că este implicată într-o serie de atacuri, în nordul Tanzaniei, alături de Congregaţia Ansar al-Sunna şi alţi actori necunoscuţi. Agitaţia din Tanzania, în direcţia unui militantism activ, atât de către reţelele extremiste clandestine, cât şi de către grupurile afiliate a făcut ca această ţară să fie unică, deoarece grupurile au căutat să se stabilească în drepturile proprii. Acest lucru a fost demonstrat, prin apariţia unui grup aspirant afiliat al Statului Islamic, Jabha East Africa, în aprilie 2016, cu sediul în Tanga, în nord-estul Tanzaniei, la graniţa cu Kenya.

Statul Islamic în Africa de Est

Figura 5: Hartă Africa de Est (sursă: Wikipedia)

Diviziunea și fracționismul în cadrul al-Shabaab sunt la fel de vechi ca și organizația însăși, rămânând remarcabil faptul că, a reușit să se impună ca o amenințare formidabilă. O posibilă explicație este stilul de conducere al lui Ahmed Abdi Godane, care era cunoscut pentru faptul, că a condus cu un grad atât de ridicat de cruzime, încât nu numai că a contribuit la faptul că al-Shabaab a devenit cea mai ucigătoare organizație teroristă de pe continent, timp de mai mulți ani consecutivi, dar care a și provocat rupturi majore la nivelurile superioare ale organizației.

Unul dintre primele incidente, care au dezvăluit caracterul lui Godane a fost atunci când, s-a crezut, că acesta a organizat uciderea lui bin Laden și a candidatului preferat al lui bin Laden pentru conducerea al-Shabaab, Fazul Abdullah Mohammed, în aceeași lună în care, liderul al-Qaeda a fost ucis. În 2013, Godane a ordonat o epurare majoră a luptătorilor străini, inclusiv Omar Hammami, care a fost contestată în mod deschis de lideri de rang înalt ai organizației, inclusiv un mentor personal de lungă durată, al-Afghani, care a fost, de asemenea, ucis de o facțiune pro-Godane, în acel an.

Astfel, Statul Islamic a apărut într-un moment oportun pentru a-i curta pe cei mai nemulțumiți membri ai al-Shabaab, în mijlocul unei dispute între facțiuni.

Până în august 2013, au apărut imagini cu susținători pro-IS, din al-Shabaab, pe canalul media al-Sham al IS (ICSR Report, 2021).

În timp ce, SI a început o campanie agresivă de curtare a afiliaților al-Qaeda, Godane a ales să reafirme public loialitatea al-Shabaab, față de al-Qaeda, într-un discurs din mai 2014, în timp ce, a epurat discret al-Shabaab de susținătorii SI. Dezertorii și membrii nemulțumiți au căutat adesea refugiu de mânia lui Godane în Yemen, unde militanții au plecat de mult timp în căutarea de tratament medical și pentru a face schimb de arme și expertiză cu AQAP(Al-Qaeda în Peninsula Arabică).

După moartea lui Godane, în septembrie 2014, SI a început să ajungă la membrii nemulțumiți ai al-Shabaab. Într-o declarație intitulată „Un mesaj pentru frații noștri din Somalia", un susținător al SI, Hamil al-Bushra, i-a lăudat pe militanții din Somalia, pentru că au luptat împotriva guvernului forțelor somaleze și pentru implementarea legii sharia, încurajându-i, în același timp, să angajeze credință față de SI.

Al-Bushra l-a întrebat, de asemenea, pe noul lider al al-Shabaab, Ahmed Umar, și consiliul său Shura de ce nu și-au oferit loialitatea față de al-Baghdadi, încheindu-și mesajul spunându-i lui Umar, cât de ușor

este să jure credinţă lui, instruindu-l chiar cu privire la procedură (Hamil al-Bushra, 2015).

La momentul respectiv, SI se afla într-o serie de succese, simbolizate prin declararea califatului şi capturarea oraşului Mosul, ceea ce a determinat o schimbare de alianţă.

În martie 2015, Abu Salman, un influent cleric al-Shabaab, a urmat pe urmele lui al-Bushra, atunci când, a emis o fatwa care a legitimat jurământul de credinţă faţă de al-Baghdadi. Şase luni mai târziu, Hassan Husein Adan, un şeic, cu sediul la Nairobi, care a exercitat o influenţă puternică asupra membrilor al-Shabaab, a scris o scrisoare în care îşi oferea sprijinul pentru al-Baghdadi şi discredita respingerea de către al-Qaeda a califatului său.

Aceste mesaje au fost urmate, în septembrie şi octombrie ale aceluiaşi an, de o serie de articole şi videoclipuri publicate de departamentul media oficial al SI şi a unor instituţii media simpatizante, în care se afirma că, al-Qaeda a devenit un grup deviant, care a abandonat crezul propriu-zis (critica lui Adan se referă, în principal, la respingerea califatului de către al-Qaeda, care este dezvoltată în seria „Primăvara islamică" a lui al-Zawahiri, care se bazează pe evenimente istorice).

În Somalia, şeicul Abd al-Qadir Mumin a apărut ca un influent cleric, susţinut de facţiunea membrilor nemulţumiţi ai al-Shabaab. El a înaintat o propunere de a schimba loialitatea faţă de SI. Abia după ce Godane a fost ucis, propunerea a fost dezbătută, în mod deschis, de către personalităţi precum Hussein Abdi Gedi, Taymullah al-Somali şi membri ai al-Shabaab, cei mai proeminenţi clerici kenyeni ai sabahabului, Abu Salman şi Hassan Husein Adan.

Până în iulie 2015, propunerea a fost deliberată de membrii de rang înalt din Jilib, unde se presupunea că, emirul adjunct Mahad Karate era pregătit să emită un angajament faţă de SI. Cu toate acestea, acest lucru nu s-a materializat niciodată şi, în schimb, a rezultat un memoriu distribuit în întreaga organizaţie, conform căruia, al-Shabaab a rămas loial al-Qaeda. Purtătorul de cuvânt al Al-Shabaab, Ali Dhere, a declarat, de asemenea, că a spus clar că grupul era singura "autoritate islamică legitimă" din ţară. În urma acestui memorandum, Ahmed Umar a continuat să îi dea curs lui Godane, în epurarea nemiloasă a dizidenţilor.

La 22 octombrie 2015, Mumin şi un grup de luptători au jurat loialitate lui al-Baghdadi, prin emiterea unei scurte declaraţii audio. Aceasta a fost urmată, la scurt timp, de alte două jurăminte de credinţă.

Primul a avut loc la 8 noiembrie, când un grup de 27 de luptători a dat bay'a (în terminologia islamică, este un jurământ de loialitate faţă

de un lider) lui al-Baghdadi, într-o înregistrare video. O lună mai târziu, la 7 decembrie, un grup mai mic de luptători, condus de Bashir Abu Numan, şi-au oferit loialitatea într-o înregistrare video, care a fost postată online, doar după asasinarea lor de către unitatea de informaţii a al-Shabaab.

Afilierea la Statul Islamic în Africa Centrală şi de Sud

Evoluția rețelelor Statului Islamic (SI) în regiune ar putea, în timp, să facă legătura între grupare şi insurgențele locale din Republica Democrată Congo (RDC) şi Mozambic. Punctul de vedere, la momentul realizării acestei cercetări, în ceea ce privește insurgențele din cele două țări, poate fi împărțit în două categorii: cei care consideră că, ADF (Allied Democratic Forces) din RDC şi ASwJ (Ahlu Sunna Wal Jama) din Mozambic sunt afiliate SI şi cei care se opun unei astfel de clasificări, susținând că, nu sunt în măsură să identifice nicio legătură între aceste grupuri.

Acest dezacord pare să fie determinat parțial, de confuzia cu privire la ceea ce înseamnă, de fapt, să fii un afiliat al SI şi, parțial, de aşteptările mari cu privire la modul în care, astfel de afilieri se traduc în practică. Această secțiune intenționează prezentarea procesului de înființare a ISCAP (Islamic State Central Africa Province) şi oferă o discuție, despre cum ar trebui să înțelegem afilierea. În iulie 2018, Institutul Hiraal a scris:

Deşi Statul Islamic cu siguranță nu consideră ADF ca făcând parte din din califatul său, iar mulți l-ar descrie mai degrabă ca pe o organizație criminală sau grup rebel local decât unul terorist, unii membri ADF şi-au exprimat sprijinul pentru Statul Islamic şi ar putea foarte bine să vadă avantajul de a avea un punct de sprijin teritorial în Africa subsahariană (Institutul Hiraal, p. 40).

Este exact ceea ce s-a întâmplat un an mai târziu, când SI a revendicat primul său atac oficial, în RDC, la 18 aprilie 2019 şi a introdus noua sa provincie din Africa Centrală (Wilayat Wasat Ifriqiyya), desemnată oficial de Statul Islamic, care este compusă din două facțiuni distincte, ce activează în două regiuni distincte, cea mai estică parte a Republicii Democratice Congo (RDC) şi nordul Mozambicului.

În august 2018, Abu Bakr al-Baghdadi a lăsat să se înțeleagă, într-un discurs, că SI avea deja luptători simpatizanți în Africa Centrală. La 3 iunie 2019, la nici două luni după prima revendicare a unui atac în RDC, o revendicare similară, pentru un atac în Mozambic, a fost publicată de

agenţia de ştiri Nashir a SI. Aceste revendicări au fost urmate de o declaraţie oficială a SI într-un video, publicat la 24 iulie 2019, care arată luptători atât în DC, cât şi în Mozambic, care jură credinţă SI ca parte a acţiunilor grupării, într-o campanie globală de reînnoire a jurământului de credinţă faţă de calif.

La 7 noiembrie al aceluiaşi an, aceasta a fost urmată de o altă imagine, în revista săptămânală al-Naba a Statului Islamic, în care erau înfăţişaţi luptători în Africa Centrală, care jurau credinţă noului calif, după moartea lui al-Baghdadi (Rev. al-Naba, 2019).

La 10 martie 2021, Departamentul de Stat al SUA a desemnat grupurile din RDC şi din Mozambic, ca fiind afiliate la SI (US Dep. of State, 2021).

Cu toate acestea, în ciuda publicaţiilor oficiale, din partea departamentului central de presă al SI şi autorităţile americane, unii observatori rămân neconvinşi, cu privire la veridicitatea legăturii dintre ADF (Allied Democratic Forces), ASwJ (Ahlu Sunna Wal Jama) şi SI. Această lipsă de convingeri se bazează pe mai multe argumente, în care pot fi condensate, astfel, patru puncte generale: nu există nicio dovadă a legăturii organizaţionale; nu toate atacurile revendicate de SI pot fi verificate; comunicarea pare a fi nesigură şi există o absenţă a unor tehnologii şi transfer tactic de la SI la grupurile din RDC şi Mozambic.

La nivel organizaţional, SI îşi gestionează filialele, prin intermediul Administraţiei pentru Provinciile Îndepărtate (idarat al-wilayat al-ba'ida), care este împărţită în grupuri separate conduse de un birou principal.

Potrivit ONU (Organizaţia Naţiunilor Unite), ISCAP acoperă Somalia, RDC şi Mozambic, iar Somalia funcţionează ca birou al sediului organizaţional pentru provincie şi, ca atare, acţionează în luarea deciziilor.

Din punct de vedere istoric, SI a pus accentul pe trei elemente, în special atunci când, decid să accepte sau nu un jurământ de credinţă: unitatea jihadistă şi o conducere desemnată; consolidarea teritorială şi comunicarea directă cu SI (Milton, al-Ubaydi, 2014, p. 22-33).

Acest lucru este în concordanţă cu procesul, declarat, de instituire a califatului, care, de asemenea, se aplică şi grupurilor din afara Levantului, care doresc să fie considerate afiliate oficial. Cu toate acestea, în practică, acest lucru nu a stat întotdeauna aşa.

Doi factori sunt importanţi în această discuţie. În primul rând, SI nu este o organizaţie la fel de puternică, precum a fost în perioada dintre 2014 şi 2016. În acest moment, a fost mai uşor pentru grup să definească

cerințele potențialilor afiliați, dar cu răsturnarea parțială a succeselor sale, nu se mai află într-o poziție de putere similară. În al doilea rând, grupul este oportunist și istoria a demonstrat, că este dispus să relaxeze cerințele pentru a facilita extinderea geografică. Acesta este, în special, cazul jihadiștilor care controlează teritoriul.

Criticii relației, dintre ADF și AswJ, pe de o parte și IS pe de altă parte, par să confunde ceea ce implică legătura organizațională și au așteptări prea mari, în ceea ce privește modul în care se traduce o astfel de legătură în practică. Așa cum a fost remarcat în Siria, ar fi o greșeală „să judecăm legitimitatea unei filiale a Statului Islamic în funcție de faptul că aceasta în esență seamănă cu Statul Islamic din Mosul sau Raqqa în jurul anilor 2014-2015" (Candland, 2021).

În ciuda relațiilor clare dintre grupuri, în ceea ce privește producția mass-media, criticii atrag atenția că nu există nicio dovadă, că relațiile organizaționale există. Deși, este posibil să nu funcționeze perfect, departamentul media al SI în publicarea de videoclipuri, fotografii și relatări ale atacurilor din RDC și Mozambic indică un anumit nivel de interacțiune organizațională, care este dificil de negat.

Astfel, grupurile diferă din punct de vedere ideologic și există o nepotrivire, între declarațiile mediatice ale ISCAP și evenimentele de pe teren. De aceea, nu pare să existe dovezi de transfer tangibil al know-how-ului de la SI, către grupurile din RDC și Mozambic. Acest dezacord se bazează pe o percepție eronată a SI și a modului în care funcționează, pe scară globală. În calitate de organizații globale, atât al-Qaeda, cât și SI sunt caracterizate prin diversitate ideologică, de la o filială la alta.

În timp ce grupurile pot încerca să își eficientizeze ideologia peste granițe, acesta este un proces care necesită timp și care, s-ar putea să nu fie niciodată complet, deoarece afiliații continuă să urmărească interese locale. Faptul că SI este oportunist, în revendicările sale de atac, nu este o noutate și nici greșelile ocazionale de ortografie a locațiilor și informațiile eronate, despre numărul victimelor, nu reprezintă o noutate. Adesea, aceste informații trec prin mai multe legături, înainte de a ajunge la departamentul de presă al SI și înante de a fi traduse în/și din arabă, ceea ce agravează problema. Dar, aceste greșeli ocazionale nu ar trebui să desconsidere toate activitățile grupurilor. În cele din urmă, transferul de know-how tehnologic și tactic necesită timp și depinde de necesitățile locale (CTC Sentinel, 2010).

În timp ce progresul, în materie de explozibili și dispozitive improvizate, în RDC poate fi rezultatul schimbului de cunoștințe din partea SI, nu este neapărat sigur, că grupurile din RDC și Mozambic vor

adopta practici similare, cu cele ale grupului din Siria, deoarece practicile şi tacticile existente funcţionează deja.

Concluzii

Concluziile acestei lucrări au în vedere validarea întrebărilor de cercetare propuse, astfel, se demonstrează următoarele: extremiştii islamişti, violenţi, transnaţionali, sunt atraşi de conflicte şi au tendinţa de a genera conflicte pe alte teritorii. Grupările jihadiste continuă să reprezinte o ameninţare gravă, pentru ţări din toate părţile lumii, fie din cauza formării de noi grupuri jihadiste, fie din cauza transformării grupurilor musulmane locale în grupuri jihadiste.

Africa a fost expusă la aceste tendinţe mai mult decât orice altă regiune. O serie de grupări, afiliate la al-Qaeda sau ISIS, acţionează în Africa în prezent, reuşind să îşi atingă obiectivul de radicalizare a conflictelor, făcându-le mai letale şi tot mai extinse, din punct de vedere teritorial.

Astfel, prin lucrarea mea mi-am îndeplinit obiectivul propus, prin faptul că, am documentat ce caracteristici are în comun extremismul islamist violent, în situaţii de conflict cu alte ideologii sau cu alte mişcări implicate în conflict.

Grupurile de conducere, de bază, ale ADF, al-Hijra, MYC în Tanzania, al-Muhajiroun şi ASwJ au fost expuse la învăţături fundamentaliste, propagate fie la nivel regional, de către clerici radicali şi reţele extremiste, fie prin intermediul lor cu educaţie religioasă în străinătate, în ţări precum Pakistan şi Arabia Saudită.

La întoarcere, ideologia lor nou descoperită, nu numai că a contestat status quo-ul, ci a făcut ca reţelele şi organizaţiile cu care au fost asociaţi, să fie înclinate ideologic spre afilierea cu organizaţiile jihadiste internaţionale.

Acest model din Kenya, Tanzania, RDC şi Mozambic evidenţiază faptul că, impactul salafismului şi al wahhabismului asupra discursului religios, în cadrul organismelor şi comunităţilor (religioase aprobate de guvern), există.

Expunerea la învăţăturile fundamentaliste a determinat astfel, o critică la adresa status quo-ului, caracterizat de o multitudine de situaţii socio-economice şi politice. În acest fel, cei care s-au întors au reuşit să trezească mişcări sociale, prin mobilizarea de resurse, folosindu-se de accesul la reţele şi actori, subliniind în acelaşi timp, nemulţumirea faţă de condiţiile socio-economice şi politice existente şi încadrarea unei serii de acţiuni, oportunităţi şi identităţi, pentru a amplifica şi a consolida

ideologia lor particulară, toate acestea, cu intenţia de a mobiliza noi recruţi.

Între timp, pe cât de mult a căutat al-Shabaab să îşi extindă zona de influenţă pe coasta Africii de Est, nu a reuşit să îşi consolideze suficient control şi supraveghere asupra recrutării şi propagandei din Kenya şi Tanzania, care aveau ambiţii de a deveni active, din punct de vedere al militantismului. Acest lucru a avut loc, pe fondul unor facţiuni beligerante în cadrul al-Shabaab şi a succeselor pe câmpul de luptă al SI în Levant, care a făcut ca o schimbare de loialitate, să fie o propunere atractivă.

Odată cu prăbuşirea califatului său fizic, SI a ajuns să recunoască promisiuni în Somalia, RDC şi Mozambic, creând astfel, un SSI şi ISCAP. Legăturile au arătat că, rolurile atribuite celor două provincii de către SI reflectă o realitate, în care militanţii din regiune sunt mai mult interconectaţi decât s-a considerat anterior. Acest lucru arată o implicare transnaţională de reţele de recrutare, instruire şi finanţare.

Se poate demonstra, în ce măsură aceste proiecte transnaţionale au făcut legături din întreaga regiune şi au fost parte integrantă a formării de militanţi şi a afilierii organizaţionale? În acest fel, explicăm modul în care, o grupare jihadistă precum SI, care de la bun început pare străină de Africa Centrală şi de Sud, a reuşit mai întâi să atragă atenţia şi mai târziu să se instituţionalizeze în RDC şi Mozambic?

Traiectoria recentă a ADF în RDC şi a ASwJ în Mozambic este imposibil de înţeles în mod corespunzător, fără a contextualiza grupurile în mediul regional mai larg al extremismului islamic şi al militantismului islamic. Reţelele militante din Kenya, Tanzania şi Uganda au fost toate esenţiale, pentru propagarea unei ideologii extremiste, precum şi pentru conectarea militanţilor din RDC, Tanzania şi Mozambic cu ecosistemul regional al militantismului islamic. Prin extinderea sa în Somalia, SI a reuşit să exploateze acest ecosistem pentru a găsi, în cele din urmă, simpatie în rândul militanţilor din RDC şi Mozambic. Ca şi în cazul Somaliei, incursiunile SI nu au rămas necontestate, în special conducerea ADF s-a fragmentat, ca urmare a acestui fapt.

În Africa de Sud, evoluţia activităţii extremiste a dus la apariţia de rapoarte privind sprijinul material acordat ADF şi ASwJ de către sindicatele criminale.

Acest lucru vine după ani în care, teroriştii străini şi, mai recent, locali au încercat să folosească Africa de Sud ca un refugiu logistic sigur, pentru a facilita taberele de antrenament, pentru a recruta, a genera venituri sau a se sustrage arestării.

Conflictul din nordul Mozambicului a atins un punct de cotitură în martie 2021, când, insurgenţa ASWJ a lansat cel mai îndrăzneţ atac de până atunci, împotriva oraşului Palma, considerat de către localnici şi comunitatea internaţională ca o insulă de relativă securitate, în mijlocul unui conflict care se extinde. În timp ce, grupul a obţinut câştiguri materiale pe termen scurt şi o creştere a notorietăţii, ca ameninţare reală la adresa statului, s-a dovedit a fi, de asemenea, picătura care a umplut paharul şi care, ar fi împins guvernul mozambican să accepte străini pe teren, pentru a-şi consolida propriile eforturi de contrainsurgenţă, transformând această victorie, pe termen scurt, într-o eroare strategică, care a prezentat grupului un mediu de luptă mai ostil şi care, are implicaţii directe asupra ameninţării terorismului în Africa de Sud. Deşi, este demn de remarcat faptul că, Statul Islamic nu are o prezenţă oficială în Africa de Sud, în prezent, acest lucru nu elimină ameninţarea actorilor sau a celulelor de lupi singuratici.

Extinderea domeniului de aplicare şi consecinţele distructive ale extremismului violent, se numără printre provocările majore la adresa securităţii globale, cu care se confruntă lumea de astăzi.

Extremismul violent şi evoluţia abruptă a creşterii activităţii extremiste în Africa reprezintă, de asemenea, provocări directe şi ameninţă să blocheze rezultatele, în materie de dezvoltare, pentru generaţiile viitoare, dacă nu vor putea fi controlate.

Bibliografie:

1. Daniel Holbrook, The Al-Qaeda Doctrine: Încadrarea şi evoluţia discursului public al liderilor (New York, Londra, Oxford, New Delhi, Sydney: Bloomsbury, 2014).

2. Daniel Milton and Muhammad al'Ubaydi, "Pledging Bay'a: A Benefit or Burden to the Islamic State?", *CTC Sentinel* vol. 8 no. 3 (March 2015).

3. Edith Wu, Rebecca Cartleton şi Garth Davies, "Discovering bin-Laden's Replacement in al-Qaeda", utilizând Social Network Analysis: "A Methodological Investigation", *Perspectives on Terrorism* vol. 8 nr. 1 (2014).

4. Hiraal Institute & Global Strategy Network, The Islamic State in East Africa.

5. IS's al-Naba newsletter no. 207, issued on 7 November 2019.

6. Josh Kron şi Mohamed Ibrahim, "Islamist Claim Atack in Uganda", 12 iulie 2010.

7. J. Stig Hansen, Horn, Sahel and Rift: Fault-lines of the African Jihad, London: C. Hurst & Co., 2019, 128.

8. Katherine Zimmerman, The al-Qaeda Network: A New Framework for Defining the Enemy (Washington D.C.: American Enterprise Institute, 2013).

Bibliografie site-uri:

9. https://www.visionofhumanity.org/wp-content/uploads/2023/03/GTI-2023-web-170423.pdf

10. https://ctc.westpoint.edu/kenyas-muslim-youth-center-and-al-shababs-east-african-recruitment/

11. https://assets.publishing.service.gov.uk/media/57a0897aed915d622c00022f/61525-Conflict_and_Countering_Violent_Extremism_Case_Studies.pdf

12. https://www.researchgate.net/publication/294482784_Tangled_Ties_Al-Shabaab_and_Political_Volatility_in_Kenya

13. https://ctc.westpoint.edu/the-islamic-states-strategic-trajectory-in-africa-key-takeaways-from-its-attack-claims/

14. https://icsr.info/wp-content/uploads/2021/11/ICSR-Report-The-Arc-of-Jihad-The-Ecosystem-of-Militancy-in-East-Central-and-Southern-Africa

IMPACTUL POPULISMULUI ASUPRA ECHILIBRULUI DE PUTERE ÎN UNIUNEA EUROPEANĂ. AMENINȚARE HIBRIDĂ LA ADRESA INTEGRITĂȚII UNIUNII EUROPENE

drd. Maria-Lorena REIT[*]

Abstract:

This article begins with a brief introduction to European populism, defining it and explaining its main characteristics, in order to provide a general context for the analysis. The paper is structured in four parts, while explaining how populism can be perceived as a hybrid threat to the European Union and analyzing the impact that this phenomenon has on the balance of power between the member states of the Union, , as well as on the global balance of power. In the first part of the paper, I analyzed the features of Hungarian and Polish populism, analyzing the discourses of PiS and Fidesz representatives. In this sense, I undertook a comparative analysis of the discursive structures of the two parties, highlighting the similarities and differences identified in the rhetoric of Viktor Orbán and Jarosław Kaczyński. In the second part of the article, I framed populism among hybrid threats, examining how this ideology can be perceived as such a threat. In the third part of the paper, I analyzed how populism affects the balance of power, approaching this theme from three perspectives, namely from the perspective of the balance of power between the member states, from the inter-institutional perspective, as well as from the perspective of the international balance of power. In the fourth part of the paper, I analyzed the actions that the European Union can take to reduce the effects generated by populism. In this sense, I brought up three means of counteracting this phenomenon, namely the use of the sanctions provided for in art. 7 of the Treaty on the European Union, the suspension from the Schengen area and the implementation of financial pressures, reaching the conclusion that financial sanctions would be the main way to force populist parties to give up this ideology. Following this research, the main conclusion I reached is that the hybrid threat character of populism and its impact on the balance of power are the collective result of populist parties in the Union. More precisely, although the two analyzed parties are the most representative for this phenomenon, the ability to influence the balance of power is possible due to the extent of the phenomenon in the European Union.

Keywords: *populist democracy, hybrid threat, balance of power, discourse analysis, social fragmentation, illiberal Fidesz, PiS, means of counteracting.*

[*] Universitatea Babeș-Bolyai, Facultatea de Istorie și Filosofie, Școala Doctorală de Relații Internaționale și Studii de Securitate, Cluj-Napoca, reitmarialorena@gmail.com

Considerații introductive

Generat de crizele de reprezentare politică și de cele financiare, populismul poate fi considerat atât o componentă a democrației, cât și o amenințare de tip hibrid la adresa acestui regim politic (Mackert, 2019, 1-2). În acest context, Bohdana Kurylo afirma faptul că, populismul generează insecuritatea și nu invers (2020, 2). Mai exact, acesta susține faptul, că populismul nu apare ca rezultat al unei stări de insecuritate, ci că apariția lui duce la insecuritate. Aș dori să adaug la această prezumpție faptul că, într-o primă fază, populismul ar trebui perceput ca fiind o vulnerabilitate la adresa politicilor Uniunii Europene, a securității naționale și regionale și la adresa elementelor care stau la baza societăților democratice, precum statul de drept, supremația legii, protecția minorităților și separarea puterilor. Cu toate acestea, trebuie să avem în vedere faptul că, în funcție de amploarea lui, acesta poate fi considerat o amenințare la adresa stabilității pe termen mediu și lung a sistemului.

Având în vedere faptul, că populismul a devenit un subiect de o relevanță majoră atât în Uniunea Europeană, cât și la nivel mondial, am analizat modul în care, acesta se manifestă ca amenințare de tip hibrid, la adresa Uniunii Europene, cât și felul în care, reprezentanții partidelor care au la bază această ideologie încearcă să destabilizeze echilibrul de putere în cadrul Uniunii. Am putut remarca un trend ascendent al populismului eurosceptic care, cu toate că și-a făcut simțită prezența și înainte, a părăsit caracterul marginal și a devenit un fenomen central, spre exemplu, odată cu reîntoarcerea la putere, în 2010 a lui Viktor Orbán, în 2015 când PiS și Syriza au ajuns la putere, în 2016 odată cu organizarea referendumului privind Brexitul sau în 2018, când coaliția M5S – Lega a ajuns la guvernare, enumerarea putând continua. Ținând cont de faptul, că acest fenomen a monopolizat scena politică a unor state membre, am expus și modurile în care, Uniunea poate contracara recurgerea la acest tip de ideologie și retorică.

Astfel, intenționez să răspund la următoarea întrebarea de cercetare, și anume „Cum se manifestă populismul ca amenințare de tip hibrid la adresa echilibrului de putere din Uniunea Europeană?". Metoda de cercetare este analiza narativă și ca tipuri de date, m-am axat, în principal, pe discursuri. Privind studiile de caz, am ales partidele Fidesz și PiS, deoarece constituie principalii reprezentanți ai populismului în Uniune, actorii politici ale acestor partide fiind cei mai vocali. Un alt motiv este faptul, că acestea sunt cele mai de succes partide populiste, reușind să își consolideze puterea. De asemenea, alegerea se datorează

faptului, că Uniunea a încercat sancţionarea celor două partide, în baza art. 7 din Tratatul privind Uniunea Europenă (TUE), însă, acestea îşi folosesc deseori dreptul de veto, pentru a se proteja reciproc.

Consideraţii teoretice

Înainte de a începe analiza, doresc să ofer un punct de plecare, în ceea ce priveşte partea teoretică a populismului. În acest sens, cu toate că nu există o definiţie unanim acceptată a termenului, consider faptul că cel mai potrivit, pentru analiza ce urmează să o întreprind în acest articol este de a urma teoria conform căreia, populismul este o ideologie subţire cu un nucleu ideologic limitat (Freeden, 1996, 77-80). Cass Mudde poziţionează dihotomia în centrul definiţiei populismului (2007, 23), societatea fiind împărţită în două "grupuri omogene şi antagoniste" (2004, 543), care au la bază politica identitară (Klaus, 2018, 7-8), liderul pretinzând faptul că, politica reprezintă materializarea voinţei generale a poporului. Această viziune bidimensională a spaţiului social are atât o dimensiune verticală, caracterizată prin opoziţia dintre „poporul pur” şi „elita coruptă”, cât şi una orizontală, dintre "interior" şi "exterior" (Brubaker, 2019, 28-31), aceasta din urmă putând fi numită şi "populism transnaţional" (de Cleen, 2017, 451-455). În acest sens, aş dori să subliniez faptul că, reprezentanţii "exteriorului", din cadrul ambelor dimensiuni, sunt comutabili şi dependenţi de context, populiştii schimbând, în funcţie de scopurile şi interesele urmărite, actorii portretizaţi ca fiind o ameninţare.

De asemenea, nefiind o ideologie de sine stătătoare, aceasta se combină cu idei naţionaliste, nativiste, anti-elitiste, etnoctatice şi rasiste(Fitzi, 2019, 58), utilizând discursuri critice şi xenofobe prin care se atacă clasa politică (Soare, 2010, 91-92). Pentru a completa cele expuse anterior, doresc să menţionez faptul că, prin "clasă politică", se poate înţelege atât cea naţională, cât şi cea a altor state sau a Uniunii, depinzând de necesităţile populiştilor la momentul articulării discursului. Emanuel Copilaş consideră faptul că, discursul populist ajută la fragmentarea câmpului social, creând opoziţii binare (2013, 113). Aş dori să adaug la această afirmaţie faptul, că fragmentarea socială se datorează, în principal, caracterului manipulator şi exploatator al retoricii.

O altă particularitate a ideologiei populiste este faptul că, poziţionarea partidelor în ceea ce priveşte dihotomia dreapta versus stânga este slab articulată, acestea coexistând prin împrumutarea idealurilor tipice ale întregului spectru politic (Soare, 2010, 91-92). Prin

urmare, subminarea acestor granițe, prin întrepătrunderea celor două genealogii, crează o confuzie ideologică. În acest sens, populismul trebuie privit ca fiind ideologia unei lumi postideologice, în cadrul căreia, guvernele domnesc peste o populaţie neinteresată de distincţia dreapta-stânga. O caracteristică a acestei ideologii în Europa, adusă în discuţie de Michael Shafir, constă în faptul, că populiştii nu sunt antidemocratici, ci antiliberali (2008, 430-431), având o abordare monistă a câmpului social, pe care îl percep ca fiind alcătuit din colectivităţi omogene. Astfel, prin atitudinea lor contrară pluralismului, populiştii vor avea o abordare antisistem, atunci când democraţia este liberală, sau o viziune pro-sistem, în cazul unei democraţii plebiscitare (2008, 464-465). Prin urmare, limitele populismului se află în interiorul politicii democratice, la graniţa dintre sistemic şi antisistemic (Soare, 2010, 112-113), în timp ce, depăşirea acestor frontiere destabilizează regimul democratic, acesta devenind autoritar şi revoluţionar (Taggart, 2019, 79-81). Aş dori să completez ideea conform căreia, societatea ar fi compusă din "colectivităţi omogene", subliniind faptul că, în funcţie de circumstanţe, populiştii pot trata comunitatea printr-o abordare pluralistă, percepând-o ca fiind formată dintr-o varietate de grupuri.

În cadrul partidelor populiste, puterea este centralizată de lideri carismatici, care se autoportretizează, ca fiind unicii salvatori şi apărători legitimi a valorilor şi identităţii naţionale şi europene (Kaltwasser, 2019, 79-81). Astfel, partidul se află într-un plan secundar, în timp ce, slăbiciunea sistemului de partide favorizează apariţia liderilor populişti (Weyland, 1999, 384). Mai mult, aceştia exploatează nemulţumirea maselor, facilitând manipularea electoratului, fără un program politic coerent şi consecvent (Stanley, 2017, 196-197). În ceea ce priveşte dimensiunea economică a sistemului politic, costurile sunt folosite la sporirea neîncrederii în clasa politică concurentă (Soare, 2010, 91-92), aducându-se în discuţie o politică de protecţie economică. De asemenea, populismul este tradiţional și religios, opunându-se imigraţiei și islamizării (Saul, 1969, 170). O caracteristică principală a populismului în Uniunea Europeană este adoptarea unei poziţii eurosceptice, prin prezentarea proiectului european ca fiind o ameninţare adusă comunităţii de origine (Soare, 2010, 92). Doresc să menţionez faptul că, această ideologie are un caracter cameleonic, astfel încât, partidelor populiste le pot lipsi anumite caracteristici consacrate sau pot dezvolta diverse specificităţi.

Analiza structurilor discursive ale reprezentanţilor FIDESZ şi PiS

În ceea ce priveşte populismul unguresc şi polonez, Péter Krekó şi Attila Juhász au susţinut faptul, că acesta excede graniţele ideologiei, numind acest stil "tribalism". Conform acestora, tribalismul este o abordare autoritară şi anti-pluralistă a politicii, prin care se modifică întregul cadru socio-cultural, discursurile fiind radicalizate în timp ce politica este percepută ca un război (2019, 69-73). Evoluţia şi încadrarea similară a celor două partide se datorează aspectelor contextuale care au favorizat apariţia acestui fenomen în cele două state. Mai exact, ambele au la bază ideea suprimării statului naţional de superputerile Europene, rezultând într-un sentiment de victimizare şi generând o cultură a conspiraţiei. În discursul lui Jarosław Kaczyński, din 2018, regăsim un exemplu în acest sens, şi anume faptul că acesta articula că „puterile" Europene au tratat Polonia ca pe o „pradă privată" (Deutsche Welle, 2018) de-a lungul istoriei. O altă similaritate contextuală constă în faptul că ambele susţin că au fost tratate ca state de clasa a doua în Uniunea Europeană, întărind astfel neîncrederea în Uniune. Cea de-a treia similaritate o constituie ideea de pierdere parţială a suveranităţii şi dispariţia, într-o oarecare măsură, a statului maghiar şi polonez. În acest caz, am putut observa că aceştia fac referire la cedarea parţială a suveranităţii către Uniune, lăsând să se înţeleagă faptul că actorii externi nu trebuie să aibă putere sau influenţă faţă de statul naţional. În ceea ce priveşte factorii sociali care au generat apariţia acestei ideologii autoritare, am avut în vedere polarizarea politică accentuată corelată cu neîncrederea instituţională şi interpersonală (Krekó, Juhász, 2019, 73).

În ceea ce priveşte structurile discursive ale reprezentanţilor celor două partide, am identificat atât asemănări, cât şi deosebiri. În primul rând, ambele fac trimiteri la pierderea identităţii istorice şi imaginii statelor. Această particularitate prin care se face referire la mândria statului de odinioară apare, spre exemplu, în discursul pentru alegerile parlamentare din 2015 a lui Kaczyński. În discurs acesta vorbeşte despre recăpătarea sentimentului de unitate şi face referire la nevoia de a reinstaura Polonia ca "o mare naţiune europeană" (Current Events Poland, 2015). Pe de altă parte, Orbán duce discursurile lui la un alt nivel, făcând trimiteri inclusiv la imaginea pierdută a Europei, portretizându-se ca „salvator" al acesteia.

Într-un discurs din 2021, prim-ministrul maghiar vorbea despre „restabilirea influenţei şi autorităţii Europei în politica externă" (Visegrád Post, „Viktor Orbán: «Wir müssen»", 2021), menţionând faptul,

că „Europa” ar trebui să contrabalanseze influența Chinei în mediul internațional. Datorită acestei retorici am putut observa aspirația Ungariei de a devenii un actor cu capacitatea de a influența echilibrul de putere a sistemului internațional. Aspirația privind influențarea politicii externe a UE, se poate remarca, spre exemplu, și în momentul în care Orbán a respins declarația comună a Uniunii privind atacurile asupra Israelului din 2021. Această acțiune demonstrează faptul că premierul încearcă să submineze, în special, autoritatea Germaniei, întrucât Orbán a susținut că statul german are o atitudine „profund non-europeană” (Visegrád Post, „Samizdat No. 8”, 2021), revendicând astfel atitudinea pro-europeană, pentru propria poziție.

Unul dintre cele mai importante elemente este faptul că, aceștia nu percep elitele ca făcând parte din parlamentul național, ci din Parlamentul European (Krekó, Juhász, 2019, 72). Mai exact, am observat că atunci când se vorbește despre amenințări, Uniunea Europeană este portretizată ca fiind principala primejdie și se pune accentul pe discrepanța dintre Vest și Est, în contextul „Europei cu două viteze” pentru a evidenția faptul că, aparent, UE marginalizează cele două state. În cazul Poloniei, mai avem ca amenințare externă și Germania, făcându-se referire la acest stat, în contextul suprimării în cadrul celui de-al Doilea Război Mondial. Pentru a legitima neîncrederea în UE, se face referire la istorie, evidențiindu-se greșelile Occidentului, precum în discursul lui Viktor Orbán în care, acesta articula faptul că, Ungaria a fost „vândută” (Visegrád Post, “Im Hinblick”, 2018) la conferința de la Yalta. Astfel, populiștii antagonizează Uniunea, susținând că este „imperială” și că are un „deficit democratic”, cu toate că, atitudinea iliberală este observabilă în statele care au la guvernare partide populiste.

O altă asemănare constă în faptul că, discursurile ambelor partide conțin referiri la cultură, religie, limbă și tradiții comune, punând accentul mai ales pe familie și valorile creștine. Mai exact, identitatea națională este construită într-un mod asemănător. Cu toate acestea, aici am putut remarca o deosebire care constă în faptul că, Fidesz acordă mai multă atenție culturii maghiare și unicității poporului. Un exemplu în acest sens, ar fi discursul în care Orbán descrie poporul maghiar ca fiind „o specie unică” (Visegrád Post, „Viktor Orbáns Rede”, 2018), legitimând astfel importanța acestora. Pe de altă parte, PiS acordă mai multă atenție familiei și valorilor creștine.

O altă particularitate a celor două partide o reprezintă faptul că, ele acordă o importanță secundară drepturilor omului și normelor procedurale, cu toate că, acestea reprezintă fundamentele democrațiilor

liberale (Krekó, Juhász, 2019, 72-74). De asemenea, folosirea monismului şi pluralismului depinde de nevoile contextuale, cele două partide văzând societatea ca fiind alcătuită fie din colectivităţi omogene, fie din grupuri de indivizi diferiţi. Am putut observa o altă similaritate în cadrul discursurilor cu privire la migraţie. Mai exact, accentul cade pe securitizare şi teama de pierderi culturale. Spre exemplu, Orbán susţinea într-un discurs faptul că, prin migraţie Uniunea Europeană urmăreşte să devină un „imperiu multicultural" (Visegrád Post, "Im Hinblick", 2018). Mai exact, acesta articula faptul că imigraţia ameninţă valorile şi cultura statelor, iar în consecinţă, acestea „vor înceta să mai existe" (Flux On-Line, 2018). Nici reprezentanţii Poloniei nu au fost de acord cu cota de migraţie impusă de UE, acest fapt putând fi observat în discursul lui Kaczyński din 2017, moment în care acesta afirma că Polonia nu a „exploatat ţările din care aceşti refugiaţi vin" (Euractiv, 2017), fiind astfel îndreptăţită să îi refuze.

Există o diferenţă fundamentală între cele două retorici, în ciuda faptului că Occidentul este descris asemănător în discursuri, adică, ca reprezentând o ameninţare la adresa statului naţiune. Mai exact, discursul PiS este mai moderat, iar Uniunea este portretizată în acelaşi timp şi pozitiv, fiind sesizabilă o aspiraţie clară de integrare, dar urmărindu-se ajungerea la un statut de egalitate cu cel al ţărilor vestice. Pe de altă parte, retorica Fidesz este extremă şi nu există o astfel de aspiraţie, făcându-se o diferenţiere radicală, între Ungaria şi Occident şi prezentându-l ca fiind o ameninţare într-un mod extrem. Această atitudine ofensivă a lui Orbán faţă de UE se datorează şi relaţiei sale cu Rusia. În timp ce Ungaria prezintă o oarecare afinitate faţă de Federaţia Rusă, Polonia nu are o relaţie atât de apropiată. Un alt motiv pentru existenţa acestui decalaj constă în faptul că, Fidesz exercită un control considerabil asupra presei, în timp ce, opoziţia este fragmentată. De asemenea, această diferenţă este sesizabilă şi din cauza faptului, că Fidesz a reuşit să îşi instituţionalizeze poziţia, fiind la guvernare de mai mulţi ani decât PiS.

Populismul ca ameninţare hibridă la adresa Uniunii Europene

Pentru a putea expune modul în care populismul reprezintă o ameninţare de tip hibrid am pornit, în primul rând, de la definiţia Comisiei, aceasta considerând ameninţarea hibridă ca fiind „momentul în care, actori statali sau non-statali, încearcă să exploateze vulnerabilităţile UE în propriul lor avantaj, utilizând într-un mod coordonat un amestec de măsuri precum cele diplomatice, militare,

economice sau tehnologice, rămânând în acelaşi timp sub pragul de război formal", având ca scop „împiedicarea proceselor democratice de luare a deciziilor prin campanii masive de dezinformare, utilizarea reţelelor sociale pentru a controla naraţiunea politică sau pentru a radicaliza, recruta şi direcţiona actori proxy" (European Commission, n.d.). În acest context, am putut remarca faptul că reprezentanţii Fidesz şi PiS prezintă particularităţile tipice ale actorilor hibrizi, aceştia afectând procesele democratice, aducând atingere valorilor care stau la baza acestora, precum separarea puterilor, statul de drept sau protecţia minorităţilor. Această împiedicare a proceselor democratice se poate observa, spre exemplu, în cazul Ungariei, în momentul în care, Orbán a implementat un proiect de lege în timpul pandemiei, acesta permiţându-i să guverneze prin decret (Amaro, 2020).

O a doua definiţie a ameninţărilor hibride, pe care doresc să o aduc în discuţie, este cea a Centrului European de Excelenţă pentru combaterea ameninţărilor hibride. Mai exact, CoE specifică faptul că, „termenul de ameninţare hibridă face referire la acţiunea actorilor statali sau non-statali, al cărei scop este de a submina sau dăuna unei ţinte prin influenţarea procesului decizional al acesteia la nivel local, regional, statal sau instituţional" (Hybrid CoE, n.d.). În cazul celor două spețe, acestea subminează procesele decizionale, prin încercarea de a destabiliza echilibrul de putere în Uniunea Europeană, această acţiune fiind posibilă din cauza tranziţiei continue a structurilor internaţionale de putere. Pentru a exemplifica modul în care cele două state se poziţionează împotriva deciziilor UE, doresc să amintesc declaraţiile comune ale Uniunii, cu privire la atacurile asupra Israelului şi cele cu privire la Hong Kong.

Având în vedere faptul, că principiile democraţiei liberale stau la baza Uniunii, pot afirma faptul că, populismul poate fi încadrat în categoria ameninţărilor hibride, ţinând cont de faptul, că „democraţia populistă" (Ágh, 2016, 1-5) este una de tip hibrid, existând între limitele democraţiei şi autoritarismului. Utilizarea campaniilor de dezinformare şi manipularea dezbaterilor şi alegerilor politice, amintite de cele două definiţii, sunt rezultatul invocării repetate a poporului şi a portretizării liderului partidului ca fiind unicul „salvator" al acestuia. Prin câştigarea încrederii electoratului, aceste partide facilitează manipularea, iar prin dihotomia verticală şi orizontală, se accentuează dezbinarea şi polarizarea sferei politice. Această viziune bidimensională a societăţii sporeşte conflictului de valori, populiştii generând un al doilea tip de ameninţare hibridă, şi anume, războiul cultural. Astfel, cu toate că

populiştii reprezintă una dintre principalele ameninţări la adresa democraţiei liberale şi a Uniunii, aceştia încadrează UE în categoria ameninţărilor, susţinând că, aceasta este „imperială" şi că se doreşte abolirea valorilor şi culturii statelor membre.

Un alt exemplu, pe care doresc să îl aduc în discuţie, pentru a contura o trăsătură a populismului, sunt campaniile de ură împotriva imigranţilor din timpul crizei refugiaţilor. În acest context, am observat cum cele două partide populiste prezintă criza ca fiind o ameninţare hibridă, cu toate că, aceasta nu generează vulnerabilităţi la fel de semnificative pentru UE ca adoptarea ideologiei populiste. Astfel, am observat faptul că, populiştii aduc în atenţia electoratului alte tipuri de ameninţare hibridă, în încercarea de a disimula existenţa propriei ameninţări.

Prin urmare, am putut încadra populismul în categoria ameninţărilor de tip hibrid, ţinând cont de faptul că, la baza acestei ideologi se află poziţia eurosceptică şi de protest. Mai exact, trăsătura specifică a populismului, în Europa Centrală şi de Est, constă în perceperea participării la proiectul european ca fiind una dintre cele mai considerabile ameninţări la adresa comunităţii de origine. Astfel, întrucât populiştii percep politica ca fiind un război, utilizarea acestei ideologii poate fi considerată, ca fiind o strategie prin care, se încearcă distrugerea instituţiilor democratice, prin legitimarea autocraţiei într-o societate a normelor democratice. În concluzie, intercalarea definiţiilor ameninţărilor hibride şi a caracteristicilor populismului, demonstrează faptul că, această ideologie face parte din gama ameninţărilor hibride. Astfel, consider faptul că, la momentul actual, acest fenomen reprezintă una dintre cele mai semnificative ameninţări la adresa democraţiei liberale, precum şi la adresa integrităţii, unităţii şi solidarităţii UE, populismul ducând la divizarea Uniunii.

Impactul retoricii populiste asupra echilibrului de putere din Uniunea Europeană

Pentru a putea demonstra modul în care cele două partide influenţează echilibrul de putere din Uniunea Europeană, doresc să prezint ceea ce se înţelege prin acest termen. Conform lui Waltz, discutăm despre echilibrul de putere în momentul în care, în cadrul sistemului internaţional, se constituie „două coaliţii", mai exact, o alianţă a statelor mai slabe împotriva celui mai puternic actor, dar nu neapărat împotriva celui mai ameninţător (1979, 127). Astfel, atunci când facem

referire la echilibrul de putere în Uniunea Europeană, vorbim despre balanța de putere dintre statele mari și cele mici (1979, 210).

Cu toate că, prin *Tratatul de la Roma* din 1957, puterea statelor a fost transferată către organismele supranaționale, oferind astfel statelor mici oportunitatea de a influența dezvoltarea proiectului european și procesul de elaborare a politicilor, inițiativa în acest proces a rămas sub influența membrilor mai mari. Astfel, deoarece aceste state au puține voturi în *Consiliul European* și, în ciuda faptului că, majoritatea deciziilor sunt luate prin consens, capacitatea lor de negociere este redusă, bazându-se mai degrabă pe persuasiune și nu pe tehnici de negociere concrete (Thorhallsson, 2015, 1-2). Prin urmare, pentru a-și putea face simțită influența, cele două state abordează poziții eurosceptice, criticând factorii de decizie ai UE. De asemenea, am remarcat faptul că, infiltrarea populiștilor în instituții aduce atingere democrațiilor liberale pe termen mediu și lung, transformând politica publică europeană. Pentru a exemplifica avem cazul Ungariei, unde instituțiile statului, precum instanțele electorale, se află sub controlul guvernului. Această abordare este adoptată și de Polonia, fiind sesizabilă în momentul în care, reformele judiciare au subminat separarea puterilor (Eiermann, Monunk, Gultchin, 2017, 18-19).

Prin urmare, dificultățile întâmpinate în procesele de negociere și concurența instituțională, au avut urmări atât asupra echilibrului de putere, dintre statele membre și a celui dintre instituțiile UE, cât și asupra coerenței și eficienței Uniunii, în ceea ce privește politica externă și balanța de putere la nivel global. Astfel, în contextul evoluției rapide a Uniunii și ținând cont de procesele decizionale complexe, din cadrul instituțiilor acesteia, am remarcat încercarea statelor mici și mijlocii, în speță Ungaria și Polonia, de a redirecționa balanța de putere din UE, dinspre Europa de Vest spre Centru și Est. Mai mult, încercarea populiștilor de a acapara puterea, din cadrul Uniunii Europene, afectează și echilibrul de putere la nivel global. Mai exact, problemele pe care populismul le generează la nivel regional, au recentrat atenția Uniunii asupra consolidării integrității acesteia, punând într-un plan secundar echilibrul de putere la nivel global (Keukeleire, Delreux, 2014, 5). Acest lucru a permis altor puteri să adopte o poziție mai favorabilă în plan internațional, destabilizând imaginea unitară a UE, în mediul internațional, aceasta lăsând impresia că este fragmentată (Gebhard, 2017, 103-104).

De asemenea, am observat faptul că, populiştii doresc să diminueze abordarea lor reactivă, înlocuind-o cu una proactivă, având ca model statele vestice. Mai exact, Ungaria și Polonia recurg la această ideologie, pentru a compensa limitările pe care acestea consideră că le au în cadrul procesul decizional al Uniunii, cu scopul de a-şi apăra interesele şi pentru a-şi lărgi sfera de influenţă în UE (Thorhallsson, 2015, 1-2). Prin urmare, acestea caută să compenseze vulnerabilităţile, pe care consideră că le-ar avea în UE, printr-o retorică eurosceptică. Mai exact, din cauza faptului, că există un puternic sentiment de inferioritate faţă de statele vestice, acestea doresc să diminueze dezavantajele structurale cu privire la capacitatea de negociere şi puterea de vot.

Am putut observa această încercare, de a transfera puterea de la statele membre mari la cele mici şi mijlocii, la începutul lunii decembrie 2021, moment în care, reprezentanţii partidelor populiste din UE, printre care Viktor Orbán şi Jarosław Kaczyński, au participat la un summit în Varşovia, care a avut ca subiect viitorul Uniunii, pornindu-se de la ideea, că UE este guvernată de o elită auto-proclamată, populiştii dorind să promoveze egalitatea şi libertatea statelor (Notes from Poland, 2021). Prin acest tip de coaliţii, se încearcă obţinerea puterii şi influenţei în cadrul UE. Astfel, cu toate că statele, în care populismul este utilizat ca principala strategie a clasei politice, observate individual, nu reprezintă o ameninţare considerabilă la adresa echilibrului de putere din cadrul Uniunii, prin cooperarea reprezentanţilor partidelor populiste, aceştia dezvoltă capacitatea de a schimba balanţa de putere, dinspre statele democratice liberale spre cele iliberale.

Modalităţi de combatere a populismului din Uniunea Europeană

Ţinând cont de valorile enunţate în art. 2 din TUE (Jurnalul Oficial, 2012, 17) şi pentru a analiza măsurile luate de Uniune, în vederea combaterii acestui fenomen, doresc să amintesc proiectele de lege ale PiS care au dus la eliminarea independenţei judiciare, precum şi reformelor sistemului judiciar unguresc din 2013, prin care legile electorale ale statului au fost schimbate în aşa fel, încât Orbán să îşi păstreze puterea (Hoffmann, 2018, 1156 – 1169). În urma acestor acţiuni, Uniunea a declanşat procedura de constatare şi sancţionare prevăzută la art. 7 din

TUE, mecanismul fiind utilizat, pentru prima dată, în cazul Poloniei.[1] Acest proces se desfășoară în două etape, statul membru fiind inițial avertizat oficial cu privire la faptul, că există un „risc clar de încălcare gravă a valorilor" UE, urmând ca, în urma încălcării persistente, să se impună sancțiuni, inclusiv suspendarea sau retragerea dreptului de vot în Consiliu (Jurnalul Oficial, 2012, 19-20). Prin această acțiune, UE ar putea face presiuni asupra partidelor aflate la guvernare, pentru a le constrânge să se realinieze la valorile Uniunii. Cu toate acestea, sancțiunile prevăzute în art. 7 sunt greu de aplicat, atâta timp, cât statele în speță își folosesc dreptul de veto pentru a se proteja reciproc. Acest sprijin mutual reprezintă cel mai mare impediment al Uniunii, în vederea utilizării acestei proceduri.

Prin urmare, soluția optimă, în cazul combaterii populismului prin această metodă ar fi ca sancționarea, în baza art. 7, să fie întreprinsă simultan în cazul celor două state, dreptul de veto fiind suspendat, având în vedere faptul că statele membre, care fac obiectul sancțiunii, nu pot vota. Sancționarea comună ar fi posibilă, întrucât ambelor state li se aduc aceleași acuzații, și anume încălcarea statului de drept, amenințarea independenței judiciare și oprimarea libertății presei (Hoffmann, 2018, 1179 – 1182). Cu toate acestea, dificultatea apare, atunci când, sancțiunea este pus în practică, deoarece art. 7 ar trebui interpretat amplu, având în vedere faptul, că articolul menționează explicit că se referă la un singur stat membru, prin expresiile „încălcări grave și persistente [...] de către un stat membru", „statul membru în cauză" și „acelui stat membru" (Jurnalul Oficial, 2012, 19).

O altă modalitate, prin care UE ar putea contracara populismul, o constituie suspendarea din spațiul Schengen, această acțiune fiind posibilă, deoarece una dintre condițiile aderării la Schengen este cooperarea cu agențiile care aplică legea din celelalte state membre, inclusiv cooperarea judiciară, iar respectarea statului de drept reprezintă o condiție în vederea aderării. Prin urmare, ținând cont de faptul că, aceste două condiții sunt imperios necesare gestionării eficiente a celor 26 de state și a acestei unici frontiere, Ungaria și Polonia

[1] Acest mecanism a mai fost folosit în cazul Austriei, împotriva liderului de extremă-dreapta, Jorg Haider, dar pe atunci nu era un era un proces care includea două etape, sancțiunile putând fi aplicate direct. Cu toate că, sancțiunile în acest caz au fost simbolice, UE a fost percepută de cetățenii austrieci, ca având o atitudine necorespunzătoare. Din acest motiv, Tratatul de la Nisa din 2001 a introdus o etapă suplimentară în cadrul art.7. Astfel, până în cazul Poloniei, acest articol nu a mai fost utilizat, Uniunea luând în considerare consecințele politice pe care le puteau genera.

ar putea fi constrânse să renunţe la reformele populiste, care ameninţă statul de drept şi independenţa judiciară, prin suspendarea apartenenţei la Schengen. De asemenea, această sancţiune ar putea fi implementată mai uşor decât cea prevăzută la art. 7, deoarece necesită numai votul cu majoritate calificată. Sancţiunea ar putea ajuta la diminuarea susţinerii electoratului faţă de partidele populiste, având în vedere faptul, că cetăţenii nu ar mai beneficia de libera circulaţie în cadrul celorlalte state membre, iar comerţul şi turismul ar fi afectate.

Cu toate acestea, în ciuda tendinţelor Uniunii de a implementa sancţiunile prevăzute la art. 7 din TUE, am putut remarca faptul, că presiunile financiare reprezintă principala modalitate de a constrânge partidele populiste, deoarece atât Polonia, cât şi Ungaria depind de fondurile primite de la UE, pentru a depăşi decalajele economice dintre aceste state şi statele mai dezvoltate. Mai mult, aceste fonduri sunt necesare partidelor, inclusiv pentru a-şi putea implementa politicile populiste (Hoffmann, 2018, 1182 – 1186). Nu consider că aceste măsuri ar putea duce la dispariţia populismului, dar reprezintă o soluţie viabilă, în vederea diminuării şi estompării efectelor lui. Cu toate acestea, aplicarea sancţiunilor trebuie făcută cu precauţie, pentru ca aceste acţiuni să nu intensifice sentimentul anti-european în rândul populaţiei. Astfel, Uniunea trebuie să evite să fie considerată, din cauza implementării sancţiunilor, un actor rău intenţionat de către cetăţenii statelor în speţă.

Consideraţii finale

Prin urmare, pot afirma faptul că, populismul este una dintre cele mai importante surse de vulnerabilitate a Uniunii, subminând principiile care stau la baza acesteia. Mai exact, am putea concluziona fapul că, prin folosirea ideologiei populiste este afectat, într-o oarecare măsură, atât echilibrul de putere dintre statele membre, cel interinstituţional, cât şi balanţa de putere la nivel global. Mai mult, având în vedere că reprezentanţii populişti înţeleg politica în sensul unui război, pot afirma faptul că, în comparaţie cu un război convenţional, acesta va fi unul de lungă durată, având în vedere că nu necesită multe resurse.

Cu toate că, reprezentanţii partidelor Fidesz şi Pis au reuşit să fragmenteze societatea, prin încercarea de a redistribui puterea în cadrul Uniunii Europene, nu am putute ajunge la o concluzie certă cu privire la efectele pe care le au partidele în speţă asupra echilibrului de putere. Mai exact, am concluzionat faptul că, impactul populismului asupra echilibrului de putere este rezultatul expansiunii fenomenului în

Uniunea Europeană, fiind un rezultat colectiv al partidelor care au adoptat această ideologie, cele două partide, percepute individual, neavând puterea de influențare suficientă.

Astfel, cu toate că reprezentanții partidelor Fidesz și PiS sunt cei mai vocali și consecvenți în retorica lor populistă și atitudinea eurosceptică, balanța de putere este afectată, din cauza amplorii fenomenului în Uniunea Europeană. Cu toate acestea, pot afirma faptul că, utilizarea populismului de către aceste două partide, poate duce la încurajarea altor politicieni de a adopta, la rândul lor, o atitudine populistă, adâncind decalajul dintre statele democratice liberale și cele în care se încearcă subminarea liberalismului.

Referințe bibliografice:

Lucrări din literatura de specialitate

1. Brubaker Rogers, "Why populism?", în *Populism and the Crisis of Democracy: Volume 1: Concepts and Theory*, Gregor Fitzi, Jürgen Mackert, Bryan S. Turner (ed.), Routledge, New York, 2019.

2. de Cleen Benjamin, "Populism and Nationalism", în *The Oxford Handbook of Populism*, Cristóbal R. Kaltwasser et al. (ed.), Oxford University Press, United Kingdom, 2017.

3. Eiermann Martin, Monunk Yascha, Gultchin Limor, *European Populism: Trends, Threats and Future Prospects*, Tony Blair Institute for Global Change, United Kingdom, 2017.

4. Fitzi Gregor, "Populism. An ideal-typical assessment", în *Populism and the Crisis of Democracy: Volume 1: Concepts and Theory*, Gregor Fitzi, Jürgen Mackert, Bryan S. Turner (ed.), Routledge, New York, 2019.

5. Freeden Michael*, Ideologies and political theory: A Conceptual Approach*, Clarendon Press, Oxford, 1996.

6. Gebhard Carmen, "The Problem of Coherence in the European Union's International Relations", în International Relations and the European Union, Christopher Hill, Michael Smith, Sophie Vanhoonacker (ed.), Ediția a III-a, Oxford University Press, Oxford, 2017.

7. Kaltwasser R. Cristóbal, "How to define populism? Reflections on a contested concept and its (mis)use in the social sciences", în Populism and the Crisis of Democracy: Volume 1: Concepts and Theory, Gregor Fitzi, Jürgen Mackert, Bryan S. Turner (ed.), Routledge, New York, 2019.

8. Keukeleire Stephan, Delreux Tom, *The Foreign policy of the European Union*, Palgrave Macmillan, United Kingdom, 2014.

9. Mackert Jürgen, "Introduction: Is there such a thing as populism?", în *Populism and the Crisis of Democracy: Volume 1: Concepts and Theory*, Gregor Fitzi, Jürgen Mackert, Bryan S. Turner (ed.), Routledge, New York, 2019.

10. Mudde Cas, *Populist Radical Right Parties in Europe*, Cambridge University Press, Cambridge, 2007.

11. Saul John, "Africa", în *Populism – It's Meaning and National Characteristics*, Ghiţă Ionescu, Ernest Gellner, The Garden City Press Limited, Letchworth, 1969, p. 170.

12. Soare Sorina, „Genul şi speciile populismului românesc. O incursiune pe tărâmul Tinereţii fără bătrâneţe şi al Vieţii fără de moarte", în *Partide şi personalităţi populiste în România postcomunistă*, Sergiu Gherghina, Sergiu Mişcoiu (ed.), Institutul European, Iaşi, 2010.

13. Stanley Ben, "Populism in Central and Eastern Europe", în *The Oxford Handbook of Populism*, Cristóbal R. Kaltwasser et al. (ed.), Oxford University Press, United Kingdom, 2017.

14. Taggart Paul, "Populism and 'unpolitics'", în *Populism and the Crisis of Democracy: Volume 1: Concepts and Theory*, Gregor Fitzi, Jürgen Mackert, Bryan S. Turner (ed.), Routledge, New York, 2019.

15. Waltz N. Kenneth, *Theory of International Politics*, Addison-Wesley Publishing Company, Massachusetts, 1979.

Articole, comunicări ştiinţifice

16. Ágh Attila, "Decline of democracy and increasing populism in East-Central Europe: Populist democracy as electoral autocracy in Hungary", ECPR Joint Sessions, Pisa, 2016.

17. Copilaş Emanuel, "Simbolistica politică românească: între populism şi cinism?", în *Sfera Politicii*, Vol. 21, No. 2 (174), 2013.

18. Hoffmann Michael, "[PiS]sing off the Courts: the PiSParty's Effect on Judicial Independence in Poland", în *Vanderbilt Journal of Transnational Law*, Vol. 51, No. 5, 2018.

19. Krekó Péter, Juhász Attila, "Beyond populism: political tribalism in Poland and Hungary", în *Turkish Policy Quarterly*, Vol. 18, No. 3, 2019.

20. Kurylo Bohdana, "The discourse and aesthetics of populism as securitisation style", în *International Relations I-21*, Sage, London, 2020.

21. Mudde Cas, "The populist Zeitgeist", în *Government and Opposition*, Vol. 39, No. 4, Cambridge University Press, 2004.

22. Segbers Klaus, "Introduction ´Populism in Europe`", în *Populism in Europa - An Overview, CGP Working Paper Series*, Segbers Klaus (ed.), Freie Universität Berlin, Berlin, 2018.

23. Shafir Michael, "From Historical to "Dialectical" Populism: The Case of Post-Communist Romania", în *Canadian Slavonic Papers,* Vol. L, Nos. 3 - 4, Taylor & Francis Ltd., 2008.

24. Thorhallsson Baldur, "How Do Little Frogs Fly?: Small States in the European Union", în *Norwegian Institute for International Affairs*, Policy Brief No. 12, Norway, 2015.

25. Weyland Kurt, "Neoliberal Populism in Latin America and Eastern Europe", în *Comparative Politics*, Vol. 31, No. 4, 1999.

Legislație europeană

26. Jurnalul Oficial al Uniunii Europene, *Versiunea consolidată a Tratatului privind Uniunea Europeană*, C 326, 2012.

Surse internet

27. Current Events Poland, "Our aim to govern is not motivated by a revenge or to get even. (…) The time of integrity is about to begin in Poland," says Jarosław Kaczyński during his speech in Warsaw.", Current Events Poland, publicat la: 24 octombrie 2015, disponibil la: https://www.currentevent spoland.com/news/Jaroslaw-Kaczynski-speech-on-2015-parliamentary-elections. html, accesat la data de 3 mai 2023.

28. Deutsche Welle, "Kaczynski: Poland will stand its ground in EU spat ", Deutsche Welle, publicat la: 26 ianuarie 2018, disponibil la: https://www. dw.com/en/kaczynski-poland-will-stand-its-ground-in-eu-spat/a-42318494, accesat la data de 3 mai 2023.

29. Euractiv, "Kaczyński: Poland did not invite refugees, has right to say 'no' ", Euractiv, publicat la: 3 iulie 2017, disponibil la: https://www. euractiv.com/section/justice-home-affairs/news/kaczynski-poland-did-not-invite-refugees-has-right-to-say-no/, accesat la data de 3 mai 2023.

30. European Commission, Defence Industry and Space, „Hybrid Threats", European Commission, disponibil la: https://ec.europa.eu/defence-industry-space/eu-defence-industry/hybrid-threats_en, accesat la data de 5 mai 2023.

31. Flux On-Line, "Discurs despre starea națiunii al lui Viktor Orban, Prim-ministru al Ungariei", Flux On-Line, publicat la: 27 februarie 2018, disponibil la: https://flux.md/stiri/discurs-despre-starea-natiunii-al-lui-viktor-orban-prim-ministru-al-ungariei#, accesat la data de 3 mai 2023.

32. Hybrid CoE, "Hybrid threats as a concept", Hybrid CoE, disponibil la: https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/, accesat la data de 5 mai 2023.

33. Notes from Poland, "Kaczyński, Le Pen, Orban and other leaders meet in Warsaw to reject EU's «social engineering»", Notes from Poland, publicat la: 5 decembrie 2021, disponibil la: data de https://notesfrompoland. com/2021/12/05/kaczynski-le-pen-orban-and-other-leaders-meet-in-warsaw-to-reject-eus-social-engineering/, accesat la data de 8 mai 2023.

34. Silvia Amaro, "Hungary's nationalist leader Viktor Orban is ruling by decree indefinitely amid coronavirus", CNBC, publicat la: 21 martie 2020,

disponibil la: https://www.cnbc.com/2020/03/31/coronavirus-in-hungary-viktor-orban-rules-by-decree-indefinitely.html, accesat la data de 3 mai 2023.

35. Visegrád Post, " Samizdat No. 8", Visegrád Post, publicat la: 24 mai 2021, disponibil la: https://visegradpost.com/de/2021/05/24/samisdat-nr-8/, accesat la data de 5 mai 2023.

36. Visegrád Post, "Im Hinblick auf die kommenden Europawahlen steht Viktor Orbán gegenüber Brüssel und dem Globalismus – Gesamte Rede", Visegrád Post, publicat la: 24 octombrie 2018, disponibil la: https://visegradpost.com/de/2018/10/24/im-hinblick-auf-die-kommenden-europawahlen-steht-viktor-orban-gegenuber-brussel-und-dem-globalismus-gesamte-rede/, accesat la data de 3 mai 2023.

37. Visegrád Post, "Viktor Orbán: „Wir müssen den außenpolitischen Amoklauf der europäischen Linken beenden." - Samisdat Nr. 9", Visegrád Post, publicat la: 8 iunie 2021, disponibil la: https://visegradpost.com/de/2021/06/08/viktor-orban-wir-muessen-den-aussenpolitischen-amoklauf-der-europaeischen-linken-beenden-samisdat-nr-9/, accesat la data de 3 mai 2023.

38. Visegrád Post, "Viktor Orbáns Rede nach seiner Vereidigung zum Ministerpräsidenten", Visegrád Post, publicat la: 12 mai 2018, disponibil la: https://visegradpost.com/de/2018/05/12/viktor-orbans-rede-nach-seiner-vereidigung-zum-ministerpraesidenten/, accesat la data de 3 mai 2023.

ECOURI ALE TRECUTULUI, CONTURÂND VIITORUL: EVOLUȚII ALE NARAȚIUNILOR STRATEGICE PROMOVATE DE VLADIMIR PUTIN ÎN DISCURSURILE DIN ADUNAREA FEDERALĂ

Andrei-Cristian MORARU*

Abstract:

The present study conducts a comprehensive content analysis of the presidential speeches delivered by Vladimir Putin at the Federal Assembly of the Russian Federation in the years 2021, 2022, and 2023. The research aims to identify the strategic narratives endorsed by the Russian government in these discourses, while also aiming to establish their evolution over time, comparing them with the national security objectives of the Russian Federation post-2021.

The analysis demonstrates a marked shift in the foreign policy of Russia from a defensive and reactive stance in the year 2021 to a more assertive and proactive one in the speeches delivered by Putin in 2022 and 2023. Such discourses have been observed to emphasize the central role played by Russia in the global arena, while also strongly advocating for the pursuit of its national interests.

Moreover, this study provides a significant contribution to the redefinition of the conceptual framework of strategic narratives, viewing them as a tool that is utilized by aggressor states to justify military actions, and more importantly, to establish a strong position in the international power dynamics.

The findings of this study offer valuable insights into the strategic narratives that are promoted by the Russian government, and the evolution of such narratives over time. The research has critical implications for policymakers, scholars, and other individuals who are interested in understanding Russia's foreign policy priorities and its positioning on the global stage. The study underscores the significance of discursive strategies and the role that they play in shaping a country's foreign policy objectives, particularly in times of geopolitical tensions. Overall, this research constitutes a relevant contribution to the understanding of Russian foreign policy and the vital importance of strategic narratives in shaping such a policy.

Keywords: *discourse analysis, presidential speeches, Vladimir Putin, Federal Assembly, strategic narratives.*

* Doctorand în cadrul Academiei Naționale de Informații „Mihai Viteazul”, București, moraru.andrei@animv.eu

Introducere

Studiul narațiunilor strategice a devenit o preocupare majoră în cercetările politico-militare contemporane, iar analiza de conținut a discursurilor publice reprezintă o metodă de cercetare relevantă, pentru înțelegerea și interpretarea narațiunilor. În acest context, prezentul articol analizează evoluția narațiunilor strategice ale președintelui rus Vladimir Putin, în discursurile susținute în cadrul Adunării Federale a Federației Ruse, din anii 2021, 2022 și 2023. Analiza este fundamentată pe un cadru teoretic realist, care presupune justificarea acțiunilor militare și asigurarea poziției Federației Ruse în dinamica de putere internațională, prin mijloace discursive.

În contextul politico-militar actual, Federația Rusă continuă să reprezinte o amenințare la adresa securității europene. În ultimii ani, statul rus a demonstrat o abordare de tip hard-power, în ceea ce privește acțiunile militare și de politică externă, după cum se poate observa în istoria recentă a regiunii est-europene – anexarea Peninsulei Crimeea în anul 2014, acțiunile militare în Siria, din anul 2015 și intervenția militară din estul Ucrainei în anul 2022. De asemenea, Rusia s-a angajat în campanii de dezinformare și propagandă, cu scopul de a influența percepțiile și de a submina instituțiile europene și a valorilor promovate, demonstrând un interes strategic pentru consolidarea poziției în regiune, prin creșterea influenței în fostele state sovietice și consolidarea alianțelor, cu state care manifestă poziții ostile față de Alianța Nord-Atlantică.

În acest context, este important să analizăm modul în care, liderii Federației Ruse folosesc narațiunile strategice pentru a justifica acțiunile militare și pentru a consolida poziția statului în balanța de putere. În mod special, pentru prezenta cercetare este relevantă înțelegerea și interpretarea evoluțiilor acestor narațiuni, în cadrul discursurilor prezidențiale, din Adunarea Federală a Federației Ruse. Prin intermediul acestor activități de origine patriotică, Adunarea Federală a devenit o platformă îngrijorătoare, prin care statul rus își prezintă viziunea asupra rolului său în cadrul comunității internaționale și în relația cu statele europene. Prin urmare, analiza narațiunilor strategice, promovate în discursurile menționate, poate dezvălui narațiuni strategice folosite de autoritățile ruse, pentru a consolida poziția în fața altor state și organizații internaționale, precum și gradul în care aceste narațiuni se adaptează la schimbările din sfera politică și militară.

Prin utilizarea analizei de conținut, ca metodă de cercetare calitativă, se urmărește identificarea și evaluarea evoluțiilor narațiunilor

strategice promovate de Vladimir Putin. Studiul propune o perspectivă realistă în interpretarea naraţiunilor strategice ruse, evidenţiind modul în care, acestea sunt folosite pentru justificarea acţiunile militare şi pentru consolidarea poziţiei statului rus, în dinamica de putere internaţională. Această abordare contribuie la dezvoltarea, în mediul academic, a perspectivei pe care liderii Federaţiei Ruse o au asupra rolului discursurilor publice şi a naraţiunilor strategice, în promovarea imaginii statului.

Stadiul cercetării în domeniu

Pentru îndeplinirea obiectivului cercetării, va fi definit conceptul de naraţiune strategică conform viziunii realiste, cu menţionarea elementelor constitutive, ulterior, fiind amintite diferenţele dintre naraţiunile constructive şi distructive.

Naraţiunile strategice sunt „reprezentările şi discursurile elaborate de actorii politici, pentru a construi şi promova anumite imagini, idei şi mesaje" (Edelman 1985, 17). Un alt autor sugerează, că termenul se referă la „sistemele de idei, reprezentări şi simboluri pe care actorii politici le folosesc pentru a-şi justifica şi promova anumite poziţii, politici şi acţiuni" (Cox 1996, 128). Aceste naraţiuni sunt construite într-un mod strategic, pentru a promova interese naţionale şi pentru a influenţa opinia publică. Conform unei conceptualizări mai recente a naraţiunilor strategice, acestea reprezintă „povestiri şi relatări construite în mod deliberat de către indivizi sau organizaţii pentru a promova anumite mesaje, interese sau ideologii, pentru a-şi consolida puterea sau pentru a influenţa opinia publică într-un anumit mod" (Wicks 2021, 23). În urma analizării definiţiilor menţionate, au fost identificate următoarele elemente, care stau la baza creării de naraţiuni strategice: simboluri – ca reprezentări, utilizate pentru promovarea mesajelor, percepţii – reflectând valori şi interese, pe care actorii încearcă să le promoveze, perspective – ca mod în care, actorii construiesc o imagine asupra evenimentelor şi a realităţii.

Naraţiunile strategice pot fi clasificate drept constructive şi distructive, în funcţie de efectele scontate. Naraţiunile strategice constructive sunt relatări, construite pentru a determina schimbări şi percepţii pozitive, prin promovarea de soluţii la problemele sociale, politice sau economice existente. În termeni realişti, naraţiunile au scopul de a determina schimbarea percepţiilor altor state sau a altor actori asupra propriului stat, în conformitate cu paradigma propusă în spaţiul public. Naraţiunile distructive descriu modul în care, anumite

state sau actori utilizează discursuri pentru a submina securitatea, stabilitatea sau imaginea altor state sau regiuni. Printre elementele caracteristice, putem aminti utilizarea de informații false sau distorsionate, crearea de imagini negative ale adversarilor sau ale grupurilor țintă și utilizarea unui discurs diviziv. Scopul principal al narațiunilor strategice distructive este crearea de tensiuni și diviziuni în interiorul diferitelor state și organizații internaționale sau în relațiile dintre acestea.

Cu scopul stabilirii stadiului cercetării în domeniu, au fost studiate lucrări științifice din domeniu, având drept metodă principală de cercetare analiza de conținut a discursurilor publice, din perspectivă realistă.

O lucrare fundamentală, recentă, care a analizat narațiunile strategice promovate de Vladimir Putin în discursurile sale, din cadrul Adunării Federale, aparține lui Smith (2021, 20-37). În cadrul acesteia, autorul a folosit analiza de conținut și analiza narativă ca parte integrată a cercetării, evidențiind rolul narațiunilor promovate în construirea imaginii Rusiei, ca putere globală și legitimarea acțiunilor militare. Relevanța studiului constă în identificarea unor teme narative de bază, precum „Rusia ca pilon principal în balanța de putere", „SUA ca instigator", „Demonizarea occidentală" și altele, care au evoluat de-a lungul timpului și oferă o confirmare postulatului lucrării de față, care susține că, discursurile lui Vladimir Putin, din cadrul Adunării Federale, sunt relevante pentru înțelegerea evoluției și prioritizării narațiunilor strategice oficiale.

În studiul lui Williams et al. (2022, 34-49), autorul sugerează că narațiunile strategice ale lui Vladimir Putin manipulează percepția publică, cu privire la politica externă a Federației Ruse și conduce la formarea de opinii favorabile, din partea societății europene, față de agresiunea rusă. De asemenea, Garcia (2021) susține că, discursurile lui Putin afectează sistemul democratic al statelor europene, subminând suveranitatea și independența acestora și producând revolte interne cu impact destabilizator. În articolul lor, Jones și Davis (2020, 75-88) subliniază importanța propagandei și a narațiunilor strategice în subminarea valorilor democratice ale statelor europene în favoarea autoritarismului. În timp ce toate cele trei studii indică impactul negativ al narațiunilor strategice ale lui Putin asupra opiniei publice, cu privire la valorile democratice, diferențele se găsesc în perspectiva și elementele analizate: Williams et al. (2022, 34-49) se concentrează pe impactul narațiunilor strategice asupra opiniei publice în Rusia și în străinătate,

Garcia (2021) pe influenţa naraţiunilor strategice asupra sistemelor democratice din Europa de Est, iar Jones şi Davis (2020, 75-88) subliniază importanţa propagandei, în subminarea valorilor democratice ale statelor europene. Toate cercetările identifică un efect negativ al naraţiunilor strategice distructive promovate de Vladimir Putin, acestea manipulând percepţia publică şi reducând valorile democratice la un nivel inacceptabil, din perspectivă statală.

Alţi cercetători din domeniul ştiinţelor comunicării şi al ştiinţelor militare explorează influenţa naraţiunilor strategice pe timpul conflictelor militare în care Federaţia Rusă a fost implicată. Brown şi David (2022, 56-74) explorează evoluţia naraţiunilor strategice ruse în perioada 2014 – 2022 (de la anexarea Crimeii până la conflictul ruso-ucrainean actual), evidenţiind utilizarea acestora pentru a justifica acţiuni militare şi politice agresive. De asemenea, Brown, Smith şi Johnson (2022, 102-120) analizează obiectivul justificativ al naraţiunilor strategice ruse, contribuind la înţelegerea implicării Rusiei în conflictul din Siria şi în regiunea Donbas din Ucraina. Kuzmina (2020, 161–179) se concentrează asupra naraţiunilor strategice ale statului rus în contextul crizei ucrainene, iar Rozin (2020, 131–145) compară naraţiunile strategice ale Federaţiei Rusiei în conflictul din Siria şi cel din Ucraina, prin analiza acoperirii pe care acestea o au în portalurile de ştiri europene. Într-un alt studiu, Shekhovtsov (2021, 52–66) examinează naraţiunile oficiale ruse, care fac referire la Ucraina şi evoluţia acestora în timp, subliniind faptul, că acestea sunt dezvoltate şi utilizate pentru a justifica intervenţia Rusiei în Ucraina şi anexarea Peninsulei Crimeea, precum şi pentru a promova politica de expansiune a statului în regiune. Analizând aceste lucrări ştiinţifice, putem identifica un obiectiv comun – autorii se concentrează asupra naraţiunilor strategice ale Federaţiei Ruse şi a modului în care acestea sunt utilizate, pentru a justifica acţiuni militare. De asemenea, toţi cercetătorii subliniază că naraţiunile strategice ruse au fost folosite pentru a promova poziţia statului pe scena internaţională şi pentru a extinde influenţa sa în regiune. Studiile evidenţiază importanţa înţelegerii naraţiunilor strategice şi a modului în care acestea sunt utilizate în scopuri politice, precum şi necesitatea dezvoltării unei strategii eficiente de comunicare, pentru a combate urmările destabilizatoare ale discursurilor subversive.

O serie de autori au studiat naraţiunile strategice, din perspectiva realistă a relaţiilor interstatale dintre Federaţia Rusă şi alţi actori statali regionali:

Deacon (2018, 4962–4978) a analizat narațiunile strategice, din perspectiva diviziunii europene Est-Vest și impactul acestora asupra relațiilor internaționale. Figueira (2019, 32–59) a examinat narațiunile strategice în contextul conflictului sirian și a relațiilor dintre SUA și Rusia. Horowitz (2018, 343–370) a analizat impactul narațiunile strategice în disputa din Marea Chinei de Sud. Jackson (2020, 82) a abordat narațiunile strategice ruse, în contextul relațiilor Federației Ruse cu Occidentul. Chen și Li Ming (2021, 115-129) au explicat gradul de asimilare în practica politicii externe a Federației Ruse, a narațiunilor expuse de Vladimir Putin în contextul relațiilor ruso-chineze. În final, Johnson, Brown și Smith (2021, 42-57) au analizat modul în care, narațiunile strategice ale lui Putin au influențat relațiile ruso-americane în ultimul deceniu. Prin explorarea relațiilor internaționale, autorii au evidențiat importanța narațiunilor strategice pentru modelarea percepțiilor, identităților naționale și promovarea valorilor. În plus, narațiunile promovate de liderii politici ai Federației Ruse sunt utilizate pentru a consolida poziția statului, în cadrul sistemului internațional și pentru a contracara influența statelor adversare. În ciuda faptului, că cercetătorii abordează relația dintre Federația Rusă și actori statali în mod diferit, aceștia își îndreaptă atenția spre construirea și utilizarea narațiunilor, ca instrumente de modelare a realității politice și sociale, în contextul relațiilor internaționale.

Metodologia cercetării științifice

Lucrarea de față, fundamentată pe lucrări științifice, care relevă impactul narațiunilor strategice distructive ale Federației Ruse asupra securității europene, vine în sprijinul instituțiilor europene, care sunt în măsură să evalueze și să prevină riscurile asociate discursurilor subversive. În acest sens, au fost formulate obiectivele, ipotezele și direcțiile aferente cercetării.

Obiectivul principal al cercetării constă în determinarea evoluțiilor narațiunilor strategice ale Federației Ruse, în perioada 2021-2023, în conformitate cu conținutul comunicării din discursurile lui Vladimir Putin, susținute cu ocazia Adunării Federale.

Obiectivul menționat a fost stabilit, ca urmare a stabilirii următoarei ipoteze de lucru: Narațiunile strategice promovate de Vladimir Putin în discursurile din cadrul Adunării Federale, din perioada 2021-2023 au caracter evolutiv distructiv, având drept scop destabilizarea spațiului european.

Pentru îndeplinirea obiectivului de cercetare, pornind de la ipoteza enunţată, a fost stabilită o direcţie de cercetare. În cadrul acesteia, sunt analizate din punct de vedere al contextului comunicării discursurile vizate, ulterior fiind stabilite elemente de interes punctate pe timpul discursurilor, apoi, fiind identificate naraţiunile promovate de Vladimir Putin, în conformitate cu o schemă de codificare stabilită în secţiunea prezentă. Ulterior, este analizată evoluţia naraţiunilor oficiale, ca finalitate a cercetării.

Studiul foloseşte o metodă calitativă de cercetare pentru îndeplinirea obiectivului, analiza de conţinut. Această metodă de cercetare implică identificarea şi analizarea detaliată a unui set de date din documente, interviuri sau discursuri, pentru a identifica modele, teme şi tendinţe specifice. Conform lui Krippendorff (2013), analiza de conţinut este o metodă de cercetare, care se concentrează pe extragerea şi interpretarea semnificaţiilor din texte, prin identificarea conceptelor, ideilor şi temelor importante, comune (Krippendorff 2013, 21).

Conform lui Neuendorf (2016, 65-105), există cinci etape ale analizei de conţinut:

- *Stabilirea obiectivelor şi întrebărilor de cercetare*;
- *Selectarea unităţilor de analiză*: această etapă implică selectarea tipurilor de informaţii (cuvinte, fraze, imagini etc.) care vor fi analizate;
- *Dezvoltarea schemei de codificare*: implică dezvoltarea unei scheme de codificare care să permită categorizarea informaţiilor selectate;
- *Codificarea datelor*: poate fi realizată manual sau utilizând un software specializat;
- *Interpretarea şi raportarea rezultatelor*.

În cercetarea de faţă, unitatea de analiză este reprezentată de conţinutul discursurilor lui Vladimir Putin, susţinute cu ocazia Adunării Federale, în perioada 2021-2023. Conform obiectivului de cercetare stabilit, am dezvoltat următoarea schemă de codificare, având drept criteriu principal scopul naraţiunilor promovate:

Categoria 1 (C1): *Naraţiuni strategice constructive*

1.1.: Promovarea şi menţinerea intereselor strategice ale Federaţiei Ruse în Europa şi în regiunea Caucazului şi Asiei Centrale;

1.2.: Asigurarea independenţei economice şi politice a Federaţiei Ruse;

1.3.: Superioritatea istoriei și valorilor culturale ale Federației Ruse.

Categoria 2 (C2): *Narațiuni strategice distructive*

2.1.: Discreditarea valorilor democratice din Uniunea Europeană;

2.2.: Exacerbarea tensiunilor geopolitice în Europa;

2.3.: Încurajarea separatiștilor și a altor mișcări anti-guvernamentale în Europa;

2.4.: Susținerea mișcărilor extremiste în Europa și în regiunea Caucazului și Asiei Centrale.

Categoriile menționate acoperă tematici din discursurile lui Putin, care sunt legate de obiectivele de securitate națională ale Federației Ruse post-2021. În aplicarea schemei de codificare, vom analiza conținutul discursiv, identificând următoarele coduri:

Actorii:

- Federația Rusă;
- Aliați;
- Adversari.

Poziționarea:

- Defensivă (se apără anumite poziții sau acțiuni ale Federației Ruse);
- Ofensivă (se atacă poziția altor state sau organizații internaționale).

Subiectul:

- Securitatea națională (cu accent pe obiectivele și interesele de securitate națională ale Federației Ruse);
- Politica internațională (poziția și acțiunile Federației Ruse în raport cu alte state sau organizații internaționale);
- Politica internă (poziția și acțiunile Federației Ruse în raport cu problemele interne).

Acțiunea propusă:

- Diplomatică (sugerează soluții diplomatice);
- Militară (sugerează soluții care se bazează pe acțiuni militare);
- Economică (sugerează soluții economice).

Relația cu Occidentul:

- Colaborare (promovează colaborarea și cooperarea cu țările Vestice);
- Confruntare (promovează opoziția față de țările Vestice);
- Neutralitate (promovează poziții neutre în raport cu țările Vestice).

Atitudinea discursivă:

- Pozitivă (promovează atitudini pozitive sau prezintă situaţii favorabile);
- Negativă (promovează atitudini negative sau prezintă situaţii nefavorabile).

Alegerea celor trei discursuri ale lui Vladimir Putin, din perioada 2021-2023 a fost bazată pe trei factori:

- *Relevanţa discursurilor*: Cele trei discursuri din Adunarea Federală reprezintă momente-cheie în care, liderul rus adresează publicului larg şi instituţiilor naţionale probleme importante şi politici prioritare. Aceste discursuri acoperă o perioadă semnificativă de timp şi sunt susceptibile de a conţine naraţiuni oficiale şi mesaje strategice ale guvernului rus;
- *Puterea instituţională a Adunării Federale*: Adunarea Federală a Federaţiei Ruse, compusă din Duma de Stat şi Consiliul Federaţiei, are un rol important în procesul legislativ şi decizional al Rusiei. Discursurile susţinute în faţa acestei instituţii conferă o legitimitate şi importanţă sporită naraţiunilor şi politicilor promovate de liderul rus;
- *Accesul la informaţii de încredere*: Discursurile preşedintelui rus sunt disponibile publicului pe platforma online oficială. Acest aspect oferă cercetătorilor oportunitatea de a analiza cu atenţie conţinutul şi de a identifica naraţiuni specifice, care pot fi asociate poziţiilor oficiale asumate de Federaţia Rusă.

Rezultatele cercetării

Conflictul, în curs de desfăşurare, din estul Europei este o sursă de tensiune, între Federaţia Rusă şi Occident de cel puţin un deceniu. Anexarea Peninsulei Crimeea de către Rusia, în 2014 a declanşat nemulţumiri atât în rândul populaţiei ucrainene, cât şi din partea comunităţii internaţionale, iar situaţia a escaladat în ultimii ani. Ambele părţi s-au acuzat reciproc de agresiune, iar conflictul ruso-ucrainean actual a condus la victime numeroase şi persoane strămutate. Conflictul regional rămâne nerezolvat, în ciuda eforturilor diplomatice.

În acest context, Vladimir Putin a susţinut o serie de discursuri, cu ocazia Adunărilor Federale ale Federaţiei Ruse, bazându-se pe naraţiuni conexe tensiunilor dintre stat şi comunitatea europeană şi internaţională, cu accent pe implicarea Statelor Unite ale Americii în conflict. Discursurile publice susţinute de Vladimir Putin, cu ocazia

Adunărilor Federale ale Federației Ruse au fost difuzate live, nu doar pe canalele de televiziune și online, ci și în școli, clădiri guvernamentale și locuri publice din Rusia și pe spațiul teritoriilor anexate din Ucraina.

În conformitate cu criteriile de analiză menționate în secțiunea anterioară, în cadrul discursului susținut în cadrul Adunării Federale, în anul 2021 (President of Russia 2021), Vladimir Putin a abordat mai multe aspecte ale politicii interne și externe ale Federației Ruse.

În termeni de tip de discurs, acesta a avut un *caracter predominant defensiv*, întrucât Putin a prezentat și a apărat pozițiile și acțiunile Federației Ruse, în fața criticilor și presiunii internaționale. El a subliniat importanța respectării suveranității și a intereselor naționale ale Rusiei, precum și necesitatea unei abordări echilibrate în relațiile internaționale.

Tema centrală a discursului a fost *politica internațională*, punând accent pe poziția și acțiunile Federației Ruse, în raport cu alte state sau organizații internaționale. Putin a evidențiat importanța securității naționale și a cooperării internaționale, dar și a dezvoltării economice și a suveranității naționale. Liderul rus a abordat subiecte, precum securitatea regională, lupta împotriva terorismului și rolul Rusiei în politica internațională.

În ceea ce privește acțiunile propuse, Putin a sugerat *soluții diplomatice* pentru abordarea problemelor internaționale. Președintele rus a evidențiat importanța dialogului și cooperării între state, pentru rezolvarea conflictelor și menținerea păcii și stabilității globale. Acesta a subliniat necesitatea respectării dreptului internațional și a principiilor ONU, promovând astfel, o abordare bazată pe diplomație și negocieri.

În raport cu Occidentul, discursul lui Putin a avut o *atitudine de confruntare*. Acesta a exprimat critici față de politica țărilor vestice, acuzându-le de duble standarde și de intervenții în afacerile interne ale statului rus. Președintele a subliniat necesitatea respectării suveranității și independenței naționale, reafirmând poziția fermă a Rusiei în apărarea propriilor interese.

Atitudinea discursivă a fost, în mare parte, negativă. Vladimir Putin a evidențiat provocările și amenințările cu care se confruntă Federația Rusă, precum presiunile economice și politice din partea statelor occidentale. El a criticat acțiunile Vestului și a evidențiat impactul negativ al unor decizii și politici internaționale asupra suveranității și intereselor Rusiei. Prin această abordare discursivă negativă, Putin a încercat, să legitimeze și să susțină acțiunile Federației Ruse, în contextul relațiilor internaționale.

Rezumând, discursul lui Putin din Adunarea Federală, din anul 2021 (President of Russia 2021) a avut un caracter defensiv, s-a concentrat pe politica internaţională, a sugerat soluţii diplomatice, a promovat o atitudine de confruntare faţă de Occident şi a avut o atitudine discursivă negativă.

În baza analizei întreprinse, coroborat cu schema de codificare stabilită în cercetare, următoarele naraţiuni strategice au fost identificate:

„Rusia este promotoarea păcii şi prosperităţii în regiune" (C1.1): Putin a prezentat Rusia ca o forţă stabilizatoare în regiune, promovând pacea şi prosperitatea. Acesta a prezentat Rusia, ca un actor central în spaţiul geopolitic, menţinând influenţa politică şi economică în Europa şi în regiunea Caucazului şi Asiei Centrale. A subliniat importanţa consolidării parteneriatelor strategice şi a menţinerii stabilităţii regionale, pentru a-şi păstra poziţia de lider şi pentru a proteja interesele de securitate ale statului;

„Rusia îşi apără suveranitatea prin măsuri economice şi financiare" (C1.2): Putin a subliniat importanţa asigurării independenţei economice şi politice a Rusiei, comparând-o cu o fortăreaţă puternică şi impregnabilă. A argumentat că, această independenţă este esenţială pentru protejarea intereselor naţionale şi a luat măsuri, pentru diversificarea economiei şi consolidarea autonomiei financiare;

„Valorile democratice din Uniunea Europeană sunt o iluzie" (C2.1): Putin a criticat Uniunea Europeană, prezentând-o ca o iluzie a democraţiei autentice. A sugerat că, valorile democratice din UE sunt discreditate, prin corupţia instituţionalizată şi prin lipsa unei guvernări eficiente. Astfel, a încercat să submineze credibilitatea şi legitimitatea sistemului democratic european;

„NATO intervine provocator în afacerile altor state" (C2.2): Putin a descris tensiunile geopolitice în Europa, ca un „dans periculos" (President of Russia 2021), în care acţiunile NATO şi implicarea ţărilor vestice amplifică instabilitatea şi ameninţările regionale. A evidenţiat implicarea NATO în afacerile interne ale altor state, sugerând că, acest lucru alimentează tensiunile şi accentuează rivalităţile geopolitice;

„Rusia reprezintă vocea mişcărilor de liberare" (C2.3): Putin a sugerat, că Federaţia Rusă reprezintă o voce de susţinere a mişcărilor separatiste şi a celor anti-guvernamentale din Europa. A susţinut că, aceste mişcări reflectă nemulţumirile populare şi că Rusia le sprijină în lupta lor, pentru libertate şi dreptate, prezentându-se ca un susţinător al justiţiei sociale.

Aceste narațiuni au fost utilizate de Vladimir Putin în discursul său (President of Russia 2021), pentru a promova și apăra pozițiile statului rus, a legitima acțiunile Federației Ruse și a influența percepția publicului asupra evenimentelor și relațiilor geopolitice. Prin crearea unor imagini metaforice, președintele rus a încercat să capteze atenția statelor europene, să consolideze sprijinul intern și să exercite presiuni asupra statelor și organizațiilor internaționale, cu care Federația Rusă se află în relații tensionate.

În anul 2022, discursul anual al lui Vladimir Putin din cadrul Adunării Federale a Federației Ruse a fost înlocuit de o adresă, susținută public în data de 21 februarie (President of Russia 2022), marcată de un moment istoric important: recunoașterea independenței Republicii Populare Donetsk și Republicii Populare Lugansk.

Analiza discursului lui Vladimir Putin din adresa oficială, din anul 2022 (President of Russia 2022), relevă mai multe aspecte semnificative.

În ceea ce privește tipul de discurs adoptat, acesta poate fi descris ca fiind *defensiv*, concentrându-se pe apărarea pozițiilor și acțiunilor Federației Ruse. Putin încearcă să justifice politica externă a Rusiei și să răspundă criticilor și presiunilor internaționale printr-un discurs argumentativ.

Tema principală abordată în discursul său se referă la *politica internațională*, fiind descrise acțiunile Federației Ruse, în raport cu securitatea regională, relațiile bilaterale și interesele geopolitice ale statului. Astfel, liderul rus încearcă să ofere o perspectivă coerentă și consistentă asupra poziției asumate în sfera internațională.

În ceea ce privește acțiunile propuse, Putin sugerează *soluții diplomatice*, ca mijloc de rezolvare a conflictelor și consolidare a relațiilor internaționale. Acesta subliniază importanța dialogului și negocierilor în promovarea păcii și stabilității globale, evidențiind rolul crucial al diplomației, în obținerea unor rezultate pozitive. Astfel, liderul rus încearcă, să promoveze o abordare cooperativă și bazată pe dialog în rezolvarea diferendelor interstatale.

În ceea ce privește relația cu Occidentul, Putin adoptă o poziție de *confruntare*, exprimând opoziția față de anumite politici și acțiuni ale țărilor occidentale. El subliniază discrepanțele de viziune și interese, dintre Rusia și Vest, criticând presiunea și sancțiunile impuse de țările occidentale asupra Rusiei. Astfel, discursul său reflectă o atitudine de opoziție și de apărare a intereselor naționale rusești, în fața ingerințelor externe.

Atitudinea discursivă promovată de Putin în adresa sa oficială din 2022 este în mare parte *pozitivă*. Preşedintele prezintă realizările şi contribuţiile Rusiei în contextul politic şi economic internaţional, subliniind rolul pozitiv al ţării în promovarea stabilităţii şi securităţii regionale. În acelaşi timp, el accentuează importanţa respectului reciproc şi a relaţiilor bazate pe echitate şi beneficii reciproce. Prin aceasta, Putin încearcă să consolideze imaginea Rusiei ca actor global angajat în cooperarea internaţională.

În concluzie, discursul lui Vladimir Putin din anul 2022 (President of Russia 2022) se încadrează într-un tip de discurs defensiv, în care abordează teme legate de politica internaţională, oferind soluţii diplomatice şi exprimând o poziţie de confruntare faţă de Occident. Atitudinea discursivă promovată este predominant pozitivă, evidenţiind realizările şi contribuţiile Rusiei în context internaţional.

În discursul său din 2022 (President of Russia 2022), Vladimir Putin a prezentat mai multe naraţiuni sub formă figurativă, evidenţiind anumite aspecte-cheie ale politicii internaţionale şi ale poziţiei asumate de Federaţia Rusă în sfera internaţională.

„Rusia este promotoarea păcii şi prosperităţii în regiune" (C1.1): Putin a subliniat importanţa menţinerii unui echilibru strategic şi a influenţei Rusiei în Europa şi regiunea Caucazului şi Asiei Centrale. El a folosit imagini metaforice, descriind statul rus ca „un vultur în zbor", „stâlpul de susţinere al stabilităţii" şi „centrul gravitaţional" al acestor regiuni (President of Russia 2022). Prin această imagine, liderul rus îşi propune să consolideze autoritatea şi să transmită un mesaj puternic de apărare a intereselor naţionale în regiune;

„Forţa şi prosperitatea statului rus depind de coeziunea şi solidaritatea poporului rus" (C1.2): Putin a accentuat importanţa unităţii naţiunii ruse în faţa provocărilor economice şi politice. El a prezentat Rusia ca o entitate puternică şi independentă, susţinând că, forţa şi prosperitatea ţării depind de coeziunea şi solidaritatea poporului rus. Această naraţiune îşi propune să consolideze identitatea naţională şi să inspire patriotism şi angajament faţă de statul rus;

„Valorile democratice din Uniunea Europeană sunt o iluzie" (C2.1): Putin a subliniat necesitatea cooperării globale şi a construirii unui sistem internaţional, bazat pe echitate şi respect reciproc. El a criticat valorile democratice ale Uniunii Europene, descriindu-le ca fiind „o mască a manipulării" şi „o iluzie a libertăţii" (President of Russia 2022). Prin aceasta, liderul rus sugerează că Rusia este o alternativă la modelul european, promovând ideea unei ordini mondiale diferite;

„Rusia se apără împotriva amenințărilor cibernetice din partea Occidentului” (C2.2): Putin a evidențiat importanța protejării suveranității informaționale și a securității cibernetice, în contextul tensiunilor geopolitice din Europa. El a descris Rusia ca fiind „o fortăreață digitală” (President of Russia 2022) și a avertizat asupra amenințărilor cibernetice la adresa statelor și societății ruse din partea Occidentului. Această narațiune subliniază importanța pe care statul rus o acordă securității și suveranității în era digitală.

Narațiunile strategice promovate de Vladimir Putin, în adresa sa din anul 2022 (President of Russia 2022) au avut drept scop consolidarea poziției Federației Ruse în plan internațional, de a transmite putere și determinare, precum și de a contesta aspecte specifice ale ordinii mondiale. Acestea se bazează, pe o combinație de retorică patriotică, critici la adresa Vestului și promovarea intereselor strategice ale statului. Prin aceste narațiuni, președintele rus încearcă să mobilizeze sprijinul intern și extern, pentru agenda sa politică și să-și consolideze legitimitatea ca lider al Federației Ruse.

Susținerea discursului public, din anul 2023 (President of Russia 2023) a coincis cu „vizita-surpriză” a președintelui american Joe Biden la Kiev, moment în care, acesta a oferit un discurs cu ocazia primei sale vizite de la începutul invaziei. În ziua următoare, Putin a făcut o apariție scurtă, la un miting la stadionul Luzhniki din Moscova, pentru a comemora Ziua Apărătorului Patriei. Miting-ul a fost organizat, pentru a celebra curajul și vitejia soldaților și veteranilor ruși și a marca Adunarea Federală din anul 2023.

În cadrul discursului public, susținut în anul 2023 cu ocazia Adunării Federale Ruse (President of Russia 2023), au fost identificate următoarele aspecte, în conformitate cu criteriile de analiză propuse:

Discursul susținut este de tip *ofensiv*, deoarece liderul statului adoptă o poziție agresivă și acuzatoare față de NATO și țările vestice. Acesta atacă și critică pozițiile și acțiunile acestora, prezentându-i ca pe o amenințare directă la adresa Federației Ruse și sugerând, că acțiunile Alianței Nord-Atlantice fac parte dintr-un plan mai amplu, de eliminare a poporului rus de pe harta lumii.

Tema dominantă a discursului este *politica internațională*, în special relația Rusiei cu NATO și țările vestice. Vladimir Putin susține, că NATO și Statele Unite ale Americii sunt o amenințare existențială pentru Federația Rusă și denunță acțiunile lor în Ucraina, precum și în alte conflicte regionale istorice. Liderul rus subliniază nevoia statului, de a se apăra și de a proteja interesele proprii de securitate.

Liderul statului sugerează *soluţii de natură militară mai degrabă decât diplomatică*. Acesta menţionează dezvoltarea şi modernizarea armamentului strategic al Rusiei şi ameninţă că, statul rus va răspunde testelor nucleare efectuate de către SUA. Vladimir Putin a folosit un ton agresiv, pe timpul acestei părţi discursive, sugerând o abordare de tip hard-power pentru soluţionarea conflictului regional.

Discursul promovează o relaţie de *confruntare* cu Occidentul, în special cu NATO şi ţările vestice. Vladimir Putin acuză Alianţa Nord-Atlantică de ipocrizie, prin încercarea de înlocuire a actualei ordini internaţionale şi prin atacul direct la adresa intereselor naţionale ale Rusiei. Acesta promovează o imagine, care afişează Rusia într-un conflict permanent cu Occidentul, alimentând tensiunile şi polarizarea relaţiilor internaţionale.

Atitudinea discursivă este predominant negativă. Putin prezintă NATO şi Occidentul ca agresori, deoarece, conform acestuia, folosesc metode manipulative de inducere în eroare a societăţii europene, prin fake-news, în acest fel proiectându-şi „interesele malefice" (President of Russia 2023) în raport cu Rusia. Liderul rus subliniază ameninţările percepute la adresa securităţii şi a existenţei statului şi evidenţiază acţiunile şi politica agresivă impusă de Occident, asupra propriului popor, încercând să legitimeze şi să mobilizeze sprijinul poporului rus.

Astfel, discursul lui Vladimir Putin din anul 2023 (President of Russia 2023), poate fi caracterizat ca fiind unul ofensiv, cu o temă centrată pe politica internaţională, promovând soluţii militare mai mult decât diplomatice, o relaţie de confruntare cu Occidentul şi o atitudine negativă în general.

În cadrul discursului din anul 2023, au fost identificate următoarele naraţiuni strategice:

„Rusia este promotoarea păcii şi prosperităţii în regiune" (C1.1): Vladimir Putin prezintă statul rus, ca un actor cheie în menţinerea stabilităţii şi securităţii regionale pentru Ucraina şi alte ţări vecine, care au nevoie de sprijin;

„Rusia este garant al independenţei economice şi politice" (C1.2): Liderul rus subliniază rolul statului în asigurarea securităţii naţionale şi protejarea intereselor proprii, într-un context internaţional dificil. Prin această idee, Putin îşi legitimează politica de securitate şi apărare implementată şi încearcă să mobilizeze sprijinul poporului;

„Rusia este promotorul valorilor tradiţionale şi conservatoare în societatea europeană" (C1.3): Preşedintele rus a susţinut ideea, că „apărăm valorile noastre tradiţionale şi conservatoare, care sunt

fundamentale pentru identitatea și coeziunea societății" (President of Russia 2023). În același context, acesta a explicat faptul că, Federația Rusă și-a luat un angajament de promovare a acestor valori, la nivel regional și internațional, considerate ca fiind esențiale pentru identitatea și coeziunea societății europene;

„Valorile democratice din Uniunea Europeană sunt o iluzie" (C2.1): Conform președintelui rus, „valorile democratice din Europa sunt adesea doar „vorbe frumoase" (President of Russia 2023). Acesta denunță valorile democratice promovate în Europa, susținând că, elementele existente de corupție rămân probleme nerezolvate. Prin promovarea acestei narațiuni, Vladimir Putin încearcă să submineze credibilitatea și legitimitatea sistemului democratic european și să promoveze propria viziune asupra guvernării Europei;

„Rusia este victimă a acțiunilor ostile ale Occidentului" (C2.1): Vladimir Putin descrie sancțiunile aplicate Federației Ruse, ca fiind „nedrepte" și menționează că Uniunea Europeană folosește campanii de dezinformare „menite să slăbească și să submineze stabilitatea internă" a statului rus (President of Russia 2023);

„Europa este centrul de renaștere al nazismului" (C2.1): Putin a prezentat Europa, ca fiind în pragul unei renașteri a ideologiei naziste, sugerând că, valorile și politicile promovate de statele europene sunt similare cu cele ale Germaniei naziste. Președintele rus a explicat faptul că, sub influența NATO și a țărilor vestice, Uniunea Europeană a adoptat politici discriminatorii, rasiste sau extremiste, care amenință pacea și stabilitatea regională;

„Rusia și Ucraina sunt frați în lupta împotriva neo-nazismului occidental" (C2.3): Vladimir Putin face referire la amenințările și violența exercitate de către „neo-naziști occidentali" (President of Russia 2023) în regiunile Donetsk, Lugansk, Zaporozhye și Kherson. Prin menționarea termenului de „neo-naziști", Putin sugerează că, există elemente ideologice extremiste în Ucraina, care reprezintă amenințări pentru aceste regiuni și pentru poporul rus. Președintele subliniază solidaritatea dintre regiunile rusești și cele menționate, descriindu-le ca fiind „adevărați frați și surori" (President of Russia 2023).

Astfel, discursul lui Vladimir Putin susținut cu ocazia Adunării Federale, în anul 2023, relevă o serie de narațiuni strategice, care prezintă preponderent elemente distructive și critici la adresa Uniunii Europene și NATO, adoptând o poziție ofensivă, în contrast cu discursurile anterioare. Narațiunile identificate folosesc, de asemenea, termeni cu substrat istoric înrădăcinat în valorile patriotice ale

poporului rus promovate de-a lungul timpului (lupta împotriva nazismului), cu scopul de întărire a ideii, că Vladimir Putin este liderul potrivit pentru întreaga regiune. De asemenea, solidaritatea şi fraternitatea dintre Rusia şi regiunile ucrainene reprezintă idei puternic promovate în cadrul discursului, cu scopul de manipulare a maselor şi deviere a percepţiilor poporului ucrainean, despre intenţiile Federaţiei Ruse în regiune.

Ca urmare a analizei de conţinut, întreprinsă în baza obiectivului general al cercetării, au fost identificate naraţiunile strategice promovate de Vladimir Putin în discursurile publice din cadrul Adunărilor Federale, din perioada 2021-2023. Astfel, naraţiunile prezente în discursurile lui Vladimir Putin au evoluat într-o direcţie, care accentuează retorica conflictuală şi polarizarea. În timp ce unele naraţiuni, cum ar fi cele referitoare la independenţa economică şi politică a Federaţiei Ruse, au persistat şi s-au consolidat de-a lungul anilor, altele au devenit mai ostile şi distructive în ultimul an.

Aşadar, observăm o creştere a numărului criticilor aduse valorilor democratice europene în discursurile din 2023. Putin denunţă valorile democratice promovate în Europa, susţinând că, acestea nu au un substrat bazat pe adevăr şi că existenţa problemelor nerezolvate, precum corupţia, împiedică implementarea unor valori democratice coerente. În acelaşi timp, acesta promovează viziunea proprie asupra guvernării şi susţine ideea unei alternative ruseşti la modelul european.

În plus, Vladimir Putin prezintă Federaţia Rusă, ca victimă a acţiunilor ostile ale Occidentului, în mod special, în discursul din anul 2023. Sancţiunile aplicate Rusiei sunt descrise ca fiind nedrepte, iar campaniile de dezinformare ale Uniunii Europene sunt considerate o ameninţare la adresa stabilităţii interne. Această naraţiune alimentează sentimentul de victimizare şi justifică acţiunile Rusiei, în faţa percepţiei de ostilitate din partea Occidentului.

Evoluţia naraţiunilor identificate indică o schimbare în tonul şi conţinutul discursurilor lui Vladimir Putin, către o retorică mai dură şi o abordare conflictuală. Această schimbare poate fi atribuită unui cumul de factori, precum tensiunile geopolitice, rivalităţile regionale şi nevoia de a-şi consolida autoritatea şi de a cere sprijinul intern al poporului. Există o continuitate, în privinţa anumitor naraţiuni de la un an la altul, precum perspectiva Rusiei ca centru regional, care apare în toţi cei trei ani analizaţi. Aceasta subliniază importanţa menţinerii influenţei şi echilibrului geopolitic în regiune şi interesul statului rus acordat acestui obiectiv strategic.

Totodată, naraţiunea promovată de Vladimir Putin referitoare la Europa, ca centru de ideologie nazistă a evoluat de la recunoaşterea valorilor democratice şi a drepturilor omului la prezentarea Uniunii Europene, ca un focar al ideologiei neo-naziste. Această schimbare reflectă creşterea tensiunilor dintre Rusia şi Occident, iar prin denunţarea Europei, ca centru al ideologiilor extremiste, Vladimir Putin întăreşte poziţia rusă de stat adversar şi justifică politica externă agresivă, alimentând tensiunile geopolitice şi consolidând sprijinul intern, prin crearea unei percepţii de ameninţare existenţială.

De asemenea, putem observa o amplificare şi o intensificare a retoricii anti-occidentale în naraţiunile identificate, în anul 2023, comparativ cu cele din 2021 şi 2022. Această evoluţie poate fi explicată, prin deteriorarea relaţiilor dintre Rusia şi Occident în ultimii ani, precum şi prin schimbările geopolitice şi acţiunile militare desfăşurate de NATO în perioada analizată.

Coroborând informaţiile prezentate, se poate susţine confirmarea ipotezei de cercetare conform căreia, naraţiunile strategice promovate de Vladimir Putin în discursurile din cadrul Adunării Federale,, din perioada 2021-2023, au caracter evolutiv distructiv, având drept scop destabilizarea spaţiului european. În acest sens, putem observa că, în anul 2023, în cadrul discursului analizat apar naraţiuni, care includ acuzaţii mai puternice şi mai controversate, cum ar fi sugestia că Europa este în pragul unei renaşteri a ideologiei naziste. Aşadar, în discursurile mai recente ale lui Vladimir Putin, naraţiunile iau o formă conflictuală şi au rol diviziv.

Concluzii

În concluzie, cercetarea de faţă şi-a îndeplinit obiectivul general, determinarea evoluţiilor naraţiunilor strategice ale Federaţiei Ruse în perioada 2021-2023, în conformitate cu conţinutul comunicării, din discursurile lui Vladimir Putin susţinute cu ocazia Adunării Federale, iar ipoteza de lucru a fost confirmată, fiind identificat caracterul evolutiv distructiv al acestor naraţiuni.

Conform analizei de conţinut întreprinse, se poate stabili faptul că, evoluţia acestor naraţiuni se datorează încercărilor de exploatare a vulnerabilităţilor spaţiului de securitate european, prin raportare la percepţii sociale asupra conflictului şi asupra intenţiilor Federaţiei Ruse în regiune. Astfel, preşedintele rus aplică metoda intoxicării adversarului cu informaţii false, în vederea stabilirii efectelor şi a modului optim de

sabotaj a sistemului european de securitate, pentru îndeplinirea obiectelor strategice ale Federaţiei Ruse.

Limitarea principală a cercetării din prezentul articol este determinată de faptul că, perioada de timp acoperită este scurtă, din punct de vedere al evoluţiilor în relaţiile internaţionale. În plus, o abordare comparativă a discursurilor altor conducători sau reprezentanţi internaţionali ar putea oferi o perspectivă mai cuprinzătoare asupra dinamicii naraţiunilor strategice, în contextul instabilităţii determinate de conflictul ruso-ucrainean. Prin continuarea cercetării în alte articole ştiinţifice, consider că, studiul de faţă are potenţialul de a aduce plus-valoare sistemului naţional de apărare şi comunităţii naţionale de informaţii, precum şi în instituţiile europene pe plan regional şi poate susţine procesele de luare a deciziilor în domeniul securităţii şi apărării.

Bibliografie:

1. Adjei, Michael A., şi Cheryl A.R. Gallant. 2018. "Constructing a Strategic Narrative for Ghana: A Critical Discourse Analysis of President Mahama's State of the Nation Addresses." *Africa Today* 3 (65): 2–19.

2. AERA. 2022. *What is document analysis?* https://www.aera.net/Professional-Opportunities-Funding/Graduate-Student-Opportunities-and-Resources/Online-Learning-Modules/What-is-Document-Analysis

3. Bowen, G.A. 2009. "Document analysis as a qualitative research method." *Qualitative Research Journal* 2 (9): 27-40.

4. Brown, A., J. Smith, şi R. Johnson. 2022. "Putin's Strategic Narratives in the Syrian Conflict." *International Journal of Conflict and Violence* 1 (16): 89-104.

5. Brown, Sarah, şi Johnson David. 2022. "The Evolution of Putin's Strategic Narratives: From the Annexation of Crimea to the Crisis in Ukraine." *European Journal of Political Science* 1 (21): 56-74.

6. Chen, Wei, şi Ming Li. 2021. "Putin's Strategic Narratives in the Context of Sino-Russian Relations." *Asian Journal of Political Science* 2 (29): 115-129.

7. Consiliul de Securitate al Federaţiei Ruse. 2021. *Стратегия национальной безопасности Российской Федерации (National Security Strategy of the Russian Federation).* Kremlin.

8. Cox, Robert. 1996. "Social Forces, States and World Orders." *Beyond International Relations Theory* (Macmillan) 126-147.

9. Creswell, J.W. 2014. *Research design: qualitative, quantitative, and mixed methods approaches.* Thousand Oaks, California: Sage publications.

10. Deacon, Vanessa. 2018. "Strategic Narratives in International Relations: Understanding the East-West Divide in Europe." *International Journal of Communication* (12): 4962–4978.

11. ECRDC. 2021. *Document analysis.* https://ecrdc.eu/glossary/document-analysis/

12. Edelman, Murray. 1985. "Constructing the Political Spectacle." *The New York Times.* New York, 6 august.

13. Figueira, Filipa. 2019. "The Importance of Narrative in Foreign Policy: The Case of the United States and Russia in the Syrian Conflict." *Strategic Studies Quarterly* 4 (13): 32–59.

14. Garcia, Maria. 2021. *Putin's Strategic Narratives in Eastern Europe.* New York: Oxford University Press.

15. Horowitz, Michael C. 2018. "The Impact of Strategic Narratives on Great Power Politics: Lessons from the South China Sea." *Journal of Strategic Studies* 3 (41): 343–370.

16. Jackson, Michael. 2020. *Putin's Strategic Narratives and Russia's Relations with the West.* London: Routledge.

17. Johnson, R., A. Brown, și J. Smith. 2021. "Putin's Strategic Narratives and the Future of US-Russian Relations." *Journal of International Relations and Foreign Policy* 1 (9): 42-57.

18. Jones, M., și K. Davis. 2020. "Putin's Strategic Narratives and the Erosion of Democracy in Russia." *Journal of Politics and Society* 1 (31): 75-88.

19. Krippendorff, K. 2004. *Content analysis: An introduction to its methodology.* Thousand Oaks, California: Sage Publications.

20. Krippendorff, K. 2013. *Content analysis: An introduction to its methodology.* Vol. ed. a 3-a. Thousand Oaks, California: Sage Publications.

21. Kuzmina, Yulia. 2020. "Russia's Strategic Narratives on the Ukraine Crisis: A Textual Analysis of Russian and English-Language News Coverage." *Journal of International Communication* 2 (26): 161–179.

22. Lynch, Dov. 2018. "The Strategic Narrative of the Islamic State: An Analysis of English-Language Magazines 2014–2017." *Perspectives on Terrorism* 3 (12): 73–87.

23. Mannheim, Karl. 1952. "The problem of generations." În *Essays on the sociology of knowledge*, 276-320. London: Routledge.

24. Neuendorf, K.A. 2016. *The content analysis guidebook.* Thousand Oaks, California: Sage Publications.

25. Pan, Zhongdang, și Gerald M. Kosicki. 2019. "The Power of Metaphor in Strategic Narrative: How Persuasive Strategies Shape the Story of ISIS in Western Media." *Communication Monographs* 1 (86): 1–24.

26. President of Russia. 2022. *Address by the President of the Russian Federation.* 21 februarie. Accesat la data de 18 mai, 2023. http://en.kremlin.ru/events/president/news/67828

27. President of Russia. 2023. *Presidential Address to Federal Assembly.* 21 februarie. Accesat la data de 18 mai, 2023. http://en.kremlin.ru/events/president/ news/70565

28. President of Russia. 2021. *Presidential Address to the Federal Assembly.* 21 aprilie. Accesat la data de 18 mai, 2023. http://en.kremlin.ru/events/president/news/65418

29. Rozin, Igor. 2020. "Russia's Strategic Narratives on Syria and the Conflict with Ukraine: A Comparative Analysis of TV News Coverage." *European Journal of Communication* 2 (35): 131–145.

30. Shekhovtsov, Anton. 2021. "The Kremlin's Narrative on Ukraine: From Moral Equality to Russian World." *Journal of Contemporary Central and Eastern Europe* 1 (29): 52–66.

31. Simons, Greg, și Annika Werner. 2019. "Strategic Narratives and the Reconstruction of the South African State." *Strategic Studies Quarterly* 4 (13): 6–31.

32. Smith, John. 2021. "Strategic Narratives in Putin's Speeches to the Federal Assembly: Constructing Russia's Global Power Image and Legitimizing Military Actions." *Journal of International Relations* 3 (20): 20-37.

33. Wicks, R.H. 2021. "Strategic narratives: A concept analysis". *International Journal of Humanities and Social Science Research* 2 (9): 20-28.

34. Williams, Emma et.al. 2022. "The Impact of Putin's Strategic Narratives on Public Opinion in Russia and Abroad." *International Journal of Public Opinion Research* 1 (34): 34-49.

DIFUZIA PUTERII DE LA ACTORII STATALI LA CEI NON-STATALI

Octavian-Alexandru-Ştefan BROŞTEANU*

Abstract:

The diffusion of power in world politics has brought a lot of changes, regarding the importance of non-state actors on the global stage. It is a new phenomenon, amplified by the spread of the Internet and the technological revolution, and has in the foreground that states are losing control of certain aspects of everyday life, their place being taken by non-state organizations.

These new actors take advantage of the fact that you no longer have to be "great" to be relevant on the international stage, thus foreshadowing a series of conflicts between states and non-state organizations for the coming decades. Since the national security of a state remains a duty of the intelligence services, this topic can represent a starting point for the development of other scientific writings, given the fact that, in Romania, the subject of power diffusion is little addressed.

Specifically, the case study method will be used, analysing terrorist organizations, cross-border criminal organizations, hackers/hacktivists, respectively the so-called "empowered individuals" and the street movements they can cause.

The results want to underline that, apart from more or less conventional conflicts between the states, non-state actors can also represent a risk factor, or even a threat, to their security. Considering that some of the non-state actors benefit from the support of the population, then all those who look after ensuring national security must pay more attention on them, to prevent negative events.

In conclusion, states must be aware of the fact that they are no longer the only entities benefiting from power resources. Of course, we cannot talk about an equalization of power between state and non-state actors. However, we must all be aware of the role, both positive, but especially destructive, that non-states can have, it being a mistake to consider that the national security of the state can only be disturbed by conventional risks and threats.

Keywords: *power, non-states, security, conflict.*

* Student masterand în cadrul Academiei Naţionale de Informaţii „Mihai Viteazul” din Bucureşti – programul „Managementul Informaţiilor de Securitate Naţională” - anul II, e-mail octavian.brosteanu@gmail.com

Introducere

Difuzia puterii de la actorii statali la cei non-statali reprezintă o noutate în politica mondială, acest fenomen impactând major modul în care se vor desfășura interacțiunile în sistemul internațional în următoarele decenii. Având multiple cauze la bază, de la privatizarea anumitor servicii publice până la apariția unor noi spații de manifestare ale actorilor, imposibil de controlat sau de monopolizat de către actorii statali, difuzia puterii poate reprezenta atât un lucru pozitiv, cât și negativ la adresa securității statelor și a oamenilor.

În cadrul acestui articol, am intenționat să remarc unele implicații, în special de ordin negativ, ale difuziei puterii, pentru a sublinia într-un mod cât mai obiectiv anumite riscuri și amenințări la adresa statelor și a cetățenilor care pot rezulta în urma fenomenului. De asemenea, fac precizarea că m-am axat mai puțin pe descrierea fenomenului în sine, cât pe detalierea acțiunilor desfășurate de anumiți actori care beneficiază de pe urma acestuia, utilizând metodologia științifică a studiului de caz. Astfel, actorii selectați sunt organizațiile teroriste, grupările de criminalitate organizată, hackerii sau hacktiviștii, companiile private respectiv mișcările de stradă și așa-numiții *empowered individuals*[1]. Obiectivele urmărite sunt acelea de a identifica modalitatea în care, acești actori pot deveni relevanți în politica mondială, respectiv pot impacta securitatea națională a statelor.

În literatura străină există importante scrieri în domeniul fenomenului de difuzie a puterii, cele mai multe amintite și în cadrul lucrării, precum cele ale lui Joseph Nye, Richard Haass, Ian Bremmer, Keelan Waldron, Zbigniew Brzezinski, Barry Buzan sau Moises Naim. Totodată, există și autori ale căror scrieri, deși, nu au în prim-plan fenomenul de difuzie a puterii propriu-zis, ajută la înțelegerea acestuia, precum Robert Gilpin, John Mearsheimer sau Henry Kissinger. Cu toate acestea, pentru literatura românească, scrierile existente pe acest fenomen se rezumă la câteva articole de specialitate sau de presă, iar personal, consider că fenomenul trebuie să beneficieze de o atenție sporită.

Fenomenul difuziei de putere

Concret, putem remarca faptul că, politica mondială nu mai este doar atributul guvernelor naționale. Asistăm la un monopol *spart* al

[1] Persoane care au dobândit suficientă putere, ce le conferă posibilitatea de a se impune pe scena internațională, respectiv de a-i influența pe alții să-i urmeze.

statelor, în care „indivizi singulari şi organizaţii particulare, de la Wikileaks la corporaţii şi ONG-uri, teroriști şi mişcări sociale spontane, toate au de acum puterea de a juca un rol în politica lumii" (Nye, 2015, *Secolul American*).

Exemplificativă în acest sens, este modalitatea de exercitare a puterii dure – *hard*, cu precădere din perspectivă militară. Putem remarca faptul, că statele au început să piardă monopolul asupra a ceea ce înseamnă forţă armată, conflictele între grupări nestatale, între două grupuri militare organizate care nu aparţin de niciun stat, înregistrând o tendinţă ascendentă după anul 2008, devenind tot mai dese (Naim, 2015). Tehnica militară şi tehnologiile avansate, care nu până mai demult erau rezervate doar armatelor naţionale, au ajuns să fie disponibile şi altor actori, precum teroriştii sau armatele private, fenomenul fiind denumit de către Joseph Nye drept *privatizare a războiului* (Nye, 2012, *Viitorul puterii*).

De asemenea, puterea financiară şi puterea soft sunt într-o proporţie mare gestionate de operatori privaţi, cel puţin în ţările occidentale. Acestea sunt realizate, prin companii care contribuie la bugetele consolidate ale statelor ori prin instrumente culturale, precum filme sau muzică sau cu ajutorul unor personalităţi celebre, care au din ce în ce mai multă putere în a influenţa opiniile populaţiei.

Un nou areal de manifestare a difuziei puterii, pe care îl identifică Joseph Nye este cyberspaţiul. Domeniul internetului s-a dezvoltat într-un mod extraordinar în ultimele decenii, existând o transformare substanţială a tehnologiilor comunicării şi calculatoarelor, care accentuează fenomenul de difuzie (Nye, 2012, *Viitorul puterii*). Pe internet, oamenii aderă comunităţilor transnaţionale, susţin sau nu anumite iniţiative civice, realizează tranzacţii, oferă date personale, au acces la ştiri globale, diminuându-se astfel restrângerea, cauzată de teritoriul fizic al statului naţional. Datorită faptului că asistăm la cea mai mare migraţie din istoria omenirii, cea în spaţiul digital, răspândirea informaţiei va atenta la monopolul birocraţiei tradiţionale, puterea având o distribuţie mai largă atât între state, cât şi între ONG-uri, teroriști, indivizi şi organizaţii private sau corporaţii (Nye, 2012, *Viitorul puterii*).

Noii actori reprezintă interesele publice, trecând peste jurisdicţia ţărilor, respectiv ajută la dezvoltarea unor noi norme, prin intermediul presiunilor asupra guvernelor, cu scopul modificării politicilor, schimbând indirect percepţiile asupra legitimităţii (Nye, 2012, *Viitorul puterii*).

În consecinţă, avem de-a face cu un nou *pol* de putere, denumit de Moises Naim drept *microputere*. Microputerile sunt actori mici, care erau cândva neglijabili, ce au reuşit să contrabalanseze puterea marilor jucători, reuşind să-i îngrădească sau chiar să-i învingă (Naim, 2015). Ele demonstrează, că nu trebuie să mai beneficiezi de mari resurse de putere pentru a te afirma. În schimb, acestea utilizează o gamă largă de noi tehnici prin care „îi epuizează, împiedică, subminează, sabotează şi atacă prin învăluire" (Naim, 2015) pe marii jucători, creând, în special, riscuri şi ameninţări de ordin hibrid la adresa statelor. Cu toate acestea, încă, nu au o influenţă mai mare decât actorii statali în politica mondială, însă, fenomenul este început recent, se află în plină evoluţie şi merită o atenţie deosebită pentru viitor.

Actori non-statali implicaţi în fenomenul difuziei puterii

Difuzia puterii de la actorii statali la cei non-statali reprezintă un fenomen nou, amplificat de răspândirea internetului şi a revoluţiei tehnologice şi are în prim-plan faptul, că statele scapă de sub control anumite arii ale vieţii de zi cu zi, locul lor fiind luat de către organizaţii non-statale, care capătă din ce în ce mai multă putere. Aşadar, afacerile globale nu mai sunt rezervate doar statelor, ci şi organizaţiilor care nu reprezintă interesele vreunei ţări, care acţionează independent, promovând un interes comun al oamenilor şi care se bucură de susţinerea unui număr important de persoane. Astfel, putem interpreta că acţiunile non-statalilor pot genera o serie de riscuri şi ameninţări neconvenţionale la adresa securităţii statelor şi implicit a cetăţenilor.

Pe scena internaţională îşi fac locul persoane şi organizaţii care beneficiază de pe urma faptului, că nu trebuie să mai fii *mare* pentru a fi important, precum organizaţii teroriste, insurgenţi, hackeri, hacktivişti, organizaţii non-guvernamentale, companii, organizaţii de criminalitate transfrontalieră, indivizi carismatici sau mişcări de stradă spontane. Toate acestea folosesc o combinaţie de instrumente de ordin convenţional şi hibrid, de la influenţă asupra opiniei publice până la războaie cu alte state, pentru a-şi maximiza influenţa în politica mondială.

În general, microputerile beneficiază de *putere blândă*, întrucât reuşesc să atragă sprijinul populaţiei, prin măsuri care sporesc atracţia, factorul decisiv care ajută la propagarea ideilor promovate fiind *cyberspaţiul*. De asemenea, anumite microputeri beneficiază şi de pe urma deţinerii de resurse financiare, pe care le transformă în putere dură, fiind capabile să desfăşoare diverse operaţiuni armate împotriva

guvernelor, căutând să-şi promoveze interesele prin luptă. În continuare, voi detalia anumite aspecte de interes privindu-i pe actorii menţionaţi anterior şi voi încerca să explic, de ce au aceştia importanţă în politica mondială şi impact asupra securităţii statelor, în baza unui studiu de caz realizat asupra acestora.

Prima categorie de actori non-statali la care voi face referire sunt organizaţiile teroriste, în special, cele de sorginte islamistă, care au început să devină din ce în ce mai vizibile pe plan internaţional. Astfel, evenimentele din 11 septembrie 2001 din Statele Unite ale Americii, în care gruparea Al-Qaeda a distrus cele două turnuri gemene din New York, a lovit Pentagonul şi a mai deturnat încă un avion, pot reprezenta un punct de debut al influenţei globale a organizaţiilor de acest tip. În context, Al-Qaeda a demonstrat, că puterea SUA este limitată şi că nu mai trebuie să fi o mare forţă militară pentru a provoca daune importante. De altfel, atacurile au costat aproximativ 500.000 de dolari, în vreme ce, distrugerile şi intervenţia americană, ce a urmat în Orientul Mijlociu, au provocat daune SUA de aproximativ 7 trilioane de dolari. Un prim scop, urmărit de teroriști este ca statele afectate să reacţioneze disproporţionat, din cauza impactului psihologic pe care l-a produs respectivul atentat. Ulterior, Al-Qaeda a mai produs şi alte atentate în state occidentale, precum cele din Spania 2004 sau Marea Britanie 2005.

Creşterea în relevanţă a grupărilor teroriste le fac capabile să ducă confruntări directe cu armatele statale. Un bun exemplu aici, poate fi conflictul dintre Israel şi Hezbollah din 2006, în care, vreme de mai bine de o lună, armata israeliană şi luptători ai Hezbollah au purtat un război asimetric. Accesul la tehnologie militară, utilizarea propagandei, folosirea de celule bine instruite şi rachetele lansate în zone cu populaţie civilă densă au făcut ca Hezbollah să obţină o victorie politică (Nye, 2012, *Viitorul puterii*), deşi, strict militar, au avut mai multe pierderi decât Israel. Hezbollah au bombardat oraşul Haifa cu rachete de tip Katiuşa, au avariat puternic nava Hanit a forţelor israeliene, folosind o rachetă de 60.000 de dolari, în comparaţie cu nava care costase 260 de milioane de dolari şi care, era dotată cu sisteme antirachetă (Naim, 2015) şi au reuşit să respingă şi câteva atacuri convenţionale, prin folosirea războiului de gherilă, precum cel asupra oraşului libanez Bint Jbeil. De asemenea, atât Israel, cât şi Hezbollah s-au atacat reciproc, prin diverse canale media, propagând propriile idei în rândul populaţiei din zonă. Putem observa că, microputerile actuale pot *fura* victoria armatelor mai bine pregătite într-un conflict asimetric (Naim, 2015), în acest sens, fundamentându-se principiul de *privatizare* a războiului. Observăm că, putem discuta despre

o disponibilitate *la raft* a tehnologiilor militare, confecționarea armamentului necesar teroriștilor devenind mai puțin costisitoare.

Și mai recent, putem observa conflictul dintre Israel și Hamas, din luna mai a anului 2021. Ca urmare a unor tensiuni, dintre evreii și arabii din Ierusalim, organizația teroristă Hamas a lansat câteva mii de rachete asupra teritoriului statului Israel, ucigând minimum nouă persoane și rănind alte câteva sute (Drăghici, 2021). Armata Israeliană estimează, că Hamas a lansat aproximativ 3000 de rachete de tip GRAD, urmașe ale celebrelor Katiușa, încercând să lovească, în general, ținte civile (Jipa, 2021). Deși, majoritatea rachetelor au fost interceptate, pentru comunitatea internațională rămâne un semn de întrebare, de unde un actor non-statal poate avea atât de mult armament, încât să execute atacuri zile întregi împotriva unui actor statal puternic, așa cum este Israel.

Organizațiile teroriste devin din ce în ce mai răspândite pe teritoriul întregului glob, datorită revoluției tehnologice și a mijloacelor informaționale de comunicare. Radicalizarea se face mult mai ușor pe internet, *ummah* trecând în mediul online, devenind mai greu pentru autorități să contracareze fenomenul. Este mai facil, astăzi, să iei legătura cu anumite persoane din alte țări, în vederea comiterii de atentate și să ai celule teroriste interconectate, care să se sprijine reciproc cu ajutorul tehnologiei. De exemplu, prin prisma faptului că instrumentele cibernetice au devenit atât de larg folosite, DAESH sau Statul Islamic pot contacta persoane radicalizate, în vederea comiterii unui atentat terorist într-un stat occidental, mult mai rapid.

Referitor la importanța acestora în politica mondială și implicațiile în materie securitară, putem considera că, un atentat terorist comis într-o țară puternică, pe lângă victimele efective ale acțiunii, destabilizează intern statul, respectiv impactează negativ imaginea externă, obligând țara să reacționeze, în general, emoțional și disproporționat în comparație cu atacul inițial.

Totodată, hackerii, hacktiviștii și grupările de criminalitate cibernetică sunt printre cei mai noi actori, deoarece își desfășoară activitatea în arealul cyberspațiului. Aceștia beneficiază, din plin, de revoluția informației pentru a accede la masa negocierilor, profitând de anumite breșe de securitate cibernetică ale actorilor statali, utilizând instrumente cibernetice legale sau ilegale, pentru atingerea unor obiective politice și nu numai (Naim, 2015). Ei forțează guvernele, să intre într-o logică a *șoarecelui și pisicii* și, cu toate că, statele au capacitatea de a mobiliza mii de persoane specializate în protecția

acestor sisteme, un hacker poate provoca daune grave, pe fondul costurilor mici de exploatare a domeniului internetului.

Hacktiviştii sunt persoane motivate de o ideologie sau scop, care atacă în general site-uri guvernamentale sau conturi, reţele, servicii etc. ale statelor sau ale unor persoane importante dintr-o anumită ţară, pentru a le compromite. Uneori, aceştia pot provoca daune atât de grave statului, încât pot fi arestaţi sau chiar condamnaţi, cum este cazul lui Liu Xiaobo, activist al drepturilor omului din China, care, în decembrie 2009 a fost condamnat la 11 ani de închisoare, pentru incitare la subminarea puterii de stat (Nye, 2012, *Viitorul puterii*).

Cel mai cunoscut caz de hacktivism este cel al lui Julian Assange, fondatorul Wikileaks. Această organizaţie s-a specializat în divulgarea de informaţii confidenţiale, de la guverne şi corporaţii. Wikileaks a făcut publice câteva milioane de documente secrete, sute de mii de mesaje diplomatice secrete americane, informaţii despre Guantanamo Bay, Osama Bin Laden, rapoarte ale ONU, dar şi corespondenţe ale unor personaje publice, precum Hillary Clinton, date obţinute, în general, ca urmare a unor scurgeri de informaţii sau prin exploatarea unor vulnerabilităţi cibernetice. Dezvăluirile au dus la înrăutăţirea relaţiilor diplomatice, dintre Statele Unite şi aliaţii săi, precum şi la degradarea imaginii SUA în lume. Referitor la aceste aspecte, Julian Assange spune, că a dorit să arate lumii întregi detalii despre spionajul american, asupra aliaţilor săi şi ONU, să remarce ignorarea abuzurilor şi a corupţiei din ţările cliente, precum şi să evidenţieze anumite înţelegeri ascunse cu state neutre sau lobby-ul, pentru companiile de origine americană (Naim, 2015).

Hacktivismul nu este un fenomen izolat şi nu se poate restrânge doar la cazul Wikileaks. Există hackeri taiwanezi şi chinezi, care îşi atacă unii altora paginile online în mod sistematic cu graffiti electronice, Estonia a fost atacată în 2007 de unii *hackeri patriotici ruşi*, ofensaţi de faptul că, unui monument al soldaţilor sovietici din Al Doilea Război Mondial i-a fost mutată locaţia iniţială, blocând funcţionarea unor servicii de internet (Nye, 2012, *Viitorul puterii*), dar şi în România identificăm astfel de acţiuni, de tipul virusului *Poliţia Română* sau a blocării unor site-uri guvernamentale. Aşadar, prin afectarea infrastructurilor critice, a serviciilor, prin publicarea de informaţii confidenţiale sau prin promovarea unor concepte, hackerii pot influenţa idei, opinii la nivel mondial, în relaţiile internaţionale şi nu numai, devenind incomozi pentru actorii statali şi pentru securitatea acestora, căpătând astfel, relevanţă în afacerile globale.

Organizațiile neguvernamentale – ONG-urile sunt actori, care își desfășoară activitatea independent față de state, care promovează un interes general al unei comunități, de obicei în scopuri umanitare, cum ar fi apărarea drepturilor omului, protejarea mediului înconjurător, protejarea patrimoniului cultural, îmbunătățirea serviciilor de sănătate sau eradicarea sărăciei.

Acestea beneficiază, din plin, de pe urma fenomenului de difuzie și dezintegrare a puterii, deoarece, cu cât ONG-urile au mai multă putere pentru a-și atinge scopurile, cu atât guvernele au mai puțină (Naim, 2015). Drept urmare, omenirea cunoaște câteva zeci de mii de ONG-uri internaționale și câteva milioane, care acționează în granițele interne ale statelor. Acestora le este mult mai facil, în ziua de astăzi, să găsească susținători, având în vedere avansul tehnologic, prin internet, site-uri sau rețele sociale.

ONG-urile au atras persoane în general de vârste tinere, care au fost dornice de schimbare și de sacrificare pentru o cauză, astfel, au câștigat mai mult prestigiu în rândul populației, în comparație cu reprezentanții instituțiilor statelor. Organizațiile promovează un interes axat pe o singură problemă, devenind credibile în rândul publicului, fiind mai vizibile în relația cu mass-media, beneficiind de pe urma susținerii unor celebrități, ceea ce le conferă o prezență mai importantă plan mondial, în comparație cu majoritatea guvernelor (Naim, 2015).

Organizațiile din ziua de astăzi au suficient de multă putere, cât să demaște o malversațiune, să retragă sprijinul ori să blocheze o acțiune guvernamentală (Naim, 2015), putând chiar, să remodeleze peisajul politic dintr-o țară. ONG-urile încearcă să convingă statele să acționeze, atacându-le reputația, statele fiind nevoite să concureze, pentru „a crea narațiuni care cresc puterea lor blândă și o reduc pe cea a oponenților". ONG-urile profită de pe urma instabilităților interne, atât a statelor, cât, în anumite cazuri, și a Organizației Națiunilor Unite, influențând percepțiile, prin reinterpretarea dreptului umanitar și răspândirea ideilor în mass-media și social media (Nye, 2012, *Viitorul puterii*).

Vorbind concret, printre cele mai importante ONG-uri din lume sunt: Greenpeace, Habitat for Humanity, UNICEF, Amnesty International, Médecins Sans Frontières, Save the Children sau Crucea Roșie. Toate acestea au puterea de a deveni un actor important, în mediul în care își desfășoară activitatea, ieșind de sub controlul guvernelor, chiar forțându-le să adopte diverse decizii.

De exemplu, Greenpeace, care se dovedește a fi un „adevărat câine de pază al mediului" (Morari, 2015), are peste trei milioane de

susţinători în toată lumea şi încearcă să convingă atât guvernele, cât şi companiile să ducă politici sustenabile şi ecologice. Desfăşoară mitinguri de stradă, uneori paşnice, alteori violente, organizează întâlniri cu reprezentanţii altor actori, înaintează propuneri, în scopul protejării naturii şi se situează pe poziţii adverse cu guvernele unor state, cum ar fi Brazilia sau China.

Marile companii şi corporaţii pot, de asemenea, să influenţeze politica mondială. Având în vedere difuziunea puterii, corporaţiile sunt printre cei mai importanţi vectori ai acestei transformări, acestea influenţând cele două logici contrare – logica politică, ce urmăreşte maximizarea puterii unui stat, precum şi logica economică – ce urmăreşte maximizarea profitului, chiar în detrimentul logicii politice. Concret, o companie americană care investeşte în China, o ajută pe aceasta să se ridice.

Pe de altă parte, companiile multinaţionale nu mai pot fi folosite de state pentru a reprezenta interesele de politică externă ale acestora. Asistăm la un fenomen de desprindere al corporaţiilor de *ţările-mamă*, bazat pe expansiunea în diverse pieţe globale, a subcontractărilor, migraţiei industriale sau a investiţiilor, realizate de moguli individuali de diferite origini.

Companiile devin actori de sine stătători, care negociază direct cu statele naţionale, prin intermediul propriilor responsabili, pe diverse paliere de acţiune, cum ar fi realizarea de investiţii. Totodată, companiile pot influenţa politica internă a unui stat, prin promovarea unor legi şi hotărâri favorabile intereselor sale. În caz contrar, acestea ameninţă cu reducerea numărului de salariaţi sau chiar cu sistarea activităţilor economice. De asemenea, există foruri internaţionale, unde companiile negociază direct între ele sau cu alţi actori non-statali, fără ca ţările să fie luate în considerare. Totodată, în unele domenii, statul nu mai poate controla expansiunea multinaţionalelor, în special al celor informatice, precum Whatsapp, Telegram, Facebook, Twitter, TikTok.

Grupările de criminalitate organizată nu sunt noi pe scena internaţională, însă, încep să capete mai multă influenţă, ca urmare a difuziei puterii. Se încadrează în zona chestiunilor transfrontaliere, neputând fi atribuite vreunui stat, acţionând independent pe tot mapamondul, ghidaţi în general de interese economice. Acestea îşi impun punctul de vedere într-un mod violent, prin lupte, asasinate, conflicte cu autorităţile statului sau chiar între grupări rivale, ori prin intermediul coruperii sau şantajării liderilor politici. Realizează

infracţiuni economice, evaziune fiscală, spălare de bani, trafic de droguri sau trafic de persoane, fiind extinse în întreaga lume.

Referitor la relevanţa acestora în politica mondială, ele pot, în primul rând, să destabilizeze statele în care acţionează, grupările de crimă organizată fiind mai puternice decât organele coercitive ale unor ţări. Cele mai bune exemple sunt Mexic şi Columbia. Astfel, în Mexic, între 2006 şi 2012, aproape 40.000 de oameni şi-au pierdut viaţa în *Războiul Drogurilor* (Mercille, 2011). Gruparea Zetas este una dintre cele mai violente, controlând zone strategice de transport de droguri, având peste 4000 de combatanţi înarmaţi, majoritatea recrutaţi din rândul unităţilor de elită ale armatei şi poliţiei. Zetas acţionează şi asupra politicienilor regionali şi autorităţilor poliţieneşti, ducând corupţia şi dezertarea „la un nivel superior" (Naim, 2015). În Columbia, avem bine-cunoscutele carteluri, care îşi dispută influenţa tot prin aceleaşi metode – lupte şi coruperea angajaţilor statului.

Odată ce avem anumite ţări care nu fac faţă acestor grupări, este sporită instabilitatea socială, iar mulţi oameni decid să părăsească statul respectiv. Un bun exemplu sunt mexicanii care emigrează ilegal în SUA. Iar de aici, efectul acestora asupra afacerilor globale se poate manifesta în diverse moduri, de la o politică mai relaxată asupra imigranţilor sau acordării de vize până la celebra construcţie de ziduri, pentru care Donald Trump a fost aspru criticat de lideri din întreaga planetă.

Grupările mafiote pot să controleze statele chiar în mod direct, aşa cum se întâmplă în Rusia. În acest stat, se aprobă legi în favoarea grupărilor, sunt numiţi membri ai mafiei în diverse funcţii cheie în stat, se tolerează corupţia, mafia rusească fiind lăsată să se manifeste aproape liber (Galeotti, 2018), Rusia chiar fiind un *exportator de mafie*. Şi în China, în ciuda faptului că Partidul Comunist este la putere, au existat membri ai mafiei chineze, care au ocupat funcţii publice până la nivelul de secretar de stat. De asemenea, inclusiv în Albania există o puternică influenţă a grupărilor de criminalitate organizată. Şi în Italia, prezenţa mafiei este una importantă, dar a scăzut puternic influenţa în politica acestei ţări, odată cu acţiunea *Mani Pulite* din anii 1990. Deşi, nu reprezintă un actor crucial în relaţiile internaţionale, importanţa grupărilor de criminalitate organizată nu poate fi negată, acestea profitând de pe urma acelor domenii care scapă de sub capacitatea de control a statelor, având impact negativ asupra securităţii acestora.

De asemenea, mişcările de stradă din zilele noastre reprezintă un important actor în realizarea politicii mondiale. În ciuda faptului, că nu sunt efectiv un actor de sine stătător, doresc să înglobez toate mişcările

de amploare într-o singură entitate, care contează pe plan global. Sunt relevante datorită revoluţiei comunicării, a tehnologiilor pe care Larry Diamond, profesor la Stanford, le numeşte „Tehnologiile eliberării" (Naim, 2015). Putem observa faptul că, noile tehnologii au permis ca filipinezii să iasă în stradă şi să alunge din funcţie un preşedinte corupt, au facilitat mobilizarea rapidă a maselor împotriva autoritarismului, precum în Revoluţia Portocalie din Ucraina sau Revoluţia Cedului din Liban, au demascat fraudarea unor alegeri, din 2007, din Nigeria (Naim, 2015) sau au contribuit la producerea celei mai mari mişcări de stradă din ultimele decenii, bine-cunoscuta *Primăvară Arabă*.

Primăvara arabă şi consecinţele acesteia au contribuit semnificativ la importanta criză umanitară a migranţilor spre Europa, dar şi la accentuarea terorismului. Dacă remarcăm, că toate acestea au plecat de la un protest din Tunisia, răspândindu-se cu ajutorul internetului, ca un efect de domino, putem conchide că, mişcările de stradă pot avea un important rol în dezvoltarea politicii internaţionale.

Predicţii şi concluzii

Din perspectiva viitorului, consider că non-statalii vor avea o influenţă din ce în ce mai puternică în relaţiile internaţionale, punând la îndoială anumite aspecte din modalitatea de funcţionare a statelor naţionale, în viitorul mediu-îndepărtat. Răspândirea tehnologiei, accesibilitatea, susţinerea oamenilor, răspunsul cu greutate al statelor sunt doar câţiva factori care vor face din actorii independenţi de guverne să capete un loc mai important la masa negocierilor.

În primul rând, în termeni de hard power, „azi e infinit mai uşor să ucizi un milion de oameni" (Naim, 2015), iar organizaţiile teroriste, grupările paramilitare, armatele private de mercenari au acces mult mai uşor la arme de distrugere în masă, de la dispozitive improvizate până la tehnică militară de ultimă generaţie. Pentru a distruge ceva anume, nu va mai fi nevoie de mari armate, totul va fi şi mai difuz, iar aceste aspecte vor fi problematice pentru actorii statali (Buzan, 2012).

Consider că, grupările islamiste vor continua să rămână prezente, iar acestora li se vor adăuga şi alte mişcări, în special cele de ordin naţionalist-extremist. În plus, armatele private vor deveni un real instrument de rezolvare a unor probleme militare ale marilor state, puterea acestora fiind potenţată. Totuşi, este posibil ca în următoarele decenii, o entitate ca Wagner, fiind o armată privată, să lupte exclusiv de partea unei părţi contractante, care le oferă sume mai mari de bani, indiferent dacă este de partea statului-mamă sau împotriva acestuia,

creându-se astfel, armate de mercenari în cel mai serios sens, care pot înclina balanța în diferite conflicte ce vor apărea în viitor.

În termeni de putere financiară, companiile multinaționale vor rămâne actori relevanți în relațiile internaționale. În primul rând, vor continua să-și să desfășoare propria politică, să investească atât în țări partenere, cât și în țări ostile statului de proveniență, indiferent dacă sunt state democratice sau regimuri autoritare, state dezvoltate sau din lumea a III-a.

Este posibil ca, pe fondul investițiilor realizate de statele occidentale în China, în următoarele decenii, companiile din acest stat să poată dezvolta suficientă tehnologie, încât să le egaleze sau chiar să le depășească, în termeni calitativi, pe cele din Statele Unite și Europa. Un argument poate fi reprezentat de faptul că, Republica Populară Chineză are în continuare toate tehnologiile de care dispune pe teritoriul său național, în vreme ce, alte state occidentale le au răspândite pe întreg mapamondul.

De asemenea, organizațiile non-guvernamentale și activiștii civici, care se manifestă pentru diverse cauze, de la respectarea drepturilor omului la protejarea mediului înconjurător, vor deveni mai relevanți în politica mondială, datorită faptului că vor beneficia de sprijin din partea maselor de oameni din întreaga lume, ceea ce le va conferi puterea să acționeze, pentru cauza respectivă, mult mai rapid și mai eficient. Pe de altă parte, datorită difuziei puterii, ONG-urile vor putea să negocieze direct, fie cu guverne, fie cu alți actori non-statali, beneficiind de suficientă putere, cât să ocolească modul clasic în care se adoptă decizii la nivel internațional. Vor avea sprijinul oamenilor, atât moral, cât și financiar, iar asta le va întări poziția în sistem.

Totodată, mișcările de stradă vor da fiori reci regimurilor autoritare, spiritul civic devenind mai activ. Încrederea oamenilor și, în special, a tinerilor că pot produce schimbarea vor amplifica puterea pe care acestea le pot avea, în influențarea politicii mondiale. O nouă *Primăvară arabă* este posibilă oricând, deși, în alt spațiu geografic și cu alte fundamente.

O altă urmare a fenomenului de difuzie a puterii este creșterea importanței grupărilor de criminalitate cibernetică, ce se vor manifesta în cyberspațiu, iar, cum trendul este ca mai toate activitățile cotidiene să se *digitalizeze*, vom asista la atacuri cibernetice din ce în ce mai dese, care să vizeze atât vulnerabilizarea conturilor bancare, cât și spargerea de corespondențe electronice sau furtul de identitate. În funcție de scopul pe care aceștia îl urmăresc, își vor rafina metodele și mijloacele, astfel

încât, să provoace pagube din ce în ce mai mari atât actorilor statali, cât şi celorlalţi non-statali.

Pe cale de consecinţă, în opinia mea, statele naţionale şi implicit România trebuie să continue să-şi consolideze capacitatea de reacţie asupra ameninţărilor hibride, non-convenţionale, întrucât acestea vor deveni din ce în ce mai relevante atât pe linia primejduirii securităţii statelor, cât şi din perspectiva relevanţei în politica mondială. În context, eforturile României în acest cadru sunt de apreciat, ţara noastră beneficiind de specialişti în domeniul ameninţărilor hibride care, până în prezent, au reuşit să contracareze eventuale evenimente, cu impact negativ, la adresa securităţii naţionale.

În concluzie, deşi aflat încă la debut, fenomenul difuziei puterii de la actorii statali la non-statali va continua să crească în relevanţă în următoarele decenii, afacerile globale devenind mai difuze. Pe scurt, vom trăi într-o lume în care, fiecare va concura cu fiecare de pe poziţii relativ egale – în sensul că, inclusiv actorii mai mici vor putea fi relevanţi în politica mondială. De asemenea, vom avea parte atât de dispute între actorii statali, între actorii non-statali, dar şi între statali şi non-statali, unele dintre acesta, cu impact negativ asupra securităţii statelor şi a persoanelor. În final, voi încheia cu un citat al lui Moises Naim, relevant pentru modalitatea în care va fi influenţată politica mondială, de fenomenul de difuzie a puterii – „poate părea că nu este nimeni la conducere (...) dar să nu ne înşelăm căutând soluţia într-un nou hegemon (...) care să pună în ordine haosul mondial. Soluţiile (...) se vor coagula într-un mediu în care puterea este mai uşor de obţinut şi mai greu de folosit sau chiar de păstrat" (Naim, 2015).

Referinţe bibliografice:

1. Buzan, B. (2012). „No More Superpowers", discurs la TEDx Talks, Central Saint Martins, Londra, disponibil online la https://www.youtube.com/watch? v=JC27GMQoM08

2. Drăghici, M., (2021), „Surse: Israelul şi mişcarea Hamas ar putea ajunge la un armistiţiu în zilele următoare", *Monitorul Apărării şi Securităţii*, disponibil online la https://monitorulapararii.ro/surse-israelul-si-miscarea-hamas-ar-putea-ajunge-la-un-armistitiu-in-zilele-urmatoare-1-36958

3. Galeotti, M. (2018), „Gangster's paradise: how organised crime took over Russia", *The Guardian*, 23 martie, disponibil online la https://www.

theguardian.com/news/2018/mar/23/how-organised-crime-took-over-russia-vory-super-mafia

4. Jipa, F. (2021), „HAMAS a tras peste 3.000 de rachete, dar efectul la țintă a fost unul modest. Vezi ce tipuri de rachete au folosit", *Monitorul Apărării și Securității*, disponibil online la https://monitorulapararii.ro/hamas-a-tras-peste-3-000-de-rachete-dar-efectul-la-tinta-a-fost-unul-modest-vezi-ce-tipuri-de-rachete-au-folosit-1-36986

5. Naim, M., (2015), *Sfârşitul puterii. Companii care se scufundă, militari în derută, papi care abdică, guverne neputincioase, puterea nu mai este ce-a fost*, Editura Antet, Bucureşti.

6. Nye, J. S., (2015), *S-a sfârşit oare secolul american?*, Editura Comunicare.ro, Bucureşti.

7. Nye, J. S., (2012), *Viitorul puterii*, Editura Polirom, Bucureşti.

8. Morari, O. (2015), „5 ONG-uri care influențează lumea", disponibil online la https://beestrong.ro/2015/11/5-ong-uri-care-influenteaza-lumea/

EVOLUȚIA TRAFICULUI DE DROGURI DE MARE RISC DIN ROMÂNIA, ÎN PERIOADA 2016 – 2022

Adrian Laurenţiu PANĂ*

Abstract:

High-risk drug trafficking is a growing threat to Romania's national security. Organized crime has been exceedingly resilient to anti-drug policies. Despite the efforts and initiatives of national and international institutions to prevent illicit drug trade, Romania faces massive flows of drugs on its territory. Regarding the fact that Romania is located in a strategic area between high-risk drug trafficking sea routes and major European consumption markets, Romanian drug crime progress could also impact the advancement of drug trafficking at a transnational level, affecting the national security of strategic partners. Motivated by these remarks, in this paper, my aim is to analyze the open source data on evolution of drug trafficking in Romania, in period 2016-2022. This article investigates the geographical expanding of illicit high-risk drug trade in Romania and also the response of national institutions. The geographical expanding review of drug trafficking will bring out all the criminal cases in the period 2016-2022, divided even in a county perspective, where someone has been found guilty of high-risk drug trafficking in a Romanian law court. Moreover, at this stage, I am referring to national institutions reaction such as adaptation of justice system and the evolution of anti-narcotic policies. In the justice system field, I assume to review the progress of convicting this crime in Romania, in terms of number of criminal cases judged, among the mentioned time interval.

Keywords: *drug trafficking, evolution of drug trafficking in Romania.*

1. Introducere

Traficul de droguri constituie o ameninţare complexă la adresa securităţii naţionale, care are implicaţii semnificative la nivel mondial asupra sănătăţii publice, economiei şi societăţii. România este situată pe traseul celor mai importante rute de trafic de droguri operate în Estul Europei, astfel că, autorităţile statului român se confruntă permanent, cu problematica generată de consumul şi traficul de droguri. Înţelegerea evoluţiei traficului de droguri din România, în perioada 2016-2022, este

* Student doctorand în cadrul Academiei Naţionale de Informaţii „Mihai Viteazul” din Bucureşti, email pana.adrian@animv.eu

importantă pentru instituțiile responsabile cu prevenirea și combaterea traficului de droguri, din perspectiva necesității dezvoltării de strategii și politici eficiente.

În perioada de referință, activitățile de trafic de droguri derulate la nivel mondial au suferit transformări, în ceea ce privește producția de droguri, rutele de transport, modalitatea de distribuție și plată, precum și preferințele de consum. Aceste schimbări au afectat inevitabil traficul de droguri din România, determinând nevoia efectuării unei analize aprofundate a situației din interiorul granițelor țării.

Obiectivul prezentei cercetări constă în oferirea unei perspective, asupra dinamicii traficului de droguri din România. Cercetarea este concentrată, în mod specific, asupra evoluției numărului de cazuri de trafic de droguri de mare risc judecate de instanțele din România, distribuite în funcție de județele țării, pentru a stabili eventuale trenduri regionale. Examinând aceste date, se poate obține o perspectivă amplă asupra variațiilor traficului de droguri, între regiunile din România. Totodată, pot fi identificate județele cu cea mai mare incidență a numărului de situații de trafic de droguri, cu scopul de a stabili potențialii factori care contribuie la eventualele diferențe.

Mai mult, studiul își propune să contribuie la literatura de specialitate existentă, despre traficul de droguri din România. În timp ce, cercetările anterioare au descoperit informații valoroase asupra imaginii de ansamblu a traficului de droguri din țară, puține studii au examinat, în mod specific, variațiile traficului de droguri în funcție de județ. Prin obținerea acestor date specifice fiecărui județ, se poate umple această lacună în cunoaștere și se poate îmbunătăți înțelegerea dinamicii traficului de droguri din România.

Concluziile acestui studiu pot avea aplicabilitate practică pentru instituțiile din România cu atribuții în prevenirea și combaterea traficului de droguri, permițându-le să își folosească resursele, în mod eficient și să prioritizeze eforturile, în județele cele mai afectate de traficul de droguri.

2. Privire de ansamblu asupra traficului de droguri din România

Traficul de droguri reprezintă o amenințare persistentă, complexă și dinamică asupra securității naționale a României, de natură să afecteze starea de normalitate și echilibru a cetățenilor. Cu scopul înțelegerii aprofundate a problematicii, această secțiune a lucrării

prezintă o privire de ansamblu asupra literaturii existente despre traficul de droguri din România, prin evidențierea concluziilor şi punctelor cheie regăsite în cercetări anterioare.

Un studiu realizat de Buzatu (2017) a examinat caracteristicile traficului de droguri din România. Cercetarea a relevat că, România deserveşte grupărilor importante de criminalitate organizată, ca teritoriu de tranzit şi de consum pentru diferite droguri, cum ar fi cocaină, heroină şi haşiş. Autorul a subliniat importanța poziționării geografice a României, care facilitează tranzitul drogurilor, prin marile rute de transport, care leagă Europa de Est şi Europa de Vest.

În completarea datelor anterioare, am identificat un raport publicat de Agenția Națională Antidrog (2019), în care sunt consemnate rutele importante de trafic, în funcție de drog. Astfel, în ceea ce priveşte cocaina, în anul 2017, acest drog a fost traficat în România, preponderent, pe cale rutieră şi maritimă. Transporturile de droguri pe cale rutieră au vizat rutele, pe relația Olanda – România, Spania-Franța-Italia-Austria-Germania-Ungaria-România, Italia-România, Columbia-Spania-România, Belgia-România, Brazilia-Germania-România, Olanda-Germania, Austria-Ungaria-România, Columbia-Germania-Austria-Ungaria-România şi Grecia-Bulgaria-România, drogurile fiind disimulate, de regulă, în colete expediate prin intermediul firmelor de profil ori în portbagajul sau banchetele autoturismelor. Transporturile de droguri pe cale aeriană au vizat rutele, pe relația Portugalia-România-Grecia, drogurile fiind disimulate în bagaje de mână. Totodată, raportul subliniază faptul că, grupările de criminalitate organizată exploatează vulnerabilitățile frontierei României, dar şi reacțiunea slabă a instituțiilor responsabile cu aplicarea legii. Buna organizare a rețelelor infracționale, în reuşita operațiunilor de trafic de droguri, creşterea cererii pieței de droguri interne, precum şi dezvoltarea adaptabilității grupărilor de trafic de droguri, prin diversificarea anumitor rute tradiționale de trafic, generează un important risc transfrontalier la adresa securității.

Un alt studiu realizat de Lobonț, Nicolescu, Moldovan şi Kuloğlu (2017) a scos în evidență factorii socio-economici, care influențează ratele infracționalității din România, printre care şi traficul de droguri. Cercetătorii au identificat, că nivelul ridicat de şomaj, sărăcia şi excluziunea socială sunt factori de bază, care contribuie la amplificarea traficului de droguri. Aceştia au susținut faptul, că persoanele care se confruntă cu oportunități economice limitate pot recurge la săvârşirea de activități infracționale, inclusiv traficul de droguri, vizualizându-l ca un mijloc de supraviețuire financiară.

Mai mult, cercetarea demarată de Manea Liliana, Petrișor Gruia și Manea Larisa-Roxana (2019) a subliniat existența legăturii, dintre traficul de droguri și fenomenul de corupție din România. Autorii au evidențiat influența corupției, la nivelul instituțiilor de aplicare a legii, cu impact negativ major asupra necesităților de combatere a consumului și traficului de droguri.

Aceste studii subliniază, cumulativ, natura complexă a traficului de droguri derulat în România, influențată de prezența grupărilor de trafic, factori geografici facilitatori, context socio-economic vulnerabil și corupție. În mod evident, traficul de droguri reprezintă o serioasă provocare pentru instituțiile din domeniul securității, care trebuie susținute, prin asigurarea unui cadru legislativ optim, care să permită acțiunea eficientă a acestora prevenirea și combaterea traficului de droguri de mare risc.

3. Rute și modalități de trafic de droguri

Un proces important în derularea activităților de trafic de droguri este reprezentat de transportul și distribuția drogurilor. Conform unui articol, redactat de Rotariu și Sasu (2017), există numeroase rute utilizate de grupările de criminalitate organizată, o parte din ele implicând și teritoriul României. Articolul oferă o imagine de ansamblu a operațiunilor de transport, astfel că, principalele rute de trafic identificate au fost:

- Ruta Balcanică: această rută presupune transportul drogurilor din Orientul Mijlociu, Africa și Asia către Vestul Europei, traversând statele balcanice. Drogurile sunt traficate preponderent pe cale rutieră, prin intermediul autovehiculelor, mașinilor de mare tonaj sau a trenurilor.
- Ruta Mării Negre: această rută implică transportul drogurilor din state, precum Turcia, Georgia și Ucraina, către România. Drogurile sunt disimulate în containere sau în încărcătura bărcilor de mici dimensiuni.
- Ruta Aeriană: această rută utilizează serviciile companiilor de transport aerian, drogurile fiind preponderent transportate prin intermediul zborurilor comerciale sau zborurilor private. În această situație, drogurile sunt disimulate în bagaje.
- Ruta Poștală: această rută implică transportarea drogurilor prin intermediul serviciilor de coletărie, fiind de regulă traficate cantități reduse. Această metodă este folosită cel mai des în state, precum Țările de Jos și Spania.

Alte modalităţi de trafic de droguri identificate au fost transportarea drogurilor prin intermediul grupărilor de motocicliști, al victimelor traficului de persoane, transportului public, precum şi transportatorilor internaţionali de marfă.

4. Factori care influenţează evoluţia traficului de droguri

Cunoaşterea şi înţelegerea factorilor care influenţează trendurile traficului de droguri de mare risc în România reprezintă două elemente importante, în procesul de completare a perspectivei asupra dinamicii fenomenului de trafic. Această secţiune oferă o privire de ansamblu, asupra cercetărilor din literatura de specialitate, care au fost concentrate pe examinarea diferiţilor factori, care influenţează traficul de droguri de mare risc din România.

Un studiu realizat de Țlical (2019) a explorat factorii geopolitici care influenţează traficul de droguri de mare risc, în speţă, legătura dintre poziţia geografică a României şi comercializarea ilegală a cocainei. Autorul a evidenţiat importanţa conexiunii directe a României cu Marea Neagră, care determină o necesitate de cooperare inter-statală, pe mare, în vederea prevenirii şi combaterii traficului de cocaină. Principala rută de transport a cocainei în zona extinsă a Mării Negre este semnalată a se operaţionaliza, pe relaţia România-Turcia. Un exemplu relevant, indicat în respectiva lucrare este constituit de episodul din luna aprilie, anul 2019, atunci când, aproximativ 200 kg de cocaină au fost găsite plutind pe mare.

În plus, factorii socio-economici au fost identificaţi în literatura de specialitate, ca având un impact semnificativ asupra implicării indivizilor, în activităţi de trafic de droguri. În general, tinerii proveniţi din comunităţi vulnerabile, cu un grad accentuat de sărăcie şi nivel ridicat de şomaj, sunt predispuşi să săvârşească infracţiuni, inclusiv trafic de droguri (Manshor, Abdullah şi Hamed 2020).

Factorii tehnologici, asociaţi cu avansul tehnologic înregistrat la nivel mondial au facilitat şi facilitează, în continuare, activităţi de trafic de droguri. Utilizarea pieţelor negre disponibile online, pentru săvârşirea traficului de droguri (Rhumorbarbe, şi alţii 2016), precum şi achitarea drogurilor prin intermediul pieţei criptomonedelor (Foley, Karlsen şi Putnins 2019) generează provocări majore în combaterea fenomenului. Plata este realizată, prin intermediul reţelelor blockchain atât de către consumatori, cât şi de traficanţi, pe întreg lanţul operaţional, de la sursă, până la consumator. Amploarea utilizării metodelor alternative de trafic, de către grupările de crimă organizată a fost scoasă

în evidență, încă din anul 2016. Autorii unui studiu, prin care au cercetat anvergura translatării problematicii traficului de droguri și pe infrastructurile blockchain, au descoperit faptul că, în perioada ianuarie 2014 – martie 2015, dintr-un număr total de 48.000 de anunțuri de vânzare regăsite pe piața neagră online, 2.700 vizau comercializarea de droguri (Rhumorbarbe, și alții 2016). Cu scopul de a marca evoluția numărului de anunțuri de comercializare a drogurilor, în iulie 2017, pe piața neagră online erau postate mai mult de 250.000 de anunțuri, prin care se comercializau droguri (United Nations Office on Drugs and Crime 2018).

5. Metodologie

5.1. Selectarea surselor și colectarea datelor

Cu scopul de a analiza evoluția traficului de droguri de mare risc din România, în perioada 2016 – 2022, au fost culese date privind cazurile penale de trafic de droguri de mare risc, regăsite pe platforma Sintact Analytics, dezvoltată de compania Wolters Kluwer. Platforma figurează cu acces restricționat pentru publicul larg, datele putând fi accesate, în urma permisiunii obținute din partea administratorului de date. De regulă, accesul se permite contra cost. Sursele primare de informații au inclus dosare penale, înregistrate în sistemul judiciar românesc, cum ar fi hotărâri judecătorești și baze de date juridice. Aceste surse au constituit baza cercetării, fiind extrase date esențiale cu privire la cazurile de trafic de droguri de mare risc, înregistrate în fiecare județ din țară, în perioada de referință.

Pe lângă sursele primare, au fost utilizate și surse secundare de date, pentru a completa analiza. Aceste surse au inclus, în general, rapoarte ale instituțiilor statului român, cu atribuții în domenii care influențează traficul de droguri, cum ar fi economia sau societatea. Sursele secundare au oferit o perspectivă valoroasă asupra amplului context al traficului de droguri din România, putând fi trasate inclusiv tendințe, modele și provocări, cu care se confruntă autoritățile statului român, în fiecare județ.

Pentru a asigura acuratețea datelor, au fost întreprinși mai mulți pași în colectarea datelor. În primul rând, informațiile au fost revizuite amănunțit și verificate încrucișat, în mai multe surse, pentru a identifica discrepanțe ori contradicții. Erorile și ambiguitățile au fost rezolvate, prin efectuarea de verificări suplimentare. În situațiile în care, discrepanțele datelor nu au putut fi rezolvate, au fost aduse completări secțiunii cu privire la limitele cercetării.

În plus, calitatea şi credibilitatea surselor utilizate pentru a completa datele primare au fost evaluate, luând în considerare, reputaţia organizaţiilor sau autorilor responsabili cu publicarea acestora. Este important de remarcat faptul că, prezentul studiu se concentrează, în mod specific, asupra evoluţiei traficului de droguri din România, în perioada 2016-2022, fiind analizat, cu precădere, trendul fenomenului în funcţie de regiune/judeţ. În cadrul analizei, nu sunt incluse cazuri aflate încă pe rolul instanţelor de judecată ori cazurile de trafic de droguri de mare risc nedetectate de autorităţile competente.

Prin utilizarea unei metodologii riguroase, care a presupus combinarea mai multor surse de date, acest studiu oferă o analiză cuprinzătoare a evoluţiei traficului de droguri de mare risc din România, între 2016-2022. Datele colectate, de la care a pornit analiza, oferă o imagine aprofundată asupra dezvoltării traficului de droguri de mare risc, în regiunile din România.

5.2. Designul cercetării

Design-ul cercetării, pentru prezentul studiu, a fost unul de natură cantitativă. Cazurile de trafic de droguri de mare risc judecate la nivelul instanţelor din România au fost colectate şi analizate sistematic. Obiectivul principal a fost acela de a examina tendinţele traficului de droguri din România, în perioada 2016-2022.

5.3. Consideraţii etice

Consideraţiile etice au fost esenţiale în realizarea acestui studiu. Cercetarea a aderat la normele de confidenţialitate aflate în vigoare, asigurând anonimatul persoanelor implicate în cazuri de trafic de droguri de mare risc. Studiul a respectat, inclusiv, obţinerea permisiunilor şi aprobărilor necesare pentru accesarea şi utilizarea datelor.

5.4. Limitele cercetării

Este important să subliniez, limitările prezentului demers de cercetare. Studiul a vizat o analiză cantitativă, care poate limita înţelegerea profundă a motivelor şi dinamicii traficului de droguri de mare risc din România. Cercetările viitoare ar putea include metode de cercetare calitative, cum ar fi interviurile, pentru oferi o cunoaştere mai amplă a fenomenului de trafic de droguri de mare risc autohton. Mai mult, rezultatele studiului au fost interpretate, într-o manieră speculativă, prin prisma naturii cantitative a studiului. Motivele indicate în prezenta lucrare, care au stat la baza dinamicii traficului de droguri

din România se bazează pe opinii personale, racordate la realitatea unor stări de fapt identificate şi menţionate în cadrul cercetării.

6. Evoluţia numărului de dosare penale, pentru săvârşirea infracţiunii de trafic de droguri de mare risc înregistrate la instanţele din România (2016-2022)

În anul 2016, la instanţele de judecată din România au fost soluţionate 2092 de dosare penale, pentru săvârşirea infracţiunii de trafic de droguri de mare risc, dintre care numai 7 judecate la nivelul Înaltei Curţi de Casaţie şi Justiţie. Judeţele cu cele mai multe dosare penale, pentru săvârşirea infracţiunii de trafic de droguri de mare risc au fost: Bucureşti (560), Timiş (140), Prahova (107), Constanţa (105) şi Galaţi (67). Durata medie a unui proces a fost de 233 de zile.

În anul 2017, la instanţele de judecată din România au fost soluţionate 2391 de dosare penale, pentru săvârşirea infracţiunii de trafic de droguri de mare risc, dintre care 14 au fost judecate la nivelul Înaltei Curţi de Casaţie şi Justiţie. Judeţele cu cele mai multe dosare penale, pentru săvârşirea infracţiunii de trafic de droguri de mare risc au fost: Bucureşti (675), Constanţa (159), Timiş (131), Cluj (121) şi Prahova (105). Durata medie a unui proces a fost de 258 zile.

În anul 2018, la instanţele de judecată din România au fost soluţionate 2291 de dosare penale, pentru săvârşirea infracţiunii de trafic de droguri de mare risc, dintre care doar 6 au fost judecate la nivelul Înaltei Curţi de Casaţie şi Justiţie. Judeţele cu cele mai multe dosare penale, pentru săvârşirea infracţiunii de trafic de droguri de mare risc au fost: Bucureşti (732), Timiş (135), Cluj (111), Constanţa (110) şi Dolj (108). Durata medie a unui proces a fost de 248 zile.

În anul 2019, la instanţele de judecată din România au fost soluţionate 3024 de dosare penale, pentru săvârşirea infracţiunii de trafic de droguri de mare risc, dintre care 3 au fost judecate la nivelul Înaltei Curţi de Casaţie şi Justiţie. Judeţele cu cele mai multe dosare penale, pentru săvârşirea infracţiunii de trafic de droguri de mare risc au fost: Bucureşti (681), Timiş (179), Cluj (169), Dolj (141) şi Iaşi (152). Durata medie a unui proces a fost de 255 zile.

În anul 2020, la instanţele de judecată din România au fost soluţionate 3224 de dosare penale, pentru săvârşirea infracţiunii de trafic de droguri de mare risc, dintre care 12 au fost judecate la nivelul Înaltei Curţi de Casaţie şi Justiţie. Judeţele cu cele mai multe dosare penale, pentru săvârşirea infracţiunii de trafic de droguri de mare risc au

fost: Bucureşti (804), Cluj (184), Timiş (173), Dolj (171) şi Iaşi (162). Durata medie a unui proces a fost de 252 zile.

În anul 2021, la instanţele de judecată din România au fost soluţionate 4260 de dosare penale, pentru săvârşirea infracţiunii de trafic de droguri de mare risc, dintre care 6 au fost judecate la nivelul Înaltei Curţi de Casaţie şi Justiţie. Judeţele cu cele mai multe dosare penale, pentru săvârşirea infracţiunii de trafic de droguri de mare risc au fost: Bucureşti (984), Timiş (260), Cluj (218), Iaşi (210) şi Constanţa (205). Durata medie a unui proces a fost de 240 zile.

În anul 2022, la instanţele de judecată din România au fost soluţionate 1050 de dosare penale, pentru săvârşirea infracţiunii de trafic de droguri de mare risc, dintre care 2 au fost judecate la nivelul Înaltei Curţi de Casaţie şi Justiţie. Judeţele cu cele mai multe dosare penale, pentru săvârşirea infracţiunii de trafic de droguri de mare risc au fost: Bucureşti (200), Constanţa (60), Cluj (55), Dolj (50) şi Bacău (31). Durata medie a unui proces a fost de 218 zile.

În ceea ce priveşte situaţia anului curent, de la data de 01.01.2023, până la data de 26.05.2023, la instanţele de judecată din România au fost soluţionate 532 de dosare penale, pentru săvârşirea infracţiunii de trafic de droguri de mare risc. Judeţele cu cele mai mult dosare penale, pentru săvârşirea infracţiunii de trafic de droguri de mare risc au fost: Bucureşti (134), Cluj (40), Dâmboviţa (28), Dolj (26) şi Braşov (22).

Cu scopul oferirii unei perspective multidimensionale, asupra fenomenului traficului de droguri de mare risc din România şi pentru a evidenţia tendinţele traficului în funcţie de factorii economici, vom indica PIB-ul pe cap de locuitor, pentru fiecare judeţ din România, din perioada supusă analizei. În anul 2016, judeţele cu cel mai mare PIB pe cap de locuitor au fost: Bucureşti (22.323 euro), Ilfov (11.537 euro), Timiş (10.926 euro), Cluj (10.655 euro), Braşov (10.528 euro) şi Constanţa (10.246 euro) (Pele 2015). Pentru a marca trendul economic înregistrat în judeţele din România, în anul 2019, judeţele cu cel mai mare PIB pe cap de locuitor au fost: Bucureşti (26.969 euro), Cluj (14.333 euro) şi Timiş (13.419 euro) (Institutul Naţional de Statistică 2021).

7. Factorii care au influenţat evoluţia traficului de droguri în perioada 2016-2022

Luând în considerare, că analiza a fost una cantitativă, în cadrul acestei secţiuni vor fi indicaţi, într-o manieră speculativă, posibilii factori care au determinat această dinamică a traficului de droguri de mare risc din România. În perioada analizată, au fost remarcate, deseori, în top 5 al

județelor pe raza cărora au fost derulate cele mai multe activități de trafic de droguri, detectate de autorități, Municipiul București și județele Timiș, Constanța, Cluj, Dolj sau Iași. Un prim factor, care ar fi putut sta la baza orientării activităților de trafic pe raza județelor menționate, ar fi situația materială a locuitorilor. Municipiul București și județele Timiș, Cluj și Constanța au figurat, în perioada 2016-2019, cu unele dintre cele mai mari valori din țară, în ceea ce privește produsul intern brut pe cap de locuitor. În situația dată, poate fi coroborat contextul economic favorabil, cu o posibilă cerere ridicată în piață pentru drogurile de mare risc. Este necesar a fi menționat faptul că, drogurile de mare risc sunt și cele mai scumpe droguri regăsite pe piața neagră.

De asemenea, numărul atât de mare de dosare penale, pentru săvârșirea infracțiunii de trafic de droguri de mare risc, înregistrate la instanțele de judecată din Municipiul București, apare și în condițiile în care, capitala României este unitatea administrativ teritorială cu cei mai mulți locuitori din țară. În acest sens, factorul demografic constituie un alt potențial element, ce influențează dinamica traficului de droguri din plan autohton.

Totodată, au fost remarcate o serie de județe de graniță ale țării, pe raza cărora au fost derulate numeroase activități de trafic de droguri. Județele Constanța, Iași, Timiș, Dolj și Galați se regăsesc pe linia de frontieră și, de regulă, sunt incluse în cadrul rutelor de trafic de droguri, de către grupările de criminalitate organizată transfrontalieră. Poate fi observat un trend, în care sunt afectate, în principal, județele care se află în conexiune cu rute orientate către Vestul Europei, precum și județul Constanța, prin prisma contactului direct cu Marea Neagră.

În perioada 2016-2021, a fost evidențiat un trend ascendent al numărului de cazuri de trafic de droguri de mare risc, depistate pe teritoriul României. Dacă, în anul 2016 au fost înregistrate 2092 de dosare penale, până în anul 2021, numărul acestora a indicat o creștere cu 203,63%, fiind judecate 4260 de dosare penale, deschise pentru infracțiunea de trafic de droguri de mare risc. În schimb, în ceea ce privește anul 2022, au fost înregistrate doar 1050 de dosare penale, o scădere cu 75,35% față de anul precedent. În această situație, semnalez trei posibile motive pentru care a fost înregistrată scăderea, atât de bruscă a dosarelor penale.

În primul rând, scăderea numărului de activități de trafic de droguri, între anul 2021 și anul 2022, se poate datora pandemiei cu COVID-19, care a generat dificultăți atât în domeniul transportului marfar, cât și în ceea ce privește mobilitatea oamenilor. Reducând

frecvenţa transporturilor transnaţionale şi intensificând controalele la graniţă, există posibilitatea, ca traficanţii de droguri să fi fost descurajaţi să operaţionalizeze rutele de trafic tradiţionale. Pornind de la această idee, se deduce un al doilea posibil motiv, pentru care a fost înregistrat un număr redus de dosare penale.

Este cunoscut faptul că, grupările de criminalitate organizată au o capacitate de adaptare deosebită, astfel că, există scenariul în care rutele de trafic consacrate, utilizate de-a lungul timpului, să fi fost înlocuite cu altele noi. În aceste condiţii, operaţiunile clandestine ar fi putut să fie derulate în continuare, fiind doar nedetectate, încă, noile rute de trafic operaţionalizate de grupările de criminalitate organizată transfrontalieră.

Un al treilea motiv poate fi acela, că Oficiul Naţiunilor Unite pentru Droguri şi Infracţionalitate (UNODC) a actualizat strategia de prevenire şi combatere a consumului şi traficului de droguri, pentru perioada 2021-2025. Pe lângă faptul, că România este racordată la noutăţile oferite de UNODC, în prevenirea şi combaterea consumului şi traficului de droguri, în perioada de analiză, în plan autohton, au fost actualizate Strategia Naţională Anticorupţie, pentru intervalul 2021-2025, precum şi Strategia Naţională Anti-drog, pentru perioada 2022-2026. Aparent, în ceea ce priveşte traficul de droguri, legislaţia din România este destul de clară, luând în considerare numărul redus de cazuri judecate la nivelul Înaltei Curţi de Casaţie şi Justiţie (ÎCCJ). În perioada analizată, anual, a fost înregistrat un număr maxim de 14 dosare judecate ÎCCJ, la nivelul anului 2017. Legea nr. 143/2000 privind prevenirea şi combaterea traficului şi consumului ilicit de droguri, precum şi legea 194/2011 privind combaterea operaţiunilor cu produse susceptibile de a avea efecte psihoactive, altele decât cele prevăzute de acte normative în vigoare, au fost modificate şi completate de legea nr. 45/2023, pentru a optimiza cadrul legal în care pot acţiona instituţiile statului cu responsabilităţi în domeniul de vizat. Printre modificările efectuate, se remarcă înăsprirea pedepselor, ceea ce arată o toleranţă tot mai scăzută şi o abordare mai pragmatică a problematicii propuse de traficul de droguri. Dinamica legislativă şi strategică, în lupta anti-drog demarată la nivel mondial, subliniază atât actualitatea problematicii traficului de droguri, precum şi anvergura ameninţării pe care o provoacă la nivelul dimensiunilor securităţii.

8. Importanţa rezultatelor studiului

Dinamica şi trendul dezvoltării traficului de droguri de mare risc pe teritoriul României, raportate la judeţele ţării, pot avea implicaţii

semnificative pentru instituţiile responsabile cu aplicarea legii, dar şi pentru factorii decizionali, în susţinerea şi concentrarea eficientă a resurselor, în acţiunile de prevenire şi combatere a traficului de droguri de mare risc. Concluziile studiului, privind evoluţia traficului de droguri în diferite judeţe din România, oferă informaţii valoroase pentru autorităţile statului român, utile atât în componenta de prevenţie, cât şi în activitatea de urmărire şi cercetare penală. Cunoscând regiunile şi judeţele cu cea mai mare incidenţă a activităţilor de trafic de droguri, statul român poate aloca resurse în mod strategic, pentru a eficientiza operaţiunile de prevenire şi combatere a traficului. Această abordare ar putea aduce un succes mai mare, în detectarea şi reţinerea persoanelor implicate în traficul de droguri.

Mai mult, luând în considerare distanţele dintre principalele judeţe, pe teritoriul cărora se derulează cele mai multe activităţi de trafic de droguri de mare risc din ţară, subliniem importanţa consolidării schimbului de informaţii inter-instituţional şi abordării integrate, de către instituţiile cu atribuţii în domeniu. De asemenea, organele de aplicare a legii ar trebui să promoveze parteneriate solide şi în plan internaţional, luând în considerare natura transnaţională şi complexă a traficului de droguri. Schimburile regulate de informaţii, dar şi acţiunile comune, pot spori eficacitatea eforturilor de destructurare a reţelelor de trafic de droguri.

Concluziile studiului oferă perspective şi asupra dinamicii revizuirii şi actualizării cadrului legislativ autohton ori internaţional. Monitorizarea şi evaluarea continuă a statisticilor, de tipul celor analizate în cadrul prezentului studiu, pot sprijini eforturile statului român de a reduce anvergura fenomenului de trafic de droguri de mare risc.

9. Concluzii

9.1. Puncte cheie

Prezentul studiu a avut ca scop, examinarea evoluției traficului de droguri de mare risc din România, în perioada 2016-2022, cu accent pe dinamica fenomenului, determinată de numărul de cazuri de trafic de droguri, judecate în diferite județe din România. Analiza datelor și parcurgerea literaturii de specialitate au condus la câteva constatări importante.

În primul rând, s-a înregistrat o creștere notabilă a numărului de cazuri de trafic de droguri judecate în România, în perioada 2016-2021.

Acest aspect sugerează intensificarea operaţiunilor de trafic de droguri pe teritoriul României, fiind necesare măsuri de gestionare mai eficientă a acestei probleme, aflate în dezvoltare.

În al doilea rând, analiza a evidenţiat variaţii ale numărului de cazuri de trafic de droguri, între diferitele judeţe din România. Înţelegerea acestor variaţii poate fundamenta alocarea resurselor şi direcţionarea strategiilor şi eforturilor în anumite regiuni ale ţării, pentru a combate mai eficient traficul de droguri.

Mai mult, factorii geografici de tipul localizării României şi proximitatea acesteia faţă de regiuni de interes, pentru grupările de trafic de droguri, au contribuit la dezvoltarea activităţilor de trafic pe teritoriul statului român. Cunoaşterea principalelor rute de trafic, în care este implicat şi teritoriul României, poate constitui un avantaj strategic important, în detectarea operaţiunilor de trafic de droguri.

9.2. Contribuţii ale cercetării şi direcţii viitoare

Acest studiu aduce câteva contribuţii importante la cunoaşterea existentă despre traficul de droguri din România. Cercetarea oferă o analiză cuprinzătoare a tendinţelor şi caracteristicilor traficului de droguri, indicând dinamica şi variaţiile regionale, din interiorul graniţelor ţării. Iterăm contribuţia pe care o poate avea cercetarea, pentru instituţiile responsabile cu aplicarea legii şi cu prevenirea şi combaterea traficului de droguri.

Totodată, prezentul studiu oferă perspective care necesită investigaţii suplimentare. Cercetările viitoare ar putea include demersuri calitative, cum ar fi interviul, pentru a obţine o înţelegere mai aprofundată a motivaţiilor persoanelor implicate în traficul de droguri de mare risc. De asemenea, prin intermediul unor metode calitative, pot fi analizaţi factorii, care au influenţat dinamica traficului de droguri între judeţele din România, aflaţi la stadiul de speculaţii în actuala lucrare.

În plus, cercetarea arată că, monitorizarea şi analiza continuă a tendinţelor traficului de droguri pot fi esenţiale, pentru a rămâne la curent cu complexitatea şi anvergura provocărilor asupra securităţii. Odată cu modificările acţiunilor grupărilor de trafic de droguri şi reacţiunea statului trebuie să fie adaptată şi aplicată pe specificul ameninţării.

Bibliografie:

1. Agenția Națională Antidrog. *Raport național privind situația drogurilor.* România - Noi evoluții și tendințe, REITOX, 2019.

2. Buzatu, Nicoleta-Elena. „Romania – A Tranzit Territory for the Traffic of." *International Journal of Academic Research in Business and Social Sciences* 7, nr. 5 (2017): 527-535.

3. Foley, S., J. Karlsen, și T. Putnins. „Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies?" *The Review of Financial Studies* 32, nr. 5 (2019): 1798 - 1583.

4. Institutul Național de Statistică. „Produsul intern brut - date anuale definitive." 2021.

5. Lobonț, Oana-Ramona, Ana-Cristina Nicolescu, Nicoleta-Claudia Moldovan, și Ayhan Kuloğlu. „The effect of socioeconomic factors on crime rates in Romania: a macro-level analysis." *Economic Research-Ekonomska Istraživanja* 30, nr. 1 (2017): 91-111.

6. Manea, Liliana, Gruia Petrișor, și Larisa-Roxana Manea. „ANALYSIS OF THE SPECIFIC MONEY LAUNDERING CRIMINAL CASES EVOLUTION IN ROMANIA." *Internal Auditing & Risk Management* 14, nr. 3 (2019): 37-49.

7. Manshor, Z., S Abdullah, și A. B. Hamed. „Poverty and the social problems." *International Journal of Academic Research in Business and Social Sciences* 10, nr. 3 (2020): 614-617.

8. Pele, Alexandra. „Prognoză în profil teritorial: Cum va arăta economia fiecărui județ în 2016." *Curs de Guvernare*, 2015.

9. Rhumorbarbe, D., L. Staehli, J. Broseus, Q. Rossy, și P. Esseiva. „Buying drugs on a Darknet market: A better deal? Studying the online illicit drug market through the analysis of digital, physical and chemical data." *Forensic Science International* 267 (2016): 163-182.

10. Rotariu, T, și C. Sasu. „Typology of the drug trafficking phenomenon in Romania." *International Journal of Criminology and Sociology*, nr. 6 (2017): 138-149.

11. Țlical, George-Marius. „Trends of cocaine trafficking at the level of Romania." *Revista Academiei de Științe ale Securității Naționale* 1, nr. 16 (2019): 104-114.

12. United Nations Office on Drugs and Crime. „Global Overview of drug demand and supply." 2018, 7.

COOPERAREA ÎN INTELLIGENCE DINTRE ALIANȚA NORD-ATLANTICĂ ŞI UNIUNEA EUROPEANĂ

Şerban-Dan PREDESCU[*]
Tiberiu TĂNASE[*]

Abstract:

Russia's invasion of Ukraine violates international law and UN rules, undermining global geopolitical security and stability to an unprecedented extent. Therefore, the collaboration and cooperation between NATO and the EU must be stronger than ever in order to succeed in overcoming all the obstacles to democracy and human rights.

An important dimension for the NATO-EU partnership to achieve its objectives is collaboration and cooperation in intelligence, and the main element is the formation of a center of excellence in intelligence analysis in Bucharest, Romania having an extremely important role in the supervision and defense of the eastern flank of NATO.

By collaboration we refer to the initiation and development of specific actions aimed at obtaining, verifying and capitalizing on information and information products, while cooperation implies the organization, coordination, support and joint realization of specific actions by the structures of the information community.

Punctually, through a collaboration and cooperation between all the intelligence structures of the member states under the same strategic umbrella, the NATO-EU alliance could come up with a much faster joint response to the actions of terrorism, disinformation and destabilization of unfriendly states, succeeding so that the desired becomes a reality - a world in which peace and freedom prevaill.

Keywords: *intelligence, intelligence center, NATO, EU, Romania.*

Obiectivele cercetării

În prezenta lucrare de cercetare, obiectivul principal este constituit din încercarea de a identifica principalul element, ce stă la baza cooperării dintre NATO şi Uniunea Europeană. Pentru realizarea obiectivului primordial, consider că, este necesară îndeplinirea

[*] Şcoala Naţională de Studii Politice şi Administrative, Bucureşti, predescu_serban@yahoo.ro
[*] Universitatea Româno-Americană, Bucureşti, tiberiu_tanase@yahoo.com

următoarelor criterii: norme şi valori comune, capacităţi, mijloace şi beneficii .

Primul element ce stă la baza criteriilor este constituit din identificarea principalelor componente operative şi legislative, ce fac posibilă existenţa unei cooperări la nivelul NATO-UE. Un al doilea element este constituit din identificarea principalelor motivaţii, ce stau la baza acestui deziderat. Cel de-al treilea element, esenţial de atins, este reprezentat din identificarea principalelor metode şi mijloace, prin care cooperarea dintre NATO şi UE poate fi realizată. Ultimul element fundamental este constituit din identificarea principalelor beneficii, ce ar rezulta în urma unei astfel de cooperări.

Metodologia de cercetare

Cercetarea este bazată următoarele metode:

1. Metoda descriptivă, ce presupune identificarea şi relatarea faptelor sau a evenimentelor şi de asemenea, pe definiţii, atribuţiile şi rolurile unor instituţii şi organizaţii.
2. Metoda explicativă, întrucât prin intermediul acesteia sunt relatate principalele motive, pentru care cooperarea NATO-UE este esenţială, explicând şi modul în care această cooperarea poate fi consolidată şi îmbunătăţită.
3. Metoda predictivă, întrucât la final, sunt regăsite anumite perspective în legătură cu potenţiale structuri instituţionale, care vor rezulta în urma cooperării NATO-UE.

Introducere

Ca urmare a atacurilor teroriste din 11 septembrie 2001, comunităţile de informaţii vor deveni conştiente de importanţa colaborării şi cooperării, pentru înlăturarea ameninţărilor comune.

Stabilirea înţelegerilor bilaterale/multilaterale şi evoluţia instrumentelor regionale/ internaţionale vor îndepărta riscurile adresate securităţii statelor partenere.

Aşa cum reiese din analizele amănunţite ale analiştilor de intelligence, vom aborda cele 2 definiţii ale componentelor *colaborare* şi *cooperare*, pentru a înţelege cu exactitate importanţa acestora.

Colaborarea (etimologie: din limba latină – *com/cu* + *laborare/a lucra*) este procesul prin care, două sau mai multe persoane, entităţi sau organizaţii lucrează împreună, pentru a îndeplini o sarcină sau a atinge un scop. Colaborarea cunoaşte mai multe nuanţe, ea putând fi bazată pe

leadership (bazată pe un model de referinţă pentru toţi actorii) sau socială (bazată pe principiul egalităţii).

Cooperarea (etimologie: limba latină – *cooperari*) este procesul prin care, grupuri de organisme lucrează sau acţionează împreună pentru beneficii comune, reciproce sau oarecare subiacente, spre deosebire de lucrul în competiţie, pentru beneficii egoiste.

Cooperarea în domeniul intelligence face referire la schimbul de informaţii secrete, utile din punct de vedere politic între state, având ca interes major apărarea şi securitatea teritoriului comun.

Există multe conexiuni importante între preocupările cheie ale cooperării, în domeniul informaţiilor şi problemele şi soluţiile de cooperare de succes, în tradiţiile dominante ale teoriei relaţiilor internaţionale (realism, liberalism şi constructivism) şi lucrările privind politica birocratică şi organizaţională. Acestea sunt surprinse într-o tipologie descriptivă, care descompune relaţiile de cooperare în domeniul informaţiilor în patru clase, reflectând numărul de stări şi calitatea reciprocităţii implicate. Acestea sunt cooperarea bilaterală tranzacţională; cooperarea bilaterală relaţională; cooperarea multilaterală tranzacţională şi cooperarea multilaterală relaţională. În aceste categorii, se găsesc cele mai importante concepte, presupuneri şi enigme ale cooperării în domeniul informaţiilor.

Cooperarea în materie de intelligence la nivelul Uniunii Europene

În prezent, există patru structuri la nivelul Uniunii Europene, ce au ca scop protecţia informativă sau optimist, o comunitate a unei agenţii de intelligence aflată la început:

- European Union Intelligence and Situation Centre (EU INTCEN) (Hărmănescu 2006, 199);
- European Union Military Staff (EUMS) (Revista Geopolitica, 2023);
- European Union Satellite Centre (EUSC);
- European Union Agency for Law Enforcement Cooperation (EUROPOL)(Wetzling 2023).

Serviciul de intelligence al Statului Major şi Centrul de Observare prin Sateliţi al Uniunii Europene îndeplinesc, în mod colectiv, cerinţe stricte în această problemă, dar în cazul Centrului Comun de Evaluare şi al Agenţiei Europene de Poliţie este considerat suficient de critic, pentru

a justifica reforma. În acest sens, reforma în cadrul Centrului Comun de Evaluare și al Agenției Europene de Poliție este recomandată, pentru consolidarea și extinderea centrelor comune de întărire a cooperării cu serviciile de intelligence și cu alte organizații comunitare. Aceste tendințe pot fi remarcate, încă din anul 2022, când, Centrul Comun de Evaluare raporta Înaltului Reprezentant al Uniunii Europene pentru Afaceri Externe și Politică de Securitate (PESC) (Institutul European pentru Studii de Securitate - EUISS 2023).

Direcția de cooperare UE-NATO

Busola Strategică a Uniunii Europene reprezintă un instrument complex, prin care se oferă un plan concret de acțiune cu privire la consolidarea păcii și securității, până în 2030. Pe componenta securității, Busola Strategică pune un accent ridicat pe cooperarea în intelligence, la nivelul statelor membre.

Se dorește crearea unei capacități unice de analiză a informațiilor la nivelul Uniunii Europene, care să cuprindă o cooperare strânsă cu serviciile de intelligence din țările membre. Analizele, care urmează a fi făcute, se vor desfășura în vreme de pace, o dată la cel puțin 3 ani, iar în cazul unui conflict, vor fi făcute cu regularitate. Totodată, până în 2025, se dorește consolidarea Centrului Satelitar al UE, menit să creeze autonomie în materie de informații geospațiale. Astfel, se va derula și o îmbunătățire a mecanismului Galileo, prin intermediul rețelei de sateliți și se va oferi o imagine cât mai exactă, cu privire la poziționarea în spațiu a potențialelor amenințări.

Busola Strategică prevede ca, la nivelul mării să existe un spațiu comun pentru schimbul de informații (CISE) și de supraveghere maritimă (MARSUR) – în contextul creșterii viitorului pericol, reprezentat de migrație, terorism și amenințări hibride. Busola Strategică va pune un accent însemnat pe cooperarea cu NATO, Parteneriatul Strategic UE-NATO fiind o componentă esențială, în contextul Invaziei din Ucraina. Busola Strategică prevede consolidarea cooperării interorganizaționale, pe bază de intelligence. Pe lângă cooperarea internațională cu NATO, se dorește și o cooperare la nivel European cu alte agenții, precum EUROJUST (Euopean Union Agency for Criminal Justice Cooperation), CEPOL (European Union Agency for Law Enforcement Training), FRONTEX (European Border and Coast Guard Agency).

Limitările „busolei” constau în faptul că, la fel ca în cazul Uniunii, funcționează principiul de unanimitate în materie de decizii, statele

putând oricând să se opună anumitor decizii luate la nivel majoritar, în materie de securitate. De asemenea, o altă limitare constă în faptul că, Busola Strategică funcţionează şi în baza Articolului 51 al Cartei ONU, în baza căruia, apărarea se poate face doar cu acordul Consiliului de Securitate. Astfel, se crează un conflict în materie de decizii, întrucât unul dintre statele faţă de care este îndreptată strategia busolei, Rusia, este membră permanentă a Consiliului de Securitate, având posibilitatea de a bloca orice decizie (Busola Strategică pentru Securitate şi Apărare a Uniunii Europene 2023).

Potrivit deciziei 2010/427/UE a Consiliului Uniunii Europene se doreşte înfiinţarea şi funcţionarea unui serviciu european de intelligence şi stabilirea prezenţei serviciilor de informaţii la nivel supranaţional, dar nu şi la nivel naţional (Jurnalul Oficial al Uniunii Europene. 2010).

Elveţia, între diplomaţie publică şi diplomaţie secretă

Lipsa războaielor, pentru o perioadă de peste 500 de ani, a permis Elveţiei să se dezvolte diferit faţă de restul ţărilor, ea rămânând neutră faţă de orice conflict. Neutralitatea a transformat Elveţia, în spaţiul favorit de negociere al politicienilor, diplomaţilor şi al serviciilor de intelligence, Geneva fiind oraşul favorit al negocierilor (Jürg şi Fischer 2003).

Ţara cantoanelor se remarcă, de asemenea, la capitolul apărare naţională, stagiul militar fiind obligatoriu pentru ambele sexe. Totodată, ţara se bucură şi de o securitate ridicată pentru toate sectoarele, pentru strategia naţională de securitate, participând atât entităţi de stat, cât şi private. Acest lucru face, din statul elveţian, un actor important în schimbul de informaţii la nivelul comunităţilor de intelligence, Geneva fiind oraşul cu cea mai mare concentrare şi diversitate, în materie de Comunităţi de Intelligence (Dutly 2007, 171-176).

Clubul de la Berna

Clubul de la Berna este un club de intelligence, care înglobează serviciile de informaţii din cele 27 de state ale Uniunii Europene, Norvegia şi Elveţia şi care, poartă numele oraşului Berna. Aşa numitul club este o instituţie, bazată pe schimbul voluntar de secrete, experienţe şi opinii, precum şi pe discutarea problemelor. Clubul a luat naştere în anul 1971, neavând un secretariat general şi totodată, neavând drept legal în luarea unor decizii.

Grupul Counter Terorism (CTG) este o ramură a clubului şi împărtăşeşte informaţii despre terorism. Oferă evaluări ale ameninţărilor

factorilor de decizie din Uniunea Europeană și totodată, este o formă de colaborare în intelligence (The portal of the Swiss government 2023). Grupul a fost creat după atacul terorist de la 11 septembrie, din Statele Unite, având ca scop, cooperarea în intelligence între structurile europene (MI5 2023). Asemenea Clubului de la Berna, Grupul Counter Terorism se află în afara instituțiilor UE, dar comunică cu acestea, prin participarea la centrul de analiză de informații al UE (EU INTCEN) (Rettman 2011). Deși, se află în afara UE, președinția Grupului Counter Terorism se schimbă odată cu președinția Consiliului UE și acționează ca o interfață oficială, între Clubul de la Berna și Uniunea Europeană (MI5 2023).

Începutul colaborării în intelligence între Europa de Vest și Israel

În iunie 1971, a avut loc, în premieră, întâlnirea dintre directorii serviciilor de informații, care alcătuiau Clubul de la Berna și șefii intelligence-ului israelian, iar în finalul întâlnirii, israelienii au sugerat, crearea unei rețele comune de partajare a informațiilor. Rețeaua avea la bază o linie secretă de comunicare directă, între intelligence-ul israelian și cel al membrilor clubului, bazată pe programul intitulat Kilowatt. La data de 4 octombrie 1971, în cadrul reuniunii membrilor Clubului de la Berna, era acceptată în unanimitate propunerea Israelului, iar odată cu sfârșitul lunii octombrie, programul Kilowatt devenea operațional.

La un an de la demararea colaborării împotriva terorismului, avea loc și prima analiză, iar pentru a evidenția concret beneficiile acesteia, au fost luate în considerare următoarele 6 aspecte:

- Identificarea profilului unei persoane cu potențial terorist;
- Identificarea grupurilor ce au ca scop susținerea terorismului;
- Identificarea strategiilor și acțiunilor teroriste, prin intermediul informatorilor și a spionilor;
- Identificarea armelor și a tehnologiei utilizate de grupările teroriste;
- Identificarea atentatelor și a atacurilor teroriste, prin intermediul interogărilor sau a arestărilor teroriștilor;
- Identificarea timpurie a planurilor grupărilor teroriste.

În continuare, s-a constatat faptul că, printre cele mai frecvente schimburi de informații au fost despre potențiali teroriști. Informațiile provenite prin intermediul programului Kilowatt s-au bazat pe date (nume, proveniență, număr buletin, aspect fizic), cu privire la persoane

care erau sau urmau să fie implicate în acţiuni teroriste. Aşadar, era posibilă o reconstituire a celor mai comune trăsături a profilului unui suspect, motivele pentru care, suspectul intra în atenţia serviciilor de intelligence şi activităţile avute de-a lungul timpului.

Între octombrie 1971 şi decembrie 1972, au existat nu mai puţin de 300 de schimburi de documente cu privire la persoane, majoritatea dintre acestea fiind implicate în acţiuni teroriste. Cel mai adesea, aceste persoane erau originare din Orientul Mijlociu, ţările fruntaşe fiind Liban, Egipt, Iran şi Tunisia, în timp ce, doar 2 teroriști proveneau din ţări latine, precum Brazilia şi Columbia. Media de vârstă a teroriştilor era cuprinsă între 21 şi 35 de ani, iar culoarea pielii era descrisă ca fiind „închisă" (Guttmann 2017, 193-227).

Cooperarea în domeniul intelligence-ului în cadrul Alianţei Nord-Atlantice

NATO nu are propria structură independentă de intelligence, care să acţioneze ca un organism central de coordonare, însărcinat cu colectarea şi diseminarea informaţiilor furnizate de autorităţile naţionale. Rolul coordonator al unor servicii de informaţii îi este atribuit unui Departament de Intelligence, din cadrul NATO, unde sunt reuniţi şefii tuturor serviciilor de Informaţii, ale statelor membre aliate. Totodată, există numeroase grupuri de lucru şi întâlniri, pentru situaţiile de interes în intelligence-ul militar. În cadrul NATO, multiple organizaţii pot să primească, dar şi să ofere produsele analitice necesare factorilor de decizie politici şi militari, desfăşurându-şi activitatea în departamente diferite, din cadrul International Staff (IS) (Revista Geopolitica 2023).

O problemă apărută, în coordonarea centrală a acţiunilor, ce privesc intelligence-ul din coaliţie este de a oferi factorilor de decizie produse de informaţii, care să le răspundă nevoilor într-un format analitic, cu mai multe surse pe care să-şi bazeze deciziile. Este legată de lipsa unei agenţii unice (Medar şi Lăţea 2007, 88). Deoarece, fiecare dintre aceste structuri deţine canale de comunicare separate, informaţiile ajung la factorii de decizie în diferite forme (Medar 2006, 187).

Analiza informaţiilor primite şi planificarea priorităţilor este responsabilitatea coordonatorului executiv, al biroului directorului general al IMS (International Military Staff) (Office of Information and Press NATO 2001, 248). Structura de informaţii a International Military Staff cooperează cu structurile de informaţii militare ale ţărilor membre, deoarece nu are o capacitate independentă de culegere de informaţii. Conceput pentru a oferi factorilor de decizie analize, bazate în principal

pe baze militare, pe lângă furnizarea de suport zilnic de informaţii, acesta îndeplinește și funcţii strategice de avertizare timpurie și de gestionare a crizelor; pe baza acestor contribuţii, acționează ca instituţii centrale, organizaţii și ţări care colectează, evaluează și difuzează informaţii (Office of Information and Press NATO 2001, 249).

Agenția de Securitate a NATO – NOS cooperează cu structurile de informaţii și securitate ale statelor membre, pentru a furniza informaţii despre terorism, spionaj și crimă organizată, precum și alte informaţii de securitate internațională și regională raportate de directorul NOS. Astfel, se va face totodată schimb de informaţii, legate de domeniile de interes ce țin de competențele generale ale Secretarului General al NATO.

Anumite aspecte ale informațiilor de securitate sunt transmise și prin alte structuri speciale, precum Direcția Generală pentru Economie a Apărării (DEP) sau Centrul pentru Arme de Distrugere în Masă (WMDC) raportează la nivelul superior al Forțelor Aliate (Medar și Lățea 2007, 89).

Având în vedere, că operaţiunile coaliției conduse de NATO, includ națiuni neparticipante și riscul ca informaţii de securitate, să fie preluate de către entități, care nu constituie destinatarii de drept a acestora, alianțele și alte organizaţii internaționale de securitate (OSCE, ONU, UE) este dificil de a face schimb de informaţii. În acest sens, situația „din teren" necesită adesea schimburi de informaţii foarte riguroase, fapt ce determină, ca rezultatul să nu fie întotdeauna cel dorit și, prin urmare, NATO trebuie să permită schimbul de informaţii între toți partenerii Uniunii. Reglementările actuale, în domeniul securității, trebuie să fie adaptate la situațiile extrem de complicate din teren, precum atacul din 30 decembrie 2009 asupra centralei CIA din Khost, Afghanistan (Riedel 2019).

Schimbarea structurală a NATO, cu privire la intelligence, implică coordonarea și modificarea fiecărei componente a ciclului de producție a informațiilor: planificare, colectare, prelucrare, analiză, diseminare și partajare a informațiilor.

Pentru a răspunde cerinţelor operaţiunilor multinaționale, Uniunea Europeană trebuie să colaboreze cu NATO, pentru a lucra împreună într-un cadru comun, având ca scop, abordarea amenințărilor întâmpinate de către aliați. Structurile de intelligence europene trebuie să poată colabora cu structurile omoloage ale NATO, pentru a identifica riscurile și amenințările actuale și pentru a sprijini acțiunile politice, diplomatice și militare ale NATO și ale UE. Astfel, eficiența recunoașterii la nivel operational și strategic, se traduce prin capacitatea de a sprijini

operaţiunile desfăşurate de cele două organizaţii. Liderii politici şi coordonatorii operaţiunilor, alături de personalul acestora, trebuie să fie sprijiniţi în mod continuu, cu fluxul necesar de informaţii pentru a lua cele mai eficiente decizii.

Pentru a spori schimburile de informaţii cu forţele Uniunii, NATO a înfiinţat Unitatea de Informaţii privind Ameninţarea Teroristă (TTIU). Reprezentat de SUA, Germania, Regatul Unit şi Spania, TTIU (Terrorist Threat Intelligence Unit) şi-a început activitatea în anul 2005 (cooperarea cu UE fiind încă în faza incipientă). Terrorist Threat Intelligence Unit prezintă rapoarte de informaţii, asigurând cooperarea directă cu serviciile de intelligence ale statelor membre NATO, statelor care aparţin parteneriatelor de pace şi statelor care, colaborează în cadrul Dialogului Mediteranean (Bendiek 2006, 16).

O comunicare a Comisiei către Parlamentul European şi Consiliul Uniunii Europene, denumită Consolidarea luptei împotriva terorismului (11 noiembrie 2007) stabileşte dimensiunile internaţionale ale abordării UE pentru combaterea acestui fenomen, dar ia în considerare terorismul. Fiind un fenomen global, UE lucrează îndeaproape cu ţările partenere şi organizaţiile internaţionale, în domeniul dreptului anti-terorism, al aplicării legii şi al cooperării judiciare. Un rezultat major al acestei cooperări a fost un acord, cu SUA şi Canada, privind schimbul datelor din PNR (Passenger Name Record), program ce permite o identificare şi mai rapidă a ameninţărilor teroriste, asigurând totodată protecţia datelor cu caracter personal (Revista Geopolitica 2023).

Alianţa Nord-Atlantică nu posedă (de moment) propria structură de intelligence, motiv pentru care, aliaţii depind de serviciile de informaţii ale statelor membre. Aşadar, NATO nu poate garanta primirea de informaţii optime, pentru funcţionarea în cele mai bune condiţii a structurilor de intelligence ale UE şi NATO. Analiştii de intelligence europeni şi americani susţin că, pentru reducerea vulnerabilităţii parteneriatului euro-atlantic, este obligatorie fondarea unei structuri euro-atlantice de intelligence, care va creşte considerabil distribuţia informaţiilor de securitate între toţi participanţii, aducând un plus extrem de mare tuturor misiunilor comune.

În pofida preocupărilor legitime cu privire la necesitatea unei protecţii sporite a fluxurilor de informaţii, o reţea integrată cu acces nerestricţionat, din partea statelor membre, poate răspunde nevoilor tot mai mari de informaţii. În plus, aceasta include partajarea capacităţilor naţionale în domeniile SIGINT şi IMINT (Introduction to Imagery

Intelligence) la o scară mult mai mare decât oricând, precum și colectarea de informații din astfel de surse.

Aceasta va stabili standarde comune NATO și UE, pentru activitățile de informații și va permite un flux continuu de informații, pentru a ajunge la reprezentanții din conducerea Uniunii Europene, cu scopul de a stabili strategia externă. Acest fapt va avea un impact pozitiv, asupra capacității Uniunii Europene de a acționa, în comun cu NATO și Statele Unite, în cadrul războiului centrat pe rețea. Serviciile de informații atât ale UE, cât și ale NATO, precum și serviciile de informații ale statelor membre, urmăresc să asigure consolidarea structurilor de intelligence în zonele considerate a fi de mare interes pentru Comunitatea Atlantică Europeană (Guenther 2008).

Marea Neagră: Lac Rusesc sau avantaj NATO în flancul estic?

Raportându-ne la teoria complexului regional de Securitate, putem privi actuala Invazie din Ucraina ca fiind o întrepătrundere a zonelor de Securitate NATO-Rusia, în regiunea Mării Negre. În acest context, trebuie văzut dacă regiunea Mării Negre reprezintă pentru NATO o zonă vulnerabilă, în materie de securitate sau dacă reprezintă o oportunitate pentru Alianța Nord Atlantică, să își proiecteze umbrela securității în Hinterland și Rimland.

Odată cu atentatele teroriste, din New York și Washington D.C. de la 11 septembrie 2001 (când Al-Qaeda prelua controlul a trei avioane civile, lovind World Trade Center și Pentagonul), în contextul războiului cu terorismul global, NATO a elaborat o nouă strategie Euro-Atlantică cu privire la regiunea Mării Negre, creând, totodată, și un nou concept, care să fie cât mai potrivit pentru noua realitate geopolitică. Conceptul va fi creat de către Ronald Asmus și va merge pe ideea de "Wider Black Sea Region" – Regiunea Extinsă a Mării Negre (Asmus și Jackson 2004, 19-20).

Privind poziția geografică a Mării Negre, observăm că aceasta reprezintă o punte de acces către Marea Mediterană, prin Strâmtorile Bosfor și Dardanele, oferă o zonă de acces în Balcani, prin intermediul Bulgariei, constituind, de asemenea, și o zonă de acces către Caucazul de Sud și Nordul Orientului Mijlociu. În acest sens, putem aprecia faptul că, Marea Neagră reprezintă o importantă zonă, din punct de vedere geopolitic, controlul asupra sa oferind actorului dominant proiecția de putere(hard și smart) către toate zonele geografice enumerate mai sus.

În acest sens, raportându-ne la regiunea extinsă a Mării Negre, din punct de vedere geostrategic și geopolitic, vom analiza potențialul Mării Negre în contextul invaziei din Ucraina, de a deveni fie un ,,lac

rusesc", fie să devină un front esenţial pentru securitatea NATO. (Cojocaru 2014, 184)

Marea Neagră – lac rusesc

La începutul anilor 2000, Rusia adopta un nou concept în materie de politică externă, prin care se autolegitima să intervină în conflictele îngheţate post sovietice, autoproclamându-se a fi o mare putere pe scena internaţională (Smith 2000). Acest lucru a fost pe deplin resimţit pe scena internaţională, Rusia întreţinând conflictele îngheţate din fostele republici sovietice şi intervenind, totodată, în mod activ şi în anumite mişcări separatiste la nivelul acestor state.

Rusia a fost cea mai activă în dezideratele sale, în materie de politică externă, în relaţia sa cu statele riverane Mării Negre. Nu întâmplător, în anul 2015, Rusia a adoptat o nouă Doctrină Navală, care oferea Mării Negre o însemnătate deosebită, atât la nivel operativ ofensiv, cât şi la nivel defensiv, respectiv economic. Mai exact, prin Doctrina Navală adoptată în anul 2015, Rusia marca în plan ideologic un revizionism secular, caracteristic perioadei ţariste specifică lui Petru cel Mare, privind Marea Neagră, ca fiind un lac rusesc destinată satisfacerii intereselor sale.

La nivel ofensiv, prin anexarea Crimeii (portavionul Mării Negre) Rusia a reuşit să obţină controlul şi influenţa căilor de comunicaţie de pe întreg acvariul mării, de la Est la Vest. Rusia a beneficiat de poziţia excepţională a Crimeii la nivel geopolitic şi geostrategic, pentru prima dată în anul 2015, când a reuşit să trimită din Crimea trupe ruseşti, în cadrul conflagraţiei din Siria, demonstrând capacitatea Rusiei de a crea presiuni pe flancul sudic al NATO, Africa de Nord, Orientul Mijlociu, dar şi o cale de acces secundară către Oceanul Planetar (Russian Maritime Studies Institute şi Davis 2015)

La nivel defensiv, Rusia privea Marea Neagră, ca fiind un mijloc esenţial de blocare al extinderii NATO şi implicit de blocare a desfăşurării capacităţilor militare în apropierea graniţelor sale. La nivel economic, Rusia deţinea principalele rute comerciale de la nivelul Mării Negre (Russian Maritime Studies Institute şi Davis 2015).

Marea Neagră – un front esenţial pentru securitatea NATO

Prima referire specifică la regiunea Mării Negre, într-o declaraţie NATO, a fost la Summit-ul de la Istanbul din iunie 2004. S-a evidenţiat importanţa regiunii Mării Negre pentru securitatea euro-atlantică şi dorinţa identificării oportunităţilor de valorificare a mecanismelor de

cooperare existente, între țările din regiune, pentru sprijinirea eforturilor regionale de îmbunătățire a securității și stabilității acesteia (Cojocaru 2014, 201-202).

Deciziile adoptate la Riga (2006), București (2008) și Strasbourg (2009) au reflectat, de asemenea, accentul pus de alianță asupra regiunii Mării Negre. Din punct de vedere istoric, Summit-ul de la București al Alianței este lămuritor, în ceea ce privește diferitele viziuni din cadrul Parteneriatului Euro-Atlantic, cu privire la problema extinderii NATO în Bazinul Estic al Mării Negre, chiar dacă mesajul la nivel de declarație nu a fost pozitiv.

În contextul Invaziei din Ucraina, Regiunea extinsă a Mării Negre a căpătat un grad crescut de importanță pentru NATO și implicit pentru statele componente din structura sa.

Astfel, în data de 16 martie 2023, Președintele Comisiei Permanente Selectate pentru Informații a Camerei Reprezentanților, Mike Turner, împreună cu congresmanul Bill Keating, membru de rang înalt al Subcomisiei pentru Afaceri Externe a Camerei Reprezentanților pentru Europa au introdus Legea pentru Securitatea Mării Negre din 2023, completată ulterior, de Senat. Legea are drept subiect de interes oprirea extinderii conflictelor la nivelul Mării Negre, acestea fiind percepute drept o chestiune de securitate pentru Statele Unite. De asemenea, la nivelul legii se stipulează și o componentă din domeniul intelligence, fiind menționată combaterea amenințărilor hibride (Congress.gov 2023).

Limitări SUA în regiunea Mării Negre, creșterea importanței României pe flancul estic al NATO

Deși proiectul de lege este unul ambițios, acesta cunoaște anumite limitări. Principala limită este una de natură juridică, reprezentată de Convenția de la Montreux din 1936. Potrivit acesteia, navele de război ale statelor care nu au ieșire directă la Marea Neagră, nu trebuie să depășească un tonaj de 15.000 de tone, neputând să rămână pentru o perioadă mai mare de 21 de zile în apele mării (Ministry of Foreign Affairs – Republic of Türkiye 2023). O altă limitare este reprezentată de cooperarea dintre anumite state riverane membre NATO. Relevant este cazul Turciei, care de-a lungul timpului a avut o atitudine ambiguă, cu privire la Rusia. În acest sens, singurii aliați NATO care se bucură de foarte mare încredere sunt Bulgaria și România.

România are potențialul de a deveni cel mai important jucător NATO în regiunea Mării Negre, întrucât, pe lângă componenta fizică,

determinată de poziția geostrategică foarte bună, România posedă şi o componentă psihologică, românii fiind populaţia cea mai rusofobă din rândul statelor riverane Mării Negre, ce aparţin NATO. Potrivit unui raport din cadrul NATO Archives, din 1952, poporul român a fost în întreaga sa existenţă, nemulţumit de influenţa externă sau de control, acest lucru fiind în special valabil, în relațiile cu rușii, implicit Uniunea Sovietică la vremea respectivă (NATO Archives 1952).

Odată cu Summit-ul NATO de la Istanbul, România şi-a dovedit utilitatea pentru NATO, prin transportul desfăşurat pe Marea Neagră ale trupelor NATO spre Afghanistan, prin utilizarea portului Constanţa în rotirea contingentelor de militarii americani din KFOR şi prin participarea României cu două fregate, în operaţiunile NATO din Marea Neagră şi Mediterană (Cojocaru 2014, 201-202).

Summit-ul de la Madrid

Atacul Rusiei din 24 februarie 2022 a demonstrat că, realismul şi componenta hard power, încă, au un rol important în determinarea relaţiilor dintre state. Acest lucru a determinat implicit şi o schimbare de paradigmă la nivelul NATO, trecându-se de la starea de „moarte cerebrală" (expresie utilizată de Preşedintele Franţei, Emanuel Macron, în cadrul unui interviu dat pentru The Economist) (Economist, 2019) la reîntărirea garanţiilor de securitate colectivă, specifice articolului 5 al Tratatului de fondare NATO.

Ca urmare a invaziei Rusiei asupra Ucrainei, NATO a organizat Summit-ul de la Madrid. În cadrul acestuia, se accentua ideea de unitate între statele membre şi aliaţi, ca principal mijloc de acţiune şi de descurajare a agresorilor, prin reafirmarea ideii de unitate şi cooperare trans-atlantică, respectiv de colaborare bazată pe norme şi principii comune (A comparative analysis of Article 5 Washington, 2022). S-a introdus şi un nou concept în materie de apărare, DDA, care presupune descurajarea agresiunii şi apărarea zonei euroatlantice. În tandem cu conceptul DDA, a fost adoptat şi conceptul Warfighting Capstone (NWCC), care are drept scop ghidarea şi dotarea membrilor NATO cu armamentul necesar, pentru a putea face faţă potenţialelor ameninţări. De asemenea, Summit-ul de la Madrid a marcat un moment istoric, Finlanda şi Suedia primind invitaţiile, oficiale, de a se alătura Alianţei (NATO 2022).

Summit-ul de la Vilnius

Principiile stabilite în cadrul Summitului de la Madrid urmează să fie completate de viitorul Summit de la Vilnius (12 iulie 2023), Jens Stontelberg declarând că, acesta va fi unul transformativ pentru alianţă. De asemenea, Summit-ul de la Vilnius va regăsi statele membre ale NATO și într-un context mai sensibil, care reamintește mai mult de perioada Războiului Rece, ca urmare a anunţului Preşedintelui rus Vladimir Putin de a intenționa, să mute arme nucleare în Belarus.

Un subiect important al Summit-ului va fi reprezentat de invazia Rusiei în Ucraina.

Scopul principal – sprijinirea Ucrainei, prin crearea unei contraofensive împotriva Rusiei pentru a câștiga războiul, pentru a oferi o stabilitate în rândul Alianţei pe termen lung și pentru a proteja Europa, împotriva unei viitoare agresiuni ruseşti, asigurând astfel, securitatea tuturor statelor membre.

Pe agenda summit-ului a fost abordată inclusiv China care este văzută ca o amenințare pentru Alianţă. Ca urmare a acestui fapt, Vilnius a marcat și revizuirea conceptului de partener, prin redefinirea relației avute cu partenerii neutri europeni (Elveția, Austria şi Irlanda), dar și intensificarea relaţiilor cu partenerii tradiţionali din afara Europei, precum Israel, Japonia, Coreea de Sud, Australia și Noua Zeelandă.

Astfel, Summitul de la Vilnius a fost unul de succes, atingând următoarele puncte ale agendei:

- ajutorul oferit în continuare Ucrainei, pentru a face faţă invaziei provocate de Federaţia Rusă;
- consolidarea relaţiei NATO- Ucraina;
- asigurarea descurajării nucleare;
- creşterea cheltuielilor militare din PIB, pentru a se atinge ţinta de minim 2%;
- stabilirea unei colaborări transatlantică – transpacifică, pentru a opri ascensiunea Chinei;
- constituirea unui nucleu dur al alianţei format din Finlanda şi Suedia și extinderea mandatului de secretar general a lui Jens Stoltenberg.

De asemenea, un alt obiectiv major care trebuia atins la Vilnius a fost prima implementare a Structurii Forţelor NATO 15, care să înlocuiască vechea structură a NATO, NRF (Forța de Răspuns a NATO).

Concluzii

Balanţa de putere este înlocuită cu balanţa terorii. Astfel, este marcată o schimbare, în materie de logică şi paradigmă în înţelegerea relaţiilor internaţionale. Schimbarea rezidă în faptul că, înaintea războiului din Ucraina, statele îşi formau alianţele în scopul contrabalansării unei puteri, care avea capacitate de a deveni hegemon la nivel global. Aici putem aminti ţările din cadrul BRICS, pentru contrabalansarea economiilor occidentale, a ţărilor din cadrul Tratatului de la Shanghai, ca o posibilă contrabalansare pentru NATO, sau binomul SUA-China pe scena internaţională, cu scopul de a forma o lume bipolară. Odată cu desfăşurarea conflictului din Ucraina, statele îşi vor schimba optica în materie de alianţe, ele ghidandu-se după optica impusă de balanţa terorii. Fiind un concept enunţat în lucrarea The Origins of Alliances de Stephen Walt, atunci când statele se ghidează după principiile balanţei terorii, ele iau în calcul 4 variabile, în definirea unei ameninţări: puterea (hard sau soft), proximitatea geografică, capacităţile ofensive şi intenţiile statului de a îşi utiliza capacităţile ofensive. Conceptul balanţei terorii aduce o îmbunătăţire conceptului balanţei de putere, prin faptul că, aceasta adaugă intenţia de utilizare a capabilităţilor militare. În acest sens, putem observa aderarea Finlandei şi Suediei la NATO şi renunţarea la conceptul de neutralitate, ca urmare a ameninţării reprezentate de Federaţia Rusă.

Crearea unui centru de intelligence la nivel NATO – pe lângă componenta clasică din domeniul apărării – NATO trebuie să îşi creeze un serviciu propriu de informaţii, care să funcţioneze după modelul comunităţii de intelligence americane. Personalul serviciului de intelligence NATO ar urma să fie compus din agenţii structurilor de securitate, din statele alianţei.

Creşterea importanţei flancului estic în domeniul de intelligence – raportat la cazul României, SRI (Serviciul Român de Informaţii) şi SIE (Serviciul de Informaţii Externe) au constituit întotdeauna nişte servicii de informaţii profesioniste, care şi-au îndeplinit perfect sarcinile. Deoarece flancul estic constituie cea mai dinamică regiune a NATO, acesta trebuie să primească mai multe investiţii în proiecte economice, politice şi sociale din partea statelor membre, fiind necesar, ca serviciile de informaţii din această regiune să capete importanţă mai mare, în materie de opinii, sugestii şi decizii.

Fondarea unui centru de intelligence NATO la Bucureşti – încă din perioada celui de Al Doilea Război Mondial, România a constituit un spaţiu esential pentru comunitatea de intelligence americană. Acest fapt

este evidențiat de misiunea OSS (Oficiul Serviciilor Strategice) la București, numindu-l pe Frank Wisner șef al spionajului extern american în România, ce avea ca scop spionarea URSS-ului. Legături istorice în materie de intelligence, între România și Statele Unite sunt foarte relevante în acest context, întrucât ele se pot realiza, în baza Parteneriatului pentru Pace lansat în anul 1997, care are 3 componente esențiale: durabilitate, comprehensivitate și includerea aspectelor militare și de securitate, aspecte care, sunt foarte importante pentru realizarea unui viitor centru de intelligence al Alianței Nord-Atlantice la București. Astfel, istoria relațiilor dintre România și Statele Unite va conta foarte mult pentru constituirea centrului, întrucât, deși România și SUA s-au aflat la un moment dat al istoriei în tabere separate, ele au avut mereu o situație de amiciție, iar acest lucru s-a datorat și cooperării istorice în materie de intelligence.

Bibliografie:

1. Asmus, Ronald D și Jackson Bruce P. 2004. *The Black Sea and the Frontiers of Freedom*.

2. Bendiek, Annegret. 2006. "EU Strategy on Counter-Terorism". SWP Research Paper: 16.

3. Blake Harris Law. 2022. "Swiss Banking: The Basics". Blake Harris Law. Octombrie 26, 2022. https://blakeharrislaw.com/blog/swiss-banking

4. Cojocaru, Marius George. 2014. *NATO și Marea Neagră.* Editura Cetatea de Scaun. Târgoviște.

5. Dutly, Markus. 2007. "CHAPTER 10: The Swiss Initiative on private military and security companies". Institute for Security Studies. Mai 17, 2023. https://issafrica.org/chapter-10-the-swiss-initiative-on-private-military-and-security-companies-markus-dutly

6. Clapp, Sebastien și Verhelst, Anne. 2022. "A comparative analysis of Article 5 Washington Treaty (NATO) and Article 42(7) TEU (EU)" in European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/739250/EPRS_ATA(2022)739250_EN.pdf

7. Fehr, Ernst și Gächter, Simon. 2002. "Altruistic punishment in humans". *Nature,* 415: 137-140. https://www.nature.com/articles/415137a#citeas

8. Guenther, Weisse K. 2008. *Intelligence Cooperation among European Nations, Young Europeans for Security (YES)*.

9. Guttmann, Aviva. 2017. *The Origins of International Counterterrorism*. Editura Brill. Olanda.

10. Hărmănescu, Ingino şi Ioniţă, Cornel. 2006. *Arhitectura de Informaţii la nivelul Uniunii Europene, în "Informaţiile militare în contextul de securitate actual*". Bucureşti.

11. Institutul European pentru Studii de Securitate. 2023. "About Us." EUISS. Mai 17, 2023. https://www.iss.europa.eu/about-us

12. Jürg, Martin Gabriel şi Fischer, Thomas. 1945-2002. *Swiss Foreign Policy*.

13. Jurnalul Oficial al Uniunii Europene. 2010. „DECIZIA CONSILIULUI din 26 iulie 2010 privind organizarea şi funcţionarea Serviciului European de Acţiune Externă (2010/427/UE)." Jurnalul Oficial al Uniunii Europene. https://eur-lex.europa.eu/legalcontent/RO/TXT/PDF/?uri=CELEX:32010D0427&from=HU

14. Kohn, Alfie. 1992. *No Contest: The Case Against Competition.* Ediţia a II-a Houghton Mifflin.

15. Marinez-Moyano, Ignacio J. 2006. *Exploring the Dynamics of Collaboration in Interorganizational Settings.* Jossey-Bass/Wiley.

16. Medar, Sergiu T. 2006. Informaţiile Militare în contextul de securitate actual. Editura CTEA, Bucureşti.

17. Medar, Sergiu T şi Lăţea, Cristi. 2007. *Intelligence pentru comandanţi*. Editura CTEA. Bucureşti.

18. Ministerul Afacerilor Externe (MAE). 2020. „Parteneriatul strategic România – SUA. Expoziţie aniversară: 140 de ani de la stabilirea relaţiilor diplomatice dintre România şi SUA". Mai 25, 2023. https://www.mae.ro/node/4944

19. Ministry of Foreign Affairs – Republic of Türkiye. 2023. "IMPLEMENTATION OF THE MONTREUX CONVENTION." https://www.mfa.gov.tr/ Mai 17, 2023. https://www.mfa.gov.tr/implementation-of-the-montreux-convention.en.mfa

20. NATO. 2001. *Manualul NATO*. Editura Office of Information and Press NATO. Belgium.

21. NATO. 2022. "Madrid Summit Declaration." North Atlantic Treaty Organization. Iulie 22, 2022. https://www.nato.int/cps/en/natohq/official_texts_196951.htm

22. NATO Archives. 1952. *IMS, Report by The Intelligence Committee to the Standing Group on Intelligence for the Standing Group and Intelligence Guidance for the Major NATO Commands and the Commands Associated with NATO, SG 176/1, 17 March 1952.*

23. Rettman, Andrew. 2011. "EU commission keen to set up new counter-terrorism office." EUObserver. Martie 31, 2011. https://euobserver.com/eu-political/32104

24. Revista Geopolitica. 2023. „COOPERAREA ÎN DOMENIUL INTELLIGENCE-ULUI ÎN SPAŢIUL EUROPEAN ŞI EUROATLANTIC". Mai 26, 2023.

25. Revista Intelligence. 2013. „Cooperarea în intelligence, factor determinant în faţa noilor ameninţări la adresa mediului de securitate

internațional". Martie 7, 2013. https://intelligence.sri.ro/cooperarea-intelligence-factor-determinant-fata-noilor-amenintari-la-adresa-mediului-de-securitate-international/

26. Riedel, Bruce. 2019. "The remarkable case of the triple agent and the bombing in Khost, Afghanistan – 10 years later". Decembrie 6, 2019. https://www.brookings.edu/blog/order-from-chaos/2019/12/06/the-remarkable-case-of-the-triple-agent-and-the-bombing-in-khost-afghanistan/

27. Russia Maritime Studies Institute. 2015. *The 2015 Maritime Doctrine of the Russian Federation.* Tradusă în engleză de Anna Davis. RMSI Research 3.

28. Security Service MI5. 2011. "European counter terrorism meeting." Security Service MI5. Mai 16, 2023. https://web.archive.org/web/20110611105418/ – https://www.mi5.gov.uk/output/news/european-counter-terrorism-meeting.html

29. Smith, A M. 2000. *Russian Foreign Policy 2000: The Near Abroad.* Editura F71.

30. Spence, Muneera U. 2006. *Graphic Design: Collaborative Processes – Understanding Self and Others.* Art 325: Collaborative Processes. Fairbanks Hall, Oregon State University, Corvallis, Oregon.

31. The Economist. 2019. "Emmanuel Macron warns Europe: NATO is becoming brain-dead". Iunie 20, 2023. https://www.economist.com/europe/2019/11/07/emmanuel-macron-warns-europe-nato-is-becoming-brain-dead

32. The portal of the Swiss government. 2023. "«Club de Berne» meeting in Switzerland". The Federal Council – The portal of the Swiss geovernment. Mai 16, 2023. https://www.admin.ch/gov/en/start/dokumentation/medienmitteilungen.msg-id-24089.html

33. The Strategic Compass of the European Union. 2023. „Busola Strategică pentru Securitate și Apărare a Uniunii Europene". https://www.strategic-compass-european-union.com/

34. U.S. Congress. House. *S. 804 To provide for security in the Black Sea region, and for other purposes.* Introdusă în congres pe Martie 15, 2023. https://www.congress.gov/bill/118th-congress/senate-bill/804/text

35. Wetzling, Thorsten. 2023 "Intelligence Cooperation: Dimensions, Activities and Actors." www.se2.dcaf.ch/serviceengine

TEORIA DISCURSULUI: APLICABILITATE ÎN ANALIZA SCHIMBĂRILOR DE PARADIGMĂ ÎN STUDIILE DE SECURITATE

Robert-Ionuț STANCIU*

Abstract:

This article examines discourse theories, its components (tools or manifestations) and their applicability in security studies. Starting from the generic framing of discourse theories in social sciences, the research aims to particularize and niche the attention towards causal links, and specific markers, which can be used methodologically to identify a paradigm shift in security studies. In this context, the research was based on the following questions: What is discourse theory? What are the tools of discourse theory? How can these act as a litmus in revealing a paradigm shift in security studies? The methodology used was the transversal analysis of discourse theories and its relevance in security studies. Process tracing and document analysis techniques were also used to determine causality effects between speeches and security postures.

The main findings of the research reveal that discourse theory is an important tool for understanding the way in which language can be used to influence beliefs, social and political attitudes, but also for the transmission of warning messages regarding a change of position in addressing security and defense. Discourse theory also offers insights into how language can be used to maintain existing power structures. The assertion applies equally to both social groups and entities that are part of the international security system (states, organizations, institutions, etc.). Using language in specific ways can influence institutional behavior in a manner favorable to the sender, provided that the promoters of the messages are referential authorities called hegemonic agents. Based on these benchmarks, we believe and prove that the use of methodological language/speech analysis mechanisms could provide a priori relevant information regarding intentions, objectives and positions that the issuer can adopt. All this could contribute to the (pre)notification of an implicit or explicit paradigmatic change.

Keywords: *discourse theories, security studies, international relations, international crises, strategic communication.*

* Cercetător postdoctoral la Școala Doctorală „Paradigma Europeană" a Facultății de Studii Europene a Universității Babeș Bolyai, Cluj-Napoca. Email: stanciu.robert.ionut@gmail.com

Teoria discursului este un instrument important pentru înțelegerea manierei în care, limbajul poate fi folosit pentru a influența convingerile, atitudinile sociale și politice, dar și pentru transmiterea unor mesaje cu rol de avertizare, cu privire la schimbarea unei posturi în abordarea problematicii securității și apărării. În egală măsură, în relațiile internaționale poate fi folosit pentru a analiza modurile în care, elitele politice ale unor entități/state puternice folosesc limbajul, pentru a convinge competitorii să-și armonizeze pozițiile. Aceasta este o tactică folosită de-a lungul istoriei, dar a devenit din ce în ce mai răspândită în ultimii ani, odată cu dezvoltarea tehnologică, creșterea consumului de informații, perfecționarea și diversificarea mass-media.

Teoria discursului oferă, de asemenea, perspective asupra modului în care limbajul poate fi folosit, pentru a menține structurile de putere existente. Aserțiunea se aplică, deopotrivă, atât grupurilor sociale, cât și entităților componente ale sistemului internațional (state, organizații, instituții etc.). Folosind limbajul în moduri specifice se poate influența conduita instituțională, într-o manieră favorabilă emițătorului.

În acest fel, discursul are capacitatea de a produce cunoaștere, sens și reacții. În baza acestor repere considerăm, că folosirea mecanismelor metodologice de analiză a limbajului/discursurilor poate furniza apriori informații relevante cu privire la intențiile, obiectivele și postura, pe care emitentul le poate adopta și poate contribui la sesizarea unei modificări paradigmatice de conduită, implicită sau explicită în studiile de securitate.

Teoria discursului și instrumentele sale. Relevanța acesteia în științele sociale și studiile de securitate.

Încercarea de a încadra *teoria discursului* într-o definiție, care să acopere întregul concept s-a dovedit mai dificilă decât părea, la inițierea acestui demers științific. Dificultatea demersului a survenit din două aspecte. Pe de o parte, analiza primară a asocierii termenilor *teorie* și *discurs* a generat ipoteza falsă a simplității acțiunii de definire integrată a conceptului, iar pe de altă parte, inițierea exploratorie a ceea ce ar putea însemna o teorie a discursului, trimite analistul în vastul câmp al științelor comunicării, domeniu din care, poate fi dificil a selecta acele concepte componente relevante și a le cataloga, ca elemente ale teoriei discursului.

În literatura de specialitate pot fi identificate, totuși, o serie de definiții ale teoriei discursului care, în mare, sunt centrate pe analizarea comunicatului ca sistem unitar, a efectelor acestuia asupra publicului țintă și a structurii arhitecturale a alocuțiunii. Plecând de la aceste

considerente, se pot oferi, pe de o parte, definiţii ale *teoriei a discursului* în calitate de concept integrat, iar pe de altă parte, ca un cumul de delimitări conceptuale ale unor instrumente ale teoriei discursului, cum ar fi *comunicare (politică), discurs (politic sau de securitate)* sau *analiză de discurs*. Vom trata în cele ce urmează, toate aceste concepte.

Teoria discursului apare în literatura de specialitate în jurul anului 1970, atunci când, a fost iniţiat un curent de contestare a teoriilor structuraliste ale limbajului. Această nouă abordare nu a furnizat un nou aparat de studiu, ci doar o perspectivă inovativă în contextul unor identităţi sociale, politice şi culturale în dezvoltare. Conform lui Alejandro I. Paz, teoria discursului *denotă în linii mari studiul acelor aspecte ale limbajului şi comunicării distincte de structura gramaticală tradiţională*. În acest fel, *majoritatea teoriilor discursului examinează relaţia dintre limbaj şi structura arhitecturală a comunicatului* (Paz 2013, 191). Astfel, teoria discursului este o concepţie aparţinând ramurii ştiinţelor comunicării, care studiază producerea, transmiterea şi recepţionarea comunicatelor. Teoria îşi are rădăcinile în lucrările unor oameni de ştiinţă, precum Michel Foucault (*curent post-structuralist*), considerat unul dintre autorii de referinţă, care a cercetat acest domeniu şi/sau Ferdinand de Saussure (*şcoala structuralistă de gândire*).

În teoria lingvistică, propoziţia este unitatea de bază a relaţiilor gramaticale. În cadrul acestui domeniu, discursul reprezintă modalitatea prin care, propoziţiile şi expresiile sunt astfel folosite pentru ca rezultatul aranjamentului lor să furnizeze un mesaj către audienţă, care, la rândul ei, să îşi adapteze comportamentul şi reacţiile. De altfel, aserţiunea este intuitivă, având în vedere că gramatica, apărută ca obiect de studiu la grecii antici, reprezintă doar o serie de reguli pentru a diferenţia formele corecte de cele incorecte, o disciplină normativă lipsită de o privire de ansamblu ştiinţifică, bazată pe observaţie şi conexiuni logice (de Saussure 1967, 13). În acest fel, discursurile respectă principii şi reguli diferite de cele gramaticale iar, conform curentului structuralist (*exponent: de Saussure*) coerenţa unitară a discursului este influenţată de elementele sale componente (Paz 2013, 192).

Pe de altă parte, interdependenţa elementelor componente ale unui discurs, în raport cu contextul dat, poate crea semnificaţii diferite ale aceluiaşi comunicat. Elementele descrise fac obiectul de studiu al analizei de discurs şi *sunt subscrise şcolilor post-structuraliste ale teoriei discursului*. Michel Foucault este un exponent de referinţă al acestui curent. Astfel, conform lui Focault, discursul este *o modalitate de organizare a cunoaşterii care structurează constituirea relaţiilor sociale*

(și progresiv globale) prin înțelegerea colectivă a logicii discursive și acceptarea discursului ca fapt social (Adams 2017). În acest fel, discursul structurează modul în care este percepută realitatea, determină ce este bine sau greșit, stă la baza oricărei capacități de a înțelege sau de a argumenta și guvernează asupra tot ceea ce poate sau nu poate fi spus sau știut. Potrivit lui Foucault, *discursul este un produs istoric și social care, ca și limbajul, apare sincron și evoluează diacronic* (Foucault's Concept 2017). Foucault vede discursul din perspectivă socială, mai degrabă decât din punct de vedere structural (Bhattarai 2020). Pentru Foucault, în egală măsură, plasarea discursului în contextul dat este definitorie, având în vedere că, el consideră că *logica produsă de un discurs este legată structural de epistema extinsă a perioadei istorice în care acesta ia naștere* (Adams 2017).

Astfel, dacă în viziunea structuralistă discursul poate fi descris drept o rețea celulară interconectată, ale cărei noduri reprezintă puncte de inflexiune ale comunicării, și care pot determina sensul general al înțelesului, ipoteza post-structuralistă acordă o importanță deosebită, inclusiv permutărilor posibile dintre respectivele noduri, argumentând că, prin repoziționarea acestora pot fi obținute înțelesuri multiple (Jørgensen și Phillips 2002, 25). Mai mult decât atât, și accepțiunea post-structuralistă validează parametrii de analiză multiplii, cum ar fi contextul istoric sau social. În acest fel, *crearea înțelesului (n. discursului) reprezintă un proces social* (Jørgensen și Phillips 2002, 25). *Ingineria inversă* acestui proces reprezintă obiectul de studiu al analizei de discurs, al cărei principal obiectiv îl constituie plasarea în spațiu și timp a *nodurilor* anterior menționate.

În alte accepțiuni, cum ar fi realismul critic, discursul poate fi privit ca manieră de construire a realităților sociale. Construcțiile discursive sunt teoretizate, ca fiind modelate de posibilitățile și constrângerile inerente lumii materiale. În adoptarea unei abordări critice realiste, analiza poate include relații dintre condițiile materiale ale societății și practicile discursive. Deși, au fost încercări de a dezvolta o bază metodologică a discursului realist critic, literatura de specialitate relevă că, cercetările empirice sunt modeste. Un exponent al acestui curent de gândire este Roy Bhaskar (Warwick 2023). Parametrii săi au fost stabiliți *mai mult de o agendă și de un program de cercetare decât de o teorie sau o metodologie coerente* (Wodak 2001). Totuși, ideea centrală a realismului critic este că motivele/obiectivele pot deveni cauze. Ideea este completată de credința că, rațiunile sunt mediate de sens, ceea ce face ca semioza/discursul să capete semnificație și putere mobilizatoare.

Unul dintre dezacordurile centrale dintre cele două direcţii de gândire, *post-structuralism şi realism critic,* cu privire la teoria discursului este dacă, şi în ce măsură, discursul poate fi distins de aspectele non-discursive ale realităţii sociale.

Pe de altă parte, evoluţia teoriilor discursului în raport cu studiile de securitate a conjugat aspectele enumerate anterior, cu introducerea şi a altor valenţe în analiza teoriilor discursului, cum ar fi *puterea* şi maniera de exprimare a acesteia. Această abordare transcende abordarea iniţială, care se limitează la înţelegerea limbajului, a modului în care este organizat sau a strategiilor emitenţilor. Mai mult, teoriile dezvoltate ale discursului aplicate studiilor de securitate iau în considerare şi modul în care, instituţiile de securitate condiţionează regulile discursive de exprimare a puterii. Procesul ar fi insuficient în lipsa analizei contextului temporal sau spaţial, în care un comunicat securitar este furnizat şi a modului în care, cuvintele sunt folosite de expozanţi pentru a modela rezultatul şi a produce efecte. În acest fel, teoria discursului poate fi folosită, pentru a înţelege modul în care, dinamica puterii şi discursul securitar modelează mediul de securitate. Ceea ce înseamnă că, de fapt, discursurile securitare poartă în semiotica lor întreaga gamă de înţelesuri, care pot reconstitui sau prevede acţiunile sau postura de securitate, pe care emitentul ar putea-o adopta. Folosirea metodologiei specifice de analiză, în cadrul studiilor de securitate, poate evidenţia empiric acest conţinut, care modelează sau precedă o nouă postură de securitate.

Numitorul comun al tuturor valenţelor teoriei discursului, aplicat studiilor de securitate, este rolul central al limbajului, al comunicării şi/sau al sensului, suprapuse peste un context dat. Pornind de la această inferenţă, am identificat şi vom explora şi alte concepte asociate teoriilor discursului, concepte care, instrumentalizează teoriile discursului, considerate relevante în gama metodologică a studiilor de securitate, de la *comunicarea politică, la discursul politic şi analiza de discurs.*

Comunicarea politică şi discursul politic

Originile cuvântului *comunicare* pot fi identificate în limba latină (*communicatio*), un termen care semnifică a împărtăşi sau a pune în comun (Peters 2008). Comunicarea este definită, ca un proces de înţelegere şi împărtăşire a unui sens (Libraries 2023). De asemenea, (Fârte 2005) completează definiţia afirmând că, aceasta reprezintă o „*acţiune colectivă semiotică*". Comunicarea politică îşi găseşte rădăcinile încă din antichitate, atunci când lua forma *retoricii* şi a *discursului politic*

(Briciu 2017, 6). Ulterior, o formă nouă a comunicării politice/ discursului politic a fost dezvoltată în timpul celor două războaie mondiale, prin intermediul propagandei (*Ibidem*). Alte trei dimensiuni recente ale comunicării politice/discursului politic se referă la *studiul comportamentului de vot, efectelor mass-media,* precum și dimensiunea comunicării politice reprezentată de *presă și organizațiile guvernamentale,* respectiv a *relațiilor dintre acestea* (Briciu 2017, 7). Ca domeniu de studiu, această asociere de termeni, comunicarea politică, mai mult sau mai puțin în forma actuală, a început să se contureze ca un concept științific în Statele Unite ale Americii, odată cu cercetările lui Walter Lippmann, Harold Lasswell sau Paul Lazarsfeld (Laberge 2007, 521).

Comunicarea politică este percepută în unele accepțiuni drept un termen dificil de delimitat, din cauza multidimensionalității sale și a multiplelor științe (*științele comunicării, filologie, sociologie, marketing etc.*) care au abordat studiul acestui concept (Tănase 2014). Subsumată acestei aserțiuni este și afirmația lui Dan Lungu, care consideră că *„perspectiva teoretică evoluează între incertitudinea obiectului de studiu și câmpul teoretic concurențial*" (Lungu 2002). De altfel, prin alăturarea celor doi termeni, *comunicare* și *politică,* sensul de bază al celor două s-a denaturat, în ideea că *rolul comunicării se mută din zona valorii în zona interesului* (Briciu 2017, 8). În unele accepțiuni chiar, termenul integrat de *comunicare politică* nici măcar nu ar exista în calitate de concept (Laberge 2007), fiind mai degrabă vorba de o asociere de termeni, care poate fi definită prin rolul acordat comunicării în cadrul proceselor politice (*Ibidem*).

Studiile de securitate sunt interconectate cu definirea comunicării politice, în literatura de specialitate, prin definirea celei din urmă drept *o acțiune colectivă semiotică ce se realizează în contextul organizării și conducerii unei societăți* sau ca *un act de exercitare a puterii* (Fârte 2005). În egală măsură, Axford *et.al.* consideră, că actul de comunicare politică/ discurs politic reprezintă un demers intenționat, inițiat de actori, care acționează în marja reperelor furnizate de un sistem prin care se poate exercita puterea (Tănase 2014, 24) (Briciu 2017, 8).

Conform Fairclough & Fairclough, discursul politic este o formă primară de argumentare, care implică argumentare practică, argumentare pro sau contra unei acțiuni și argumentare care, să fundamenteze o decizie (Fairclough și Fairclough 2012). Pe de altă parte, caracterul intențional al comunicării politice și discursului politic este relevat și de către Denton & Woodward, care afirmă că, finalitatea unei astfel de acțiuni o reprezintă *realizarea obiectivelor comune,*

transmiterea unor mesaje către un public sau *redifuzarea temelor politice de către anumite entităţi media* (Denton şi Woodward 1990) *apud* (Tănase 2014, 25). Elementul de intenţionalitate nu este o valenţă generată direct de către emitent, ci indirect, având în vedere obiectivele sale declarate sau implicite (Briciu 2017, 9).

Pe plan naţional, cercetătorii în domeniu studiilor de securitate definesc comunicarea politică drept „*o interacţiune strategic reglementată prin norme juridice, ritualuri, valori, simboluri, tehnologii, organizaţii, reţele şi practici*" (Beciu 2009, 126). Desprindem noi repere ale caracterului intenţional al comunicării politice, relevante în studiile de securitate, cum ar fi existenţa unei strategii (*deci delimitarea planificată şi organizată a comunicării*), a unor norme (*crearea apriori a unui set de reguli*), precum şi a unor sisteme de transmitere (*tehnologii, reţele etc.*). Mai mult decât atât, caracterul intenţional al comunicării politice determină existenţa unui scop bine definit.

Având în vedere complexitatea reperelor menţionate, putem deduce că, toate acestea pot fi agregate şi coordonate doar într-un mediu instituţionalizat, ceea ce furnizează comunicării politice/discursului politic de securitate o *dimensiune instituţională*.

Analiza discursului de securitate

În abordarea acestui paragraf este imperios necesar să recapitulăm o serie de constatări realizate anterior. Astfel, în teoria generică a discursului se impune marcarea unor cuvinte cheie, relevante acestui domeniu, de la *limbaj*, la *putere*, *context social*, *obiective* explicite sau implicite ale naratorului. În acest context, analiza critică a discursului de securitate reprezintă o serie de proceduri metodologice, pentru realizarea/identificarea conexiunilor dintre elementele (*cuvintele cheie*) menţionate anterior.

Trebuie să ţinem cont de faptul, că orice concepţie a analizei discursului de securitate, ca abordare metodologică, va fi întotdeauna înrădăcinată într-o teorie mai largă a discursului (Atkinson, Held şi Jeffares 2010). În cadru extins, conform lui de Saussure, analiza de discurs a putut fi folosită, de asemenea, în domeniul filologiei, având ca obiecte de studiu literatura şi istoria sau analizarea şi interpretarea textelor, într-o manieră critică. Astfel, desprindem limitările perspectivei structuraliste, care se concentrează, cu predilecţie, asupra arhitecturii formale a discursului.

Pe de altă parte, analiza discursului foucaultian, aplicabilă studiilor de securitate, este o formă de analiză a discursului, cu un accent

deosebit pe relațiile dintre *limbaj*, *putere* și *context*. Metoda se bazează pe teoria discursului și controlului social a lui Foucault (Study Smarter, 2023) și își propune să expună, maniera în care, exponenții puterii pot influența audiența prin limbaj, în acest fel relevând modificări paradigmatice în studiile de securitate.

Cu alte cuvinte, *analiza discursului (de securitate) este în esență analiza limbajului în context* (Gee 2005). Astfel, practicile discursive stabilesc, ascund sau transformă relații de putere între cei implicați, într-un anumit discurs securitar.

Teoria discursului aplicată în relații internaționale și studii de securitate

Teoria discursului este relevantă pentru înțelegerea politicii, a dinamicii relațiilor internaționale și în studiile de securitate, deoarece oferă o modalitate de a înțelege modul în care puterea, intențiile explicite sau implicite și tendințele securitare sunt exprimate prin limbaj și comunicare.

Astfel, folosirea ca reper a teoriei discursului poate fi un instrument puternic, în cadrul analizelor subsumate domeniului relațiilor internaționale și studiilor de securitate. Teoria discursului poate contribui la înțelegerea rațiunilor, pentru care actorii internaționali comunică între ei și care sunt consecințele acestor interacțiuni în plan securitar. Am văzut, că teoria discursului postulează că, orice comunicare are un scop politic, adică urmărește să influențeze comportamentul altor actori (Tănase 2014, 24) (Briciu 2017, 8) într-o manieră structurată, intenționată (Denton și Woodward 1990) și sistemică. Înțelegerea acestei abordări poate fi folosită în studiile de securitate atât pentru a studia relațiile dintre state, relațiile dintre organizațiile internaționale, dar și relațiile dintre state și organizațiile internaționale.

Plecând de la faptul, că teoriile discursului plasează acțiunea de comunicare drept *o acțiune colectivă semiotică*, realizată ca *un act de exercitare a puterii* (Fârte 2005) deducem că, teoria discursului ne ajută să înțelegem nuanța persuasivă folosită de state (prin vectorii de mesaj) atunci când, se angajează în relații internaționale sau în competiții strategice de securitate. Prin analiza discursului se poate releva maniera în care, comunicarea este folosită de către state sau organizații internaționale de securitate, pentru exprimarea intereselor și convingerea/

persuadarea altor entităţi (state sau organizaţii) în acceptarea poziţiei proprii.

Am văzut că, în relaţiile internaţionale şi studiile de securitate, puterea tinde să fie asociată în cel mai bun caz cu concurenţa, iar în cel mai rău caz cu constrângerea sau dominarea (Karlberg 2005). Noţiunea de discurs a lui Foucault este un concept metodologic vital în propagarea puterii, în era poststructuralistă. În această viziune asupra discursului, puterea şi cunoaşterea sunt unite (Pitsoe şi Moeketsi 2012). În acest sens, deducem că teoria discursului poate fi aplicată unei varietăţi de probleme derivate domeniilor relaţiilor internaţionale şi studiilor de securitate, cum ar fi negocierile privind pacea, deciziile de politică externă, managementul crizelor şi chiar angajamentele militare.

Astfel, teoriile discursului au fost aplicate în analiza politicii externe, de exemplu de către Henrik Larsen în teza sa de doctorat, ceea ce a devenit mai apoi, cartea intitulată *Foreign Policy and Discourse Analysis: France, Britain and Europe.* Una dintre problemele relevate de către Larsen, în analiza discursului din domeniul politicii externe este uniformitatea limbajului şi a ideologiei. În accepţiunea sa este dificil a uniformiza înţelegerea asupra anumitor concepte, cum ar fi *Europa, stat, securitate sau natura relaţiilor internaţionale* (Larsen 1997, 1). Astfel, analiza, din domeniul politicii externe, tinde să ignore exact acel aspect delimitat de noi în debutul lucrării, adică particularităţile limbajului în contextul dat. Autorul tratează pe larg aceste aspecte în cadrul capitolului iniţial al lucrării sale, folosind ca repere aspecte de lingvistică şi teorii ale discursului politic.

Larsen foloseşte teoriile discursului, pentru a evidenţia asemănări şi deosebiri în politica externă a Franţei şi Marii Britanii, cu privire la Europa în anul 1980. Pentru a stabili un cadru referenţial, Larsen face apel la patru concepte, prin care politicile externe ale celor două ţări sunt comparate, astfel: *Europa, stat/naţiune, securitate şi natura relaţiilor internaţionale* (*Ibidem*) argumentând că, prin analizarea acestor patru paliere de studiu pot fi extrapolate asumpţii cu privire la politica externă generică a celor două naţiuni.

Teoria discursului este în egală măsură utilizată în domeniul studiilor de securitate de către Hayder S. Alkhafaji, în analiza sa privind invazia USA din Irak. În studiu său, cercetătorul a folosit lingvistica funcţională sistemică a lui Halliday (*Hallidayan Systemic Functional*

Linguistics)[1] pentru a identifica relațiile de cauzalitate dintre discursurile politice ale lui George W. Bush în raport cu invazia Irakului în 2003 de către SUA. Limbajul politic se conturează drept un instrument eficient în realizarea obiectivelor. Prin urmare, politica nu poate fi separată de limbaj, deoarece politica se realizează prin limbaj (Alkhafaji 2022). Astfel, pentru a-și verifica ipotezele, cercetătorul a folosit un corpus de zece discursuri ale președintelui Bush, care au fost analizate din punct de vedere semantic, sintactic și al manipulării pragmatice și în egală măsură asupra impactului asupra modelelor mentale ale receptorilor (Alkhafaji 2022). Un concept nou pe care Alkhafaji îl introduce în teoriile discursului este retorica, fiind considerată de cercetător o *artă a persuasiunii (Ibidem)*. Aceasta reprezintă o metodă care folosește limbajul de o manieră manipulativă în scopul modificării percepțiilor și comportamentului receptorilor. Rezultatele cercetării lui Alkhafaji relevă conexiuni directe între discursurile analizate și ideologie, obiective, tematizarea pozitivă/negativă a unor subiecte, precum și efecte asupra publicului țintă. Aceste elemente sunt operaționalizate în justificări ale unor acțiuni viitoare, ceea ce este echivalent cu faptul că discursul poate reprezenta un precursor al unei schimbări de paradigmă.

Discursul în contextul unei crize de securitate

Există fundamente empirice cu privire la faptul că, în contextul unei crize pot fi generate progrese evolutive și schimbări de paradigmă în postura de securitate (De Rycker și Mohd Don 2013, 3). Crizele internaționale pot fi definite ca evenimente, care au potențialul de a modifica definitoriu relațiile internaționale și de a afecta securitatea globală. Acestea pot lua forma unor conflicte militare, recesiuni economice, dezastre naturale, pandemii, tulburări politice sau chiar războaie contemporane, așa cum este actualul conflict din Ucraina. Toate aceste scenarii pot crea un impact semnificativ, asupra poziției de

[1] Lingvistica funcțională sistemică reprezintă studiul relației dintre limbă și funcțiile sale în mediile sociale. Este cunoscută și ca SFL, gramatică funcțională sistemică, lingvistică Halliday sau lingvistică sistemică. Sistemul lingvistic în SFL este format din trei paliere: sensul (semantică), sunetul (fonologie) și formularea sau lexicograma (sintaxă, morfologie și lexis). Lingvistica funcțională sistemică tratează gramatica ca pe o resursă de creare a sensului și insistă asupra interrelației dintre formă și sens. Acest domeniu de studiu a fost dezvoltat în anii 1960 de lingvistul britanic M.A.K. Halliday (n. 1925), influențat în munca sa de către profesorul său J.R. Firth (1890-1960). **Sursa**: Nordquist, Richard. *Overview of Systemic Functional Linguistics*, 2021. Disponibil la adresa https://www.thoughtco.com/systemic-functional-linguistics-1692022, consultat la data de 24.01.2023.

securitate a unei ţări sau organizaţii şi asupra deciziilor sale de politică externă. Relevanţa unei crize internaţionale, pentru studiile de securitate, este că se oferă o oportunitate unică, de a observa şi analiza comportamentul entităţilor internaţionale, în momente de presiune, prin intermediul discursurilor din criză.

În relaţiile internaţionale rezolvarea crizelor este un obiectiv universal. De exemplu, atât Organizaţia Tratatului de Nord (NATO), cât şi UE au paliere de gestionare a crizelor, în organigrama angajamentelor lor de securitate. De Rycker şi Mohd Don văd o relaţie de cauzalitate directă, între rezolvarea crizelor şi discursul de securitate. Aceştia afirmă că, în procesul de management al crizelor, pe lângă acţiunile pragmatice, succesul depinde de performanţa limbajului, a comunicării şi a discursurilor (De Rycker şi Mohd Don 2013, 37). Evoluţia crizelor va fi influenţată de nuanţa discursurilor. Conform autorilor, discursurile dominante tind să reducă amplitudinea unei crize (De Rycker şi Mohd Don 2013, 3).

Narativele, pe parcursul unei crize, vor purta anvelopa şi vor influenţa strategiile şi politicile referitoare la respectiva criză, precum şi efectele pe termen lung (Fairclough şi Fairclough 2012). Obiectivele pot viza două soluţii finale, pe de o parte revenirea la normal „*status qvo ante*", iar pe de altă parte modificarea radicală a sistemului (Fairclough şi Fairclough 2012). În cea din urmă situaţie, schimbarea poate fi mai mult sau mai puţin *radicală,* însă, ceea ce este important în comportamentul UE este sesizarea unei modificări a tendinţei istorice, aspect care ar putea fi debutul unei noi paradigme.

În cadrul gestionării unei crize, construirea identităţii comune este capitală (De Rycker şi Mohd Don 2013, 38). Discursul joacă un rol central, în modelarea subiectivităţii auditoriului. În aceste momente, se face apel la exponenţi referenţiali ai puterii, prin care mesajul poate fi transmis. Ulterior discursurilor, rezolvarea unei crize va trebui să vină, mai degrabă, prin măsuri concrete ale exponenţilor de mesaj decât printr-o acţiune comună, conjugată a publicului ţintă (De Rycker şi Mohd Don 2013, 39).

Teoria discursului contribuie astfel, la înţelegerea modului în care, limbajul afectează dinamica puterii între ţări sau organizaţii internaţionale, în momentul unei crize în desfăşurare. Prin analiza metodologică a discursului se poate identifica modul în care, anumite cuvinte sau expresii sunt folosite pentru a modifica echilibrul de putere, între ţări şi/sau organizaţii internaţionale, în cadrul retoricii generate de competiţia strategică manifestată prin criză.

Concluzii

Am relevat, în paragraful introductiv al acestui articol, că teoria discursului este o ramură a științelor comunicării, care studiază producerea, transmiterea și recepționarea comunicatelor. Prin interconectarea cu efectele sociale (*v. Focault – discursul ca fapt social* – (Adams 2017)) și contextul momentului (*particularitățile discursului, în raport cu un anumit context, poate crea semnificații diferite ale aceluiași comunicat*), am fost în măsură să evidențiem, că discursul are, de asemenea, capacitatea de a produce cunoaștere, sens și reacții. Pe de altă parte, analiza teoriilor discursului a introdus și alte valențe în conținutul acestuia, cum ar fi perceperea discursului, ca o manieră de exprimare a puterii. În acest fel, discursurile reprezintă o dimensiune modernă de proiectare a puterii (van Dijk 1993).

Am arătat, că teoria discursului poate contribui la construirea unei imagini adecvate, cu privire la cum diferiți actori și vectori de mesaj își construiesc și comunică mesajele despre securitate. Acest lucru este relevant, deoarece discursurile au adesea impact asupra procesului decizional și de elaborare a politicilor. Mai mult decât atât, ca o particularizare, teoria discursului poate ajuta la identificarea relațiilor de putere în domeniul securității. Acest lucru este esențial, în studiile de securitate, pentru delimitarea și definirea amenințărilor.

Analiza anterioară a avut ca obiectiv, depășirea contextului general de delimitare a teoriilor discursului, iar prin acțiunea de nișare a demersului exploratoriu, am căutat repere ale folosirii instrumentelor sale în domeniul relațiilor internaționale și studiilor de securitate. Am concluzionat că, teoria discursului a devenit din ce în ce mai populară în relațiile internaționale și studiile de securitate, deoarece oferă o modalitate de a analiza și înțelege rețeaua complexă de interacțiuni, dintre state și organizații internaționale. Teoria discursului subliniază rolul limbajului și al comunicării în modelarea relațiilor internaționale și oferă o lentilă utilă, pentru înțelegerea modului în care este exercitată puterea. Concentrându-ne asupra modurilor în care, exponenții de mesaj ai statelor/instituțiilor internaționale folosesc limbajul, pentru a construi sens, teoria discursului ne poate ajuta, să distingem aspecte necunoscute apriori și să înțelegem mai bine dinamica politicii internaționale și evoluția mediului de securitate.

În studiile de securitate, teoria discursului poate fi extrem de utilă, deoarece permite o mai bună înțelegere a modului în care, diferiți actori definesc și construiesc securitatea. Privind modul în care, actorii discută, dezbat, negociază și comunică problemele de securitate este posibil să

obţinem o mai bună înţelegere, a ceea ce se consideră a fi important şi ce fel de soluţii pot fi promovate şi susţinute. Acest lucru poate fi util atât pentru prezicerea, cât şi pentru modelarea direcţiei viitoare a posturii în domeniul securităţii.

Un rol important în aceste dezvoltări le au crizele de securitate şi am arătat, că acestea pot genera progrese evolutive şi schimbări de paradigmă, în postura de securitate a statelor sau organizaţiilor internaţionale. În cele din urmă, semnificaţia unei crize internaţionale, pentru studiile de securitate, este dublă: dezvăluie informaţii esenţiale despre relaţiile internaţionale, oferind în acelaşi timp, o perspectivă valoroasă asupra potenţialelor puncte forte şi slabe ale sistemelor de securitate existente. Cercetând, prin intermediul teoriei discursului, aceste evenimente îndeaproape şi înţelegând implicaţiile pe care le au asupra afacerilor globale şi de securitate, se pot crea evaluări privind comportamentele unor state sau organizaţii internaţionale.

Bibliografie:

1. Adams, Rachel. 2017. *Michel Foucault: Discourse*. Accessed 01 17, 2023. https://criticallegalthinking.com/2017/11/17/michel-foucault-discourse/

2. Alkhafaji, Hayder S. 2022. "The Impact of George W. Bush's Political Discourses on the Invasion of Iraq: A Corpus-Based Rhetoric Discourse Analysis". *International Journal of Social Science And Human Research*, Vol. 5; 04 05: 1209-1222.

3. Atkinson, Rob, Gerhard Held, and Stephen Jeffares. 2010. "Theories of Discourse and Narrative: what do they mean for governance and policy?" https://uwe-repository.worktribe.com/OutputFile/974342

4. Beciu, Camelia. 2009. *Comunicare şi discurs mediatic*. Bucureşti: Editura Comunicare.ro

5. Bhattarai, Prakash. 2020. "Discourse, Power and Truth: Foucauldian Perspective". *International Journal of English Literature and Social Sciences*, 5(5) Sep-Oct 2020.

6. Briciu, Arabela. 2017. *Comunicarea şi discursul politic: între teorie şi practică*. Cluj-Napoca: Presa Universitară Clujeană.

7. De Rycker, Antoon, and Zuraidah Mohd Don. 2013. *Discourse and Crisis: Critical perspectives*. Amsterdam: John Benjamins Publishing.

8. de Saussure, Ferdinand. 1967. *Cours de linguistique générale*. Edited by Grande bibliotheque Payot. Accessed 01 17, 2023. https://monoskop.org/images/f/f1/Saussure_Ferdinand_de_Cours_de_linguistique_generale_Edition_critique_1997.pdf

9. Denton, Robert E. (Jr.), and Gary C. Woodward. 1990. Political *Communication in America*. Praeger.

10. Fairclough, Isabela, and Norman Fairclough. 2012. *Political Discourse Analysis: A Method for Advanced Students*. Londra: Routledge.

11. Fairclough, Norman. 2001. "The Discourse Analysis of New Labour: Critical Discourse Analysis". In *Discourse as Data*, by Margaret Wetherell, Simeon J. Yates and Stephanie J. A. Taylor. Londra: SAGE Publications.

12. Fârte, Ghoerghe-Ilie. 2005. *Comunicarea politică: aspecte generale și ipostaze actuale*. https://www.fssp.uaic.ro/seminar_logica/gifarte/papers/argumentum2004-2005cap5.pdf

13. *Foucault's Concept of Discourse Explained*. 2017. Accessed 01 18, 2023. https://culturalstudiesnow.blogspot.com/2017/03/foucault-concept-of-discourse-explained.html.

14. Gee, James Paul. 2005. "Gee Seminar". *Aalborg Workshop*. Aalborg.

15. Jarvis, Sharon E., and Soo-Hye Han. 2009. "Political Communication". Eadie, William E. (coord.), *21st Century Communication – A Reference Handbook*, vol. II, Los Angeles, Sage Publications, 749–757.

16. Jørgensen, Marianne W, and Louise J Phillips. 2002. *Discourse Analysis as Theory and Method*. Londra: SAGE Publications.

17. Karlberg, Michael. 2005. "The power of discourse and the discourse of power: Pursuing peace through discourse intervention". *International Journal of Peace Studies*, 10(1 Spring/Summer), 1-23.

18. Laberge, Yves. 2007. "e la propagande à la communication politique: perspectives sur l'opinion publique en France, au Québec, aux États-Unis". *Canadian Journal of Political Science/Revue canadienne de science politique* Vol. 40, No. 2, 06: 519-526.

19. Larsen, Henrik. 1997. *Foreign Policy and Discourse Analysis: France, Britain and Europe*. Londra: Routledge.

20. *Libraries*. 2023. Accessed 01 17, 2023. https://open.lib.umn.edu/businesscommunication/chapter/1-2-what-is-communication/

21. Lungu, Dan. 2002. *Institutul European*. Accessed 01 17, 2023. https://www.euroinst.ro/titlu.php?id=89

22. Mihalache, Dan. n.d. "Note de curs – Marketing politic".

23. Nordquist, Richard. 2021. *Overview of Systemic Functional Linguistics*. Accessed 01 24, 2023. https://www.thoughtco.com/systemic-functional-linguistics-1692022

24. Nye, Joseph, and Robert Keohane. 1987. "Power and Interdependence Revisited". *International Organization* 41 (4): 725-753.

25. Paz, Alejandro I. 2013. *SAGE Publications*. https://www.utsc.utoronto.ca/people/aipaz/wp-content/uploads/sites/11/2014/04/Paz-Alejandro-2013-Theory-Soc-Cul-Ang-dsc-thy.pdf

26. Peters, John Durham. 2008. *Wiley online library*. https://onlinelibrary.wiley.com/doi/epdf/10.1002/9781405186407.wbiecc075

27. Pitsoe, Victor, and Letseka Moeketsi. 2012. *Foucault's Discourse and Power: Implications for Instructionist Classroom Management*. 12 08. Accessed 01 18, 2023. https://file.scirp.org/pdf/OJPP_2013020811451567.pdf

28. Rogers, James. 2007. "From 'Civilian Power' to 'Global Power': Explicating the European Union's 'Grand Strategy' Through the Articulation of Discourse Theory". *Journal of Common Market Studies*, Volume 47. Number 4., 831–862.

29. Sălăvăstru, Constantin. 1999. *Discursul puterii*. laşi: Editura Institutul European.

30. Sengul, Kurt. 2019. "Critical discourse analysis in political communication research: a case study of rightwing populist discourse in Australia". *Communication Research and Practice*, 11 25.

31. Snowdon, Claire, and Leena Eklund Karlsson. 2021. "A Critical Discourse Analysis of Representations of Travellers in Public Policies in Ireland". *Societies* 11(1):14, 02.

32. Spruyt, Hendrik. 1994. *The Sovereign State and its Competitors*. Princeton University Press.

33. *Study Smarter*. 2023. Accessed 01 17, 2023. https://www.studysmarter.us/explanations/english/key-concepts-in-language-and-linguistics/michel-foucault-discourse-theory/

34. Tănase, Tasenţe. 2014. *Comunicarea politică prin Social Media şi reacţiile publicului online*. Constanţa: Editura Universitară.

35. van Dijk, Teun A. 1993. "Principles of critical discourse analysis". *Discourse & Society* Vol. 4, No. 2, *SPECIAL ISSUE: Critical Discourse Analysis* (1993), 249-283.

36. Warwick, University of. 2023. *What is Critical Realism?* Accessed 01 18, 2023. https://warwick.ac.uk/fac/soc/ces/research/current/socialtheory/maps/criticalrealism/

37. Wodak, Ruth. 2001. "What is CDA about. A summary of its history, important concepts and its developments". In *Methods of Critical Discourse Analysis*.

38. Wodak, Ruth. 2020. "Foreword: Critical Discourse Analysis/Studies – Challenges, Concepts and Perspectives". In *Critical Discourse Analysis, Critical Discourse Studies and Beyond*, by Theresa Catalano and Linda R. Waugh, xxi-xxv. Cham: Springer.

***Notă**: Această lucrare a beneficiat de sprijin financiar prin proiectul „Dezvoltarea competenţelor de cercetare avansată şi aplicată în logica STEAM+ Health", POCU/993/6/13/153310, proiect cofinanţat din Fondul Social European prin Programul Operaţional Capital Uman 2014-2020".*

Aceasta este a doua ediție a volumului publicat de Academia Națională de Informații „Mihai Viteazul” (ANIMV), care cuprinde lucrările prezentate în cadrul Conferinței Științifice Intelligence și Cultura de Securitate 2023 (ICS2023). Inițiativa ICS2023 continuă să ofere studenților o platformă pentru dialog academic și pentru a împărtăși realizările lor științifice.

Ediția actuală își extinde participarea la un spectru mai larg de contributori, incluzând atât doctoranzi, cât și studenți din programele de master, cu un interes crescut pentru domenii precum intelligence, securitate națională, istorie și relații internaționale.

Organizarea conferinței a fost posibilă datorită eforturilor continue ale doctoranzilor și ale conducătorilor de doctorat din cadrul Școlii Doctorale Informații și Securitate Națională a ANIMV.

Anticipăm cu entuziasm noi discuții și schimburi de idei în viitoarea ediție a conferinței.

EDITURA ANIMV

ISSN 2972-1350
ISSN-L 2971-8139