Anul XII nr. 2/2020

INFOSFERA

Revistă de studii de securitate şi informaţii pentru apărare

Publicaţie indexată în bazele de date internaţionale EBSCO şi CEEOL

Revistă cu prestigiu ştiinţific recunoscut de Consiliul Naţional de Atestare a Titlurilor, Diplomelor şi Certificatelor Universitare (CNATDCU)

Direcţia Generală de Informaţii a Apărării

CUPRINS

COMUNICARE STRATEGICĂ ÎN OPERAȚIILE MILITARE MODERNE

Daniel COCOLICI*

Abstract

In contemporary conflicts, the issue of legitimacy is analyzed at the level of the international community. States are now civilized if they can justify the legitimacy of their actions before the international bodies. A series of strategic changes in the contemporary era have made the process of communication as a form of influence of both the international scene and the operational environment, to become particularly important for the current military operations. Strategic Communication is a key parameter of the comprehensive Allied approach to international crisis management adopted in April 2009 at the NATO Summit. By adopting the StratCom concept, NATO seeks to strengthen the impact of the process at the strategic level. Communication, as a means of exerting influence on all actors present in the operational environment, becomes essential in the development of modern military actions carried out mainly in hybrid key. The capacity of the North Atlantic Alliance and the member states to achieve multidisciplinary integration for better communication in support of the promotion of Allied and national objectives has increased substantially with the strengthening of the conceptual framework. At the operational level, however, Allied forces continue to face challenges since usually the StratCom doesn't properly address the concerns of the military commanders at the operational and tactical level.

Keywords*: Strategic Communications, NATO, military operations.*

Context

Dacă în trecut confruntarea militară avea, de cele mai multe ori, un caracter structurat, cu o delimitare clară a participanților şi motivației acestora, conflictele contemporane sunt caracterizate de un grad de fluiditate mult mai mare. Multe dintre acestea, pornite ca urmare a confruntărilor dintre forțe interne, atrag sub o formă sau alta implicarea unor actori externi, generând astfel internaționalizarea conflictului. Este cazul multora dintre conflictele aflate în derulare în prezent, exemplele cele mai cunoscute incluzând atât conflicte active (Siria, Libia, Yemen, Ucraina), dar şi conflicte înghețate (Moldova, Georgia), fiind cunoscută prezența în aceste teatre atât a unor actori statali externi, precum F. Rusă, Iran, Arabia Saudită sau SUA, cât şi a unor actori nestatali (organizații extremiste transnaționale, grupări paramilitare, companii private de securitate sau grupări de crimă organizată). Distincții precum cea dintre forțele combatante, dintre civili şi militari sau identificarea prezenței pe teren a organizațiilor internaționale sunt din ce în ce mai greu de realizat[1].

Internaționalizarea conflictelor contemporane aduce astfel în discuție ideea de legitimitate. În conflictele trecutului, legitimitatea era analizată din perspectiva dreptului de a apela la instrumentele de forță în cadrul statului, în limita cadrului legal oferit de legislația națională. În conflictele contemporane, problema legitimității este analizată la nivelul comunității

Expert în Ministerul Apărării Naționale.

internaționale. Spre exemplu, inițierea şi participarea la o operație în sprijinul păcii sunt astfel justificate în fața opiniei publice interne a statelor care le desfăşoară, a populației locale din zonele de conflict, precum şi în fața actorilor internaționali care au un rol-cheie în mandatarea acestor misiuni (Consiliul de Securitate al ONU)[2]. Statele sunt acum considerate civilizate dacă pot justifica legitimitatea acțiunilor în fața comunității internaționale.

Comunicarea în mediul operațional

O serie de schimbări strategice înregistrate în epoca contemporană au făcut ca procesul de comunicare, ca formă de influențare atât a scenei internaționale, cât şi a mediului operațional, să devină deosebit de important pentru operațiile militare contemporane.

În cadrul oricărui proces de comunicare, sunt avute în vedere elemente precum: publicul-țintă, mesajul, emițătorul, canalul şi momentul comunicării. Dintre acestea, o importanță deosebită o are publicul-țintă, toate celelalte elemente fiind derivate din analiza detaliată a audienței. Pentru o comunicare eficientă, pe care audiența trebuie să o perceapă ca fiind de încredere, este nevoie ca valorile publicului țintă să fie bine înțelese.

Comunicarea, la orice nivel, este un proces ciclic, constituit din variabile inter-conectate şi care vizează o conversie inversă între emitent şi beneficiar (interlocutor/organizație). **Mesajul** creat implică atât **intenția emițătorului**, cât şi **caracteristicile audienței**/receptorilor şi se bazează pe variabilele deja menționate – timp şi obiective. Cunoaşterea variabilei de tip audiență/interlocutor este cu atât mai importantă cu cât aceasta poate asigura succesul procesului de comunicare, în acest sens fiind ales şi **canalul de comunicare**. Prin adecvarea modului de transmitere a mesajului, audiența poate fi atrasă de mesaj, iar **timpul** acordat înțelegerii expunerii va fi direct proporțional cu **atenția** acordată emițătorului. Alegerea canalului de comunicare poate influența în mod pozitiv sau negativ recepția mesajului, putând concentra datele transmise şi facilita feedback-ul receptorilor. Pe de altă parte, în contextul alegerii canalului de comunicare trebuie luate în calcul şi aspecte precum proximitatea dintre emițător şi receptor şi **confidențialitatea** mesajului, în cazul comunicării de tip strategic. În procesul comunicării, apare un alt factor important, şi anume tipul de psihologie aplicată de emițător, adoptată în funcție de audiență. Astfel, *psihologia directă* presupune, ca primă etapă, expunerea ideii principale, iar în a doua etapă prezentarea explicațiilor. În ceea ce priveşte *psihologia indirectă,* aceasta urmează traseul invers: oferirea explicațiilor înainte de prezentarea ideii principale. În prezent, forma cel mai des adoptată de organizațiile vestice este aceea a psihologiei directe.

Progresul înregistrat în tehnologia informației a avut, de asemenea, un efect major asupra comunicării în lumea contemporană prin diversificarea resurselor avute la dispoziție (Internet, calculatoare, telefoane mobile) şi prin amplificarea accesului la aceste resurse la nivelul societății. Această stare de fapt a dus la sporirea exponențială a volumului de informații vehiculat, îngreunând sarcina de influențare publică. Viteza cu care un comunicator reuşeşte să îşi transmită propria viziune devine un factor crucial pentru a se asigura că publicului i se oferă propria interpretare a evenimentelor. La aceasta se adaugă concurența cu alți comunicatori, aflați şi ei în competiția de a-şi prezenta primii punctul de vedere. Un alt aspect de luat în considerare este cel al menținerii coerenței între mesajele transmise, ca un factor cheie în ancorarea unui mesaj în conştiința publicului. Pe măsură ce un mesaj este retransmis, acesta fie este alterat, fie intră în competiție cu o multitudine de alte mesaje similare, ceea ce face dificilă percepția corectă la nivelul receptorilor.

Implicarea forțelor de coaliție în operații diverse complică suplimentar procesul de comunicare. Multitudinea de parteneri prezenți face dificilă asigurarea coerenței comunicării.

Adversarii cu care forțele de coaliție se confruntă, cum sunt cele ale NATO implicate în derularea unor operații extrateritoriale, dețin o serie de avantaje nete față de acestea.

În primul rând, forțele insurgente sunt mai bine familiarizate cu terenul şi sunt mult mai bine conectate la nivelul populației, cultural şi lingvistic, din zona în care se desfăşoară o operațiune dată. În egală măsură, organizarea ca rețea delocalizată a forțelor insurgente le permite abordarea unei strategii de comunicare mult mai eficiente, atât din punctul de vedere al vitezei de reacție, cât şi din cel al coerenței comunicării. Prin contrast, structurile de coaliție sunt marcate de modul de organizare ierarhic şi rigid, precum şi de condiționare birocratică. Acțiunea unei forțe de coaliție plasează în centru, de regulă, ideea acțiunii militare, cinetice, comunicarea fiind percepută ca element de sprijin al acesteia. Prin contrast, realitatea multor teatre de operații indică faptul că, de cele mai multe ori, competiția se duce mai degrabă pentru câştigarea încrederii societății decât pentru controlul teritorial.

Perspectiva aliată asupra comunicării strategice

Comunicarea strategică reprezintă un parametru fundamental al abordării comprehensive aliate pentru managementul crizelor la nivel internațional. Alianța a reacționat astfel la noile provocări înregistrate la nivelul mediului operațional, provocări care au demonstrat incapacitatea forțelor de coaliție de a câştiga sprijinul populației locale pe toate palierele urmărite şi în cadrul temporal scontat, un exemplu consistent în acest sens fiind modul de abordare al crizei din Afganistan. Termenul de comunicare strategică/StratCom, care nu deține nici până în prezent o conotație exhaustivă, a fost creat ca un element de reîntărire a capacității NATO de a interacționa cu publicul-țintă.

Prin adoptarea conceptului StratCom, NATO încearcă să consolideze impactul procesului la nivel strategic[3]. Comunicarea, ca mijloc de exercitare a influenței asupra tuturor actorilor prezenți în mediul operațional, devine esențială în derularea acțiunilor militare moderne, cu precădere a celor desfăşurate în cheie hibridă. Revoluția tehnologiei informaționale şi caracterul multinațional al operațiilor militare au impus un grad înalt de coerență şi celeritate în procesul comunicării, destul de dificil de atins, reprezentând astfel o provocare pentru fluența comunicării. Mai mult, StratCom urmează direcția influențării mediului de securitate şi în plan umanitar, prin îmbunătățirea cooperării între instituțiile civile şi cele militare.

Pentru succesul StratCom, este necesar să fie luați în considerare o serie de parametri, precum: facilitarea vitezei şi coerenței comunicării care ajută la intensificarea colaborărilor în interiorul ierarhiei militare (cooperare pe verticală) şi între

diferite departamente (cooperare pe orizontală); soluționarea rapidă a aspectelor birocratice, în contextul în care diseminarea informațiilor şi comunicarea inter-departamentală sunt autorizate doar de factorii decidenți, ceea ce poate încetini, de cele mai multe ori, transmiterea informației.

StratCom se regăseşte în toate informațiile şi capabilitățile de comunicare. Mesajele comunicării strategice pot ajunge la variate tipuri de audiență, nu toate fiind neapărat destinatarii intenționați: de la populația propriului stat până la populația altor state, inclusiv aliați şi adversari. De aceea, comunicarea este, uneori, greu de controlat, aceasta putând avea şi beneficiari colaterali. StratCom a fost dezvoltat, parțial, ca răspuns la noul mediu de securitate în care sunt exploatate şi diseminate volume mari de informații, care pot fi accesate de oricine, instant.

În procesul de evoluție al oricărei armate, un element important este constituit de metamorfoza activităților de comunicare. La nivelul NATO, Diplomația Publică (tipul de activitate de relații publice practicat la nivelul Secretarului General şi al structurilor subordonate acestuia) şi Informarea publică (formulă adoptată la nivelul NATO ca organizație multinațională, practicată la nivelul comenzilor militare) sunt supuse procesului general de transformare a Alianței[4]. Principalele obiective ale transformării în domeniul informării şi relațiilor publice constau în: dezvoltarea sprijinului public pentru NATO, sporirea capacității de desfăşurare şi susținere în teatrele de operații a structurilor de informare şi relații publice (capabilități expediționare), creşterea efectelor acțiunilor de informare şi relații publice prin coordonarea cu operațiile informaționale şi îmbunătățirea sistemului doctrinar şi de pregătire pe linie de specialitate[5].

În lumina unei terminologii vaste a conceptului, NATO a adoptat această denumire din două motive: 1. Conotația nu este atât de puternică precum cea a termenului „influențare", deoarece cel din urmă poate fi interpretat ca „dezinformare", acțiune integrată în categorii separate de operații[6]. În acest sens, multe state membre ar fi respins termenul. 2. Termenul era deja folosit în SUA, motiv pentru care preluarea acestuia în terminologia doctrinară a NATO a fost considerată, mai degrabă, pragmatică. Cu toate acestea, NATO sugerează statelor membre să adopte propria terminologie în doctrinele conceptuale proprii.

Conceptualizarea comunicării strategice în domeniul securității a apărut, inițial, în *Department of Defense Dictionary of Military and Associated Terms*, în anul 2001, fiind utilizat şi în alte domenii; acest tip de comunicare este practicat de instituții, organizații, companii care urmăresc obținerea unui impact major, pe termen mediu şi lung, asupra categoriilor de public pe care le relaționează, în scopul promovării propriilor valori[7].

Un document oficial semnificativ, în care se subliniază rolul comunicării strategice în promovarea la nivel internațional a valorilor naționale, este Strategia națională a SUA pentru diplomație publică şi comunicare strategică, adoptată în iunie 2007, care stabileşte următoarea taxonomie a obiectivelor StratCom: promovarea demnității umane; consolidarea alianțelor împotriva terorismului; dezamorsarea conflictelor regionale; prevenirea amenințărilor cauzate de armele de distrugere în masă; încurajarea dezvoltării economiei globale; extinderea zonelor dezvoltate; cooperarea cu alte centre de putere globale şi transformarea instituțiilor de securitate națională ale SUA pentru a putea face față provocărilor şi oportunităților secolului al XXI-lea[8].

În 2009, Comitetul Întrunit al Şefilor de State Majore ale forțelor armate ale SUA[9] propunea următoarea definiție a StratCom: „comunicarea strategică reprezintă alinierea unor multiple direcții de operare, precum implementarea doctrinelor, afacerile publice, manevra forțelor, operațiile informaționale etc., care generează efecte pentru a susține obiectivele naționale. Astfel, comunicarea strategică reprezintă partajarea comunicării în sprijinul obiectivelor naționale/strategice. Acest proces implică atât receptarea, cât şi transmiterea, aplicându-se nu numai informațiilor, dar şi comunicării fizice – acțiunilor care transmit înțelesuri"[10].

În august 2010, NATO adoptă Concepția militară pentru Comunicarea Strategică, care oferă o definiție a acesteia din perspectiva Alianței: „Comunicarea strategică a NATO reprezintă un proces specific de conducere cu scopul principal de dezvoltare a abilității Alianței de a-şi prezenta în mod coerent strategiile narative, temele şi mesajele audiențelor externe şi interne. Comunicarea strategică NATO oferă orientare strategică politică şi militară conform unei strategii de informare aprobate de Consiliul Nord-Atlantic”[11]. După cum se observă, în viziunea NATO, comunicarea strategică priveşte nu doar publicul-țintă intern, dar, mai ales, pe cel extern.

Cu toate acestea, în noua politică militară a NATO privind comunicarea strategică extinsă[12], apărută în anul 2017, aceasta este definită sub forma integrării capacităților de comunicare cu activitățile militare, în vederea înțelegerii şi modelării mediului informațional, pentru îndeplinirea obiectivelor şi scopurilor NATO[13].

Potrivit doctrinei NATO, StratCom este definit ca ansamblu de capabilități şi proces coordonat de activități de comunicare aflate în sprijinul politicilor, operațiilor şi activităților NATO, în vederea promovării propriilor obiective strategice[14]. Dintre aceste capabilități fac parte: Diplomația Publică, Politici Publice, Relații Publice în sistemul de apărare, structura de Informații-Operații şi Operații Psihologice. Comunicarea strategică se referă la toate mesajele şi acțiunile care sunt percepute şi interpretate de un public-țintă, fără a se limita la mass-media.

Totodată, StratCom este un proces de coordonare inter-ministerială a comunicării şi de consolidare a potențialului efect strategic. Obiectivul principal al unei astfel de comunicări este de a promova anumite atitudini şi comportamente pentru publicul-țintă, într-un context favorabil intereselor actorilor generatori ai comunicării, mai exact conturarea mediului operațional[15].

StratCom la nivel național

În România, în domeniul apărării naționale, comunicarea reprezintă o funcție esențială de conducere şi de comandă. Eficacitatea şi eficiența eforturilor de comunicare ale MApN se află într-o strânsă corelație şi depind de modalitatea în care liderii militari şi civili se implică activ în exercitarea procesului de comunicare şi în stabilirea unor obiective şi strategii comune[16].

Legea 203/2015 privind planificarea apărării aliniază procesul de planificare a apărării din Armata României cu procesele similare din cadrul NATO şi UE. Potrivit Cartei Albe a Apărării, din 2017, printre misiunile generale ale armatei României, precum apărarea independenței, suveranității şi integrității teritoriale şi participarea la apărarea aliaților şi partenerilor săi, în cadrul NATO şi UE, este enumerată şi promovarea stabilității regionale şi globale, inclusiv prin folosirea diplomației apărării[17]. În acest sens, parteneriatele strategice constituie fundamentul construirii unor relații solide şi cuprinzătoare între state în domeniul securității şi apărării[18]. Aceste parteneriate strategice nu pot fi inițiate fără existența unei comunicări strategice eficiente şi coordonate la nivel aliat.

Structurile MApN reprezentate în Grupul de sprijin decizional (GSDS)[19] şi în Centrul de analiză strategică, monitorizare, identificare riscuri şi evaluare (CASMIRE)[20] sunt responsabile de comunicarea la nivel strategic, prin determinarea vulnerabilităților de imagine ale MApN şi ale liderilor acestuia, identificarea surselor şi retoricii ostile, evitarea transformării acestora în riscuri imagologice şi limitarea efectelor unor eventuale crize de imagine.

Comunicarea strategică este un proces inițiat pentru a combate consecințele nefaste şi periculoase ale acțiunii de dezinformare. StratCom se adresează nu numai audienței interne/naționale, având ca obiectiv primordial rezistența la acțiunile informaționale agresive şi false, dar şi audienței externe față de care inițiatorii comunicării de tip strategic au ca obiectiv promovarea intereselor naționale. De aceea, din anul 2010, acest tip de comunicare a devenit un element de necesitate în contextul dezvoltării exponențiale a *social media*, al intensificării campaniilor on-line de dezinformare, al diversificării mijloacelor, surselor şi țintelor campaniilor de influențare manipulativă,

al acutizării deficitului de încredere în sistemul democrațiilor liberal-occidentale ș.a.[21].

Cu toate acestea, se poate observa că procesul StratCom național are drept preocupare principală confruntarea informațională specifică acțiunilor adverse generate de o abordare de tip război hibrid. Sprijinul în domeniul comunicării, necesar comandanților detașamentelor naționale dislocate în teatrele de operații, se exercită indirect prin participarea la elaborarea politicilor de comunicare strategică dezvoltate la nivel aliat.

Concluzii

Abilitățile Alianței Nord-Atlantice şi ale statelor membre de a realiza o integrare multidisciplinară pentru o mai bună comunicare în sprijinul promovării obiectivelor aliate şi naționale au sporit substanțial odată cu întărirea cadrului conceptual. La nivel strategic, acțiunile NATO beneficiază de sprijin pe toate planurile din perspectiva justificării legitimității implicării în gestionarea crizelor internaționale. Statele aliate contribuie decisiv la susținerea efortului aliat, mesajul transmis de autoritatea centrală fiind clar şi coerent, în deplină consonanță cu viziunea transmisă de capitalele statelor membre.

La nivel operațional totuşi, forțele aliate continuă să fie privite cu circumspecție de populația locală. De exemplu, în cazul Irakului, populația exercită presiuni asupra guvernului de la Bagdad pentru a negocia retragerea forțelor NATO de pe teritoriul național, în ciuda beneficiilor pe care această prezență a adus-o pentru securitatea statului şi pentru profesionalizarea forțelor armate naționale. Similar, în Afganistan, Mişcarea Talibană reuşeşte să se relaționeze mai bine cu populația locală reuşind să limiteze drastic controlul teritorial atât al forțelor aliate, cât şi al forțelor naționale afgane. Astfel de situații indică faptul că, în pofida coerenței sporite a procesului de comunicare strategică, la nivel operațional există în continuare o dimensiune a interacțiunii militare pe care o forță internațională nu reuşeşte să o descifreze în totalitate, aceea a interacțiunii socio-culturale. În Afganistan, Mişcarea Talibană recurge la acțiuni violente ca modalitate de a comunica. Țintele sunt alese cu grijă pentru a produce un impact mediatic maxim, mesajul transmis cu ajutorul acestor acțiuni violente fie este acela de a menține presiunea asupra coaliției internaționale, fie de a insufla în rândul populației frică şi neîncredere în capacitatea comunității internaționale de a reforma şi moderniza statul afgan. În sine, modernizarea statului afgan este interpretată drept o modalitate a Occidentului de a impune valori străine culturii afgane. În exemplul Irakului, influența clerului şiit, în general, precum şi cea a milițiilor pro-iraniene asupra guvernului central este dificil de contracarat numai prin mesaje de tip StratCom.

Nu în ultimul rând, obligația forțelor de coaliție de a respecta, în interacțiunea cu forțele inamice, norme stricte de comportament bazate pe concepte etice şi morale derivate din cultura occidentală, comportament bine studiat şi înțeles de insurgența locală, face ca libertatea de acțiune a acestora să fie limitată drastic. Această vulnerabilitate permite forțelor insurgente să folosească populația locală ca mediu de mascare şi de suport, forțele de coaliție având adesea dificultăți în identificarea opozanților, ceea ce le predispune la erori cuantificate într-un număr ridicat de victime colaterale. O modalitate de a compensa această vulnerabilitate a fost aceea de a sprijini constituirea unor forțe de securitate națională care să preia misiunea principală de contracarare a mişcărilor insurgente, cu forțele de coaliție preluând un rol secundar, de sprijin al acestui efort. Această abordare a generat rezultate mixte în teatrele în care a fost aplicată. O explicație posibilă ar fi aceea că palierul preponderent pe care această cooperare a fost construită a fost cel militar. Probabil, este nevoie ca şi la nivel operațional abordarea comprehensivă să se manifeste prin constituirea de parteneriate politice, în care implicarea militară să constituie numai una dintre fațetele cooperării.

Bibliografie:

1. *Carta Albă a Apărării*, Bucureşti, 2017.
2. DEAC, Ioan; BULUC, Ruxandra; „Dezvoltarea conceptuală a comunicării strategice în domeniul securității”, *Impact Strategic*, nr.1-2, Universitatea Națională de Apărare, Centrul de Studii Strategice de Apărare şi Securitate, Bucureşti, 2019.

3. MUNTEANU, Nicoleta Annemarie, *Strategia de comunicare a Ministerului Apărării Naționale. Investiție esențială pentru o armată a României competitivă în cadrul NATO și UE*, Departamentul de Științe Politice, Relații Internaționale și Studii de Securitate din cadrul Universității „Lucian Blaga", Sibiu, 2013.
4. REDING, Anaïs; WEED, Kristin; GHEZ, Jeremy J.; „Defining Strategic Communications" în *NATO's Strategic Communications concept and its relevance for France*, Joint Forces Centre for Concept Development, Doctrine and Experimentation (Centre interarmées de concepts, de doctrines et d'expérimentations, Etat-major des Armées), Franța, 2010.
5. Van BEIJNUM, Mariska; Van Den BERG, Willem; Van VEEN, Erwin, *Between a rock and a hard place. Monitoring aid implementation in situations of conflict*, CRU Report, Netherlands Institute of International Relations 'Clingendael', September 2018, disponibil online la adresa: https://www.clingendael.org/sites/default/files/2018-09/between-a-rock-and-a-hard-place.pdf, accesată la data de 24.04.2020.
6. Von BILLERBECK, Sarah B. K.; GIPPERT Birte Julia, *Legitimacy in Conflict: Concepts, Practices, Challenges*, în Journal of Intervention and Statebuilding, Volume 11, 2017, disponibil online la adresa:https://www.tandfonline.com/doi/full/10.1080/17502977.2017.1357701, accesată la data de 24.10.2020.

[1] Mariska Van Beijnum,Willem Van Den Berg, Erwin Van Veen, *Between a rock and a hard place. Monitoring aid implementation in situations of conflict*, CRU Report, Netherlands Institute of International Relations 'Clingendael', September 2018, disponibil online la adresa: https://www.clingendael.org/sites/default/files/2018-09/between-a-rock-and-a-hard-place.pdf, accesată la data de 24.04.2020.

[2] Sarah B. K.Von Billerbeck, Birte Julia Gippert, „Legitimacy in Conflict: Concepts, Practices, Challenges", în *Journal of Intervention and Statebuilding*, Volume 11, 2017, disponibil online la adresa:https://www.tandfonline.com/doi/full/10.1080/17502977.2017.1357701, accesată la data de 24.04.2020.

[3] Anaïs Reding, Kristin Weed, Jeremy J. Ghez; „The emergence of NATO's concept of Strategic Communications", în *op.cit.*, p. 4.

[4] Nicoleta Annemarie Munteanu, *op.cit*., p. 168.

[5] *Idem*.

[6] În Franța, acțiunile de dezinformare (*deception*) sunt folosite în așa-numitele „operații de dezinformare", în timp ce în SUA sunt cunoscute sub denumirea de „operații psihologice".

[7] Ioan Deac, Ruxandra Buluc, „Dezvoltarea conceptuală a comunicării strategice în domeniul securității", *Impact Strategic*, nr.1-2, Universitatea Națională de Apărare, Centrul de Studii Strategice de Apărare și Securitate, București, 2019, p. 41.

[8] *Idem*, *op.cit*., p. 42 apud U.S. National Strategy for Public Diplomacy and Strategic Communication, 2007, URL: http://www.au.af.mil/au/awc/awcgate/state/natstrat_strat_comm.pdf.

[9] *Idem*, *op.cit*., p. 42, apud Department of Defense, Joint Staff, URL: https://dod.defense.gov/.

[10] *Idem*, *op.cit*., p. 42 apud Joint Staff's October 2009 Joint Integrating Concept for Strategic Communication, URL: https://apps.dtic.mil/dtic/tr/fulltext/u2/a510204.pdf, p. ii.

[11] *Idem*, *op.cit*., p. 43 apud Military Concept for NATO Strategic Communications, 12 august 2010, p. 2, URL: https://publicintelligence.net/nato-stratcom-concept/.

[12] *Ibidem,* apud NATO Military Policy on Strategic Communications, 14 august 2017.

[13] *Ibidem.*

[14] Anaïs Reding, Kristin Weed, Jeremy Ghez, „Defining Strategic Communications" , în *NATO's Strategic Communications concept and its relevance for France*, Joint Forces Centre for Concept Development, Doctrine and Experimentation (Centre interarmées de concepts, de doctrines et d'expérimentations, Etat-major des Armées), Franța, 2010, p. 7.

[15] *Idem*, „Description of NATO's Strategic Communications concept", *op.cit*., p. 9.

[16] Nicoleta Annemarie, Munteanu, „Strategia de comunicare a Ministerului Apărării Naționale. Investiție esențială pentru o armată a României competitivă în cadrul NATO și UE", Departamentul de Științe Politice, Relații Internaționale și Studii de Securitate din cadrul Universității „Lucian Blaga", Sibiu, 2013, p. 167.

[17] *Carta Albă a Apărării*, București, 2017, p. 32.

[18] *Idem*, p. 24.

[19] Din care fac parte: secretarul de stat pentru politica de apărare, planificare şi relaţii internaţionale, şeful Statului Major al Apărării, şeful Direcţiei generale de informaţii a apărării, şeful Direcţiei operaţii, şeful Direcţiei informare şi relaţii publice, purtătorul de cuvânt al MApN, şeful Trustului de presă al armatei;

[20] Din care fac parte specialişti aparţinând următoarelor domenii funcţionale: informare şi relaţii publice militare – Direcţia Informare şi Relaţii Publice; diplomaţia publică/diplomaţia apărării – Departamentul pentru politica de apărare, planificare şi relaţii internaţionale, Direcţia informare şi relaţii publice şi Direcţia informaţii militare; dinamica mediului de securitate – Centrul de Studii Strategice de Securitate şi Apărare/Universitatea Naţională de Apărare „Carol I"; operaţii media – Direcţia informare şi relaţii publice; operaţii informaţionale (InfoOps) – Direcţia operaţii; operaţii psihologice (PSYOPS) – Direcţia operaţii; informaţii şi contrainformaţii militare – Direcţia generală de informaţii a apărării.

[21] Ioan Deac, Ruxandra Buluc, *op.cit*., p. 46.

NOUA GEOPOLITICĂ GLOBALĂ ÎN ERA POST-COVID-19

Iulian CHIFU*

Abstract

Crises are usually sudden changes on the evolution that prompt a threat to basic values, emergency and the sense of urgency in order to limit the effects and costs and to bring back the society at stake closer to the original situation[1]*. Crises are accelerating the processes and trends that happened before that moment. The coronavirus crisis is in the same situation and the changes in the society, politics and international relations are as present. It is too early to name the outcome of the crisis in medical terms and time frame. But we already see interdependent and superposed crises as a result of the pandemic. It is, however important to try to foresee the possible way of managing the international world order after the crises, the trends and alternative futures as well as the new shape of the post-pandemic geopolitics and World Order.*

Keywords*: pandemic, coronavirus, crisis, alternative futures, the end of oil, the New Geopolitics.*

Alternativele unei crize: adaptări, schimbări profunde, turbulență majoră

Pandemia de COVID-19, cauzată de noul coronavirus sau SARS-CoV-2, cum a fost el cuantificat de Organizația Mondială a Sănătății, a venit brusc în viețile noastre şi amenință să producă schimbări profunde. A încerca, în prezent, să anticipăm aceste schimbări e prematur; totuşi, avem şansa să conturăm un număr de opțiuni şi scenarii în acest domeniu, care ne sunt oferite de către medici epidemiologi, toate depinzând de caracteristicile necunoscute încă ale virusului în cauză.

Cea mai importantă problemă a momentului este „când" şi „cum" se va sfârşi criza generată de coronavirus. Care sunt scenariile şi cum ieşim din coşmar[2]. Folosind o evaluare medicală din *The Atlantic*[3], am raționalizat analiza termenului şi impactului în materie de decizie în criză şi a scenariilor prospective. Opțiunile merg de la o sincopă a omenirii de trei luni, până absorbim şi ne obişnuim cu criza şi cu virusul, până la o amenințare eternă şi constantă la adresa omenirii, cu un virus ce se adaptează şi se schimbă în fiecare sezon şi care trebuie combătut cu vaccin potrivit de fiecare dată. Ceea ce ne obligă să ne obişnuim să trăim cu virusul, de aici înainte, cam cum trăim cu virusul gripal. Doar cu un alt impact asupra sănătății şi vieții noastre.

Ca la orice pandemie, scenariile sunt patru. Primul, considerat azi improbabil, pe baza virulenței şi vitezei de răspândire globală - dar mai ales a descoperirii unui număr mare de tulpini la nivel global, în fiecare țară, care subliniază răspândirea masivă şi absența unui „pacient zero" - ar fi ca virusul să dispară aşa cum a venit[4]. Omenirea reuşeşte să-l identifice, să-l conțină, să izoleze bolnavii de restul populației, să păstreze distanța între sursele de virus care au supraviețuit pe diferite obiecte, astfel încât, aşa cum s-a întâmplat la SARS şi, în mare măsură, la MERS, epidemia/pandemia de acum să se stingă natural.

Iulian CHIFU este preşedintele CPCEW, conf. univ. dr. la UNAp şi profesor asociat la SNSPA, specializat în Analiză de Conflict şi Decizie în criză. A fost consilier prezidențial pentru Afaceri Strategice, Securitate şi Politică externă (2011-2014).

Scenariul al doilea, considerat varianta periculoasă, este acela de a încerca blocajul prin imunizarea rapidă a unei părți mari a populației active şi puțin expuse complicațiilor, care să devină barieră în calea pandemiei, din lipsă de subiecți activi imediați care să fie neimunizați. O variantă care ar dura 3-6 luni, cu efecte de mortalitate statistice relevante. Abordarea a fost încercată, în primele momente, în SUA lui Donald Trump şi Marea Britanie a lui Boris Johnson, fiind abandonată la presiunea publică şi în urma analizei experților responsabili. A rămas utilizată în Suedia, acolo unde se şi vorbeşte despre eşecul protejării populației vulnerabile – cu preponderență cea peste 65 de ani, cu comorbidități[5].

Scenariul al treilea e cel mai bun şi sigur, chiar dacă este de durată. Mai exact, acceptând că sunt vaccinuri deja la nivelul începutului testării, este necesară respectarea pas cu pas a procedurilor care duc la un vaccin sigur, eficient şi fără efecte secundare, în 12-18 luni. Atunci vaccinarea e cea care opreşte virusul, creând imunitatea pe această cale, acceptând că este un virus tradițional care reacționează normal şi are rata de mutații acceptabilă. Contraexemplele sunt două. Mai întâi, nu există încă un vaccin împotriva virusului SARS original, chiar dacă îl ştim de 17 ani. Unii spun că au studiat, s-au apropiat, dar li s-au întrerupt finanțările. Cum epidemia s-a închis în şase luni, natural, nu a mai fost nevoie de un vaccin. Pe de altă parte, nici HIV nu are azi un vaccin, deşi e cunoscut şi studiat de mai bine de 40 de ani, fiind descoperit formal în 1981. Timpul şi dezvoltările măresc numărul de tulpini şi rezistența la un vaccin făcut pe baza variantei de plecare a virusului.

În plus, avem şi un scenariu patru, cu un impact pe durată mai lungă – dacă virusul suferă mutații succesive rapide şi, până ajungem să validăm un vaccin, apare o tulpină deja rezistentă la vaccinul nostru. Gripa sezonieră este modelul cel mai cunoscut în acest sens: te poți vaccina cu un număr de tulpini, cele mai probabile într-un sezon, şi totuşi să faci gripă pe o tulpină necunoscută şi pentru care nu eşti pregătit. Vorbim despre durata imunizării – imunitatea poate dura un an, după ce ai cunoscut virusul şi dezvoltat anticorpi, poate dura mai mulți ani sau toată viața, pentru o anumită tulpină de virus. În cazul SARS, s-a demonstrat că imunizarea[6] celor (puțini) infectați şi vindecați a avut loc pe o perioadă de mai mulți ani. Dar caracteristicile SARS-CoV-2 nu sunt încă cunoscute, ne confruntăm cu el de cel mult cinci luni şi în mod serios de doar vreo trei în lume.

Scenariul patru este şi cazul cel mai grav şi mai dur pentru omenire, când nu avem un vaccin eficient, nu există variantă de imunizare mulțumitoare, virusul şi boala revin, îşi schimbă forma, iar boala care se tot transformă infectează anual, ciclic, oamenii din zonele cele mai expuse şi vulnerabile ale societății. Acest scenariu al pandemiei fără sfârşit, fără formă fixă şi fără vaccin sau tratament eficient, ne obligă la modificări structurale majore, profunde şi de durată ale modului nostru de viață.

Crize suprapuse şi interdependente

Criza generată de pandemia de coronavirus are deja efecte majore. La nivelul tuturor statelor, indiferent de greutatea strategică, capacitatea sistemului medical, dezvoltarea cercetării şi a îngrijirii, modul de finanțare al sănătății, impactul a fost major. Dacă e să luăm marii actori globali sau cu potențial recunoscut şi greutate strategică specifică relevantă[7] - care dau trendul, creionează modelele, pot identifica tratamente şi pot găsi vaccinul - tot avem reacții diverse şi eficiență diferită. Populiştii pierd pe toate meridianele în fața expertizei, profesioniştilor şi a politicienilor serioşi, care au acționat în criză şi au făcut minuni. Dar ceea ce ne învață criza este că nu contează câtă putere ai – stat autoritar sau democratic[8] – nu contează nici măcar cât de mare e statul – minimal în variantă neoliberală sau social, de stânga, vezi autoritară – ci contează cât de eficient este, cât de bun şi puternic în a satisface necesitățile populației, cât de eficace în a convinge publicul să respecte cât mai strict reguli restrictive[9].

Criza de coronavirus are un număr de caracteristici speciale. Principala problemă este că testează conducerea şi sistemul unui stat, nu numai sistemul de sănătate, în multiple feluri. Mai ales că pandemia de coronavirus vine cu multiple crize suprapuse, fiind, de fapt, o criză a

multiplelor crize, pe lângă criza medicală actuală:

- prima este despre războiul informațional, propagandă şi valorificarea crizei în bătăliile de prestigiu şi de imagine;
- a doua e criza de încredere a societății – în sine, conducători, decidenți, fiind totodată despre panică, credibilitate şi decizia în criză;
- a treia este despre *leadership* şi despre calitatea clasei politice;
- a patra este despre calitatea democrației liberale în epoca *social media* şi despre populism şi curente extreme versus profesionalism, meritocrație şi revenirea la conducerea de către elitele calificate într-o societate;
- nu lipseşte criza şi reaşezarea sistemului medical/sanitar, cu toate tarele şi dezechilibrele sale actuale, cu examenul dificil pe care-l pică astăzi;
- în fine, dar nu în cele din urmă, despre criza economică globală generată de coronavirus, incluzând aici şi lanțurile de furnizori şi criza comercială, şi cea a decuplării previzibile de China.

Iar criza economică pare cea mai importantă şi mai actuală, pentru că determină reaşezarea lumii de mâine. Cu amenințări existențiale, dar şi cu oportunități de preluare a controlului guvernanței globale şi a gestionării globalizării de mâine[10].

Lucrurile nu au început acum şi lumea deja avea de gestionat aceste crize care veneau, cu sau fără explozia de coronavirus din Wuhan şi răspândirea sa în lumea întreagă. Doar că pandemia le-a accelerat evoluția şi le-a adus în prim-plan. Dezvoltările tehnologice mişcaseră lucrurile pe un spectru distinct demult, dar nimeni nu s-a ocupat de efectele de trend ale acestor schimbări asupra omului, societății, politicului şi relațiilor internaționale. Am făcut-o recent într-un număr de analize[11].

Amplificarea şi accelerarea tendințelor în urma crizei, dar şi gradul de complexitate şi suprapunerea a numeroase crize interdependente creează probleme majore de gestiune, care împing nevoia ca principalele reforme să vizeze chiar statul, perfecționarea democrației, a sistemului politic, şi reformarea *leadership*-ului.

Dacă, inițial, aceste transformări date de dezvoltările tehnologice erau lente, sub nivelul percepției comune, explozia crizei determinate de pandemie a venit să accelereze şi să expună toate aceste crize:

- cea a sistemului democratic – care se cere perfecționat, pentru a promova valori, profesionalism şi meritocrație, nu numai imagine, charismă şi figuri cu popularitate, tendință care a dus la căderea spre populism şi extremisme care atrag vizibilitate şi fac audiență în *social media*;
- cea a *leadership*-ului – nevoia de a atrage din nou elita profesională şi naturală în prim-planul conducerii unui stat, în funcții executive, potrivit pregătirii şi experienței fiecăruia;
- cea a politicului – alunecarea în partitocrație a unei clase politice incapabile şi nedoritoare să mai atragă elite profesionale, închizându-se în loialități şi grupuri înguste, de unde implozia partidelor fără politică de cadre, cu oameni fără profesie, fără carieră şi fără experiență în activități altele decât cele politice, lipsite de capacitatea de împrospătare a conducerii cu oameni de valoare[12].

Opțiuni de gestionare globală

Dacă avem astăzi o identificare, în mare măsură, a crizelor cu care se va confrunta omenirea după pandemia de coronavirus, e relevant să vedem şi cine va putea gestiona aceste crize. Unele sunt profund naționale, de sistem, acolo unde statele sunt primii responsabili şi, deci, primii reformatori. Dar altele sunt mai extinse, la nivelul întregului sistem al democrației liberale sau chiar la nivelul lumii. Soluțiile de gestionare a globalizării şi crizelor de această anvergură sunt câteva şi nu trebuie să reinventăm roata, mai ales că nici lumea nu s-a schimbat aşa de dramatic peste noapte, şi nici mintea noastră, nici cea a planificatorilor de

lângă decidenți nu a evoluat şi nu va evolua atât de fantastic în 2-3-5 luni:

- **Lumea G0** – a nimănui, *No One's World*[13] – lumea anarhică fără *leadership*, după retragerea SUA lui Trump dacă nu într-o splendidă izolare, într-o postură mult mai preocupată de sine (adică politica de tip „*America first, Great again!*"[14]) decât de asigurarea *leadership*-ului global.
- Revenirea la **lumea cu *leadership*-ul SUA** – chiar dacă mai nuanțată, mai schimbată şi cu sarcinile mai limitate, cu sau fără actualul preşedinte, cu sau fără actualul *leadership* american în funcție.
- **Lumea G2** - lumea globalizată după liniile majore ale marilor actori, SUA şi China. Dacă se înțeleg. Dacă rivalitățile şi perspectiva confruntării se estompează. Dacă colaborează. Dacă China acceptă regulile şi le şi respectă. Dacă nu cad în război. Sau măcar nu rup comerțul global, polarizându-l în două, cum au pornit să o facă.
- **Tripodul SUA-China-UE** – care e mai degrabă o ambiție europeană, o asumare vizionară a lui Emmanuel Macron privind rolul global al UE între cei doi mari, echilibrându-i, dar fără resursele şi acordul motoarelor economice europene. Din nou, greu de pus probabilități relevante aici, în dreptul acestui scenariu, pe termen scurt şi mediu.
- **P5 – grupul statelor membre permanente ale Consiliului de Securitate**, ca lideri ai dezbaterii privind viitorul lumii şi gestiunea globalizării. Din nou, cu diferențe foarte mari de calitate, portanță, maniere, valori fundamentale şi greutate specifică între actori, şi cu divergențe majore între ei. Dar cu o inițiativă deja pe masă – Macron-Trump-Putin. Vedem şi liderii acțiunii şi direcțiile ei, dacă această inițiativă se va decanta în fapt. Dar există mulți absenți din ecuație, Germania şi UE în primul rând.
- **G7 (G8)** – este un cadru natural de discuție al marilor teme ale lumii, varianta G8 fiind dorința şi aspirația Rusiei, care nu se regăseşte în categoria celor mai industrializate state ale lumii, dar îşi doreşte rolul global.
- **G20 – un cadru mai larg** şi care estompează ambițiile şi tendințele politicii de mare putere pe care le relevă toate celelalte proiecte de până aici. A fost propus, ca şi cadru, într-o scrisoare publicată sub formă de editorial în *The Washington Times,* de către ministrul de externe al Turciei, Mevlüt Çavuşoğlu. Este şi aceasta o pledoarie *pro domo*, dar are substanța şi relevanța sa[15].

Analiza noastră în privința **probabilității şi fezabilității opțiunilor** a dus la conturarea **câtorva scenarii**. Deşi nu putem afirma că vreunul dintre aceste scenarii este cel mai probabil, observăm că ele aduc în prim-plan, mai degrabă, continuarea/accelerarea globalizării ca proces obiectiv.

- „***Worst case scenario"*** rămâne politica de putere - adică tendința de folosire a forței, a războiului, a influenței agresive pentru a atinge obiective politice, respectiv politica de „mare putere"- tentația Marelui Târg între marile puteri, înclinate spre împărțirea între ele a dominației lumii, ceea ce înseamnă, totodată, multipolarism, sfere de influență şi interese privilegiate, pe care să le domine fiecare şi pe seama cărora să facă tranzacțiile la masa verde între ele. Din păcate, un scenariu cu mult prea mare probabilitate de a se realiza.
- ***„Best case scenario"*** rămâne aşezarea lumii bazată pe multilateralism, pe supremația dreptului, lumea bazată pe reguli, consensualism în decizii (practic valorile UE extrapolate la nivel global). Pe cât de bun, pe atât de mică probabilitatea unei evoluții pe această direcție, în lumea de astăzi şi cu liderii politici pe care i-am moştenit, pentru a trece lumea actuală prin criza de coronavirus.
- **Scenariul cel mai probabil** oscilează între două variante, şi acestea pe scara bine-rău: *Varianta 1* - **Lumea G0, anarhică, fără *leadership*, cu rivalități între mari puteri** şi, de ce nu, războaie posibile, cu ambiții

şi lideri neadecvaţi în funcţiile de prim-plan şi cu abandonarea/marginalizarea profesionalismului şi a meritocraţiei, dar cu alunecări în partitocraţie şi închiderea sistemelor democratice; *Varianta 2* – **Leadership transatlantic** – dacă se reuşeşte depăşirea gestiunii proaste a crizei, populismului, tentaţia modificării naraţiunilor nefavorabile, cu o eventuală schimbare de *leadership* sau de opţiuni la actorii principali şi cu realizarea nevoii coordonării eforturilor globale pe linia statelor civilizate, occidentale, democratice.

Avem elementele unei falii transatlantice, dată de comportamentul neconvenţional al preşedintelui Trump şi înclinaţia sa strict financiară, dar şi de diferenţa de percepţie a nevoii de *leadership* american versus absenţa resurselor şi a voinţei de a-l oferi lumii. Dacă aceste divergenţe sunt depăşite şi falia se închide, SUA nu vor mai fi liderul pe care-l cunoaştem - va avea nevoie de sprijinul general şi de legitimitatea dată de contribuţia tuturor statelor democratice din comunitatea transatlantică. E simplu, e un drum cunoscut, bătătorit şi funcţional, are valori proprii comune la bază, e lesne de reconstruit, poate cu alţi lideri, şi pot fi catalizate voinţa şi susţinerea populaţiei pentru că nevoia este evidentă[16].

Din păcate, catalizatorul posibil al unui asemenea scenariu, deopotrivă probabil şi apropiat de un *best case,* include recursul la varianta duşmanului comun[17] pentru a cataliza toată susţinerea, respectiv desemnarea Chinei ca duşman comun! Documentele americane[18] şi multe din documentele europene şi ale statelor membre ale UE[19] încep să conţină elementele convergente pe o asemenea direcţie.

Rivalitatea SUA-R.P. Chineză. Opţiuni şi scenarii

Două procese au definit comportamentul imediat al statelor în faţa ameninţării pandemiei, ale cărei caracteristici au fost lovirea aproximativ la fel şi în acelaşi interval de timp a tuturor statelor şi construirea concomitentă a aceloraşi nevoi de produse de protecţie, medicamente, tratamente sau dispozitive medicale, precum ventilatoarele. Deci crearea unei competiţii acerbe pentru aceste produse, confecţionate majoritar în China, şi nu o succesiune care ar fi putut duce la într-ajutorarea obişnuită, care a avut totuşi loc.

Am avut, deci, mai întâi, o prăbuşire imediată a solidarităţii şi apariţia exceselor de individualism, excepţionalism şi egoism de criză, şi nu e vorba numai despre pornirile naţionale, ci şi de cele locale, formule exagerate manifestate prin păstrarea locurilor din spitale şi a materialelor necesare tratamentelor pentru „ai mei” – cei din localitate, rude, cunoscuţi – care trebuie trataţi preferenţial şi înaintea altora - venetici, străini, alţii. Comportament profund uman, de a-i salva primii pe ai mei - reprobabil, neetic, imoral, condamnabil, dar profund uman[20].

Al doilea proces este acela al rivalităţilor globale şi tendinţa de a folosi criza în scopuri de imagine, politice şi geopolitice (pun deoparte îmbogăţiţii de război şi trambulinele electorale de viitor), prin propagandă şi război informaţional, pentru a arăta că un sistem e mai bun ca altul, că autoritarismul şi naţionalismele rezolvă problema în timp ce liberal-democraţia şi societatea deschisă o amplifică, că liderul de mână forte e soluţia şi nu decizia luată democratic, prin dezbatere sau consens[21]. Cu exportul de *soft power* prin diplomaţia măştilor, respectiv pseudo-ajutoare inutile sau cu defecte, dar cu ambiţii şi doleanţe de a atinge obiective politice – vezi ruperea Italiei de Europa, ajutorul Chinei şi Rusiei pe când „UE nu face nimic” şi multe altele, identificate deja de către UE[22].

O sumă de evenimente au făcut ca varianta Administraţiei Trump pentru această epocă post-criză să se traducă în definirea Chinei ca duşman[23]. Prima direcţie de atac a fost cea a responsabilităţii Chinei în apariţia coronavirusului, fie că provenea dintr-o piaţă de animale vii din Wuhan, fie dintr-o manipulare neatentă în laborator[24]. Dacă bătălia finală în privinţa responsabilităţii s-a mutat de la faza probei dincolo de orice dubiu din justiţie la credibilitatea afirmaţiilor care pot fi susţinute doar de elemente sau capete de probă, devine clar că relaţia China-SUA este la nivelul cel mai de jos al istoriei. Războiul comercial a traversat doar primul episod, cel mai simplu de reglat,

cel al deficitelor comerciale, iar angajamentele chineze de a importa mărfuri americane de 200 mld. dolari şi alimente şi mărfuri de la fermieri de 50 mld. dolari sunt greu de îndeplinit anul acesta. Celelalte teme rămân pe masă, ca şi sancţiunile diferite, inclusiv cele pentru achiziţia de lansatoare de rachete S400 din Rusia, la rândul ei ţară supusă sancţiunilor, sau eventualul petrol adus din Iran, alt stat sancţionat de către Trezoreria Americană.

Criza de coronavirus a fost un moment nefast care s-a adăugat acestei situaţii, prin întârzierea comunicării informaţiilor veridice, influenţarea Organizaţiei Mondiale a Sănătăţii, în prima fază, pentru a nu declara pandemia şi a prelua naraţiunea chineză - că ar fi vorba despre un virus despre care nu s-a probat că se transmite de la om la om - şi cazurile din Wuhan pot fi conţinute şi controlate. Manipularea ajutoarelor sanitare şi a preţurilor, blocarea în depozite şi creşterea artificială a costurilor de achiziţie, când livrările externe au fost blocate din ianuarie, pe dimensiuni unde China e stat cvasimonopolist, interzicerea cercetării epidemiei în orice punct – ajutorul american în ianuarie, investigaţia internaţională de azi – toate adaugă argumente grele privind vinovăţia şi responsabilitatea Chinei, care sunt greu de respins de către publicul global, mai ales de către statele occidentale, unele confruntate şi cu constrângeri sau condiţionări pentru furniturile materialelor de protecţie în timpul crizei[25].

Nu e de mirare, deci, că există chiar un raport intern chinez care avertizează asupra unei pierderi sistematice şi rapide a imaginii şi brandului Chinei şi chiar susţine că, în prezent, China se confruntă cu un oprobriu public generalizat la nivel mondial de dimensiunea celui de după represiunea din Piaţa Tiananmen, în 1989. Un val de sentimente anti-chineze, declanşat cu precădere în SUA, este deja înregistrat, iar pregătirile din China includ şi cel mai prost scenariu, o confruntare militară. Raportul este atribuit *China Institutes of Contemporary International Relations (CICIR)*, un think tank afiliat Ministerului Securităţii de Stat, potrivit Reuters[26].

Opţiunile şi scenariile relaţiilor sino-americane sunt câteva, în acest caz:

1. Aplanarea divergenţelor, eventual contra unor recunoaşteri parţiale a responsabilităţilor şi conlucrării americano-chineze în varianta G2, pentru relansarea economică. Acest scenariu ar avea probabilitate mai relevantă în cazul înfrângerii la prezidenţiale a lui Donald Trump şi a unei temperări a comportamentalului agresiv al Chinei în plan imagologic şi mediatic.
2. Confruntarea directă, soldată cu repatrierea sau relocarea unei mari părţi a capacităţilor de producţie şi a investiţiilor din China şi impunerea unei izolări comerciale globale a Chinei, eventual a unei strategii de tip „cu noi sau împotriva noastră" de către preşedintele Trump, eventual revenit în funcţie. Varianta poate duce la ciocniri şi asprimi ale manifestărilor militare şi politice la nivel global. O altă variantă aici ar fi polarizarea lumii pe cei doi vectori majori – China şi SUA – în materie de model de guvernare, parteneriat comercial şi acces la tehnologie. Diferenţa este de nuanţă şi depinde de amploarea scindării lumii şi capacitatea Chinei de a menţine o sferă de influenţă comercială măcar în Asia de Sud-Est.
3. Rivalitate surdă, dar suficient de puternică pentru a genera decuplări şi efecte majore asupra economiei globale, cu accentuarea recesiunii şi repatrierea industriilor, dar şi limitată, prin evitarea decuplării totale a Chinei sau a Lumii Chineze. Comerţul se va face în continuare, dar cu evitarea Chinei şi a lumii din jurul său, tot mai redusă ca dimensiune, iar relaţiile economice se vor restrânge drastic pe baza unui protecţionism securitar. Lipsa gestiunii negociate va duce la o anarhie în sistem, o lume G0 a nimănui.

Geopolitica lumii de mâine. Disiparea puterii, rivalitate sino-americană, multilateralism consensual

Tendinţele cele mai probabile astăzi sunt cele mai confuze şi neclare, cele mai puţin radicale, în căutarea unei formule de reaşezare finală.

La nivel global următoarele tendințe sunt manifeste:

- **Disiparea puterii la nivel global**. Criza economică şi recesiunea globală vor schimba fundamental raportul de forțe, SUA scăzând într-un trend mai degrabă modest – pe seama repatrierii resurselor şi a acordurilor parțiale comerciale cu China, în timp ce China îşi va diminua relevanța dramatic. În schimb se vor detaşa un număr de actori de relevanță medie, puteri regionale a căror prezență la negocieri este tot mai relevantă. Grupul G7 îşi va spori relevanța, ca şi statele din G20, cu un acces tot mai mare la decizia globală, în diferite formate.
- **Rivalitatea sino-americană** (dar şi cea dintre lumea liberal democrată şi modelul autoritar) va rămâne o constantă în lumea de mâine. SUA va ține întotdeauna China responsabilă de criza de coronavirus, de manipularea monedei *renminbi*, de furtul de proprietate intelectuală şi transferul forțat al acesteia în cazul unor investiții pe tărâm chinez, iar agenda de confruntări şi ciocniri va rămâne bogată, pe termen mediu.
- **Multilateralism consensual**. Nevoia unei soluții şi a administrării globalizării este un factor care va impune o bază minimală de înțelegere, în primul rând mediată, între SUA şi China, dar mai ales un cadru de discuție global. Pe termen mediu, abordarea va viza, credem noi, implicarea în formulă multilaterală şi pe baze consensuale (de tip UE) a tuturor actorilor relevanți. În caz contrar, vom avea soluții parțiale, în care acceptabilitatea soluției va fi dată tocmai de prezența în decizie a cât mai multor actori relevanți.

Important este că, pe termen scurt şi mediu, lumea şi actorii relevanți – între care statele UE/UE şi F.Rusă, Japonia, India, Australia, Marea Britanie – vor trebui să accepte conturarea rivalității sino-americane, viabilitatea unei părți mari a argumentelor vizând responsabilitățile Chinei, dar şi nevoia ca Beijingul să fie prezent în orice formă de gestiune a afacerilor globale. Manevrarea între cei doi rivali şi dorința de a evita un nou război rece şi scindarea lumii pe linii de forță va reclama formule novatoare de evitare a alinierii stricte cu unul sau altul dintre actori şi nevoia de a alege între ei, dar şi păstrarea identității (şi a distanței, a limitelor dependențelor) față de cei doi şi a libertății comerțului, atât timp cât nu vizează elemente de securitate şi transfer tehnologic ilegal.

În aceste momente se croiesc deja bazele unei „noi geopolitici globale", care va constitui rațiunea pe baza căreia, în final, vom avea o adaptare şi reaşezare a lumii potrivit noilor reguli create de criza de coronavirus. Discuțiile despre sfârşitul petrolului şi reorganizarea energetică a bazelor economiei de mâine au pornit deja, iar Acordul de la Paris[27] şi Angajamentele UE împotriva încălzirii globale[28], ca şi prăbuşirea prețului petrolului ca urmare a războiului OPEC-Rusia[29] sunt probe directe ale acestei schimbări.

Bibliografie:

1. BORRELL Josep, *The post-Coronavirus World is already here*, European Council of Foreign Relations, 30 April, 2020.
2. BREMMER Ian, *Every Nation for Itself. Winners and Loosers in a G0 World*, Portfolio Penguin, 2012, ISBN 978-1-59184-468-6, 229 p.
3. BROWN Ashley, „Pompeo says 'enormous evidence' for unproven theory that coronavirus came from lab", *ABC News*, 3 May 2020.
4. BRUCKNER Pascal, *Melancolia democrației. Cum să trăieşti fără duşmani?,* Editura Antet, 1994, ISBN 973-9241-09-3, 164 p.
5. CHIFU Iulian, „Amenințări neconvenționale şi noile tipuri de amenințări hibride în secolul 21", *Revista Gândirea Militară Românească,* nr. 1/2020, pp. 10-29, ISSN Print: 1454-0460.
6. CHIFU Iulian, „Bătălia lumilor în vreme de coronavirus: meciul China – SUA autoritarism – democrație pierdut de populism", *Adevărul*, 30 aprilie.
7. CHIFU Iulian, „Bătălia publică, subterană şi ocultă pentru conducerea lumii de după COVID-19", *Adevărul*, 9 aprilie.
8. CHIFU Iulian, „Criza de coronavirus, Globalizare, politică de Mare Putere şi Concertul Mondial în 5", *Adevărul*, 6 aprilie 2020.

9. CHIFU Iulian, *Decizia în criză*, Editura Rao, 2019, ISBN 978-606-006-349-0, 335 p.
10. CHIFU Iulian, „Infodemie trilaterală în pandemia de coronavirus: China, Rusia, Iran împotriva Lumii Libere", *Adevărul*, 28 aprilie 2020, la https://adevarul.ro/international/in-lume/infodemie-trilaterala-pandemia-coronavirus-china-rusia-iran-lumii-libere-1_5ea70e405163ec42712fa672/index.html.
11. CHIFU Iulian, „Istoria unei provocări. Conceptul unei Strategii de Securitate Națională a României viitorului", în *Adevărul*, 11 mai 2019.
12. CHIFU Iulian, „Josep Borrell, omul care l-a trimis pe Emmanuel Macron în bancă la gândirea strategică europeană", în *Adevărul*, 14 mai 2020.
13. CHIFU Iulian, „O periodizare a amenințărilor globale. Cea de-a cincea generație de amenințări", *Infosfera*, nr. 4/2019, pp. 3-17, ISSN 2065-3395.
14. CHIFU Iulian, „Sfârşitul coşmarului: scenariile prospective pentru criza de coronavirus – pauza de 3 luni, îngheț un an sau amenințare eternă a omenirii", *Adevărul*, 3 aprilie 2020.
15. CHIFU Iulian, „Testul suprem pentru Regimul Dodon: pregătirea de criza Covid-19 şi credibilitatea conducerii de la Chişinău", în *Adevărul*, 1 aprilie 2020.
16. CHIFU Iulian, „Trump şi campania *China e duşmanul*. Cazul coronavirusului – probe şi presupuneri", în *Adevărul,* 6 mai 2020.
17. COLOMBEL Mary; Katy DARTFORD, „Sweden's coronavirus strategy: Is the older generation paying the price?", *Euronews*, 27 April 2020.
18. KENNEDY, Will, „Why the OPEC-Russia Blowup Sparked All-Out Oil Price War", *Washington Post,* 14 April 2020.
19. KUPCHAN Charles A, *No One's World. The West, The Rising Rest and the Coming Global Turn*, Oxford University Press, 2013, ISBN 978-0-19-973939-4, 258 p.
20. ROGER James, *Audit of Geopolitical Capability. An assessment of 20 major powers*, Henry Jackson Society, January 2019, ISBN: 978-1-909035-50-8, 64 p., la https://henryjacksonsociety.org/wp-content/uploads/2019/01/HJS-2019-Audit-of-Geopolitical-Capability-Report-web.pdf.
21. TRUMP, Donald J., *Great Again. How to Fix Our Crippled America*, Threashold Editions, New York, 2015, ISBN 978-1-5011-3800-3, 193 p.
22. TSENGN, Chien-Te, SBRANA Elena, IWATA-YOSHIKAWA Naoko, NEWMAN Patrick C.,GARRON Tania, ATMAR Robert L., PETERS Clarence J., COUCH Robert B., POEHLMANN Stefan, Editor, *Immunization with SARS Coronavirus Vaccines Leads to Pulmonary Immunopathology on Challenge with the SARS Virus,* PLoS One, 2012 Apr 20.
23. YONG Ed, „How Will the Pandemic End", în *The Atlantic,* 25 March 2020.
24. *National Security Strategy of the United States of America*, Decembrie 2017, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.
25. BBC, „Coronavirus: Chinese state media take aim at US 'lab theory' ", 5 May 2020.5.17, https://www.bbc.com/news/world-asia-52540737.
26. COVID-19 disinformation – EEAS Special Report, 2-22 April 2020, at https://euvsdisinfo.eu/eeas-special-report-update-2-22-april/.
27. Department of Health and Social Care, UK Government, *Press release, COVID-19 detection dogs trial launches,* 16 May 2020, at https://www.gov.uk/government/news/covid-19-detection-dogs-trial-launches.
28. European Commission, COM 2013(16.04.2013), An EU Strategy on adaptation to climate change, at https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0216:FIN:EN:PDF.
29. Office of the DNI, *Intelligence Community Statement on Origins of COVID-19*, 30 April 2020, athttps://twitter.com/ODNIgov/status/1255868108356681728.
30. Paris climate conference (COP21), *The Paris Agreement*, 13 December 2015 at https://unfccc.int/resource/docs/2015/cop21/eng/10a01.pdf.
31. Reuters, „Exclusive: Internal Chinese report warns Beijing faces Tiananmen-like global backlash over virus", 4 May 2020, at https://www.reuters.com/article/us-health-coronavirus-china-sentiment-ex/exclusive-internal-chinese-report-warns-beijing-faces-tiananmen-like-global-backlash-over-virus-idUSKBN22G19C.

[1] Iulian Chifu, *Decizia în criză*, Editura Rao, 2019, ISBN 978-606-006-349-0, 335 p

[2] Iulian Chifu, „Sfârșitul coșmarului: scenariile prospective pentru criza de coronavirus – pauza de 3 luni, îngheț un an sau amenințare eternă a omenirii", *Adevărul*, 3 aprilie 2020, la https://adevarul.ro/international/in-lume/sfarsitul-cosmarului-scenariile-prospective-criza-coronavirus-pauza-3-luni-inghet-an-amenintare-eterna-omenirii-1_5e86bdb55163ec427167438b/index.html

[3] Ed Yong, „How Will the Pandemic End", în *The Atlantic*, 25 March 2020, at https://www.theatlantic.com/health/archive/2020/03/how-will-coronavirus-end/608719/

[4] Department of Health and Social Care, UK Government, *Press release, COVID-19 detection dogs trial launches,* 16 May 2020, at https://www.gov.uk/government/news/covid-19-detection-dogs-trial-launches

[5] Mary Colombel & Katy Dartford, *Sweden's coronavirus strategy: Is the older generation paying the price?*, Euronews, 27 April 2020, at https://www.euronews.com/2020/04/27/sweden-s-coronavirus-strategy-is-the-older-generation-paying-the-price

[6] Chien-Te Tseng, Elena Sbrana, Naoko Iwata-Yoshikawa, Patrick C. Newman, Tania Garron, Robert L. Atmar, Clarence J. Peters, and Robert B. Couch, Stefan Poehlmann, Editor, *Immunization with SARS Coronavirus Vaccines Leads to Pulmonary Immunopathology on Challenge with the SARS Virus,* PLoS One, 2012 Apr 20, at https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3335060/

[7] James Roger, *Audit of Geopolitical Capability. An assessment of 20 major powers*, Henry Jackson Society, January 2019, ISBN: 978-1-909035-50-8, 64 p., la https://henryjacksonsociety.org/wp-content/uploads/2019/01/HJS-2019-Audit-of-Geopolitical-Capability-Report-web.pdf.

[8] Iulian Chifu, „Bătălia lumilor în vreme de coronavirus: meciul China – SUA autoritarism – democrație pierdut de populism", *Adevărul*, 30 aprilie, la https://adevarul.ro/international/in-lume/batalia-lumilor-vreme-decoronavirus-meciul-china-sua-autoritarism-democratie-pierdut-populism-1_5eaa66865163ec427146286e/index.html

[9] Iulian Chifu, „Josep Borrell, omul care l-a trimis pe Emmanuel Macron în bancă la gândirea strategică europeană", în *Adevărul*, 14 mai 2020, la https://adevarul.ro/international/europa/josep-borrell-omul-l-a-trimispe-emmanuel-macron-banca-gandirea-strategica-europeana-1_5ebce72b5163ec4271c38d7f/index.html

[10]Iulian Chifu, „Testul suprem pentru Regimul Dodon: pregătirea de criza Covid-19 şi credibilitatea conducerii de la Chișinău", *Adevărul*, 1 aprilie 2020, la https://adevarul.ro/moldova/politica/testul-suprem-regimul-dodon-pregatirea-criza-covid-19-credibilitatea-conducerii-chisinau-1_5e8363bc5163ec42715755a1/index.html; deschide.md, 31 martie, 2020, la https://deschide.md/ro/stiri/editorial/63637/IChifu--Testul-suprem-pentru-Regimul-Dodon-preg%C4%83tirea-de-criza-Covid-19-%C8%99i-credibilitatea-conducerii-de-la-Chi%C8%99in%C4%83u.htm

[11]Iulian Chifu, „Amenințări neconvenționale şi noile tipuri de amenințări hibride în secolul 21, *Revista „ Gândirea Militară Românească",* nr. 1/2020, pp. 10-29, ISSN Print: 1454-0460; Iulian Chifu, „O periodizare a amenințărilor globale. Cea de-a cincea generație de amenințări"*, Infosfera*, nr.4/2019, pp. 3-17, ISSN 2065-3395.

[12]Iulian Chifu, „Istoria unei provocări. Conceptul unei Strategii de Securitate Națională a României viitorului", în *Adevărul*, 11 mai 2019, la https://adevarul.ro/news/eveniment/istoria-provocari-conceptulunei-strategii-securitate-nationala-romaniei-viitorului-1_5eb80cbd5163ec4271a42547/index.html.

[13]Charles A. Kupchan, *No One's World. The West, The Rising Rest and the Coming Global Turn*, Oxford University Press, 2013, ISBN 978-0-19-973939-4, 258 p.; Bremmer, Ian, *Every Nation for Itself. Winners and Loosers in a G0 World*, Portfolio Penguin, 2012, ISBN 978-1-59184-468-6, 229 p.

[14]Donald J.Trump, *Great Again. How to Fix Our Crippled America*, Threashold Editions, New York, 2015, ISBN 978-1-5011-3800-3, 193 p.

[15] Iulian Chifu, „Criza de coronavirus, Globalizare, politică de Mare Putere şi Concertul Mondial în 5", *Adevărul*, 6 aprilie 2020, la https://adevarul.ro/international/in-lume/criza-coronavirus-globalizare-politica-mare-putere-concertul-mondial-5-1_5e89eab25163ec427175a514/index.html; Iulian Chifu, *Bătălia publică, subterană şi ocultă pentru conducerea lumii de după COVID-19,* Adevărul, 9 aprilie, la https://www.caleaeuropeana.ro/iulian-chifu-batalia-publica-subterana-si-oculta-pentru-conducerea-lumii-de-dupa-covid-19/

[16] *Idem.*

[17] Pascal Bruckner, *Melancolia democrației. Cum să trăiești fără dușmani?*, Editura Antet, 1994, 164 p.

[18] ******National Security Strategy of the United States of America*, Decembrie 2017, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

[19] Josep Borrell, *The post-Coronavirus World is already here*, European Council of Foreign Relations, 30 April, 2020, at https://www.ecfr.eu/publications/summary/the_post_coronavirus_world_is_already_here

[20] Iulian Chifu, „Infodemie trilaterală în pandemia de coronavirus: China, Rusia, Iran împotriva Lumii Libere", *Adevărul*, 28 aprilie 2020, la https://adevarul.ro/international/in-lume/infodemie-trilaterala-pandemia-coronavirus-china-rusia-iran-lumii-libere-1_5ea70e405163ec42712fa672/index.html

[21] *Idem*.

[22]COVID-19 disinformation – EEAS Special Report, 2-22 April 2020, at https://euvsdisinfo.eu/eeas-special-report-update-2-22-april/

[23] Iulian Chifu, „Trump şi campania *"China e duşmanul"*. Cazul coronavirusului – probe şi presupuneri", în *Adevărul,* 6 mai 2020, la https://adevarul.ro/international/in-lume/trump-campania-china-e-dusmanul-cazul-coronavirusului-probe-presupuneri-1_5eb242ab5163ec42717ebc4b/index.html.

[24] Ashley Brown, „Pompeo says 'enormous evidence' for unproven theory that coronavirus came from lab", *ABC News*, 3 May 2020, at https://abcnews.go.com/Politics/pompeo-enormous-evidence-unproven-theory-coronavirus-lab/story?id=70472857; BBC, *Coronavirus: Chinese state media take aim at US 'lab theory'*, 5 May 2020, https://www.bbc.com/news/world-asia-52540737; Office of the DNI, *Intelligence Community Statement on Origins of COVID-19*, 30 April 2020, at https://twitter.com/ODNIgov/status/1255868108356681728.

[25] Iulian Chifu, „Trump şi campania *China e duşmanul*. Cazul coronavirusului – probe şi presupuneri"; Iulian Chifu, „Infodemie trilaterală în pandemia de coronavirus: China, Rusia, Iran împotriva Lumii Libere", *Adevărul*, 28 aprilie 2020, la https://adevarul.ro/international/in-lume/infodemie-trilaterala-pandemia-coronavirus-china-rusia-iran-lumii-libere-1_5ea70e405163ec42712fa672/index.html

[26] Reuters, „Exclusive: Internal Chinese report warns Beijing faces Tiananmen-like global backlash over virus", 4 May 2020, at https://www.reuters.com/article/us-health-coronavirus-china-sentiment-ex/exclusive-internal-chinese-report-warns-beijing-faces-tiananmen-like-global-backlash-over-virus-idUSKBN22G19C

[27]Paris climate conference (COP21), *The Paris Agreement*, 13 December 2015 at https://unfccc.int/resource/docs/2015/cop21/eng/10a01.pdf

[28] European Commission, COM 2013(16.04.2013), An EU Strategy on adaptation to climate change, at https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0216:FIN:EN:PDF

[29] Will Kennedy, „Why the OPEC-Russia Blowup Sparked All-Out Oil Price War", *Washington Post*, 14 April 2020, at https://www.washingtonpost.com/business/energy/why-the-opec-russia-blowup-sparked-all-out-oil-price-war/2020/04/13/0c222f5e-7d94-11ea-84c2-0792d8591911_story.html

LUMEA POST-PANDEMIE ÎN EPOCA ACCELERAȚIEI - QUO VADIS? ARE CIVILIZAȚIA DE TIP OCCIDENTAL CAPACITATEA „DE A EȘUA RAPID”?

Iuliana-Adriana DUMITRACHE*

Abstract

The world nowadays is caught within the twirl of the acceleration age, where surprising factors cause fast, new evolutions. Human society should adapt its reactions and answers in order to keep up the pace with all the developments, mainly with those induced by information technology and by highest technology. Even the way institutions work and the way decision is taken should be done with flexibility, on the run, innovating.

COVID-19 Pandemic comes onto this complex context as another element that certainly causes alterations among almost all the domains of human existence. The impact is immense, evolving from the contaminated people's lives to the highest geopolitical arena. Certain states' capacity of making decisions "failing faster", on the run, has been tested. It requires leaving aside the leaders' ego or reputation and focusing on minimizing the negative effects, on considering the foreign know-how and the epidemiologists' knowledge and also on cooperating with the local administration.

The collateral effects of the virus on the current context are surprising. Some of them will determine further separate evolutions. To answer the needs of Infosfera's readers, the current article will concentrate on geopolitical and security situation, as well as on the additional possible effects which can be predicted for the moment.

Keywords: *acceleration age, technology, COVID-19 pandemic, „infoxication".*

„Ne aflăm într-o perioadă foarte, foarte gravă a lumii"
Henry Kissinger [1]

Bun venit în epoca accelerației. *Expect the unexpected! the future is now!*

Ca urmare a două determinante care au modelat ultimele decenii, globalizarea şi implementarea tehnologiei informaționale, trăim azi în *epoca accelerației*[2], definită de un cumul de evoluții în toate domeniile, de o explozie a descoperirilor şi aplicațiilor în sfere diferite de producție, comerț, tehnologie, comunicații etc. Invențiile şi inovațiile dintr-un domeniu potențează noi elemente în alt domeniu. Este o spirală rapidă a dezvoltării, care scurtează timpul de optimizare a proceselor şi grăbeşte obținerea de rezultate. Există teorii care pretind că dezvoltarea tehnologică reprezintă, în lanțul evolutiv, o singularitate – un eveniment cu impact major, care determină o cotitură în felul în care omul şi lumea se dezvoltă. La nivel individual şi social se produc mutații, pe care le conştientizăm sau nu, prin noi tipuri de manifestare personală, interacțiune umană şi comunitară. După cum apreciază Luciano Floridi (profesor de filozofie şi etica informației, director de cercetare la Oxford Internet Institute), „omul însuşi capătă

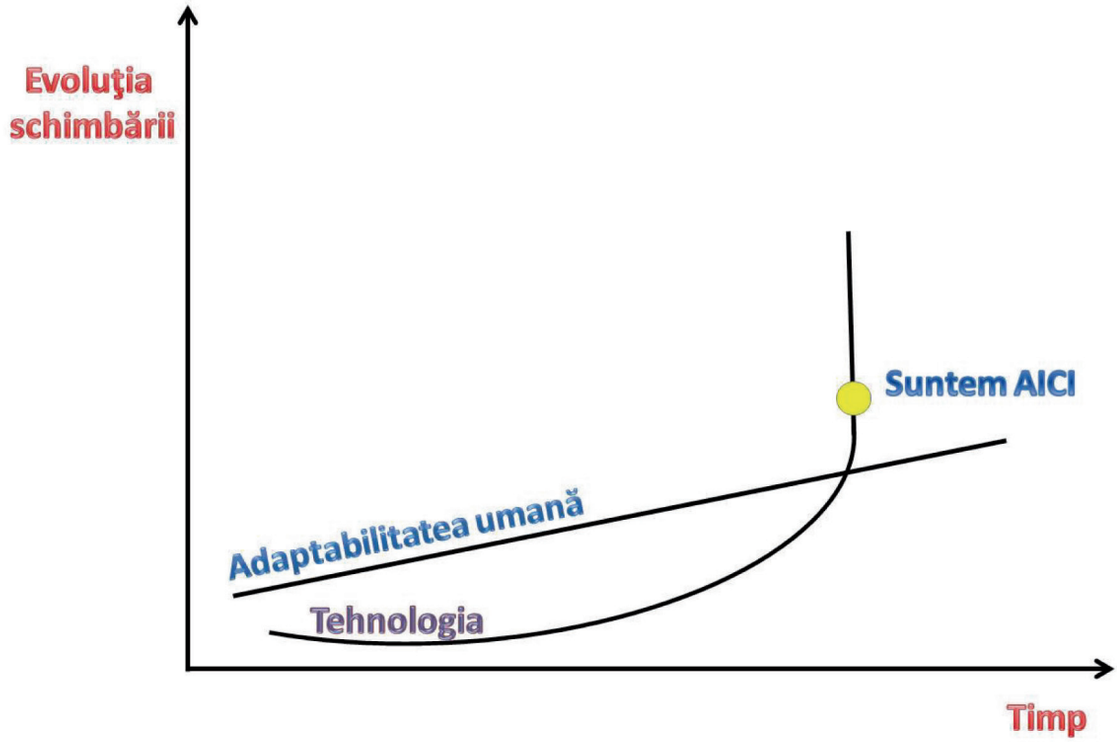
Expert în cadrul Ministerului Apărării Naționale.

o personalitate *onlife*, diferită de ceea ce suntem strict în lumea reală, nedigitală, pe măsură ce societatea noastră devine şi ea din ce mai mult o infosferă, un amestec de experienţe fizice şi virtuale”[3].

Faimosul analist şi futurolog Alvin Toffler, în cartea sa *Al treilea val*, anticipa un alt fenomen, care deja îngreunează situaţia înţelegerii realităţii, şi anume inundarea permanentă cu informaţii – *„infoxication”/„infobesity”*, pe care omul nu mai are răgaz să le parcurgă, să *„*le cearnă*”*, să le înţeleagă. Din această perspectivă, reacţiile oamenilor sunt diferite, tinzând către două atitudini-tip: unii se simt claustraţi, inadaptaţi, alienaţi, mergând până la autoizolare şi respingere a tehnologiei în ansamblu[4]; alţii îmbrăţişează tehnologizarea şi încearcă să se adapteze, să asimileze, să o „internalizeze”, să evolueze. Cu toate acestea, oamenii de ştiinţă pretind că adultul societăţii moderne va fi tot mai des confruntat cu starea de „dislocare – o stare în care există sentimentul că nu poate ţine pasul cu contextul care se schimbă atât de repede” (Craig Mundle, creator de computere speciale, coordonator pentru strategii şi cercetare în cadrul Microsoft[5]). Fenomenul pe care îl trăim, al evoluţiei accelerate, este descris de către Eric Teller, coordonatorul diviziei cercetare-dezvoltare de la Google X, printr-un grafic simplu[6], al cărui principiu este că ritmul schimbărilor tehnico-ştiinţifice (şi nu numai) depăşeşte viteza cu care oamenii şi societatea se pot adapta.

Evident că evoluţia tehnologică (şi a tuturor domeniilor în general) nu poate fi încetinită; dezvoltarea va continua în accelerare non-lineară. Tot Teller explică şi care ar fi atitudinea corectă pentru a supravieţui epocii accelerării: „*vremea stabilităţii statice a trecut (...) trebuie să ne adaptăm la o stabilitate dinamică. (...) nu ne mai putem permite să stăm, ci să fim în permanentă mişcare, ca şi cum am merge, am dormi, am fi permanent pe bicicletă. Nu este starea noastră naturală, dar devine o obişnuinţă naturală şi nu mai simţim dificultatea”; „Umanitatea trebuie să înveţe să funcţioneze în această stare, care este sinonimă cu re-învăţarea permanentă. (...) acum nu ne pregătim copiii pentru stabilitatea dinamică, însă va trebui să facem asta pentru că aceasta va fi noua stare de echilibru*”[7].

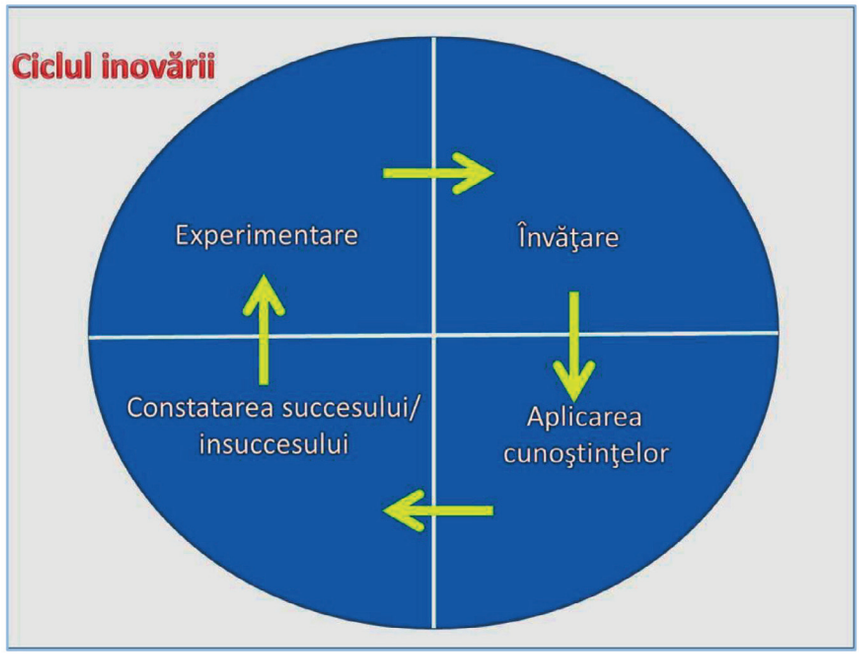
În contextul amintit, ţesătura cauză-efect este foarte complexă şi generează multe elemente-surpriză, benefice sau îngrijorătoare, printre care şi *efecte perverse*[8] (termen care, în



socio-antropologie, desemnează tipuri de evoluții care nu pot fi prevăzute, ca urmare a faptului că sunt cauzate de factori aparent dispersați și greu de conexat, care nu urmează un algoritm existent anterior sau care apar ca efect al unor determinanți încă inexistenți în momentul în care se dorea realizarea unei prognoze - „factorul hazard”). Prin urmare, va fi mult mai greu pentru analiști să realizeze previziuni și analize pertinente, mai ales proiecții pe termen mai lung, pentru că totul este într-o continuă reconfigurare accelerată. Uneori, inclusiv momentul prezent surprinde și se pune întrebarea post-factum *„cum s-a ajuns aici”,* pentru că există prea mulți factori despre care *„nu știm că nu știm”.*

Teller[9], acesta afirmă că motto-ul laboratorului pentru cercetare și dezvoltare al Google X este „eșuează mai repede” (însemnând, de fapt, „experimentează/inovează mai repede”).

Când se dorește identificarea unei soluții, se propune un plan și, din aplicarea rapidă a acestuia, se vede cât este de performant. Dacă soluția nu este bună, se trece rapid la aplicarea unei variante îmbunătățite, renunțând la ce a dus la rezultate negative și păstrând ce a fost funcțional. Cu alte cuvinte, chiar dacă nu se obține succesul din prima încercare, o soluție imperfectă este un proces de învățare, o etapă intermediară obținerii unui succes ulterior sau unei soluții mai apropiate de succes. Procesul este reluat până la obținerea



Acest lucru s-a întâmplat și în cazul actualei pandemii. Oamenii sunt uimiți că *„s-a întâmplat”* asta, că nu a putut fi anticipată viteza și magnitudinea răspândirii virusului, impactul socio-economico-politic, că nu au fost avertizări inițiale (deși acestea au existat, dar nu suficient de convingătoare sau penetrante).

Soluția: capacitatea „de a eșua rapid”

O îmbunătățire a reacției și adoptării de soluții în epoca actuală se bazează pe accelerarea inovării, în sensul eficientizării rapide a cursului de acțiune, uneori chiar în cadrul procesului în desfășurare. Făcând din nou trimitere la Eric

unui rezultat cât mai aproape de deziderat. Vorbim despre o inovare continuă și de adaptare permanentă la noile realități. Deși rezultatul nu este perfect, în mod sigur este mai bun decât aplicarea completă a unui plan nefuncțional sau mai bun decât actualul model instituțional, prin care se stabilește un set de reguli stricte pentru o perioadă de timp, constatându-se ineficiența/ ineficiența parțială (sau succesul, de ce nu?!) abia după încheierea perioadei de timp stabilite pentru analiza ulterioară.

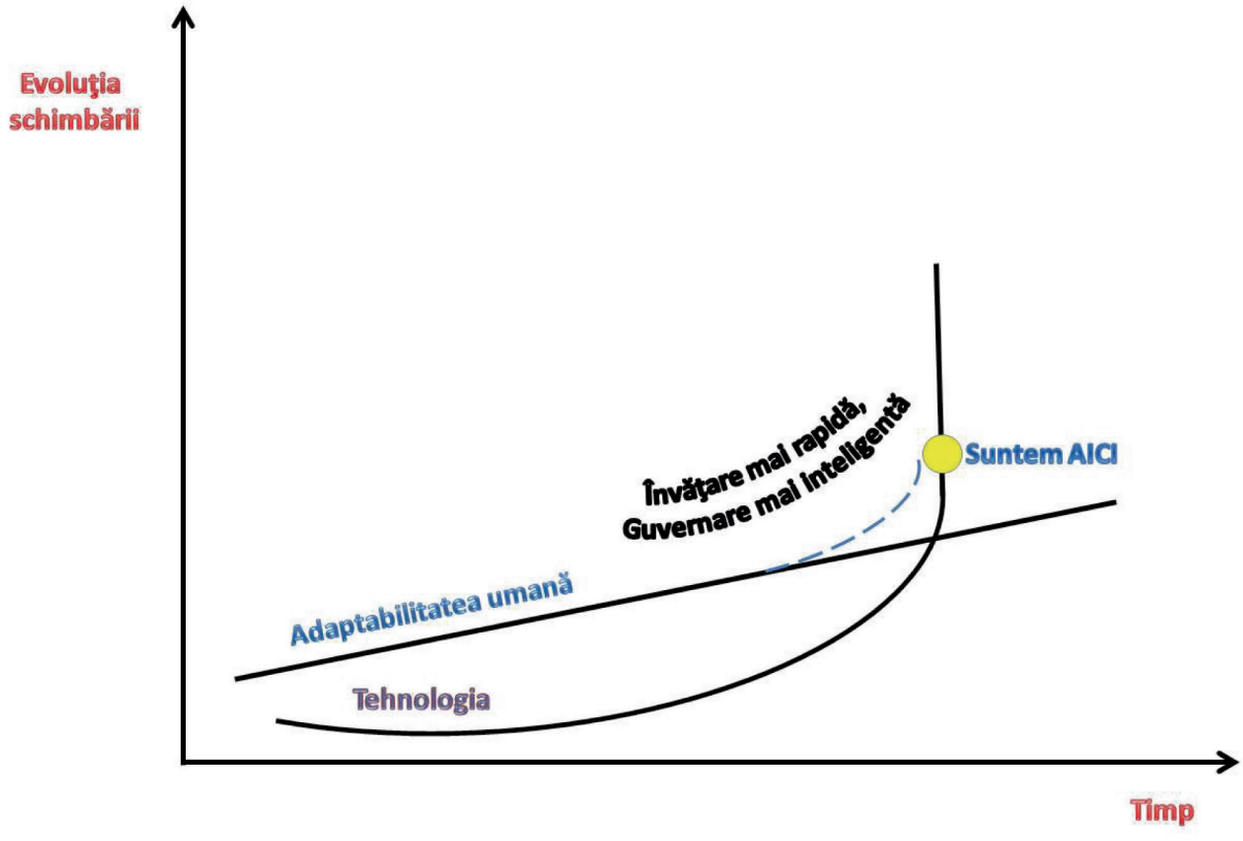
Acest tip de abordare este complementar cu strategiile manageriale specifice gândirii laterale propuse de Eduard de Bono[10], strategii care ne

ajută să avem alertă atenția distributivă, să avem în minte cât mai multe alternative simultan, cât mai multe variabile care pot schimba scenariile prezente şi efectele ulterioare ale fiecăruia dintre ele.

În legătură cu inovarea decizională, Thomas Friedman constată[11] că, în actuala conjunctură, este vital ca inclusiv instituțiile/organizațiile publice (chiar şi cele de guvernare şi elaborare de acte normative) să fie preocupate, pro-active, deschise către optimizarea rapidă a activității, către experimentare rapidă şi asimilarea atitudinilor de corectat din lecții învățate. Ținta ar fi să se răspundă cât mai rapid scopului pentru care funcționează, respectiv optimizarea relației cu cetățenii, furnizarea şi armonizarea serviciilor solicitate de aceştia, adoptarea altor servicii în raport cu evoluția socială şi necesitățile imperative ale momentului. Adaptabilitatea instituțională este o sursă de flexibilitate decizională şi acțională, ceea ce poate spori eficiența şi rapiditatea adaptării instrumentelor în noul context, fie el local, național, regional, global.

Pandemia în epoca accelerației – factor de surprindere strategică?

În cadrul unei conferințe pe teme de securitate (2017), dl. Sorin Ducaru, invitat de onoare, afirma: „Vacanța strategică [a Europei] s-a sfârşit. Puneți-vă centurile de siguranță!”. Deşi domnia sa făcea această afirmație într-un context în care Europa se confrunta cu alte probleme (criza migranților, creşterea tendințelor naționaliste la nivel continental şi decuplarea SUA de la angajamentul, anterior de neconceput, al asigurării securității bătrânului continent), sintagma ni se pare extrem de potrivită pentru descrierea situației actuale şi viitoare şi nu doar referitor la Europa, ci la civilizația de tip occidental, în general. Epoca accelerației îşi pune amprenta asupra situației geopolitice, factorii de îngrijorare deja cunoscuți (terorismul, sărăcia, migrația, slaba guvernare, proliferarea armelor de nimicire în masă, deteriorarea condițiilor de mediu) intrând acum în interacțiune cu un factor neanticipat până de curând, şi anume pandemia COVID-19. Este un exemplu de element aparent minor, greu de anticipat, care, potențat de alți



factori (globalizarea/circulația persoanelor şi a mărfurilor, tiparele comportamental-societale, etc.), ajunge să genereze, într-un interval relativ scurt de timp, una dintre cele mai dificile crize ale umanității din ultimele decenii, cu sute de mii de decese şi repercusiuni asupra indivizilor, societății, economiei, conducerii locale şi a organismelor decizionale naționale, regionale, internaționale.

COVID-19 pune la încercare capacitatea de reacție, de adaptare, de gestionare, şi, respectiv, credibilitatea autorităților, de la cele de nivel local până la cele de tip organizație internațională. Impactul pe care l-a generat a fost şi el greu de anticipat. Virusul care a afectat mii de cetățeni chinezi din Wuhan, la finalul anului 2019, a atras puțină atenție la nivel global. Opinia generală la nivelul multor state - mai ales al celor din Occident - a fost că acest virus va afecta în mare parte doar Asia de Est. S-au comis două erori: pe de o parte, încrederea într-un pattern deja cunoscut – cel al sindromului respirator acut sever (SARS) din 2003 (care a avut un impact minim asupra Occidentului şi s-a presupus că şi acest virus va fi asemănător) şi, pe de altă parte, *wishful thinking* – adoptarea unei estimări dezirabile („pe noi nu ne poate afecta", „nu are cum să ajungă la noi", „sistemele noastre medicale sunt mai competente decât cele chineze"). Când, inevitabil, pandemia a atins Europa (respectiv Italia, în primă fază), în celelalte capitale vest-europene şi în SUA viața a continuat ca de obicei, fără să fi stârnit îngrijorare prea mare. Abia după ce virusul a început să se manifeste cu agresivitate şi Italia a fost depăşită de situație au început să fie trase semnale de alarmă. Acest fapt se datorează inerției instituționale şi probabil încrederii sporite pe care cetățenii o aveau în capacitatea propriilor guverne/autorități de a supraveghea, de a gestiona eficient situația şi de a avertiza din timp populația. Efectele negative ulterioare ar fi putut fi limitate dacă ar fi existat o reacție pro-activă şi alertă a autorităților şi o adaptare din mers a măsurilor de limitare a transmiterii virusului, de testare şi tratament.

Din acest punct de vedere, reacția autorităților române a fost eficientă comparativ cu cele adoptate de alte state mult mai potente politic, economic şi medical, datorită faptului că „a eşuat rapid", adică a adaptat din mers măsurile la noile realități, luând în calcul sfaturile experților în virusologie şi a managerilor situațiilor deosebite, „lecțiile învățate" avute la dispoziție în momentele respective (din China, unde se încheiase epidemia, respectiv Italia, unde contaminarea era în desfăşurare). S-a adoptat rapid situația de urgență, instituirea carantinei persoanelor intrate în țară, îmbunătățirea managementului spitalelor cu instituirea unui management militar acolo unde situația o impunea, pachetul de restricții de circulație şi de distanțare socială etc. Reacțiile au fost oportune, flexibile, rapide, îmbunătățite din mers, inclusiv cele economice, efectele benefice urmând să se simtă nu doar în limitarea contaminării populației, ci, foarte important, în limitarea contractării economiei, care oricum urmează să aibă de suferit[12].

(Geo)politica pe timp de pandemie

Ce ne-a surprins în felul în care au decurs lucrurile? Înainte de pandemie, am fi fost tentați să credem că nivelul de trai şi gradul de dezvoltare al unui stat sunt factorii cu cel mai mare impact asupra evoluției pandemice în țara respectivă, precum şi asupra succesului revenirii economice după trecerea perioadei critice. Pe măsură ce lucrurile au evoluat, s-a dovedit că a contat mult coerența în abordări a liderilor, viteza de reacție a autorităților centrale şi locale, precum şi gradul de flexibilitate în a accepta recomandările oamenilor de ştiință privind măsurile de prevenție şi de limitare a contaminării. Tot un astfel de factor îl reprezintă şi gradul în care populația este dispusă la respectarea limitărilor recomandate.

S-a constatat că nu a existat şi nu există o abordare strategică integratoare a eforturilor de combatere a pandemiei între SUA şi Europa[13], ceea ce contribuie la întărirea percepției existenței unui clivaj între SUA şi aliații săi tradiționali din Europa Occidentală.

Reacția statelor de pe vechiul continent a fost neunitară, individualizată pe state. Italia a fost izolată şi s-a confruntat aproape singură cu efectele aproape necunoscute ale pandemiei, de la debut până aproape de jumătatea curbei

ascendente a acesteia. Ulterior, fiecare stat a acționat după propriul model, adoptând strategii diferite de luptă cu virusul: în timp ce unele aplicau măsuri de distanțare socială, altele promovau imunizarea în masă. Unele permiteau deschiderea granițelor, altele au închis accesul. Majoritatea s-au orientat pentru obținerea de materiale sanitare şi medicația COVID-19, interzicând exportul acestor produse şi încercând să obțină prin importuri preferențiale produsele deficitare, uneori chiar intrând în conflicte tacite.

Cetățenii au perceput reacția Uniunii Europene ca întârziată şi axată, în primul rând, pe îngrijorările de ordin economico-financiar, şi abia secundar pe cele de ordin socio-demografic (primele măsuri care vizau stocurile comune de materiale sanitare şi medicamente au fost luate la aproximativ o lună după începerea crizei pe bătrânul continent). Există o diferență pe care cetățenii de rând nu o percep: UE este o alianță de state suverane şi nu un guvern central, autoritățile de la Bruxelles având control doar asupra comerțului extern şi concurenței. Pentru restul domeniilor, organul executiv al UE, Comisia Europeană, nu poate decât urmări cooperarea, fără a avea puterea să o impună. În pofida limitărilor sale, UE a reuşit totuşi să întreprindă unele demersuri. Au fost relaxate reglementările pentru a permite guvernelor naționale să susțină mediul afectat al afacerilor, iar limitele asupra datoriei guvernamentale au fost suspendate. Banca Centrală Europeană a anunțat un pachet de salvare în valoare de 750 mld. EUR. Austria, Franța şi Germania au trimis măşti de protecție Italiei; Germania, având o situație mai bună decât vecinii săi, a preluat pacienți din Italia şi Franța; frontiera comună a fost închisă. Şi sunt disponibile mai multe instrumente, cel mai notabil fiind Mecanismul European de Stabilitate, un fond de salvare creat ulterior crizei financiare din 2008, în valoare de peste 400 miliarde Euro pentru a ajuta statele aflate în criză.

Cel mai notabil aspect în cadrul crizei actuale este acela că sănătatea publică este lăsată complet în responsabilitatea guvernelor naționale. Aceasta nu conduce la un răspuns eficient la criză. Totuşi, diversitatea planurilor anti-pandemie a avut şi un efect pozitiv: demontarea acelor strategii care nu au funcționat (imunizarea în masă).

Pandemia a generat efecte colaterale neanticipate: valuri migraționiste ale forței de muncă înapoi spre țările-mamă (Vest-Est), urmate de alte valuri spre statele occidentale cu cerere masivă de forță de muncă (Est-Vest). Conştientizarea dependenței unor sectoare vitale ale economiei şi sănătății de produse fabricate

în state care dețin monopol (China, Turcia). Dificultatea de a obține aceste produse (aparate de respirație artificială, măști, combinezoane, substanțe biocide) în condiții de piață liberă. Conştientizarea efectelor negative pe care le-a avut lichidarea haotică a unor sectoare de producție şi de cercetare strategică, de stat, şi a unor unități spitalicești.

Efecte. Ce s-a schimbat? Pandemia îşi pune amprenta asupra geopoliticii la vârf. O primă consecință este exacerbarea şi încleştarea ambițiilor americane şi chineze, context în care F.Rusă vine în sprijinul Beijing-ului (care o avantajează tangențial). Deşi *clash-ul* americano-chinez are fundamente mai vechi, în mare parte de sorginte economică, actuala etapă este suficient de puternică încât să ducă la o deteriorare gravă, poate chiar ireversibilă, a relațiilor bilaterale[14]. În plus, pandemia vine pe fondul unor schimbări politice majore pe care SUA le-a făcut în direcția unei retrageri unilaterale din politica globală[15], în timp ce China militează pentru primul rol, cel puțin în zona Asiei de Sud-Est.

Oficialii de la Washington, alături de unele state occidentale, au avut o poziție agresivă la adresa Chinei, învinuind-o de răspândirea intenționată a COVID-19. Dincolo de această atitudine, SUA nu au avut alte contribuții pe plan extern care să o favorizeze în ceea ce priveşte cooperarea internațională pentru învingerea pandemiei (cu excepția celor din cadrul NATO, de transport al materialelor sanitare dintr-un stat în altul). Episodul în care preşedintele Trump a încercat cumpărarea unui eventual vaccin în vederea utilizării sale doar în folos american poate fi productiv pentru aducerea de voturi la alegerile prezidențiale din toamnă, însă a fost în egală măsură perceput drept negativ, egocentrist, de către opinia internațională.

Pe plan intern, COVID-19 a dezvăluit slăbiciuni importante ale sistemului politic american, începând de la discursul preşedintelui Trump pe tema pandemiei (discurs decuplat de la evidențele medicale) şi continuând cu nearmonizarea acțiunilor cu experți în virusologie, negarea lipsei de resurse medicale, explozia contaminării în zone puternic populate (ex.: New York), efectele sociale grave din zonele sărace. Această situație nu afectează deocamdată în niciun fel poziția de lider global a SUA, însă este posibil ca o eventuală criză internă să schimbe prioritățile de angajare externă şi magnitudinea acestei angajări a Washington-ului.

Apar noi curente şi instrumente de exercitare şi propagare a influenței: propaganda prin intermediul sprijinului medical şi dezinformarea pe tema pandemiei.

NATO s-a implicat în prevenirea şi combaterea crizei prin implementarea măsurilor de prevenire a pandemiei. Cel mai cunoscut efort al Alianței s-a concretizat în stabilirea unor culoare aeriene în spațiul european, în vederea livrării de echipamente medicale, la solicitarea miniştrilor de externe din statele membre NATO.Ca urmare a acestui efort, sute de tone de echipamente medicale au fost donate şi livrate.

„Diplomația halatelor albe" a funcționat, iar China şi F.Rusă au utilizat-o şi vor continua să o folosească în zonele în care aveau deja influență, dar şi acolo unde anterior nu puteau interveni. China se erijează în rolul singurei puteri mondiale capabile să gestioneze cea mai mare amenințare globală la acest moment – pandemia, fără a afirma deschis că doreşte să se afirme ca cea mai mare putere mondială. Lee Kuan Yew sublinia, cu ani în urmă, că „autoritățile de la Beijing discută rar despre faptul că R.P. Chineză doreşte să devină lider, însă acesta este obiectivul nedeclarat din spatele ascensiunii sale".

Beijing-ul a exportat know-how în gestionarea practică a activității intra-spitalicești, a furnizat materiale sanitare (măști, combinezoane impermeabile, medicamente) şi a participat cu echipe medicale oriunde a putut. Magnitudinea impactului COVID-19 pe plan intern este încă o necunoscută, însă propaganda chineză se concentrează pe a demonstra că revenirea economică este o poveste de succes. Producția şi exportul de materiale sanitare şi substanțe de bază pentru medicamente reprezintă domenii de nişă pe piața mondială, care în prezent avantajează Shanghai-ul.

F.Rusă nu este nici ea imună la infectarea cu SARS-CoV-2. Înainte de Paştele ortodox, multe dintre spitalele din Moscova erau ocupate la capacitate maximă şi nu mai puteau face faţă noilor solicitări. F.Rusă foloseşte şi ea diplomaţia medicală, contribuind în zonele în care îi este permis (exemplu: timp de o lună de zile, medici militari din cadrul forţelor armate ruse au tratat cetăţeni italieni în cadrul unei secţii de terapie intensivă a spitalului de campanie din Bergamo). Cu precădere acţionează, însă, în statele balcanice.

În prezent, UE este concentrată, financiar, înspre gestionarea problemei din interior. Deşi o recomandare-cheie a strategiei sale globale din 2016 a fost aceea de a îmbunătăţi capacitatea de rezistenţă în plan politic şi economic a partenerilor săi regionali, această direcţie este în mod evident pusă în pericol. State precum R.Moldova, Ucraina, Turcia, Siria, Irak, Egipt şi alte state din nordul Mediteranei se vor confrunta cu dificultăţi economice de durată, având de gestionat probleme anterioare grave, amplificate de pandemie (migraţia forţei de muncă, inechitate socială, existenţa unor zone de conflict pe teritoriul naţional, migraţia, sărăcia endemică, slaba guvernare etc.)[16]. În acest moment, sprijinul acordat acestor state este de 15,6 miliarde Euro – aproximativ 3% din suma alocată pentru necesităţile interne ale UE.

Organismele financiare internaţionale au avut reacţii întârziate, dar s-au mobilizat în vederea limitării unor efecte negative care s-ar fi putut, ulterior, permanentiza. Au fost lansate iniţiative globale de sprijin, cum ar fi programele de reducere a datoriilor coordonate de Fondul Monetar Internaţional. UE a acordat sprijin financiar pentru statele grav afectate de pandemie, în cooperare cu marile concerne bancare, atât pentru combaterea epidemiei, cât şi pentru sprijinirea companiilor mici şi mijlocii sau amânarea plăţii creditelor pentru persoanele afectate. Pachetul *Echipa Europa*, lansat în luna aprilie a.c., alocă 500 miliarde Euro acestor deziderate[17]. Se observă o schimbare de strategie faţă de criza financiară din 2008, când s-a limitat consumul şi au contat mai puţin efectele asupra persoanelor fizice, companiilor mici şi mijlocii, accentul fiind pus pe sprijinirea, în primul rând, a sistemului bancar, ceea ce a prelungit şi a afectat pe mai departe evoluţia crizei.

Actuala criză internaţională din domeniul sănătăţii are implicaţii geopolitice majore. În afară de R.P.Chineză, opt din cele mai afectate zece state sunt economii occidentale (un alt stat din cele zece fiind Iranul). La sfârşitul lunii aprilie a.c., cele opt economii occidentale reprezentau mai mult de trei cincimi din numărul de cazuri la nivel global, iar numărul de decese raportate în Italia şi Spania era deja de cinci ori mai mare decât cel din R.P.Chineză.

În Statele Unite se aşteaptă o contractare a economiei cu 25%, o magnitudine similară fiind înregistrată de SUA pe timpul Marii Recesiuni de după 1929. Însă, dacă Depresiunea s-a desfăşurat de-a lungul a patru ani, implozia provocată de pandemia de COVID-19 are loc accelerat, în doar 3 luni. Pachetul de stimulente aprobat de Congresul SUA pentru cei care au trebuit să îşi închidă activitatea din cauza pandemiei este evaluat ca fiind cel mai generos acordat vreodată de SUA pe timp de pace. Din păcate, aceste eforturi sunt neutralizate de creşterea rapidă a şomajului: dacă la începutul lunii martie acest indicator era la una dintre cele mai scăzute rate înregistrate vreodată, la sfârşitul lunii martie atingea 13 procente (cea mai ridicată rată după al Doilea Război Mondial). Potrivit *Foreign Policy*[18], în raportările săptămânale ulterioare, formularele pentru şomaj au fost completate de 3,3 milioane de cetăţeni, apoi de 6,6 milioane, apoi de alte 6,6 milioane. O astfel de rată de creştere nu a mai fost înregistrată de SUA niciodată. Economistul Justin Wolfers sublinia, pentru *New York Times,* că şomajul creşte cu aproape 0,5% pe zi, ceea ce ar însemna ca, la începutul verii, dacă se menţine trendul actual, să atingă 30%. 73% din gospodării au suferit pierderi de venituri în cursul lunii martie în SUA. În aceste condiţii economice dificile, cum va evolua situaţia în interiorul SUA, cum va influenţa acest lucru votul pentru alegerile prezidenţiale din toamnă şi va mai fi oare posibilă o reluare a relaţiei SUA-UE la nivelul celei din anul 2016 sau Washington-ul va continua politica de dezangajare, având în prim-plan stabilitatea internă?

Beijingul continuă să se prezinte drept o putere excepțională, recenta „diplomație a măștilor" continuând eforturile deschise de inițiativele *Belt and Road* și *„17+1"*. Mesajul promovat va fi că modelul chinez de luptă împotriva bolii este superior celui occidental. China are în buzunar un alt atu important: peste 90% din antibioticele necesare, aproximativ 70% din necesarul de paracetamol și derivatele sale, și peste 50% din necesarul SUA de anticoagulante sunt furnizate din China, care reprezintă al doilea mare furnizor al FDA (Food and Drug Administration)[19]. Pe plan intern, Partidul Comunist Chinez va pune probabil și mai mult accent pe guvernarea politică autoritară, promovând ideea ineficienței guvernării politice occidentale. Capacitatea Partidului de a controla populația îi permite să aplice măsuri eficiente, spre binele general, chiar dacă acestea pot fi considerate a fi incompatibile cu noțiunile occidentale privind drepturile omului și libertățile individuale. Conform *Foreign Policy*[20], rata șomajului în China este de 6,2%, cea mai mare rată din 1990 până în prezent (1990 fiind momentul când au început să emită raportările). Neoficial, se pare că 205 milioane de lucrători au fost parțial afectați sau au rămas fără loc de muncă, ceea ce ar corespunde unui sfert din capacitatea forței de muncă a Chinei.

Probabil că inclusiv India se va confrunta cu o perioadă de criză extinsă. După o perioadă de închidere a activităților economice de 21 de zile, economia va fi sigur afectată, mai ales că din totalul de 471 de milioane de persoane care constituie forța de muncă a Indiei doar 19% au asigurare socială, două treimi nu au contract de muncă oficial și cel puțin 100 de milioane sunt muncitori sezonieri.

Organizația pentru Cooperare și Dezvoltare Economică a emis predicții grave, dintre care unele aparent surprinzătoare: Japonia va fi foarte grav afectată economic, deși nu în mod direct afectată de COVID-19, tot ca urmare a tendinței de contractare a puterii de cumpărare în perioada pandemiei, fapt care afectează industria auto în mod deosebit.

Pe fondul criticilor americane aduse R.P. Chineze ca agent generator și propagator al pandemiei, F.Rusă apără poziția celei din urmă. Este posibil ca această cooperare să fie doar una de conjunctură, F.Rusă neavând interesul de a opta cu adevărat pentru una sau alta dintre părți. Pentru moment, atâta timp cât au interese comune, Kremlinul și Beijingul vor coopera. Este posibil ca, profitând de moment, cele două să aibă în vedere diminuarea dependenței de dolarul american și derularea de acțiuni care să avantajeze acest scenariu. Deși atât China, cât și F.Rusă promovează o atitudine a neamestecului în treburile interne ale altui stat, Moscova pare a nu agrea stilul din ce în ce mai agresiv cu care China condamnă promovarea democrației și egalității în drepturi a cetățenilor de către Washington, iar acest subiect poate genera divergențe ulterioare pe axa Moscova-Beijing. Paradoxal, deocamdată, F.Rusă a avut de profitat de pe urma sancțiunilor impuse în urma ocupării Crimeii în sensul că, în ultimii cinci ani, a reușit să acumuleze rezerve valutare semnificative și o rată redusă a datoriei publice (Rusia își menține poziția stabilă în grupa BBB - conform S&P Global Ratings). De asemenea, Moscova a restricționat importurile alimentare din SUA și UE, concomitent cu creșterea propriei producții agricole, ceea ce îi permite să fie mai rezistentă la șocurile comerțului alimentar internațional[21]. F.Rusă a folosit și va continua să promoveze intens „diplomația halatelor albe" și dezinformarea și propaganda pe tema pandemiei, subliniind ineficiența sistemelor sanitare occidentale, în special a celor americane, precum și lipsa grijii statelor „capitaliste" față de proprii cetățeni, expuși riscurilor epidemice și economice. Președintele Vladimir Putin este pragmatic, lăsând autonomie de decizie autorităților regionale în privința gestionării problemei și a măsurilor de combatere necesare. Mai mult ca sigur, însă, și F.Rusă se va confrunta cu o contractare a economiei.

La nivelul bătrânului continent, pandemia reprezintă cea mai mare provocare de la sfârșitul celui de-al Doilea Război Mondial. Din această perspectivă, unul dintre aspectele importante ar trebui să fie urmărirea asigurării unui echilibru între acțiunile puternice și eficiente ale guvernelor pe timpul pandemiei, pe de o parte, și gradul de

limitare sau afectare a drepturilor democratice ale cetățenilor[22]. Se pare că şi recesiunea economică va fi pandemică. Se înregistrează o accelerată scădere a consumului (ex: consumul produselor petroliere a scăzut în Europa cu 88% în perioada martie-aprilie) şi a dispoziției de investiții/ capitalizare, nenumărate cazuri de faliment, delincvență şi creşterea datoriilor pentru consum.

Deşi de ceva timp se vehiculează ideea generării *hub*-urilor pentru echipamente medicale, nu sunt semnale care să confirme materializarea acestora. Actualmente se vehiculează principiul *pooling and sharing* ca motor principal pentru redobândirea coeziunii. Strict economic vor exista politici coerente ale UE de sprijinire a economiilor pe timp de pandemie şi se prefigurează o politică solidară în vederea revenirii şi refacerii post-COVID. Virgil Popescu, ministrul Economiei, apreciază că un efect pozitiv al pandemiei va fi relocarea unei mari părți a producției industriale în zona europeană[23]. Cele mai multe efecte vor fi însă negative şi statele europene vor suferi un şoc economic, neanticipat poate la adevărata magnitudine. Există un ciclu al sectoarelor economice care sunt afectate. Inițial - cele mai volatile sectoare ale economiei – sectorul imobiliar, respectiv construcțiile, apoi cele care depind de investiții sau care sunt subiect al competiției internaționale (ex: construcțiile de maşini). Afectarea acestor sectoare, care de obicei concentrează circa un sfert din forța de muncă, se repercutează asupra celorlalte domenii ale economiei, vânzările cu amănuntul, imobiliare, educație, entertainment, restaurante (domenii care în SUA concentrează 80% din forța de muncă ocupată). Pentru micile magazine, închiderea temporară şi vânzările online pot însemna sfârşitul afacerii în sine. Nordul Italiei produce 50% din PIB-ul acestui stat. PIB-ul Germaniei va suferi o cădere mai mare decât cea a SUA, din pricina dependenței de exporturi, dar şi ca urmare a opririi producției industriei auto.

Dacă pentru Europa există posibilități sporite de gestionare a pandemiei (infrastructură, politici comune, resurse financiare), nu acelaşi lucru se poate afirma despre zona din proximitatea Europei de Sud-Est – zonă fragmentată şi frământată de conflicte în desfăşurare sau tensiuni latente. Pentru Turcia, Grecia, Siria, dar şi pentru state din zona balcanică, sunt condiții pentru o agravare serioasă a situației de securitate din cauza suprapunerii unor factori agravanți, interdependenți: creşterea fluxului de refugiați prin Marea Mediterană, criză financiară, instabilitate politică. În condițiile suprapunerii pandemiei peste problemele deja existente, este posibil să asistăm la o exacerbare a fenomenelor marcate de violență, pe măsură ce criza se va adânci[24]. Turcia se remarcă şi ea prin desfăşurarea de acțiuni de tip umanitar/„diplomația halatelor albe" pentru statele în care urmăreşte creşterea influenței de ani buni (Albania, Macedonia de Nord, Kosovo). O posibilă acțiune europeană s-ar putea concretiza prin implicarea Băncii Centrale Europene (BEC) în încheierea unor acorduri de schimb cu băncile centrale ale statelor partenere din vecinătate, care să permită statelor beneficiare să obțină euro de la BEC, în paralel cu propria monedă. Acest ajutor ar asigura statelor beneficiare lichidități valutare şi le-ar reface rezervele. Un astfel de lucru a fost întreprins de Rezerva Federală a SUA, care a stabilit deja un astfel de mecanism cu 14 state.

În gestionarea răspândirii COVID - 19, statele africane depind cel mai mult de perspectiva apariției unui vaccin produs la scară largă şi accesibil financiar, însă această perspectivă pare tot mai îndepărtată. Puțini actori de nivel internațional se preocupă de soarta Africii. Organizația Mondială a Sănătății a furnizat teste pentru 47 de state africane[25].

Concentrarea atenției şi finanțelor pe limitarea efectelor pandemiei poate abate atenția decidenților de la alte amenințări care nu au dispărut în această perioadă şi a căror manifestare ar putea reveni cu mai multă forță: radicalizarea şi terorismul islamic. Activitatea organizației Statul Islamic, de exemplu, continuă în Siria şi alte zone, unde face în continuare victime; aceste grupări profită de moment pentru a se regrupa şi reorganiza. Taberele de refugiați din Siria, Irak, Turcia sunt zone vulnerabile, fiind posibil să se continue acțiunile de recrutare şi radicalizare.

Un alt efect colateral care poate afecta escaladarea insecurității în unele regiuni fierbinți este reprezentat de predarea controlului prematur al unor zone către autoritățile locale insuficient pregătite sau înzestrate, dacă prezența militară în anumite zone de criză nu ar mai fi considerată prioritară de către decidentul politic, pe fondul acutizării stării de urgență induse de COVID-19, ceea ce ar reprezenta o risipă a eforturilor şi a resurselor investite în timp şi o perpetuare a problemelor de instabilitate politică, de guvernare şi de menținere a situației de securitate.

Tot referitor la terorism, ar trebui să se țină cont că insurgenții nu sunt în izolare socială. Este posibil ca aceştia să profite de vulnerabilitatea societății occidentale din acest moment, precum şi de presiunea pusă pe forțele de menținere a ordinii publice, ale căror eforturi sunt acum redirecționate în gestionarea pandemiei. Un factor pozitiv ar fi posibilitatea scăzută ca aceştia să afecteze mulțimi de oameni în condițiile în care manifestările cu un număr mare de oameni sunt limitate, însă nu pot fi excluse acțiuni care să afecteze puncte strategice sau simboluri de importanță națională, lideri politico-militari sau organizarea altor tipuri de lovituri (ex: substanțe chimice sau radiologice).

Concluzii

Încă este incertă perspectiva de evoluție a pandemiei: se va stinge de la sine sau se va face o trecere lină către un alt val de contaminare în toamnă? Va trebui să coabităm cu virusul pe o perioadă mai lungă şi, dacă da, ce impact va avea acest lucru la nivel mondial, regional, național şi în viața noastră de fiecare zi? Cum vor putea guvernele să gestioneze efectele sanitare, sociale, demografice, dar şi pe cele indirecte – economice, politice şi de securitate? Ce efecte psihologice are pandemia asupra generațiilor viitoare? Vor avea guvernele şi liderii capacitatea „să eşueze rapid" şi să inoveze în domeniul decizional, astfel încât să obțină maximul posibil din ceea ce se poate întreprinde? Ce învățăminte putem trage şi ce ar trebui să adaptăm dacă pandemia va reveni?

Într-un articol din 09.04.2020 al publicației online *Foreignpolicy.com*[26], ni se atrage atenția că, potrivit datelor aflate la dispoziția SUA, lumea este în cea mai mare cădere liberă înregistrată vreodată şi că ce ştiam despre vechile reguli din domeniile economic şi politic nu se va mai aplica. Asta deoarece tipul acesta de amenințare – pandemia – va reprezenta un şoc istoric din punct de vedere al impactului pe care îl va avea. Se pare că e prima dată când, după cel de-al Doilea Război Mondial, economiile de piață emergente se vor contracta. Asistăm la cel mai mare efort fiscal lansat vreodată. Cu toată generozitatea acordării de împrumuturi/fonduri de către FMI şi UE, acest efort va avea efect timp de câteva luni, apoi e posibil să se constate că această primă rundă nu este suficientă.

Premierul din Singapore, Lee Hsien Loong, a subliniat probabilitatea ca evoluția COVID-19 să se extindă, posibil chiar pe durata mai multor ani. În aceste condiții, este esențial ca marile puteri să colaboreze pentru a combate pandemia, aceasta fiind şi varianta preferată de multe state. În acest moment, este evident că nu trebuie să fii o mare putere pentru a gestiona eficient pandemia. Succesul în combaterea COVID-19 în locuri precum Singapore, Taiwan şi R.Coreea se datorează mai degrabă unei guvernări dinamice, flexibile, adaptative în momente de criză. Premierul din Singapore consideră că puterile mici şi mijlocii dețin instrumente importante pentru a determina evoluția situației, cu condiția să existe suficientă determinare la nivel politic, capital social şi încredere între guverne şi cetățeni. Într-adevăr, ar fi o eroare să nu fie luate în considerare observațiile şi lecțiile statelor mai mici. Astfel, apare în atenție un posibil scenariu la nivel global, respectiv varianta în care puterile mici şi mijlocii vor avea capacitatea să joace un rol în modificarea ordinii globale în timpul şi după pandemia de COVID-19[27].

Virusul cu care ne confruntăm este încă o necunoscută. Asistăm la descoperiri medicale în ceea ce îl priveşte, săptămânal, referitoare la efecte manifestate după vindecare, la feluri în care atacă diverse organe, la ritmul diferit de propagare în zone diferite ale lumii. Încă învățăm despre el şi urmează ca strategiile decidenților să se adapteze la acestea.

Din această perspectivă, în lipsa unui vaccin, situația în care guvernele *vor eşua rapid* în sensul îmbunătățirii măsurilor care să limiteze contaminarea şi să permită derularea vieții în condiții cât mai normale va fi esențial, mai ales în perspectiva tot mai vehiculată a posibilei apariții de valuri succesive ale contaminării, pe termen lung[28].

Concurența pentru cine va inventa primul vaccinul anti-COVID-19 este acerbă. Rezolvarea sa de către unul sau altul dintre actorii angajați în cursă va însemna un imens argument pentru consolidarea poziției de lider a unei țări anume – „criteriu devenit peste noapte referință pentru tot ceea ce înseamnă avans tehnologic de excepție, dublat de capacitate de cercetare de vârf şi mijloace de producție necesare pentru a asigura cererea viitoare de piață"[29]. Dincolo de interesele politice, nu trebuie neglijate cele esențiale – binele umanității şi viața fiecăruia dintre noi. Mai multe laboratoare au anunțat că sunt gata să demareze ultima fază a procesului de testare clinică a formulelor pe care le au acum aproape finalizate, mai ales cele care au trecut cu succes faza testării pe animale[30]. În plus, apare şi posibilitatea ca, tocmai datorită urgenței, o țară sau alta să aprobe intrarea în producție a unei asemenea vaccin fără să mai fie îndeplinită şi această ultimă cerință a testării pe subiecți umani – fapt care ar putea avea urmări greu de estimat.

Un efect pervers al actualei pandemii îl constituie faptul că va determina o criză alimentară de proporții, „fiind posibil ca mai mulți oameni să moară din cauza impactului economic decât din cauza virusului[31]". ONU estimează că aproximativ 130 de milioane de persoane se vor confrunta pe viitor cu această criză. David Beasley, director al World Food Programme, afirmă că pe lista celor care suferă din pricina lipsei de alimente în acest moment se vor mai adăuga cei care provin din 36 de țări, printre care Yemen, R.D. Congo, Afganistan, Venezuela, Etiopia, Sudanul de Sud, Sudan, Siria, Nigeria, Haiti. Zece dintre aceste țări au peste 1 milion de oameni care se confruntă cu foametea. Motivele sunt existența zonelor de conflict, recesiunea economică, declinul cantității de ajutoare şi prăbuşirea prețului petrolului.

Bibliografie:

1. „A murit futurologul şi scriitorul Alvin Toffler. Ce-a prezis pentru următorii 40 de ani", în Anaarecarti.ro (30 iunie 2016), accesat la 19.10.2018, ora 15.14.
2. BOUDON, Raymond, *Efecte perverse şi ordine socială*, Editura Eurosong, 1998.
3. BRYNJOLFSSON, Erik; McAFEE, Andrew, *The second Machine Age Work, Progress and Prosperity in a Time of Brilliant Technologies*, 2014.
4. KISSINGER, Henry, „Interviu*"*, *Financial Times*, 19.07.2018.
5. „Pandemia de coronavirus ar putea schimba calculele Federației Ruse în Orientul Mijlociu", *Al Jazeera*, 14.04.2020, accesat la 15.04.2020, ora 11.
6. FLORIDI, Luciano, *The Fourth Revolution: How the Infosphere is Reshaping Human Reality,* Oxford University Press, 2014.
7. FRIEDMAN, Thomas L., *Thank you for being late. An optimist's Guide to thriving in the age of accelerations,* Penguin Books, Marea Britanie, 2017.
8. „COVID-19: va afecta aceasta ordinea globală?", în *Eurasia Review*, 18.04.2020.
9. „Pandemia de coronavirus va provoca o foamete de proporții biblice", avertizează ONU. *Digi24.ro,* 22.04.2020, accesat la 13.05.2020, ora 11.00.
10. PÂRLOG, Adriean, „Riscuri existențiale succesive de tip cauză-efect. Pandemia şi criza economică, în derulare. Urmează cea politică?" *Financialintelligence.ro*, 02.04.2020, accesat la 07.04.2020, ora 18.00.
11. PICHETA, Rob, „Coronavirus pandemic will cause global famines of biblical proportions", *UN warns*, *CNN*, 22.04.2020, accesat la 13.05.2020.
12. POPESCU, Virgil, „Economia are o contracție de 30-40%", interviu pentru *Radio România Actualități,* 13.04.2020, preluat de Agerpres şi *financialintelligence.ro,* accesat la 14.04.2020, ora 11.30.
13. ISCHINGER, Wolfgang, declarație în cadrul conferinței *The Challenges of the Pandemic to democratic World*, organizată online de New Strategy Center, accesată pe contul de Facebook al Excelenței sale, dl. Sorin Ducaru la 16.04.2020, ora 10.00.

14. *Secretarul general al ONU: consider că doar un vaccin ar permite revenirea la normalitate*, financial intelligence.ro, 16.04.2020, accesat la 16.04, ora 10.32.
15. ULGEN, Sinan „The Coronavirus is Creating a Crisis on Europe's Borders" în *Foreign Policy,* 01.05.2020, accesat la 12.05.2020, ora 16.25.
16. TOOZE, Adam, *The normal economy is never coming back,* 09.04.2020, foreignpolicy.com, accesat la 13.04.2020, ora 8.50.
17. UNTEANU, Cristian, „După miza cine va lansa primul om în spațiu acum cine va breveta primul vaccin pentru Covid-19", 09.04.2020, *Adevărul. ro*, accesat la 13.05.2020, ora 10.40.
18. SIMES, Dimitri Alexander, „Will Russia Be the real Loser in the New US-China Cold War?", în *The National Interest*, 02.05.2020, accesat la 12.05.2020, ora 16.20.

[1] Interviu acordat publicației *Financial Times* la 19.07.2018, referitor la schimbarea mondială în contextul evoluției rapide.

[2] Concept implementat de Andrew McAfee şi Erik Brynjolfsson - profesori de business la Massachusets Institute of Technology (MIT) şi care se referă la trăsăturile definitorii ale actualului context evolutiv. Potrivit acestora, „simultan, nu doar că lucrurile se schimbă cu viteză, dar şi viteza cu care lucrurile se schimbă este în creştere continuă". Erik Brynjolfsson, Andrew McAfee, *The second Machine Age Work, Progress and Prosperity in a Time of Brilliant Technologies*, 2014.

[3] Luciano Floridi, *The Fourth Revolution: How the Infosphere is Reshaping Human Reality,* Oxford University Press, 2014, introduction.

[4] „A murit futurologul şi scriitorul Alvin Toffler. Ce-a prezis pentru următorii 40 de ani", în Anaarecarti.ro (30 iunie 2016), accesat la 19.10.2018, ora 15.14.

[5] Citat în Thomas L. Friedman, *Thank you for being late. An optimist's Guide to thriving in the age of accelerations,* Penguin Books, Marea Britanie, 2017, p.29.

[6] Idem, p. 30.

[7] Idem, p 33.

[8] Raymond Boudon, *Efecte perverse şi ordine socială*, Editura Eurosong, 1998.

[9] Idem, p. 29-33.

[10] Edward de Bono, *Cursul de gândire al lui Edward de Bono – instrumente eficiente pentru a vă transforma modul de gândire,* Bucureşti, Editura Curtea Veche, 2009.

[11] Idem.

[12] Virgil Popescu, „Economia are o contracție de 30-40%", interviu pentru Radio România Actualități,13.04.2020, preluat de Agerpress şi *financialintelligence.ro*, accesat la 14.04.2020, ora 11.30.

[13] Adriean Pârlog, *Riscuri existențiale succesive de tip cauză-efect. Pandemia şi criza economică, în derulare. Urmează cea politică?,* în *Financialintelligence.ro*, 02.04.2020, accesat la 07.04.2020, ora 18.00.

[14] Xin Zhang, expert privind relațiile chinezo-ruse în cadrul „East China Normal University" din Shanghai: „dacă relațiile dintre SUA şi R.P. Chineză se întrerup cu adevărat, în loc să fie doar o etapă în cadrul negocierilor, atunci R.P. Chineză îşi va direcționa atenția către F.Rusă şi Eurasia drept potențiale destinații pentru reorganizarea lanțurilor de producție industrială", citat din *Will Russia be the real Loser in the New US-China Cold War*?, în *The National Interest*, 02.05.2020, accesat la 12.05.2020, ora 16.20.

[15] Retragerea SUA din Parteneriatul Trans-Pacific, retragerile masive ale trupelor din Irak şi Siria, adoptarea de măsuri protecționiste în problemele economice şi participarea semnificativ redusă în cadrul instituțiilor internaționale multilaterale.

[16] *Foreign Policy* menționează câteva argumente similare: „Turcia, Ucraina, Egipt şi Maroc, state, în general, cu venituri medii, nu beneficiază de inițiativele globale cum ar fi programele de reducere a datoriilor conduse de Fondul Monetar Internațional, care vizează statele mai puțin dezvoltate. (…) acestea nu dispun de resursele interne pentru a-şi reveni din recesiunea majoră care va urma. Nivelul în creştere al aversiunii față de riscuri de pe piețele globale le-a limitat acestora opțiunile privind datoriile. Bunăstarea lor economică a fost într-o măsură şi mai mare subminată de recesiunea economică provocată de pandemia COVID-19", citat din articolul „The Coronavirus is Creating a Crisis on Europe's Borders", în *Foreign Policy,* 01.05.2020, accesat la 12.05.2020, ora 16.25.

[17] Idem.

[18] Adam Tooze, „The normal economy is never coming back", 09.04.2020, *foreignpolicy.com*

[19] Adriean Pârlog, „Riscuri existențiale succesive de tip cauză-efect. Pandemia şi criza economică, în derulare. Urmează cea politică?", *Financialintelligence.ro*, 02.04.2020, accesat la 07.04.2020, ora 18.00

[20] Idem

[21] Idem

[22] Ambasador Wolfgang Ischinger, preşedintele Conferinței de Securitate de la München, *The Challenges of the Pandemic to democratic World*, conferință organizată online de New Strategy Center, declarație accesată pe contul de Facebook al Excelenței Sale dl. Sorin Ducaru la 16.04, ora 10.00.

[23] Virgil Popescu: „Economia are o contracție de 30-40%“, interviu pentru Radio România Actualități la 13.04.2020, preluat de Agerpres și *financialintelligence.ro,* accesat la 14.04.2020, ora 11.30.

[24] Tot *Foreign Policy* atenționează asupra unui efect imediat al pandemiei: grava afectare a turismului - un mijloc semnificativ de venit pentru multe dintre statele din sudul şi estul Europei. „În 2018, ponderea veniturilor din turism în totalul exporturilor de bunuri şi servicii a atins 41% în Iordania şi 25% în Egipt, potrivit Organizației Mondiale a Turismului a ONU. În cifre absolute, cel mai înalt nivel al veniturilor Turciei provenite din turism, inclusiv transportul internațional, a fost de 37 miliarde USD, ceea ce înseamnă aproximativ 5% din PIB. Această sursă importantă de venit urmează să dispară pe fondul pandemiei. Colapsul industriei turistice va avea, de asemenea, repercusiuni semnificative pentru menținerea numărului de locuri de muncă. Pentru Iordania, Maroc şi Tunisia, turismul asigura aproximativ 7% din numărul total al locurilor de muncă, comparativ cu ponderea medie globală de 3,8%”.

[25] „Secretarul general al ONU: consider că doar un vaccin ar permite revenirea la normalitate”, *financialintelligence.ro*, 16.04.2020, accesat la 16.04, ora 10.32.

[26] Adam Tooze, *The normal economy is never coming back,* 09.04.2020, foreignpolicy.com, accesat la 13.04.2020.

[27] Opinie a premierului din Singapore detaliată în articolul „Lumea după pandemia de COVID-19: va afecta acesta ordinea globală?”, în *Eurasia Review*, 18.04.2020.

[28] Cristian Unteanu, „După miza cine va lansa primul om în spațiu, acum cine va breveta primul vaccin pentru Covid 19”, 09.04.2020, *Adevărul.ro*, accesat la 13.05.2020, ora 10.40.

[29] Idem.

[30] „Centrul Național de Cercetare în virusologie şi biotehnologie VEKTOR din Novosibirsk, F.Rusă, a anunțat că urmăreşte lansarea testelor clinice pentru trei vaccinuri experimentale începând cu 29 iunie. Moderna Therapeutics din SUA a anunțat că la 16 martie a lansat primul test clinic de amploare, administrând un produs unui grup de 45 de voluntari o dată la 30 de zile. Procedura a fost criticată de Institutul Pasteur, calificând-o drept în contradicție cu reglementările internaționale care spun că nu poate fi testat pe oameni un vaccin a cărui eficiență nu a fost dovedită. Compania NOVAVAX din Maryland va efectua un test cu un prototip de vaccin testat în faza preclinică la jumătatea lunii mai. China a început etapa clinică a testelor pe oameni la 17 martie. OMS a demarat operațiunea Solidarity, prin care 90 de companii farmaceutice îşi propun o testare clinică la nivel internațional pentru găsirea unui tratament eficient pentru COVID 19”. Citat din Cristian Unteanu: „După miza cine va lansa primul om în spațiu, acum cine va breveta primul vaccin pentru COVID 19”, 09.04.2020, *Adevărul.ro*, accesat la 13.05.2020, ora 10.40.

[31] „Pandemia de coronavirus va provoca o foamete de proporții biblice, avertizează ONU”, *Digi24.ro*, 22.04.2020, accesat la 13.05.2020, ora 11.30, preluând date din Rob Picheta, 22.04.2020, „Coronavirus pandemic will cause global famines of biblical proportions, UN warns”, *CNN*, accesat la 13.05.2020, ora 11.30.

INTELLIGENCE VERSUS FAKE NEWS ÎN CONTEXTUL COVID-19

Marian ŞTEFAN*

Abstract

Within the current geo-strategic context, a decreasing trend of the conventional threats (violent military conflicts generated by state entities) is registered, while unconventional threats - called hybrid threats, are increasing. These "threats without enemies", considered a "gray area" within the international security studies, tend to be much more ambiguous in their complexity, processes and effects, therefore highly perceived as risks and vulnerabilities to some systems.

Among these threats, "problems without a passport" have been identified - clearly transnationally originated, not assumed by any state/non-state entity/organization and impossible to be defeated by conventional military means.

Keywords: *medical crisis, security, threats, disinformation.*

Crizele medicale şi securitatea umană

Unul dintre cei mai importanți factori de risc din categoria celor neconvenționali îl reprezintă pandemiile[1], afirmație susținută şi de faptul că bolile infecțioase reprezintă încă o cauză principală de mortalitate în lume, fiind responsabile de aproximativ 17 milioane de decese anual. Dezbaterea internațională în legătură cu faptul dacă pandemiile sunt sau nu riscuri de securitate pentru sistemul internațional datează de cel puțin 50 de ani. Confruntarea de idei are un numitor comun şi anume modul în care pandemiile, naturale sau deliberat provocate, afectează stabilitatea economică, socială şi politică internă a statelor şi, nu în ultimul rând, relațiile dintre state atunci când răspândirea unei boli nu poate fi stopată în interiorul frontierelor unui stat. Deloc întâmplător, în cadrul Strategiei HIV/AIDS a Departamentului de Stat al SUA, din anul 1995, bolile infecțioase sunt considerate a avea potențialul de a „iniția conflicte" şi chiar de a „determina felul în care se vor încheia războaiele".

În contextul unor astfel de provocări la adresa securității internaționale se evidențiază o deplasare a abordării teoretice a conceptului de „securitate" de la componenta de analiză strict militară către o interpretare mai cuprinzătoare a interdependenței dintre factorii de risc şi amenințările convenționale, pe de o parte, şi cele neconvenționale, pe de altă parte[2] (Şcoala de la Copenhaga – reprezentanți principali Barry Buzan, Ole Waever şi Jaap de Wilde).

Conceptul de „securitate umană", intrat în dezbaterea internațională odată cu introducerea sa în „Raportul pentru Dezvoltare Umană" al Adunării Generale a Organizației Națiunilor Unite (1994), consideră că protecția personală a individului nu rezultă doar din apărarea securității unui stat, ci şi din asigurarea

Expert în cadrul Ministerului Apărării Naționale.

accesului cetățeanului în mod adecvat la bogăție şi creşterea standardului de viață. Raportul propune o schimbare profundă de paradigmă şi trecerea de la „securitatea nucleară la securitatea umană", în sensul de rezolvare a „problemelor cronice precum foametea, bolile şi represiunea" şi protejarea față de „modificările abrupte ale vieții cotidiene domestice, la locul de muncă şi în comunitate", ameninţări care pot afecta societățile la orice nivel indiferent de gradul de dezvoltare sau venit[3]. Astfel, devine clar că orice ameninţare a calității vieții, diminuarea accesului la sănătate, educație, drepturi etc., este considerată o ameninţare de securitate.

Reversul este de asemenea adevărat – îmbunătățirea protecției şi calității vieții cetățeanului se va reflecta şi în gradul de securitate al statului, după cum remarca, în anul 2018, Secretarul General al ONU în exercițiu, Antonio Guterres: *„Securitatea umană, securitatea naţională şi securitatea globală sunt indivizibile. Atunci când oamenii se tem pentru viețile lor, comunitățile, societatea şi țările sunt expuse unui risc mai crescut. Când oamenii se bucură de siguranță, la fel şi țările lor şi întreaga lume"*[4]. Ecoul acestei declarații îl regăsim în mesajul Secretarului General adresat comunității internaționale în contextul pandemiei actuale (13 martie 2020): *„Controlul pandemiei…necesită o implicare personală, naţională şi internaţională fără precedent. Trebuie să declarăm război acestui virus. Acest lucru înseamnă că țările au obligația să accelereze, să intervină şi să extindă. (...) şi noi toți avem o responsabilitate de asemenea. (...) Prevenirea extinderii COVID-19 este o responsabilitate comună pentru noi toți."*

Securitatea medicală *(health security),* una dintre componentele securității umane care are în vedere mai ales *„dinamicile obişnuite ale relațiilor internaționale şi dinamicile speciale determinate de ameninţarea microbilor patogeni"*[5], prezintă un interes deosebit şi pentru studiile de securitate.

Bolile infecțioase reprezintă o ameninţare la adresa securității economice, stabilității politice şi vieții sociale şi încetinesc dezvoltarea democratică a statelor afectate pe o perioadă îndelungată, generând intensificarea stării de tensiune politică între țări din cauza embargourilor, boicoturilor, pierderilor comerciale şi nerespectării unor acorduri internaționale, precum şi a disputelor asupra unor resurse medicale esențiale (medicamente, vaccinuri, materiale sanitare, aparatură medicală performantă).

Pandemia COVID-19 demonstrează pe deplin că scenariile de tip *wild card* sunt reale, într-o lume obsedată de capacitățile inteligenței artificiale, a descoperirilor cuantice, călătoriilor spațiale, vehiculelor autonome etc., care nu a putut concepe, chiar şi în condițiile unor avertismente repetate, magnitudinea consecințelor produse de astfel de ameninţări „medievale". Ignorarea repetată de către decidenți sau percepțiile generale că astfel de crize medicale sunt evenimente uşor surmontabile, care determină turbulențe regionale sau globale limitate, recuperabile într-o perioadă redusă de timp, nu modifică cu nimic probabilitatea lor de materializare, însă contribuie la lipsa de reziliență societală şi reacție rapidă.

În contextul pandemiei COVID-19, considerăm că elaborarea unei viziuni securizatoare pe termen îndelungat, care să reprezinte o componentă permanentă şi acționabilă a strategiilor de securitate şi politicii externe naționale, trebuie să abordeze în mod prioritar „problemele fără frontiere", aşa cum sunt conceptualizate de către „securitatea umană". În acest sens, considerăm că se impune, în mod accelerat, regândirea competențelor postuniversitare cu scopul de a selecta şi forma experți în cadrul unor programe interdisciplinare de securitate medicală şi diplomație a sănătății globale (sănătate publică, drept, diplomație etc.). În absența unei resurse umane înalt calificate şi loiale, care să poată fi coagulată sub forma unor instituții adecvate provocărilor contemporane, ne vom regăsi în imposibilitatea de a anticipa, preveni şi reacționa rapid la viitoarele crize medicale şi de mediu[6].

Medical intelligence – de la informația epidemiologică la salvarea de vieți

Complexitatea problemelor de sănătate globale şi, în special, posibilitatea generalizării

epidemiilor cu risc înalt, i-a determinat pe experţi să lanseze un semnal de alarmă referitor la capacitatea redusă de reacţie în timp real, obţinerea datelor tehnice verificate, integrarea informaţiilor provenite din surse multiple, colaborarea internaţională şi interdisciplinară, coordonarea reacţiilor de răspuns etc.. Nevoia de a fuziona rapid informaţii actualizate, provenite din mai multe domenii ştiinţifice şi surse credibile, de a genera „ştiinţe şi teorii de problemă", de a forma echipe interdisciplinare, parteneriate inter-instituţionale şi internaţionale etc., a determinat apariţia unor structuri cu rol anticipativ-preventiv, de tip intelligence: *medical*-, *public health*-, *epidemic/infectious diseases intelligence*.

Denumirea de *Public Health Intelligence* este atribuită cel mai frecvent unor instituţii civile specializate în identificarea timpurie a potenţialelor ameninţări pentru sănătatea publică, evaluarea şi investigarea acestora, cu scopul de a realiza propuneri şi măsuri destinate prevenţiei şi controlului. Există încă o discuţie la nivelul organismelor internaţionale şi autorităţilor naţionale dacă aceste structuri să fie concepute strict pentru a monitoriza riscurile epidemiologice sau să se adreseze unui spectru mai larg de ameninţări pentru sănătatea umană[7].

Cele mai importante direcţii de acţiune în domeniul prevenirii şi combaterii bolilor infecţioase sunt date de formarea, sub auspiciile Organizaţiei Mondiale a Sănătăţii (OMS), a Global Outbreaks Alert and Response Network/ GOARN şi semnarea noului acord inter-guvernamental International Health Regulations – IHRs, confirmând astfel recunoaşterea, la nivel de guverne, a necesităţii acordării unei atenţii prioritare realizării unui cadru conceptual global şi a construirii de reţele de monitorizare şi control a bolilor infecţioase, prin crearea şi/sau îmbunătăţirea sistemelor naţionale de control al bolilor epidemice.

La nivelul Uniunii Europene, The European Centre for Disease Prevention and Control (ECDC), instituţie de tip *infectious diseases intelligence*, este responsabilă de alerta epidemiologică timpurie la nivel comunitar. ECDC colectează date obţinute din sistemele naţionale de supraveghere epidemiologică pentru a le analiza în cadrul Sistemului European de Supraveghere (European Surveillance System/ TESSy), rezultatele relevante fiind comunicate autorităţilor naţionale de sănătate publică prin intermediul Sistemului de Alertă Timpurie şi Răspuns (Early Warning and Response System/ EWRS).

Printre priorităţile organismului comunitar se află: determinarea unor noi metode de identificare rapidă a epidemiilor produse de boli emergente şi re-emergente, îmbunătăţirea capacităţilor de răspuns în mod coordonat pe teritoriul mai multor state europene, eficientizarea comunicării cu structurile naţionale care prezintă capacităţi similare, îmbunătăţirea capacităţii de analiză şi previzionare strategică.

Un rol deosebit de important, alături de organismele internaţionale, comunitare şi intra-statale, îl au şi instituţiile private de tip centre de analiză, sondare a opiniei publice, *think-tank*-uri consacrate, corporaţii, mediile academice specializate în realizarea de estimări profunde referitoare la riscurile de natură medicală şi de mediu, inclusiv în arii geografice îndepărtate. În absenţa unor capacităţi proprii, astfel de servicii private pot completa cunoaşterea existentă, deşi costurile pot fi, în unele situaţii, prohibitive.

Datorită numărului foarte mare de necunoscute şi, mai ales, multiplelor interdependenţe neliniare şi contraintuitive, care limitează inclusiv simulările complexe realizate cu cele mai avansate programe informatice şi supercomputere, analiza problematicii întâlnite în crizele medicale şi de mediu necesită echipe interdisciplinare de analişti, cu un grad ridicat de neurodiversitate şi „asimetrie cognitivă", capabile să genereze şi să integreze în produsul analitic final abordări inovatoare sau poziţii tranşante argumentate[8].

Ce este „medical intelligence"?

Medical Intelligence (*MEDINT*) are drept scop (conform definiţiei Departamentului Apărării din SUA) colectarea, evaluarea, analiza şi interpretarea informaţiilor externe de natură medicală, ştiinţifice şi despre mediul înconjurător

care prezintă interes din perspectiva planificării militare strategice şi a celei medico-militare a forţelor proprii şi aliate, precum şi evaluarea capacităţilor medicale civile şi militare din alte ţări[9].

NATO adoptă o definiţie mai generală, considerând structurile de medical intelligence o componentă informativă specializată şi, în general, cu dimensiuni reduse, care, deşi este implicată în activitatea de monitorizare globală a riscurilor medicale, este dedicată servirii intereselor strategice naţionale[10].

Profilul acestor entităţi de „medical intelligence" poate varia în funcţie de estimarea necesităţilor, de resursele disponibile, colaborări şi parteneriate, de tradiţia şi cultura instituţională dominantă etc. – de la servicii distincte aflate în componenţa unor agenţii de intelligence (cazul SUA – The National Center for Medical Intelligence, componentă a Defense Intelligence Agency/DIA[11]), la nuclee reduse de specialişti militari şi civili care pot apela la capacităţi de intelligence naţionale şi instituţii civile pentru rezolvarea unor situaţii bine definite.

În esenţă, rolul unei astfel de structuri este de a solicita, colecta/obţine şi analiza informaţiile din toate sursele (deschise, confidenţiale, obţinute prin metode specifice de intelligence – HUMINT, IMINT, SIGINT etc.) pentru a genera cunoaştere acţionabilă pentru decidentul politic şi a câştiga timpul necesar reorganizării activităţii serviciilor naţionale implicate în gestionarea unei crize medicale şi informarea timpurie a populaţiei. Flexibilitatea de acţiune, precum şi utilizarea unor canale rapide de informare permit realizarea unor estimări de tip avertizare timpurie (*early warning*), prognoze şi planuri de măsuri[12].

Se estimează că principalele direcţii de activitate ale structurilor de medical intelligence sunt: monitorizarea la scară globală a focarelor epidemice; identificarea şi monitorizarea riscurilor epidemiologice care pot afecta securitatea cetăţenilor şi pe cea naţională; dezvoltarea capacităţilor naţionale cu rol în rezolvarea unei crize medicale; controlul diseminării biotehnologiilor, echipamentelor duale, tehnologiilor informatice sau a cunoaşterii în domeniul producerii de arme biologice, chimice, radiologice către actori non-statali ostili; protejarea împotriva spionajului economic în instituţiile de cercetare biomedicală; prevenţia cyber-atacurilor cu efecte biologice şi protecţia cibernetică a instituţiilor-cheie (infrastructurii critice) cu rol în gestionarea unei crize medicale; promovarea culturii de securitate în domeniul sanitar şi identificarea de parteneri în societatea civilă; cooperarea cu structuri naţionale şi internaţionale cu preocupări şi capacităţi similare etc.

Abordarea şi strategia din spatele acestor structuri de tip *medical intelligence* se încadrează în tiparul organizaţiilor de intelligence din cea de-a patra generaţie[13], ca răspuns adaptativ la volatilitatea mediului tradiţional de securitate şi la ambiguitatea rezultată din erodarea graniţelor dintre virtual şi real, intern şi internaţional, comercial şi militar, pace şi conflict.

Această paradigmă de gândire îşi propune să realizeze fuziuni între aptitudinile umane tradiţionale şi progresul tehnologic accelerat, noi parteneriate şi abordări care asimilează diversitatea şi oferă posibilitatea de afirmare generaţiei tinere.

Capacitatea de a colabora în cadrul unor echipe dinamice, de a accesa orice mediu socio-profesional, utilizarea maximală a mediului tehnologic şi a avantajelor asimetrice subliniază, încă o dată, importanţa capacităţilor naţionale, a resursei umane de excepţie, a profesionalismului şi a loialităţii.

Răspândirea COVID-19 a devenit una dintre cele mai puternice crize mondiale. Dincolo de impactul direct asupra sănătăţii populaţiei, COVID-19 creează efecte economice, sociale şi geopolitice, unele evidente şi imediate, altele încă neclare şi pe termen lung.

Cu siguranţă că trăim în timpuri VUCA (*Vulnerability, Uncertainty, Complexity, Ambiguity*), cum ar spune cei care lucrează în managementul afacerilor. Covid-19 ne-a arătat cât suntem de vulnerabili cu toţii, că suntem egali în vulnerabilitate indiferent de organizaţie, stat sau zonă geografică. Suntem, în general, slab pregătiţi pentru a face faţă unui asemenea

duşman nevăzut. Am putut constata ezitările, întârzierile, limitările deciziilor luate de către guverne şi diferite autorităţi şi am putut vedea şi diferenţele dintre metodele adoptate de către acestea. Preşedintele american, Donald Trump, a luat decizia de a interzice călătoriile dintre SUA şi UE, fără a da un aviz prealabil europenilor şi a fost dispus să cumpere spre beneficiul exclusiv american patentul tratamentului antivirus din Germania, oferind un miliard de dolari. Ambasadorii Chinei din întreaga lume răspândesc, în mod oficial, ştirea potrivit căreia la originea pandemiei se află un complot american. Statele membre ale Uniunii Europene au dovedit întâi un reflex naţional şi abia pe urmă reflexe comunitare.

Incertitudinea este o altă caracteristică a acestei crize. Nu ştim când se va termina criza sanitară, nu ştim ce efecte pe termen mediu şi lung va avea în termeni economici, pentru România, pentru Europa, şi, în ultimă instanţă, nu ştim ce efecte va avea asupra propriei noastre vieţi şi aceasta pentru că trăim într-o lume interconectată, pentru că ceea ce ni se întâmplă nouă depinde de acţiunile celorlalţi. Nici nu se putea concepe o situaţie mai bună din care să învăţăm că acţiunile noastre au efecte majore şi, în acelaşi timp, pot avea efecte letale asupra altor oameni.

Fenomenul *fake news* în contextul pandemiei COVID-19

România este ţinta a două mari ameninţări: virusul SARS-CoV-2 şi mesajele de propagandă de tip fake news ruseşti. Sunt numeroase persoane şi instituţii ce propagă, voit ori sub impulsul panicii de moment, pe diferite platforme de socializare, mesajele infectate, de genul: „Rusia şi China oferă ajutor Italiei”, „Europa a abandonat Italia”, „Europa nu ajută România”, „Franţa primeşte 300 miliarde euro şi România doar un miliard” şi multe altele. Toate aceste ştiri au fost demontate argumentat atât de Comisia Europeană, cât şi de statele menţionate. Însă, orice încercare ulterioară de a prezenta adevărul are un impact de 10 ori mai mic decât minciuna deja propagată.

În momentul de faţă, NATO şi-a asumat rolul de generator de securitate în faţa oricăror ameninţări la adresa securităţii statelor membre şi este puternic implicată în operaţiuni militare desfăşurate în sprijinul populaţiilor şi sistemelor medicale aliate: spitale de campanie instalate, zboruri militare pentru aducerea de teste şi echipamente medicale, medici militari alături de medici civili, întărirea sprijinului pentru poliţia de frontieră, cea rutieră şi de ordine publică, echipamente create de inventatorii militari şi multe altele. În acest context, Comandamentul

armatei americane în Europa a trimis un ajutor medical de urgență Lombardiei, cu avioane militare. Comisia Europeană a decis alocarea celui mai consistent ajutor financiar pe plan mondial, 37 miliarde euro pentru toate statele membre UE în lupta împotriva pandemiei; deschiderea unor culoare speciale în spațiul european pentru fluxul alimentelor şi medicamentelor; suspendarea efectelor Tratatului UE privind deficitele naționale, pentru ca țările să poată cheltui masiv în domeniul medical; redirecționarea unor miliarde de euro din fondurile europene spre domeniul medical şi de sănătate din țările membre; sprijin medical şi militar între țările UE grav afectate de COVID-19 (Germania preia pacienți din Italia) şi multe altele.

În pofida realităților evidente şi observabile, un aflux de mesaje false, instigatoare şi bine ambalate în sens manipulator, a invadat Internetul. Prin lecturi şi lecții învățate, prin experiența dobândită în ani de bătălie cu agresiva campanie *fake news* a F.Ruse, trebuie să ne asumăm lupta pe două direcții de acțiune simultan: combaterea virusului SARS-CoV-2 şi combaterea virusului propagandistic virtual.

Dezinformare şi infectare

Specialiştii ciberneticieni europeni au identificat sute de ştiri false de origine rusă referitoare la tema COVID-19. Multe amintesc de propaganda Războiului Rece, scrie Deutsche Welle.

Acum, lumea cu toate aspectele sociale, economice şi chiar politice s-a relocat în mediul virtual, astfel încât am ajuns să avem lecții şi cursuri online, programe de asistență socială virtuale, sfaturi economice, fiscalitate şi detalii bugetare virtualizate şi şedințe, comisii şi adunări parlamentare în videoconferință.

Organizația Mondială a Sănătății (OMS) vorbeşte deja despre o *infodemie* în legătură cu noul coronavirus. Nu numai virusul se propagă în lumea întreagă, ci şi o cantitate din ce în ce mai mare de informații. Cu toate acestea, multe informații sunt dezinformare pură şi sunt folosite ca mijloc de exercitare a influenței politice. Iar Rusia este deosebit de activă în acest domeniu.

Un raport al grupului operativ de comunicare strategică al Serviciului European de Acțiune Externă (SEAE) a identificat sute de cazuri de dezinformare în actuala criză. Numai între 22 ianuarie şi 19 martie 2020 au existat 110 ştiri false de origine rusească despre coronavirus. Autorii şi mesajele sunt întotdeauna aceleaşi şi au o lungă tradiție în sistemul de influență rusă în străinătate.

Deutsche Welle[14] a prezentat, încă de la începutul lunii martie, pe portalul publicației, exemple de dezinformări şi ştiri false despre noul coronavirus. Conform raportului UE, actuala campanie rusă de dezinformare se concentrează cu precădere pe un aspect: o presupusă origine artificială a virusului, care ar fi folosit în scopuri politice minore.

Platforme informatice precum „southfront.org" sau „RT" şi „Sputnik" sunt deseori citate de UE ca inițiatori şi multiplicatori ai acestui mesaj. Uneori, aceste ştiri false propagă mesaje de genul „elitele secrete se află înspatele pandemiei", „SUA sunt generator de arme biologice" sau „industria farmaceutică are interese obscure".

Potrivit evaluărilor UE, obiectivele acestei campanii de dezinformare sunt clare: crearea de confuzie, slăbirea încrederii în guverne, mass-media, autorități, sisteme de sănătate publice şi în capacitatea de răspuns a acestora, crearea neîncrederii şi a discordiei la nivelul UE, precum şi între statele membre şi SUA[15].

Prezentare generală a relatărilor false în tendință actuală

- Coronavirusul este o armă biologică desfăşurată alternativ de China, SUA, Marea Britanie sau chiar Rusia (cu scopul de a distruge UE şi NATO);
- Pandemia nu a izbucnit în Wuhan, China - SUA îşi ascund adevărata origine, care este, de fapt, laboratoarele americane din întreaga lume;
- Focarul a fost cauzat de migranți, iar migranții răspândesc virusul în UE;
- Coronavirusul este legat de tehnologia 5G (de exemplu, Wuhan ca teren de testare 5G);

- UE nu a reuşit să gestioneze criza - UE este un dezastru pentru Europa/ nu este pregătită să ofere sprijin urgent statelor sale membre - în schimb, acestea trebuie să se bazeze pe sprijin extern (de exemplu, Italia), China fiind menționată cel mai adesea drept sursa unei astfel de asistențe;
- China vine să salveze UE pe măsură ce Bruxelles abandonează statele membre ale UE;
- Schengen nu mai există - europenii sunt în carantină, dar migranții se pot deplasa liber;
- Coronavirusul este o farsă, nu există;
- UE ar putea impune vaccinări în masă;
- Leacuri: susține că există remedii naturale pentru vindecarea virusului, care sunt adesea combinate cu narațiuni anti-vaccinare;
- Diverse teorii conspirative: predicții istorice despre pandemie, ciumele care lovesc planeta, încercări secrete de „stat profund" de a controla creşterea populației, pandemia fiind cauzată de *chemtrails,* sau care duc la cel de-al treilea război mondial.

Actuala criză sanitară oferă posibilitatea de a analiza mecanismele de funcționare a dezinformării ruseşti, dusă, în timp, la rang de artă operativă. În principiu, motorul de propagandă al fostei Uniuni Sovietice, utilizat în continuare de către structuri oficiale ale statului rus şi de către serviciile de informații, a folosit trei tipuri de dezinformare: albă, gri şi neagră. Propaganda *albă* provine de la canale de stat, structuri departamentale (ex: Ministerul de Externe) sau departamentele de

informare ale instituțiilor de stat. Exemple de propagandă *gri* practică radio difuzorul rus „RT" şi portalul de ştiri „Sputnik". Deşi par să fie instituții media civile, acestea sunt considerate o portavoce neoficială a mesajelor Kremlinului, paravane ale serviciilor de informații şi platforme de multiplicare a mesajelor de intoxicare. Propaganda *neagră* este de departe cea mai complicată, deoarece are loc în secret. În limbajul profesional al serviciilor de intelligence ruse, acest tip de propagandă vizează conceptul denumit *măsuri active,* constând în lansarea deliberată de informații false, pe jumătate adevărate sau distorsionate, neatribuite unor organizații din spațiul rus. Aceste entități, ori vectori de propagare aparținând diviziei de trolli, au la dispoziție resurse importante şi beneficiază de avantajul istoric al geopoliticii: în perioada comunistă au fost create numeroase edituri, oficii de informare, ziare, reviste sau broşuri pe întreg spațiul de influență sovietică. Cu toate acestea, principala modalitate de difuzare a dezinformării s-a realizat utilizându-se canale secrete, „agenți de influență" sau vectori de opinie. În actuala eră digitală, această metodă complicată şi lentă de intoxicare şi îndoctrinare s-a adaptat, transformându-se odată cu avantajul tehnologic într-o adevărată armată virtuală. Serviciul rus de informații FSB utilizează adevărate *„fabrici de trolli*", camuflate în companii şi ONG-uri care utilizează programe software şi specialişti IT, pentru a „planta", a aprecia (cu "like"), a distribui şi a trimite informații şi mesaje pe platforme de socializare, site-uri şi publicații online, utilizate din ce în ce mai mult de către marea masă a oamenilor autoizolați în lumea virtuală.

Concluzii

F.Rusă exploatează contextul crizei sanitare pentru a contribui la panica generală şi confuzia din Uniunea Europeană, folosind armele obişnuite – *fake news* şi dezinformare. Experții UE au înregistrat peste 100 de cazuri de dezinformare legată de virus în ultimele două luni, inclusiv afirmațiile potrivit cărora virusul este o armă biologică fabricată în Occident. Trusturi de presă şi portaluri precum *Russia Today*, *Sputnik*, *News Front*, *Oriental Review*, *Geopolitika.ru* şi altele sunt folosite pentru a continua războiul informațional. Miza este, ca de fiecare dată, obținerea unor avantaje strategice, spații, zone, arii de influență, controlul infrastructurilor critice şi dependența energetică, transformând astfel criza sanitară globală într-o criză politico-militară pe termen lung.

Bibliografie:

1. CRUCERU, Marin; Carmen Mureşan, *Bioterorismul şi pandemiile: riscuri majore de securitate în secolul XXI*, Bucureşti, Top Form, 2010.
2. STROESCU, Mara, *Pandemia şi viitorul securității medicale. Amenințările „fără paşaport"*, apr. 1, 2020, Analize LARICS.
3. *Raportul pentru Dezvoltare Umană al Adunării Generale a Organizației Națiunilor Unite din anul 1994*, pag. 22-23.
4. https://www.un.org/press/en/1998/19980623.sgsm6609.html
5. https://www.e-ir.info/2013/02/01/towards-a-critical-securitization-theory-the-copenhagen-and-aberystwyth-schools-of-security-studies/Ali Diskaya
6. https://www.un.org/sg/en/content/sg/speeches/2018-05-24/launch-disarmament-agenda-remarks
7. https://www.cfr.org/expert/david-fidler
8. https://www.militaryfactory.com/dictionary/military-terms-defined.asp?term_id=3315
9. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4941003/
10. https://www.dia.mil/coronavirus/
11. https://www.gov.uk/government/speeches/mi6-c-speech-on-fourth-generation-espionage
12. https://www.dw.com/en/coronavirus-and-the-fake-news-outbreak/av-52999958
13. https://eeas.europa.eu/headquarters/headquarters-homepage/75968/eu-action-against-coronavirus

[1] Marin Cruceru, Carmen Mureşan, *Bioterorismul şi pandemiile: riscuri majore de securitate în secolul XXI*, Bucureşti, Top Form, 2010, https://www.geopolitic.ro/19238-2/?fbclid=IwAR0Hk5uM85jjsutXTZWNP5hkZtQz3Dm8HNTf9vIYggt0HPGWTgvtYgv0Yc

[2] https://www.e-ir.info/2013/02/01/towards-a-critical-securitization-theory-the-copenhagen-and-aberystwyth-schools-of-security-studies/ Ali Diskaya

[3] Raportul pentru Dezvoltare Umană al Adunării Generale a Organizației Națiunilor Unite din anul 1994, pag. 22-23

[4] https://www.un.org/sg/en/content/sg/speeches/2018-05-24/launch-disarmament-agenda-remarks

[5] https://www.cfr.org/expert/david-fidler

[6] https://larics.ro/covid-19-pandemia-si-viitorul-securitatii-medicale-amenintarile-fara-pasaport/*COVID-19: pandemia şi viitorul securității medicale. Amenințările „fără paşaport”*, Stroescu Mara, apr. 1, 2020, Analize

[7] Ibidem

[8] Ibidem

[9] https://www.militaryfactory.com/dictionary/military-terms-defined.asp?term_id=3315

[10] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4941003/

[11] https://www.dia.mil/coronavirus/

[12] https://larics.ro/covid-19-pandemia-si-viitorul-securitatii-medicale-amenintarile-fara-pasaport/*COVID-19:pandemia şi viitorul securității medicale. Amenințările „fără paşaport”*, Stroescu Mara, apr. 1, 2020, Analize

[13] https://www.gov.uk/government/speeches/mi6-c-speech-on-fourth-generation-espionage

[14] https://www.dw.com/en/coronavirus-and-the-fake-news-outbreak/av-52999958

[15] https://eeas.europa.eu/headquarters/headquarters-homepage/75968/eu-action-against-coronavirus_en

ABORDAREA PSIHOLOGICĂ A EFECTELOR PANDEMIEI DE COVID-19

*Cristian DOBRE**

Abstract

The article presents a psychological approach to the global pandemic of COVID 19, reviewing both the security imperatives imposed by this pandemic, but, in particular, the relevant psychological aspects, to be considered in the case of such a global infection.The vulnerabilities and psychological recommendations related to the even more effective management of the current pandemic crisis are the strengths of this article.

***Keywords**: corona-virus, COVID 19, pandemic, psychological vulnerabilities, psychological recommendations.*

Provocări la adresa securității aduse de COVID-19

Securitatea națională este un concept generos, care include nu numai chestiunile legate de apărare, ci şi elemente relaționate de independența energetică, exploatarea resurselor naturale, respectarea drepturilor şi libertăților cetățeneşti fundamentale, statul de drept, o justiție liberă, dreptul la educație şi, nu în ultimul rând, sănătatea cetățenilor.

În contextul în care la nivel internațional a izbucnit epidemia de coronavirus, clasificată, ulterior, de Organizația Mondială a Sănătății ca şi pandemie, sănătatea cetățenilor a devenit prioritatea absolută a conducerii de stat şi a întregii administrații centrale şi locale, sprijinite de MAI şi MApN şi alte organizații şi instituții.

Răspândirea cu repeziciune a SARS-CoV-2 şi infectarea populației în progresie geometrică au impus instaurarea stării de urgență, pentru limitarea efectelor devastatoare, înainte de a fi prea târziu.

Dincolo de această criză sanitară fără precedent în istoria omenirii, care a anulat întâlniri la nivel înalt, alegeri, evenimente internaționale, aproape a distrus industria turismului şi pe cea a divertismentului şi sportului, a paralizat Uniunea Europeană, a anulat derularea unor exerciții militare planificate de NATO, oamenilor de rând le este foarte greu să creadă că ceea ce trăiesc este real şi continuă să aibă un reflex de sfidare şi eludare a regulilor.

În acest context extrem de complex, în care prioritatea numărul unu este cea sanitară, psihologiei îi revine misiunea de a înțelege firea umană şi de a acționa, atunci când se impune, în sprijinul reducerii efectelor pandemiei.

Efectele psihologice ale COVID-19

Aşadar, răspândirea rapidă a COVID-19 la nivel planetar şi declararea sa ca şi pandemie de către Organizația Mondială a Sănătății a reprezentat un semnal de alarmă foarte puternic şi serios, atât pentru fiecare structură guvernamentală din lume, cât şi pentru fiecare cetățean al Planetei, în parte.

La puțin timp după răspândirea virusului în Europa şi luarea primelor măsuri oficiale de limitare a sa, psihologii din întreaga lume, inclusiv din România, şi-au oferit serviciile pentru a ajuta la efortul general de eradicare a sa.

***Expert în cadrul Ministerului Apărării Naționale.**

Acest demers se înscrie, fără îndoială, domeniului „psihologiei de urgență”, o ramură a psihologiei generale destinată să ofere suport psihologic în situații dramatice, în care viața noastră normală este puternic perturbată de evenimente pe care nu le putem controla în întregime, cum ar fi: calamități naturale (cutremure, inundații, tsunami, erupții vulcanice, alunecări de teren, secetă etc.), dezastre de toate tipurile (accidente nucleare, chimice, biologice, tehnologice etc.), accidente (aviatice, rutiere, naufragiile, deraierile de trenuri etc.), devastarea produsă de conflictele armate, acțiunile teroriste, pandemiile etc.

Inițiativa de referință a venit în întâmpinarea sau pentru rezolvarea unor probleme pe care din ce în ce mai mulți oameni le întâmpină.

Dacă la începutul epidemiei de COVID-19 cei mai mulți au localizat-o departe, în China, adică departe de preocupările noastre zilnice, de viața noastră, de slujba noastră, de școala copiilor noştri, de părinții şi prietenii pe care fiecare îi are, treptat, coronavirusul s-a apropiat de fiecare dintre noi, mai mult sau mai puțin direct, iar într-un timp extrem de scurt a ajuns să ne conducă viețile – să ne trezim cu școlile închise, cu rafturile magazinelor goale, cu un program de lucru schimbat ori chiar cu pierderea locului de muncă, cu închiderea spațiilor unde ne distram şi relaxam în mod curent (mall-uri, săli de sport, restaurante, hoteluri, teatre, muzee, cinematografe, magazine de haine etc.), cu limitarea posibilității de a călători în concediu şi chiar cu interzicerea părăsirii domiciliului. S-au impus, totodată, în vocabularul nostru curent cuvinte auzite extrem de rar: „stare de urgență”, „izoletă”, „carantină”, „contaminat”, „COVID-19”, „lucrul de acasă”, „dosar penal” etc. Locurile de muncă s-au transformat în adevărate bastioane şi şi-au limitat drastic activitatea curentă la strictul necesar, iar instituțiile de stat, şi nu numai, au pus la dispoziția Comitetului pentru situații de urgență toate resursele la dispoziție.

Liderii mondiali şi-au anulat deplasările şi întâlnirile neesențiale, multe state şi-au închis granițele naționale sau au impus condiții extrem de dure la intrare, s-a interzis exportul de produse sanitare, competiții internaționale şi evenimente mondene (campionate de fotbal, expoziții internaționale, spectacole de modă etc.) - înainte producătoare de milioane de euro - şi-au suspendat activitatea, companiile aeriene şi-au limitat zborurile internaționale, băncile au început să impună politici de austeritate dure, industria turistică s-a prăbuşit, militarii şi-au anulat exercițiile şi aplicațiile planificate, au apărut restricții de circulație chiar în orașe, riguros reglementate şi sancționate, spitalele din numeroase state ale lumii sunt supra-aglomerate, iar medicii sunt depăşiți de complexitatea cazurilor pe care le au de tratat, canalele mass-media difuzează non-stop ştiri cu privire la evoluția coronavirusului şi numărul de îmbolnăviri şi decese, la nivel mondial, mediul virtual a fost inundat de tot felul de *fake news*, serviciile religioase s-au suspendat necondiționat, conaționalii izolați prin cine ştie ce stat al lumii strigă după ajutor, după ce şi-au pierdut locul de muncă. De parcă nu ar fi suficient, mulți experți, bine cotați la nivel internațional, se întrec în a vorbi de efectele post-COVID-19, cu accent pe recesiunea economică ce amenință întreaga Planetă, comparând-o, cu nonşalanță, cu efectele celui de-al Doilea Război Mondial, adăugând, astfel, şi mai mult stres asupra fiecăruia dintre noi.

Totul pare a fi desprins dintr-un scenariu hollywoodian de suspans sau pare a fi un experiment social derulat la scară planetară, în care fiecare dintre noi a devenit, fără voie, subiect de cercetare.

În acest context internațional şi național, extrem de volatil, impredictibil, complex şi ambiguu (VUCA), alături de eforturile naționale pe linie politică, guvernamental-managerială, sanitară, polițienească şi militară, se impune ca o atenție specială să fie acordată şi componentei psihologice.

Dacă majoritatea autorităților statului se adresează, în principal, printr-un sistem bine pus la punct, dar bazat pe resursele limitate avute la dispoziție la un moment dat, problemelor fizice destinate limitării şi eradicării pandemiei (carantină, izolare, tratare), psihologii trebuie să se adreseze, deopotrivă, minții şi sufletului fiecăruia, fie el salvator sau salvat.

Acest demers psihologic îl poate ajuta pe fiecare să înțeleagă mai bine amenințarea reprezentată de COVID-19, să se protejeze pe

sine, în mod rațional, să sprijine autoritățile în mod real pentru limitarea pandemiei, să depășească momentele stresante, să nu devină un factor perturbator în societate şi, de ce nu, să-şi extindă limitele de rezistență psiho-fizică.

Vulnerabilități psihologice în fața COVID-19

Acest subcapitol încearcă să prezinte, pe scurt, principalele vulnerabilități pe care le prezentăm în fața coronavirusului, evident, dintr-o perspectivă psihologică.

Relațiile interpersonale. Prin natura sa omul este o ființă gregară, care are nevoie de ceilalți semeni pentru a comunica, pentru a se relaționa şi interacționa, pentru a supraviețui. Restricțiile impuse de pandemia COVID-19 atacă chiar această trăsătură fundamentală a ființei umane, cerându-i omului să nu mai interacționeze cu semenii săi, să nu se mai ducă în locurile sale preferate, să se supună unor restricții de deplasare dure, să stea în carantină, în izolare. O astfel de perspectivă este, pentru cei mai mulți, una inacceptabilă, iar tendința este de a găsi soluții „ingenioase" de a păcăli regulile impuse de autorități, în detrimentul propriei sănătăți şi a sănătății colective.

Tendința de a nu respecta regulile. Probabil, unul dintre cele mai puternice comportamente ale românului este acela de a face altfel decât dictează regula, norma sau legea. Aşa am fost educați, aşa am înțeles, în timp, că funcționează societatea românească sau poate chiar aşa funcționează, dar în situație de normalitate. În general, atunci când unei persoane i se impune, împotriva voinței sale, un anumit comportament, imediat ce iese din supravegherea imediată a celui ce îl impune are tendința de a face exact pe dos. Aşa se explică de ce românii respectă, cu strictețe, legislația auto doar dacă află că într-o anumită zonă este un echipaj de poliție, un radar sau un sistem de verificare ce poate aplica sancțiuni. Cel mai probabil, acest gen de comportament va fi prezent şi în cazul acestei pandemii, dar, din păcate, de această dată consecințele pot fi mult mai grave, echivalente cu condamnarea la moarte a altor semeni.

Tendința de a nega gravitatea fenomenului. În general, oamenii sunt empatici cu necazurile şi suferințele altora, dar, de cele mai multe ori, le proiectează, mental, undeva departe de ei. Deşi suntem solidari cu sărăcia şi foametea din statele africane, cu victimele unei inundații catastrofale, cu cei care suferă de pe urma conflictului din Siria, cu bolnavii de cancer, cu familiile îndurerate ale sutelor de morți răpuşi de COVID-19 în Italia sau China, de cele mai multe ori aceste imagini rămân pe sticla ecranului TV-ului/computerului, departe de noi. Cu alte cuvinte, până când nenorocirea nu ne afectează direct părem a fi intangibili, infailibili, imuni, chiar şi în fața contaminării cu coronavirus. O astfel de atitudine, evident se transformă într-o vulnerabilitate atât la adresa propriei persoane, cât şi a comunității, îngreunând eforturile autorităților de limitare a pandemiei.

Tendința de a amplifica gravitatea fenomenului. Alte persoane, influențate de ştirile care vorbesc neîntrerupt despre pandemie, încep să gândească viciat şi se plasează pe ele însele în postura de victime sigure ale COVID-19, deşi în realitate nu sunt mai expuse decât majoritatea populației. În acest context, îşi impun atât lor, cât şi apropiaților lor măsuri extreme de protecție şi dezvoltă comportamente panicarde, golind rafturile magazinelor, făcându-şi provizii serioase de medicamente de toate felurile, autoizolându-se aproape complet în locuințe, blocând contactul cu cei dragi, autosuspendându-se de la îndatoririle de serviciu curente, dezvoltând comportamente obsesiv-compulsive etc.

Recomandări psihologice pentru gestionarea COVID-19

Deşi o astfel de epidemie ne afectează în mod grav viața şi măsurile primordiale ce se impun sunt de natură sanitar-managerială, cele de natură psihologică nu trebuie excluse din ecuație, pentru diminuarea efectelor COVID-19. Acestea sunt complementare efortului general de limitare a pandemiei şi se adresează gândirii, gestionării eficiente a emoțiilor, adoptării unor comportamente raționale, combaterii şi diminuării stresului – domenii care aparțin, prin excelență, psihologiei.

În continuare, se vor prezenta unele dintre cele mai la îndemână modalități psihologice care pot contribui la limitarea răspândirii coronavirusului.

Măsuri de natură relațională. După cum am afirmat mai sus, interzicerea şi limitarea interacțiunilor directe dintre oameni, cu scopul de a îngrădi răspândirea COVID-19 ar putea crea un disconfort major pentru foarte multe persoane. Psihologii recomandă continuarea interacțiunii cu cei dragi, însă într-o formulă virtuală (prin Internet), a cărei funcționalitate a fost deja demonstrată în cele mai diverse situații: contactele dintre militarii dislocați în teatrele de operații militare şi cei dragi, lucrul de acasă practicat de marile companii, tele-shoppingul etc. În aceste momente dificile, este necesar ca nivelul de comunicare dintre cei dragi să crească, pentru a compensa alte comportamente ce umpleau, în trecut, rutina zilei.

Măsuri de evitare a agresiunii psihologice. Odată cu apariția COVID-19 au apărut şi o mulțime de „fake news", destinate să producă panică, să construiască o atitudine „contra" – de negare a pandemiei, să promoveze anumite produse comerciale, să slăbească încrederea în autorități, să construiască percepții deformate cu privire la pandemie, să dezvolte o mulțime de teorii conspiraționiste etc. Aceste informații sunt livrate prin mijloace mass-media clasice, utilizând metode deja consacrate şi specifice războiului psihologic: zvonul, denigrarea, calomnia, subversiunea, prozelitismul, manipularea etc. În lipsa unor surse oficiale de informare, credibile şi în măsură să livreze mesaje inteligibile şi raționale către populație, în mod oportun, formele de agresiune psihologică vor avea de câştigat, iar promotorii lor îşi vor atinge scopul, cu consecințe grave pentru populație. Unii psihologi (Duvac, 2020) au numit latura psihologică a actualei pandemii PSIHOVID19, urmare a implicațiilor psihologice pe care le presupune. Psihologii recomandă prudență maximă în asimilarea informațiilor din surse neverificate, precum şi utilizarea canalelor oficiale de informare.

Gestionarea eficientă a emoțiilor. Gestionarea emoțiilor în situații de urgență nu este un lucru prea uşor, având în vedere gravitatea situației pe care o trăim. Primele reacții emoționale fireşti în astfel de situații sunt cele de anxietate, panică, agitație. De la om la om, în funcție de stabilitatea emoțională a fiecăruia, reacțiile emoționale se pot deplasa şi spre limitele spectrului de normalitate clinică, luând forma unor nevroze, depresii sau chiar psihoze. Unele persoane mai evlavioase au tendința de a dedica din ce în ce mai mult timp relației cu Divinitatea (rugăciuni, ritualuri mistice etc.), neglijând obligațiile sociale ce decurg din viața reală. Psihologii recomandă simplu: „Păstrați-vă calmul!". Rămâneți cât mai mult raționali şi încercați să înțelegeți, cu adevărat, ceea ce vi se întâmplă. Rămâneți informat, dar nu înecat în informații şi manipulat.

Gestionarea eficientă a comportamentelor. Fiecare persoană şi-a format o anumită rutină zilnică. Aceasta îi asigură confortul, odihna, bucuria de zi cu zi a vieții. Fără îndoială, această pandemie a bulversat dramatic rutina zilnică. Copiii nu mai merg la şcoală, au ore de acasă, bona a plecat acasă, programul de la serviciu s-a schimbat, sala de gimnastică s-a închis, la fel şi cinematograful, teatrul şi sala de jocuri preferată, prietenii nu se mai pot întâlni la club, bunicii au rămas izolați în casele lor, concediul a fost amânat, plimbările prin parc sunt descurajate de autorități şi asta nu este tot – aşa ar putea arăta un scenariu banal de schimbare radicală a comportamentului. Psihologii recomandă redescoperirea creativității. Fiecare dintre noi are o resursă suficientă şi, de multe ori, neexploatată de originalitate şi creativitate. Site-urile on-line abundă în idei creative care pot ajuta la descoperirea/redescoperirea unor talente ascunse şi pot oferi acele condimente speciale ce fac viața frumoasă. La acestea se pot adăuga lecturile şi desenul.

Gestionarea eficientă a ştirilor negative. Din păcate, în situațiile de urgență, derulate pe timpul calamităților naturale, majoritatea veştilor sunt de natură negativă şi au un caracter de limitare a drepturilor şi libertăților. Această pandemie, însă, nu poate fi mai gravă decât un cutremur devastator, decât un conflict armat sau un alt astfel de eveniment cu o natură cinetică definitorie. În general, românii sunt bine-cunoscuți pentru simțul umorului şi pentru calitatea lor de a face „haz de necaz". Psihologii recomandă valorificarea acestei calități, a simțului umorului, asociată cu optimismul. De altfel, mediul virtual este plin de glume care ridiculizează pandemia. Totul este ca

fiecare să le acceseze şi să se bucure de ele. O altă modalitate eficientă, recomandată de psihologi, pentru depăşirea momentului în astfel de situaţii este dată de reducerea disonanţei cognitive, adică o gândire de tipul: „în definitiv se putea şi mai rău" sau „în fond, o astfel de situaţie nu o să fie eternă" ori „s-au terminat ele războaiele mondiale, cu suferinţe inimaginabile, dar această pandemie", „în definitiv, o gripă normală poate ucide mai mulţi oameni decât acest coronavirus" etc.

Stimularea gândirii raţionale. Dacă un cutremur, o inundaţie, un incendiu de proporţii ar fi fost uşor vizibile de oricine, iar dimensiunea dezastrului ar fi fost lesne de evaluat, în cazul pandemiei COVID-19 aceasta este invizibilă şi, cu atât mai mult, greu de înţeles pentru că efectele sale sunt percepute indirect (prin restricţiile impuse de autorităţi), doar rareori prin parcurgerea unor regimuri de izolare, carantină sau tratament. Într-un asemenea context, se face apel la gândirea abstractă, la operaţiile gândirii (analiza, sinteza, compararea, generalizarea, particularizarea, abstractizarea, concretizarea) pentru a înţelege cu adevărat ce ni se întâmplă. Psihologii recomandă creşterea ponderii activităţilor cognitive astfel încât fiecare persoană să realizeze cât mai bine toate dimensiunile situaţiei şi să aplice metodele rezolutive cele mai eficiente, adaptate la cazul său.

Apelul la instanţele morale. Oare în ce împrejurări se văd cel mai bine valorile pe care fiecare persoană le respectă din proprie iniţiativă, pentru că aşa consideră ea, pur şi simplu? Acestea se relevă, într-adevăr, în situaţiile de criză/ de urgenţă. Valori precum responsabilitatea, solidaritatea, curajul, spiritul de sacrificiu, altruismul, camaraderia, patriotismul – sunt de dorit a fi văzute la cât mai mulţi cetăţeni, în astfel de perioade. Psihologii recomandă ca fiecare să dea ceea ce are mai bun în el, pentru că în acest fel se va trece mult mai uşor peste pandemia COVID-19.

Gestionarea eficientă a stresului. Stresul există şi în situaţiile normale de viaţă şi, cu atât mai mult, în cele speciale, cum ar fi cea generată de pandemia de COVID-19. Unele griji (cu privire la copii, rude, propria persoană, locul de muncă, procurarea celor necesare pentru traiul zilnic etc.) se cumulează apar, fără voia noastră, stări de anxietate, panică, disperare, reacţii obsesive, nervozitate şi irascibilitate sau, din contră, pasivitate şi deznădejde profundă, insomnii etc. - la gândul că nu putem gestiona corespunzător provocările ce ne sunt ridicate în faţă. Toate acestea se contabilizează în „contul" stresului, care va creşte, pe neobservate, şi va conduce la dezadaptare socială în propria lume. Psihologii recomandă: consultarea specialiştilor atunci când o persoană simte că a acumulat prea mult stres, sesizarea specialiştilor atunci când cineva observă la altă persoană că este stresată peste măsură. De asemenea, instituţiile/ organizaţiile trebuie să implementeze măsuri de gestionare eficientă a personalului, pentru a evita suprasolicitarea acestuia (elementele motivaţionale pot fi eficiente în astfel de cazuri).

Gestionarea psihologică a riscului. Analiza riscului, raportat la pandemia COVID-19, permite luarea unor măsuri de prevenire, dar nu exacerbarea măsurilor de protecţie dincolo de limitele raţionalului. Analizele efectuate în China pe un număr de 70.000 de cazuri de persoane contaminate cu COVID-19 au arătat că aproximativ 80% din bolnavi au avut o formă uşoară şi numai15 - 20% au prezentat boli grave. Din cele 70.000 de cazuri, doar aproximativ 2% au fost la persoane mai mici de 19 ani. Aceasta pare a fi o boală care afectează adulţii. Şi, cel mai serios, adulţii mai în vârstă, începând cu vârsta de 60 de ani, în mod progresiv şi proporţional cu vârsta. Cel mai mare risc de a contacta o formă gravă şi de deces este la persoanele cu vârsta de peste 80 de ani. De asemenea, persoanele cu condiţii grave de sănătate sunt mai susceptibile să dezvolte forme grave, inclusiv decesul. Aşadar, persoanele care prezintă cel mai mare risc sunt cele mai în vârstă şi care au, de asemenea, afecţiuni grave de sănătate pe termen lung, precum diabetul, bolile de inimă sau bolile pulmonare. Psihologii recomandă cunoaşterea faptelor, deoarece puteţi învăţa să vedeţi situaţia mai raţional, decât să reacţionaţi emoţional într-o formă impredictibilă.

Creşterea rezilienţei. Renumitul profesor dr. Mircea Miclea a fost unul dintre primii psihologi

care a abordat public aspectele psihologice ale pandemiei, recomandând o serie de modalități de creștere a rezilienței la criza determinată de COVID-19:

- **Perseverența în proiectele personale**. „Deşi o criză ne scoate din ordinea firească a vieții, ne pune sub semnul întrebării modul în care trăim, proiectele noastre de viață, dacă mintea noastră se încăpățânează să fie orientată spre viitor, dacă întâmpinăm ziua de mâine cu un plan, nu cu o nouă teamă, devenim mult mai puțin vulnerabili la ce ni se întâmplă în prezentul imediat."
- **Autodisciplina**. „În criză, realitatea oferă oricâte motive doreşti să nu te mai focalizezi pe sarcini, ci pe stările pe care le trăieşti. Ai putea încălca regulile fireşti de viață, ai toate alibiurile. Exact în această situație e necesar să ne stabilim noi înşine reguli şi să ne ținem de ele cu strictețe. Regulile ne reduc din anxietate".
- **Dezvoltarea caracterului.** „Criza e ca un reactiv chimic: scoate la iveală toate caracteristicile ascunse pe care le avem. Dar criza oferă şi şansa enormă a dezvoltării personale, a descoperirii şi trăirii valorilor în care merită să credem."
- **Solidaritatea.** „Cei care i-au ajutat pe alții, în situații limită, au devenit ei înşişi mai robuşti. Psihologic, solidaritatea ne ajută să ieşim din obsesia autoprotecției personale şi să riscăm ajutându-i pe alții".
- **Cultivarea emoțiilor pozitive.** „Închipuiți-vă echilibrul emoțional ca pe o balanță. Acum e dezechilibrată, emoțiile negative sunt mult mai multe şi mult mai grele decât cele pozitive. Putem însă echilibra balanța, dacă ne producem mai multe emoții pozitive".

Concluzii

Pandemia COVID-19 va dispărea, mai devreme sau mai târziu, iar viața va reveni, treptat, la normalitate. Cu certitudine, vor rămâne multe lecții învățate şi, în mod cert, întreaga lume se va remodela după această experiență dramatică.

O mulțime de aspecte de neconceput înainte de pandemie vor intra în firesc, legislația se va adapta noilor realități, tehnologia informației şi mediul virtual vor revoluționa lumea, oamenii vor trata cu mai multă atenție riscurile de natură biologică şi vor investi mult mai mult în sistemele de sănătate, întreaga populație va fi mai rezilientă.

Încheiem acest articol despre locul şi rolul psihologiei într-o situație de criză, precum cea generată de pandemia de COVID-19, fără a fi finalizat tema supusă atenției. Această temă va rămâne deschisă mult timp de aici înainte, iar orice contribuții ale colegilor psihologi şi nu numai ar fi benefice, pentru ca data viitoare să fim mai pregătiți în fața unei asemenea agresiuni la adresa securității naționale şi a fiecăruia dintre noi în parte.

Bibliografie selectivă:

1. CARBONNEL, D.A., *The Worry Trick: How Your Brain Tricks You into Expecting the Worst and What You Can Do About It*. Oakland, CA: New Harbinger Publications, Inc., 2016
2. DOBRE, C., „Psihologia de urgență în structurile de apărare şi securitate națională", în *Psihologia militară – multiplicator al eficienței operaționale,* Editura UNAp „Carol I" , Bucureşti 2014;
3. MICLEA, M., *Arta de a trăi în vremuri de criză*, Realitatea.net, 2020, la https://www.realitatea.net/stiri/actual/mircea-miclea-arta-de-a-trai-in-vremuri-de-criza_5e6f3094690eea3da532d6b6
4. https://www.cnbc.com/2020/03/13/how-to-stay-calm-amid-coronavirus-pandemic-anxiety-relief-tips.html
5. https://www.nytimes.com/live/2020/coronavirus-update-03-13
6. https://pro.psychcentral.com/recovery-expert/2020
7. https://cpa.ca/corona-virus/
8. https://www.psychology.org.au/COVID-19-Australians
9. https://www.apa.org/practice/programs/dmhi/research-information/pandemics
10. https://www.businessinsider.com/how-to-cope-with-coronavirus-covid-19-anxiety-psychologist-2020-2
11. https://psychology.illinois.edu/news/2020-03-17/covid-19-mental-health-resources

REȚELELE DE SOCIALIZARE ŞI IMPACTUL ACESTORA ASUPRA SECURITĂȚII ORGANIZAȚIEI MILITARE

Silviu SAFTA*

Abstract

Information era and the organisations' and people's dependence on technology has both advantages and disadvantages, overcoming the new asymmetric threats requiring knowledge, measures and adaptability. The spread of technologies in all social strata, simultaneously with the new types of threats, creates the premises for the manifestation of cyber threats.

The security culture of individuals and the technological level can be pillars in countering possible threats, as well as in the education of the masses.

The quantity and quality of information, in the context information propagation speed in the online space represent challenges for specialized defense structures, gathering open source information (OSINT) involving several steps to confirm the veracity of the information and use it to ensure state security.

Keywords*: Internet, social media, military organization, security culture, adaptability.*

Elemente introductive

Internetul s-a statuat ca fenomen global odată ce a „infiltrat" toate păturile sociale şi toate domeniile, iar în prezent activitățile zilnice sunt influențate semnificativ de facilitățile acestuia, precum micşorarea *„distanței"* dintre indivizi, creşterea numărului surselor de informare, schimbarea nevoilor de cunoaştere şi necesitatea adoptării celor mai bune decizii pentru creşterea calității vieții.

Cu toatea acestea, pe lângă avantaje, mediul virtual generează o serie de amenințări la adresa societății, mai mult sau mai puțin conştientizate de către publicul larg, amenințări care se pot răsfrânge şi asupra instituției militare. Vulnerabilitatea în fața ciber-infractorilor, „*intoxicarea*" cu informații false, răcirea relațiilor interumane, informarea insuficientă a populației cu privire la amenințările şi riscurile la care se expune pe Internet, pierderile de date importante pentru indivizi, organizații şi state sunt doar câteva dintre realitățile actuale ale erei informaționale. De asemenea, omniprezența tehnologiei influențează capacitatea oamenilor, instituțiilor şi statelor de a filtra sau restricționa dimensiunea informațiilor.

În acest context, organizația militară se află, la rândul ei, sub influența acestui fenomen, încercând să se adapteze continuu şi să îl utilizeze în interesul națiunii, alianțelor şi coaliților pe care le reprezintă. Înțelegând mediul de securitate ca fiind totalitatea factorilor din mediul înconjurător care asigură sentimentul de încredere şi linişte, prin garantarea absenței oricărui pericol, atât pentru individ, cât şi pentru societatea din care acesta face parte[1], se poate deduce faptul că securitatea nu poate fi definită doar în parametri militari, ci încorporează şi securitatea politică, economică, socială, energetică, de mediu, a infrastructurilor informaționale etc.

Expert în cadrul Ministerului Apărării Naționale

Plecând de la una dintre misiunile organizației militare, aceea de a îndeplini necondiționat misiunile constituționale şi cele ce decurg din calitatea statului de membru al unei alianțe politico-militare, rezultă că adaptabilitatea structurii militare este o cerință ce ocupă un rol primordial în îndeplinirea obiectivelor, ținând cont de incertitudinea şi complexitatea mediului actual de securitate. De altfel, profesionalizarea organizației militare şi nevoia de progres tehnologic sunt caracteristici de bază ale structurilor armate. În acest sens, factorul uman reprezită principalul pilon în realizarea obiectivelor şi a performanței în organizația militară.

Faptul că organizația militară îşi desfăşoară activitățile coroborat cu celelalte domenii ale societății conduce la nevoia de adaptare a proceselor, fenomenelor şi modului de îndeplinire a misiunilor pentru o eficiență maximă. Performanța sistemului militar depinde, în cea mai mare măsură, de nivelul de identificare şi contracarare în timp util a amenințărilor provenite din exterior, dar şi a vulnerabilităților proprii, atât prin prisma factorului uman, cât şi al celui tehnic. Cele două elemente nu pot fi tratate în mod separat, unul fără celălalt nefiind capabil să facă față cerințelor actuale. Cu o tehnologie învechită omul nu poate dispune de informații oportune şi nu poate lua decizii corecte, cum, de altfel, fără personal profesionist şi instruit în manevrarea tehnologiei nu pot exista rezultate favorabile. Nevoia de comunicare rapidă este esențială pentru organizația militară, când informația circulă cu mare viteză şi în cantități uriaşe, datorate globalizării şi progresului tehnologic.

Ca urmare, Internetul şi rețelele de socializare au, la rândul lor, un impact semnificativ asupra organizației militare, prin apartenența indivizilor la acestea, dar şi prin activitățile desfăşurate în mediul online. O mare cantitate de informații ce vine în ajutorul organizației, atât despre forțele proprii, cât şi despre entitățile ostile, poate fi găsită din surse deschise, în special în mediul online. Astfel, spațiul virtual reprezintă un punct de sprijin, dar şi o vulnerabilitate dacă informațiile proprii nu sunt protejate corespunzător. Putem vorbi despre aceleaşi riscuri, amenințări şi vulnerabilități aferente spațiului public, însă de dimensiuni mult mai extinse şi cu repercusiuni la un nivel mai ridicat.

Aşadar, deschiderea societății în era informațională şi creşterea potențialului de exploatare cu care tehnologia şi Internetul îi înzestrează pe adversari au determinat o schimbare de paradigmă în activitatea serviciilor de informații, dar şi nevoia adoptării de noi strategii de comunicare şi transmitere a datelor importante.

Amenințări, riscuri şi vulnerabilități orientate asupra organizației militare, provenite din rețelele de socializare

În prezent, securitatea nu mai poate fi privită doar prin prisma alegerilor politice, a capacității şi intențiilor unui stat, deoarece riscurile, amenințările şi vulnerabilitățile au căpătat o semnificație sistemică. În plus, datorită globalizării şi erei informaționale putem afirma că securitatea națională nu mai porneşte de la stat, ci de la cetățean. Accesul larg la informație al tuturor cetățenilor a crescut importanța şi influența oamenilor în menținerea unui climat de securitate, cel puțin la nivel zonal.

Progresele tehnologic*e* la care asistăm creează, pe lângă numeroasele avantaje, noi paradigme de înțelegere a stării de securitate. Dacă în trecut era o misiune relativ uşoară identificarea unui potențial adversar, în secolul al XXI-lea identificarea acestuia reprezintă excepția, cel puțin în mediul virtual. Pe lângă structurile statale cu atribuții în menținerea securității naționale, regăsim tot mai multe grupări, participanți non-statali sau indivizi cu posibilități şi calități în achiziționarea de tehnologie performantă, capabilă să amenințe starea de securitate individuală şi statală. Astfel, dacă în conflictele anterioare războiul asimetric era considerat a fi arma combatantului mai slab, prin prisma încercării exploatării vulnerabilităților celuilalt, astăzi reprezintă arma celui mai inteligent. De aceea, afirmații precum cea a lui Jim Langevin, membru al Comisiei pentru securitate internă a Camerei Reprezentanților din Congresul SUA,

conform căreia „*niciodată nu vom mai asista la un război major fără o importantă componentă cibernetică*”, au o valoare de adevăr şi previziune ridicată.

Ameninţările, riscurile şi vulnerabilităţile ce vizează organizaţia militară din perspectiva spaţiului cibernetic se pot răsfrânge atât asupra tehnologiei folosite în cadrul activităţilor organizaţiei, cât şi asupra indivizilor ce folosesc echipamente conectate la Internet şi reţele de socializare. Factorul uman poate reprezenta veriga slabă în relaţia organizaţie militară-mediu virtual, deoarece tehnologia existentă, măsurile de protecţie împotriva ciber-infractorilor şi protocoalele de securitate digitală sunt adesea capabile să reziste şi să respingă un atac informatic. În schimb, infiltrarea unui virus sau malware din partea unui individ din interiorul organizaţiei, în mod voit sau nu, poate afecta semnificativ structura militară a unui stat.

Modelul noii ameninţări este, în prezent, unul neguvernamental, neconvenţional, dinamic sau aleatoriu şi neliniar în apariţie, fără îngrădiri sau reguli în ceea ce priveşte desfăşurarea sa. Nu are o doctrină cunoscută, este aproape imposibil de depistat în avans şi este sprijinit de forţe aparent nelimitate de criminali, traficanţi de droguri şi indivizi corupţi. Este, practic, un set de ameninţări asimetrice[2].

În actualul context, nevoia de asigurare a securităţii fizice a personalului, a documentelor clasificate, INFOSEC, securitatea industrială, planificarea şi organizarea securităţii, dar şi necesitatea unei culturi de securitate dezvoltate şi controlul regulat al sistemelor informaţionale sunt de o importanţă vitală, fiind necesară protecţia tuturor componentelor organizaţiei militare.

Protecţia informaţiilor în sistemele de comunicaţii şi informatică (SIC) este parte integrantă a securităţii generale, iar pentru realizarea acesteia este necesară aplicarea, în condiţii specifice, atât a unor măsuri cu caracter general (precum organizarea securităţii, măsuri de protecţie fizică, de protecţie a personalului, a documentelor, de protecţie juridică şi de securitate industrială), cât şi a unor măsuri specifice SIC. Măsurile de protecţie a SIC au ca principal scop asigurarea integrităţii şi disponibilităţii acestora, dar şi minimizarea daunelor în cazul în care sunt accesate neautorizat.

Informaţiile stocate, procesate şi vehiculate în SIC sunt vulnerabile la accesul, modificarea sau distrugerea de către utilizatori neautorizaţi din cauza unor factori, precum:

- volumul foarte mare de informaţii stocate, accesate şi transferate cu viteze foarte mari;
- dificultăţi în realizarea controlului accesului la informaţiile stocate în SIC;
- posibilitatea de a evita măsurile de securitate de către utilizatorii experimentaţi;
- capacitatea mediilor de stocare care facilitează sustragerea unui volum mare de informaţii;
- defecţiuni ale componentelor hardware şi software;
- posibilitatea interceptării comunicaţiilor pe canale neprotejate sau a emisiilor compromiţătoare[3].

Cu toate acestea, erorile umane reprezintă cel mai adesea cauzele incidentelor online ale organizaţiilor militare, fiind generate de nerespectarea măsurilor de securitate sau a superficialităţii controalelor efectuate. Concomitent, nivelul tehnologic este o variabilă la fel de importantă ca şi componenta umană. Prin menţinerea unei performanţe tehnologice cât mai ridicate este necesară şi suplimentarea numărului de specialişti IT în structurile specializate în vederea menţinerii securităţii militare. Creşterea importanţei spaţiului virtual în actualul mediu de securitate presupune atât personal pregătit în domeniu, cu un nivel ridicat de cultură de securitate, cât şi controale regulate şi tehnică capabilă să răspundă cerinţelor actuale.

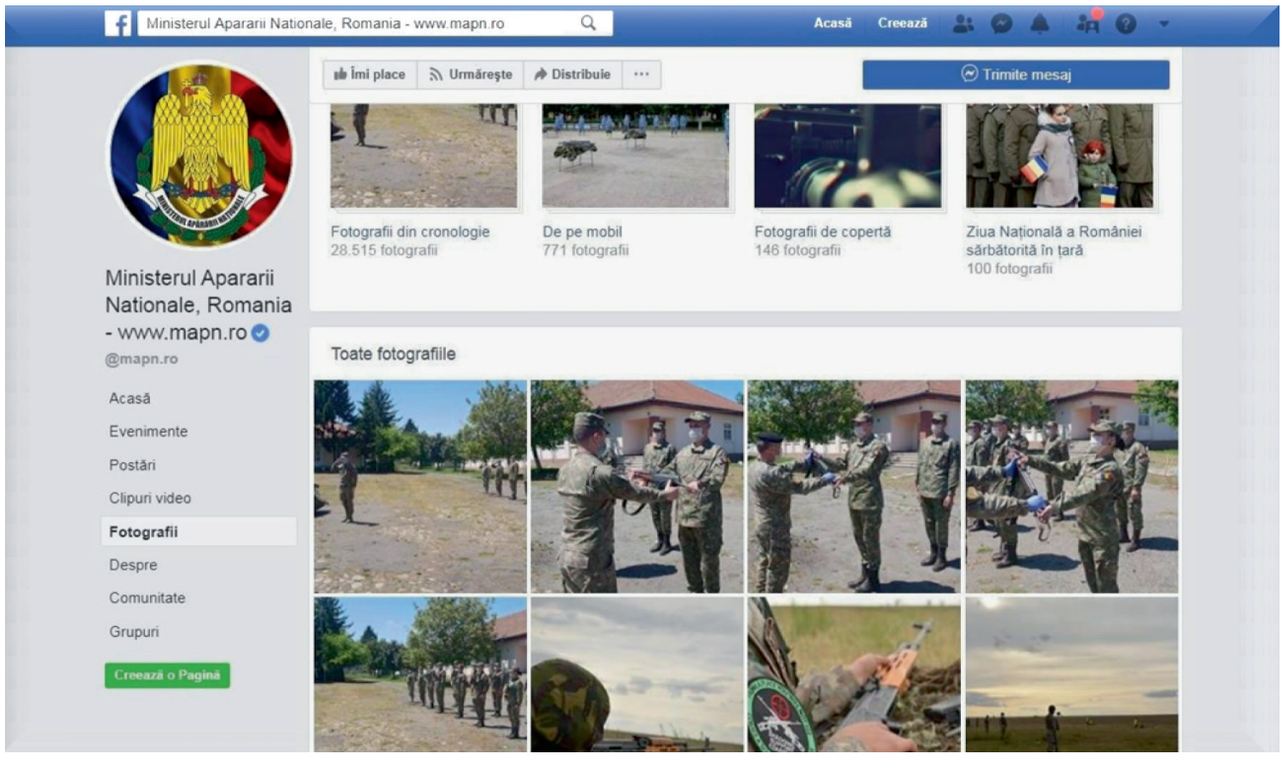
În context, încălcarea procedurilor de securitate referitoare la accesul la informaţii clasificate sau utilizarea unor medii de stocare nepermise pot reprezenta premisele manifestării unor viitoare ameninţări la adresa securităţii organizaţiei militare şi, implicit, a statului. Conexiunea la Internet şi utilizarea reţelelor de socializare sunt canale de comunicare care,

prin erori umane sau de sistem, oferă posibilitatea forțelor ostile să compromită informații sensibile, prin distrugere sau acces neautorizat.

Importanța culturii de securitate nu ar trebui abordată doar din perspectiva individului, membru al organizației militare, ci ar trebui privită în ansamblu, finalitatea acesteia fiind cultura de masă. Acest proces educațional ar trebui să fie unul de durată şi adaptat perioadelor educative ale maselor. Din perspectiva Internetului şi a rețelelor de socializare, conştientizarea de către utilizatori a pericolelor şi aplicarea politicilor de securitate în domeniu nu fac decât să crească siguranța mediului virtual şi pot conduce la descurajarea potențialilor atacatori.

de contracarat, pot fi identificate şi respinse din timp.

Rețelele de socializare, în contextul extinderii mediului virtual şi al globalizării, sunt canale ce pot fi folosite de către adversari în vederea exploatării vulnerabilităților organizației militare. Resursele tehnologice şi cele umane, prin valorificarea erorilor, conduc la premisele transpunerii pericolelor în acțiuni reale. În general, specialiştii şi nivelul tehnologic au capacitatea să stopeze astfel de activități, iar prin cultura de securitate şi respectarea procedurilor indivizii contribuie la menținerea în siguranță a informațiilor sensibile, atât la locul de muncă, cât şi în viața de zi cu zi.



Referitor la domeniul militar, prezența culturii de securitate reprezintă o condiție sine-qua-non în vederea identificării şi contracarării amenințărilor. Prin educarea personalului, pe categoriile activităților specifice, se va reuşi consolidarea valorilor democratice din interiorul şi exteriorul organizației, reuşind crearea unei relaționări între mediul civil şi cel militar. Astfel, modalitățile de agresiune militară şi cele nonmilitare (unde pot fi incluse şi agresiunile cibernetice), care sunt oricum dificil

Provocări generate de Internet şi rețele sociale

Omniprezența tehnologiei informaționale de astăzi a influențat capacitatea oamenilor, a instituțiilor şi a statelor de a controla informațiile sau de a le restricționa dimensiunea. În ceea ce privește structurile de securitate, avantajul competitiv s-a mutat spre cele apte să exploateze rapid activitatea celorlalți, prin culegerea informațiilor din surse deschise, spre deosebire de cele capabile să lucreze doar în secret[4].

Societatea informațională contemporană are la bază trei componente: informația, comunicarea şi controlul. În ceea ce priveşte componenta controlului, accesul tot mai extins şi în timp real la informația provenită din sursele deschise a avut un important impact asupra activității de intelligence şi a politicilor din domeniul securității naționale.

În ceea ce priveşte modelul noului serviciu de informații, acesta trebuie să cuprindă şi să se adapteze la explozia informațională, în mod deosebit la cea digitală în diferite limbi, capabil să obțină date reale pe teren despre orice problemă, în orice punct de pe glob, folosind ofițeri de informații pregătiți în acest scop.

Elementele de interes în procesul OSINT sunt acele informații neclasificate care au fost descoperite, selectate, filtrate şi diseminate pentru o audiență specifică, în vederea răspunderii la o anumită solicitare. Aplicate într-un mod sistematic, produsele OSINT pot reduce cererile de colectare a informațiilor secrete, limitând aceste solicitări doar la subiectele pentru care nu se poate oferi un răspuns din surse deschise[5].

Cu toate avantajele pe care le prezintă culegerea informațiilor din surse deschise, nu trebuie supraestimată utilitatea acestora în dauna culegerii de informații secrete prin mijloace specializate. Printre avantajele oferite de posibilitățile OSINT se numără eliberarea capacităților secrete de culegere, satisfacerea nevoilor de utilizare în comun a informațiilor, acoperirea cu informații a unor necesități neprevăzute, semnalarea unor potențiale crize şi pericole sau conştientizarea contextuală. Ca dezavantaje ale utilizării OSINT se regăsesc inexactitatea informațiilor, părtinirea, irelevanța, dezinformarea, intoxicarea, ştirile false, influența sau supraîncărcarea informațională.

Experiența în activitatea de exploatare a surselor deschise evidențiază aspecte care trebuie să fie conştientizate în organizarea procesului de culegere a informațiilor, astfel:

- 80% din necesarul de informații nu e disponibil online;
- 60% din necesarul de informații nu este disponibil într-o limbă cunoscută;
- 90% din hărțile de care este nevoie nu există;
- 90% din datele geospațiale necesare sunt în sectorul particular;
- 80% din totalul informațiilor necesare se găsesc în sectorul particular.

De asemenea, nu trebuie să cădem în capcana absolutizării utilității Internetului, avându-se în vedere că experiența de până acum a demonstrat faptul că pe Internet se găsesc doar 5-10% din datele publice necesare. Mai mult, doar aproximativ 1% din conținutul Internetului îl constituie date reale, existând circa 50 de site-uri foarte bune pentru culegerea de informații, 500 bune, celelalte fiind reclame, opinii diverse etc.[6]

Din punct de vedere cantitativ, Open Sources reprezintă principala sursă de informare. Potrivit unor estimări, majoritatea serviciilor de informații primesc circa 80-85% din totalul de informații din surse deschise. Cu toate acestea, existența surselor deschise nu presupune automat și accesul direct al serviciilor de informații la aceste surse. Astfel că, pentru a elabora produse de intelligence din surse deschise, este necesar un proces complex și deloc ieftin, implicând aici descoperirea, diferențierea, filtrarea și selectarea acelor fragmente de informații care, integrate și interpretate, să ducă la obținerea unor produse utile[7].

În ceea ce privește rețelele de socializare, acestea constituie o categorie aparte a social media și sunt reprezentative pentru creșterea exponențială a rolului informației în societate și în munca serviciilor de informații, prin simplul fapt că integrează tehnologie, interacțiune socială și creație. Acestea sunt premisele unei globalizări virtuale, ce unește domenii și oameni cu naționalități, tradiții și viziuni diferite, cel mai mult contând punctele comune în interacțiunea cu ceilalți[8].

Odată cu progresul tehnologic au apărut și noi soluții de eficientizare a activităților OSINT, determinând organizațiile din domeniul intelligence-ului să se adapteze la ultimele instrumente. Pentru a depăși erorile inerente din punct de vedere al selectării, filtrării, sintetizării, integrării și analizării surselor deschise, structurile de informații specializate în activitatea OSINT sunt nevoite să apeleze la tehnologii care au ca scop colectarea, traducerea, clasificarea pe domenii de interes și prelucrarea informațiilor. Internetul reprezintă o platformă pentru astfel de programe, ce poate oferi softuri specializate și upgradate permanent.

În principiu, creșterea numărului și tipului de surse informaționale a determinat sporirea conținutului ce ar trebui să fie analizat, ridicând astfel problema identificării unor soluții pentru gestionarea volumului de informații. Astfel, au fost create baze de date pentru a monitoriza și stoca informațiile vehiculate pe Internet, cu precădere a celor care circulă prin telefon și pe rețelele de socializare.

Un alt avantaj al mediului virtual îl reprezintă dezvoltarea continuă a platformelor colaborative de lucru, perfecționate în vederea mulării pe natura informațiilor obținute prin culegerea și prelucrarea datelor din sursele deschise. Astfel de sisteme nu doar că permit accesul la baze de date specializate, dar facilitează și colaborarea între specialiști, prin partajarea informațiilor și prin primirea de feed-back-uri rapide.

Cu toate acestea, odată cu cantitatea uriașă de informații vehiculată în spațiul virtual, apare problema veridicității acesteia, iar fenomene precum dezinformarea, diseminarea de informații false sau manipularea reprezintă amenințări pentru indivizi, organizații și state. Validarea surselor și a informațiilor apare, astfel, ca o necesitate pentru elaborarea produselor informative capabile să satisfacă cerințele decidenților și să ducă la îndeplinirea obiectivelor organizației militare și a celor naționale.

Spre deosebire de mijloacele mass-media tradiționale (cărți, studii, televiziune etc.), unde volumul de informații este controlabil, iar emițătorul este cunoscut, pentru validarea surselor online este nevoie de o abordare diferită, ținând cont de diversitatea și specificul lor.

Una dintre consecințele principale ale extinderii Internetului a fost apariția într-un număr foarte mare a rețelelor de socializare, blogurilor, forumurilor, creșterea conținutului provenit de la utilizatori în toate limbile, lipsa filtrelor devenind astfel o problemă a mediului virtual. De aceea, odată cu oportunitatea oricărui utilizator de a posta pe Internet date și informații, printre acele resurse ce pot fi valorificate se regăsesc și datele îndoielnice. Aparentul anonimat al utilizatorilor și retransmiterea informațiilor posibil false pun astfel în dificultate analiștii și necesită resurse financiare, umane și de timp pentru verificarea și validarea acestora.

Particularizând, rețelele de socializare sunt generatoare de date și informații care pot facilita munca serviciilor de informații prin exploatarea platformelor virtuale. Tendința utilizatorilor de a publica cât mai multe date personale se transpune în materie primă, care, în urma analizării, poate deveni informație de interes.

Cu toate acestea, existența acestor tipuri de vulnerabilități şi în organizația militară proprie poate fi exploatată de serviciile de informații ostile. Importanța existenței unei educații de securitate în organizația proprie, concomitent cu conştientizarea acestor amenințări provenite din exterior prin mediul virtual, reprezintă măsuri de protecție a personalului, a documentelor şi a informațiilor vehiculate în rețelele proprii de calculatoare.

Privind în ansamblu, cu ajutorul OSINT serviciile de informații au oportunitatea de a promova în rândul societății civile cultura şi educația de securitate, prin acțiuni comune şi informări, ținând cont că educarea cetățenilor în propriul beneficiu nu poate decât să faciliteze activitatea de intelligence.

Evoluția Internetului şi caracteristicile rețelelor de socializare creează o dependență directă a procesului OSINT de acestea, determinând mijloacele folosite şi consolidarea rolului în activitatea de informații. Pentru exploatarea eficientă a resurselor spațiului virtual este necesară adaptarea metodologiei şi elaborarea unor standarde capabile să răspundă avansului tehnologic. Colaborarea cu specialişti în domeniu, chiar cooptarea acestora în sistem şi apariția platformelor colaborative între serviciile de informații sunt măsuri de cooperare ce pot duce doar la dezvoltarea organizației militare în actualul context al securității.

Studiu de caz OSINT: dezinformarea şi ştirile false în contextul pandemiei de COVID-19

Cea mai recentă şi de anvergură provocare la adresa mediului de securitate global şi național a fost, şi probabil va fi în continuare, pandemia cu noul coronavirus, care a reprezentat o adevărată *„lebădă neagră”*, conform conceptului de eveniment neprevăzut cu impact major pentru securitatea unei entități, în viziunea lui Nassim Taleb[9].

Totuşi, pe lângă efectele negative în plan sanitar, economic şi social, pandemia cu noul coronavirus a generat o campanie de dezinformare şi ştiri false, care poartă numele generic de „*infodemie*”, cu scopul de a vulnerabiliza suplimentar statele afectate de criza actuală[10].

În acest sens, specialişti militari şi civili în monitorizare mass-media au identificat numeroase site-uri, o parte dintre acestea fiind promovate intens pe rețelele sociale, care diseminau informații false în legătură cu originea, efectele şi impactul virusului. Mai mult, aceste platforme online răspândeau informații false în ceea ce priveşte măsurile adoptate de autorități în prevenirea şi combaterea pandemiei, de multe ori oferind informații contradictorii, de natură să genereze atât panică, cât şi neîncredere în rândul consumatorilor de conținut online[11].

Totodată, trebuie precizat faptul că o serie de instituții, printre care şi Comisia Europeană, au stabilit că originea unora dintre aceste platforme de ştiri false şi dezinformare este Federația Rusă[12], demonstrându-se, astfel, faptul că indiferent de contextul de securitate, entități ostile sunt pregătite să exploateze vulnerabilități şi amenințări pentru a acționa împotriva intereselor unui stat sau unei organizații. Aşadar, cele peste 2.700 de mostre de *fake news* referitoare la pandemie au fost capabile să genereze reacții şi acțiuni ale cititorilor, unele care s-au transpus în acte de violență având caracter de ilegalitate (spre exemplu, în Anglia, mai mulți cetățeni au incendiat turnuri de telecomunicații 5G, atacând angajații unei companii din acest domeniu).

În acest context de securitate volatil, marcat de impredictibilitate, revine în sarcina structurilor abilitate, în special a celor din domeniul apărării, prevenirea şi combaterea unuia dintre efectele adverse ale tehnologizării – dezinformarea şi ştirile false - întrucât mediul militar este una dintre țintele predilecte pentru acest gen de acțiuni ostile care, după cum numeroase rapoarte o arată, sunt susținute inclusiv de guverne străine[13].

Concluzii

Secolul al XXI-lea prezintă conceptul de intelligence încadrat într-o paradigmă nouă, aceea de conştientizare a impactului revoluției informaționale. Îngrijorător este că, indiferent de eforturile depuse de către specialiştii în securitate cibernetică, riscurile şi amenințările

din mediul virtual se vor manifesta în continuare, iar vulnerabilitățile tehnologice şi umane vor fi mereu exploatate de către ciber-infractori.

Cu toate acestea, confortul conferit de rețelele de socializare trebuie întărit de o educație proprie referitoare la mediul virtual. Socializarea online nu ar trebui să fie o activitate generatoare de pericole atunci când utilizatorul cunoaşte şi aplică reguli de bază ce îi asigură siguranță şi este în cunoştință de cauză în ce priveşte riscurile şi amenințările comunicării digitale.

Prezintă interes nevoia de conştientizare a influenței rețelelor de socializare din spațiul virtual asupra individului, organizației militare şi a societății, a faptului că beneficiile acestora vin, în acelaşi timp, şi cu amenințări şi riscuri, iar necunoaşterea pericolelor ne face vulnerabili.

Totodată, faptul că rețelele de socializare reprezintă astăzi o platformă pentru culegerea de informații din surse deschise (OSINT) a structurilor de informații nu mai este un element de noutate, acest lucru putând fi posibil atâta timp cât tehnologia structurilor respective şi personalul lor sunt capabile să exploateze resursele „infinite" oferite de Internet. Astfel că, în actualul context al securității, adaptabilitatea ar putea fi cuvântul de ordine pentru îndeplinirea obiectivelor statului-națiune de către structurile de informații şi celelalte entități cu atribuții în apărarea statelor şi a populației.

Bibliografie:

1. RICHICINSCHI, Iurie, „Evoluții ale mediului internațional de securitate", în *Administrare publică,* nr. 1, 2017, Chişinău, p. 99-104;
2. PIVARIU, Cornel, *Lumea secretelor*, Editura Pastel, Braşov, 2007;
3. TOHĂNEAN, D., *Securitate şi informații. Note de curs,* Sibiu, Editura Academiei Forțelor Terestre „Nicolae Bălcescu", 2014;

4. IVANOV, M. (coord.), *Pentru o lume mai sigură într-o eră a incertitudinii: contribuția serviciilor de informații,* Sibiu, Editura Academiei Forțelor Terestre „Nicolae Bălcescu", 2013;
5. TALEB, Nassim Nicholas, *Lebăda neagră*, Editura Curtea Veche, ed. a III-a revizuită, 2018, pp.504;
6. http://www.orniss.ro/ro/585cap8.html;
7. https://www.academia.edu/4547633/curs_OSINT, coord. S. Marius, *Curs Open Source Intelligence* (OSINT);
8. http://www.oss.net/dynamaster/file_archive/030201/ca5fb66734f540fbb4f8f6ef759b258c/NATO%20OSINT%20Handbook%20v1.2%20-%20Jan%202002.pdf;
9. https://moldova.europalibera.org/a/epidemia-de-coronavirus-%C8%99i-infodemia-de-fake-news/30499782.html;
10. https://www.digi24.ro/stiri/actualitate/epidemia-de-fake-news-cum-ii-viruseaza-rusia-pe-romani-cu-minciuni-periculoase-sunt-echipe-de-sociologi-psihologi-agenti-secreti-1290557;
11. https://www.dw.com/en/nato-russia-targeted-german-army-with-fake-news-campaign/a-37591978.

---

[1] Richicinschi, Iurie, Evoluții ale mediului internațional de securitate, în revista *Administrare publică,* nr. 1/2017, accesat în 17.05.2020.

[2] C. Pivariu, *Lumea secretelor*, Editura Pastel, Braşov, 2007, p. 266.

[3] http://www.orniss.ro/ro/585cap8.html, accesat în 18.05.2020.

[4] https://www.academia.edu/4547633/curs_OSINT, coord. S. Marius, *Curs Open Source Intelligence (OSINT)*, accesat în 18.05.2020.

[5] http://www.oss.net/dynamaster/file_archive/030201/ca5fb66734f540fbb4f8f6ef759b258c/NATO%20OSINT%20Handbook%20v1.2%20-%20Jan%202002.pdf, accesat în 19.05.2020.

[6] C. Pivariu, *op. cit.*,p. 83.

[7] Tohănean, D., *Securitate şi informații. Note de curs,* Sibiu, Editura Academiei Forțelor Terestre „Nicolae Bălcescu", 2014, p.86.

[8] Ivanov, M., *Pentru o lume mai sigură într-o eră a incertitudinii: contribuția serviciilor de informații,* Sibiu, Editura Academiei Forțelor Terestre „*Nicolae Bălcescu*", 2013, p. 188.

[9] https://www.academia.edu/35828846/Nassim_Taleb-Lebada_neagra.

[10] https://moldova.europalibera.org/a/epidemia-de-coronavirus-%C8%99i-infodemia-de-fake-news/30499782.html.

[11] *Idem*.

[12] https://www.digi24.ro/stiri/actualitate/epidemia-de-fake-news-cum-ii-viruseaza-rusia-pe-romani-cu-minciuni-periculoase-sunt-echipe-de-sociologi-psihologi-agenti-secreti-1290557.

[13] https://www.dw.com/en/nato-russia-targeted-german-army-with-fake-news-campaign/a-37591978.

IMPLICAȚIILE TEHNOLOGIEI 5G ASUPRA SECURITĂȚII NAȚIONALE

Marius PREDA
Constantin NILĂ
Cornel ARGINT*

Abstract

5G Technology, while being operationalized before the implementation of the specific assigned standard IMT-2020, is considered to be a game changer in the communications field with an impact on the industry and society equivalent with the Internet breakthrough. 5G has the capacity to enhance civil and military communications systems, the intelligence field and critical communications infrastructures. Despite all the benefits brought by the new technology, 5G has become the source of the first strategic dispute between US and China in the technological field (non-literary known as the first „cold war in technology field"). This article is presenting an analytic perspective of the risks associated with the 5G with regard to national security.

Keywords: *5G, IoT, cyber security, critical infrastructures, national security.*

Introducere

5G reprezintă o nouă generație a tehnologiei mobile fără fir, aflată încă în fază de dezvoltare, care promite o viteză mult mai mare de transfer a datelor, latență redusă și aplicații noi pentru Internet of Things (IoT) prin utilizarea a milioane de antene instalate pe turnurile de telecomunicații, dar și pe alte structuri publice și private, precum stâlpi de iluminare, clădiri, poduri etc. Această tehnologie este proiectată să suplimenteze și să îmbunătățească serviciile de telecomunicații oferite de standardele actuale, oferind viteze superioare, comparabile cu rețelele clasice pe cupru și fibră optică.

În România, potrivit *„Strategiei naționale de implementare a tehnologiei 5G"* [1], ANCOM (Agenția Națională pentru Reglementare în Domeniul Comunicațiilor) a alocat resurse suficiente de spectru pentru buna funcționare a serviciilor comerciale 5G în benzi de frecvențe radio utilizate cu predilecție în Europa: 700MHz și 3.4-3.8 GHz în anul 2019, urmând ca până la sfârșitul anului 2020 să fie adăugate și benzile milimetrice (24.25-27.5 GHz, banda de 26 GHz). În același document este subliniată ideea de utilizare a rețelei 5G (anul 2025) pentru serviciile de siguranță publică și intervenție în caz de dezastru.

Tehnologia 5G reprezintă răspunsul la cererile consumatorilor care au modelat serviciile mobile din ziua de azi. În ultima perioadă s-a observat o migrare a clienților dinspre serviciile clasice de voce și mesagerie către servicii de date, datorită caracteristicilor oferite de aplicațiile online multimedia, precum *FaceTime, Telegram, WeChat și Whats App,* și calității superioare a serviciilor furnizate. Creșterea anticipată a traficului de date, a numărului de dispozitive, servicii, precum și cererea de accesibilitate sporită au condus la identificarea unor soluții inovatoare și la reutilizarea unor benzi de frecvență în acest scop.

Autorii sunt experți în cadrul Ministerului Apărării Naționale.

În prezent, rețelele 3G și 4G se confruntă cu provocări din ce în ce mai mari în deservirea ecosistemelor digitale moderne (case, clădiri și orașe inteligente, realitate virtuală, automatizarea industriei, autovehicule autonome). Conform furnizorilor de tehnologie, 5G va permite transferul a zeci de Gbps, conectarea în mod fiabil a unui număr extrem de mare de dispozitive și procesarea acestui volum de date cu o întârziere minimă, contribuind astfel la realizarea tuturor celor 17 obiective de dezvoltare durabilă (*Sustainable Development Goals)* stabilite de Națiunile Unite pentru anul 2030[4].

Caracteristicile tehnologiei 5G

La fel ca în cazul tehnologiei 4G, Uniunea Internațională a Telecomunicațiilor (*International Telecommunications Union*/ITU) a organizat o serie de grupuri de lucru (ITU-R WP5D) în vederea standardizării cerințelor și parametrilor specifici tehnologiei emergente (IMT-2020) [2]. În urma acestora, participanții au ajuns la un acord cu privire la parametrii cheie care descriu cel mai bine tehnologia 5G, conform tabelului de mai jos.

Parametru	Valoarea nominală stabilită	Referința 4G
Rată de transfer	100 Mbps – 1 Gbps	10 Mbps
Viteză maximă	20 Gbps	1 Gbps
Mobilitate	500 km/h	350 km/h
Latență	1 ms (interferențe radio)	10 ms (interferențe radio)
Densitate de conexiuni	10^6 per km^2	10^5 per km^2
Eficiență energetică	de până la 100 de ori mai mare decât 4G	
Trafic de date pe suprafață	de până la 3 ori mai mare decât 4G	

Principalele caracteristici specifice tehnologiei 5G sunt: creșterea vitezei de trafic a utilizatorilor la valori de 10-20 Gbps, cu o experiență reală a utilizatorilor de 100 Mbps (exterior) și 1 Gbps (interior), creșterea lățimii de bandă în același ordin de mărime, scăderea latenței la valoarea de 1-2 ms/comunicație, acoperire urbană totală cu antenele „Massive MIMO[1]", introducerea unor noi protocoale de securitate prin implementarea unui nou sistem de autentificare la rețea (5G-AKA, EAP-AKA, EAP-TLS), operaționalizarea conceptului de *„rețele definite software*" (SDN), implementarea sistemelor de separare a rețelelor în subrețele dedicate (en. *Network Slicing*) și migrarea către virtualizarea de rețea (*Network Virtual Function*/ NVF) și către sistemele de tip *native cloud*.

Totodată, în cadrul grupurilor de lucru desfășurate s-au stabilit și principalele aplicații care urmează să utilizeze tehnologia 5G. Aceste aplicații se încadrează preponderent în domeniul IoT, cele trei direcții de dezvoltare (comunicații de bandă largă, comunicații masive M2M <*Machine-to-Machine*>, comunicații ultrafiabile cu întârzieri minime) fiind concepute pentru a susține dezvoltarea unei societăți inteligente prin intermediul conectării senzorilor și dispozitivelor de automatizare la infrastructura 5G.

Principalii furnizori de tehnologie 5G

Există un număr restrâns de companii cheie care au luat parte la testarea tehnologiilor implicate, definind în esență componentele și standardele sistemului global 5G. Șapte dintre cei mai cunoscuți sunt Ericsson, Hewlett-Packard Enterprise (HPE), Intel, Nokia, Qualcomm, Huawei și ZTE.

Ericsson a introdus în anul 2017 pe piață câteva produse 5G, precum nucleul 5G, mecanismul global de acces și transport denumit *New Radio* (NR) și sistemul său 5G bazat pe segmente de rețea. Compania suedeză a completat platforma 5G NR introducând sistemul radio Air 3246, care suportă FDD[2] și MIMO. Sistemul permite operatorilor să îmbunătățească capacitatea 4G pentru abonații lor și să fie pregătiți pentru implementarea tehnologiei 5G pe viitor, utilizând același hardware [5].

În 2019, Ericsson și Telekom Germania au obținut o rată de transfer a datelor constantă de 100 Gbps într-o conexiune de test cu microunde pe o distanță de 1,5 km. Experimentul a fost realizat în cadrul Centrului de Servicii Telekom

din Atena, Grecia, şi a atins viteze de transfer de 10 ori mai mari decât soluțiile comerciale curente pe un spectru similar de unde milimetrice de 70/80 GHz[6].

Una dintre contribuțiile cele mai reprezentative ale HPE la standardul 5G este colaborarea sa continuă cu 5G LabGermany, un consorțiu de cercetători care lucrează la rețele wireless 5G. Prin această colaborare, HPE studiază impactul rețelelor wireless 5G asupra industriilor de telecomunicații şi de telefonie mobilă. Compania testează implementarea sistemelor sale *Edgeline* la marginea rețelei pentru a monitoriza performanța rețelei 5G [7].

Intenția este de a dezvolta sisteme de calcul de înaltă performanță care să poată consuma şi analiza date instantaneu pentru a răspunde nevoilor următoarei generații de aplicații de automatizare şi mobile, utilizate în oraşe inteligente. În spatele acestor nevoi de consum vor sta, foarte probabil, implementări ale algoritmilor de inteligență artificială, atât în procesul de instruire pentru testare, cât şi în cel de predicție pentru aplicații comerciale. HPE deține o vastă experiență în dezvoltarea de sisteme de calcul de înaltă performanță, fiind unul dintre principalii furnizori şi pe această piață.

Intel este un alt furnizor cheie pentru tehnologia emergentă, cu platforma sa mobilă de testare 5G, MTP[3] care susține standardul NR, şi a fost testată cu succes în anul 2017 în cadrul verificărilor de funcționare cu rețele de acces radioexistente. MTP permite testarea rapidă a interoperabilității, permițând operatorilor să simuleze situații reale şi definirea specificațiilor finale (ITU lăsând la îndemâna operatorilor anumiți parametri) [8].

În luna mai a anului 2019 Intel a anunțat că ZTE, o companie multinațională de echipamente şi sisteme de telecomunicații, a selectat dispozitivele *Intel e ASIC* pentru produsele sale wireless 5G. ZTE a optat pentru dispozitivele Intel pentru a satisface cerințele critice de cost şi putere cerute de implementările 5G la scară largă.

ZTE a utilizat în trecut dispozitive FPGA[4] pentru prototipurile sale şi implementări de test. Compania a trebuit să reducă drastic costurile pe unitate pentru a rămâne în topul marilor producători de tehnologie 5G. Compania, de origine chineză, a fost dedicată dezvoltării tehnologiei 5G şi a introdus pe piață mai multe elemente cheie, printre care se numără şi accesul partajat pentru mai mulți utilizatori (MUSA[5]), care creşte în mod semnificativ numărul de conexiuni suportate de sistem. ZTE a aplicat în mod creativ tehnologia MIMO în rețelele 4G şi a lansat cu succes produsele comerciale Pre5G pentru operatorii din întreaga lume. De asemenea, această companie a derulat primele teste de înaltă frecvență (26 GHz)[9].

Compania Nokia a realizat o demonstrație a viitoarelor rețele 5G pe o platformă comercială, utilizând tehnologia *5G-ready Air Scale Radio Access,* care funcționa împreună cu sistemul *Cloud Pachet Core* instalat pe platforma de date *Nokia Air Frame.* Această arhitectură poate deveni standard pentru sistemele 5G comerciale, atestând progresul companiei în realizarea de echipamente 5G care deservesc o lume multi-conectată. Compania finlandeză a dezvoltat în 2017 o soluție numită Nokia 5G FIRST, care cuprinde antenele adaptive *MIMO RAN*, *AirScaleMIMO* şi soluțiile de transport mobil, concentrându-se asupra segmentării în rețea şi a modului în care poate sprijini diferite alte industrii[10].

În acelaşi an, compania americană Qualcomm a anunțat sistemul prototip *5WNR mm Wave,* bazat pe specificațiile 5G elaborate de 3GPP. Sistemul opera în benzile de frecvență destinate undelor milimetrice de peste 24GHz. Acest sistem dezvoltat pentru furnizarea comunicațiilor mobile în bandă largă, cu rate de transfer de ordinul zecilor de Gbps, a convins companii rivale, precum Apple, să încheie parteneriate şi înțelegeri de colaborare cu compania multinațională americană de echipamente semiconductoare şi echipamente de telecomunicații.

Qualcomm deține aproximativ 15% din brevetele tehnologice 5G din lume, potrivit Forbes [16], în contextul în care compania este unul dintre cei mai mari producători de chipset-uri de telefoane inteligente din lume. În octombrie 2018, Qualcomm a devenit singurul producător de modem-uri şi antene 5G din Statele Unite.

În acelaşi timp, administraţia prezidenţială a SUA continuă blocarea ofertelor de miliarde de dolari pentru producătorul de cipuri, invocând securitatea naţională.

Huawei a lansat soluţia sa, *5G Simplified Solution,* în luna februarie a anului 2019, în cadrul Congresului Mondial Mobile (Barcelona). Compania şi-a concentrat eforturile pentru a sprijini operatorii în crearea de reţele 5G *simple* cu performanţă superioară la un cost redus. Totodată, compania aduce pe piaţă şi dispozitive pentru consumatori, pentru ca aceştia să poată beneficia de noua tehnologie[11].

În poziţia sa de cel mai mare furnizor de tehnologie de telecomunicaţii şi al doilea cel mai mare producător de dispozitive de tip *smartphone* din lume, compania chineză se află într-o poziţie de invidiat când vine vorba de 5G. În prezent, nicio companie americană de telecomunicaţii nu produce echipamente wireless la acelaşi nivel, vitale dezvoltării 5G. Cu toate acestea, poziţia puternică a companiei Huawei pe piaţa 5G a fost pusă sub semnul întrebării datorită apropierii de guvernul chinez.

În ciuda presiunii exercitate de SUA, compania înregistrează progrese semnificative în numeroase proiecte 5G din întreaga lume. Pe piaţa chineză, care se estimează că va depăşi piaţa din restul lumii până în 2025, compania continuă să deţină prima poziţie. Pe lângă R.P. Chineză, compania a semnat contracte vitale cu state din Africa şi America Latină, fapt ce îi va asigura o poziţie importantă pe plan global.

În timp ce acoperirea reţelelor comerciale 5G se extinde, se observă şi o creştere a numărului companiilor care prezintă interes în această zonă. Astfel, pe lângă companiile prezentate mai sus, se observă un interes al marilor furnizori de comunicaţii mobile, cei mai ambiţioşi pe plan mondial fiind AT&T şi Verizon, ce luptă pentru monopol în Statele Unite. T-Mobile a ales să utilizeze un spectru 5G cu bandă joasă în loc de tehnologiile *mmWave,* dezvoltate în prezent de AT&T şi Verizon. Această abordare prezintă potenţialul unei lăţimi de bandă mai mari în detrimentul gamei de semnal.

Pe de altă parte, pe lângă compania Samsung, care şi-a afirmat interesul de dezvoltare a dispozitivelor 5G premium, avem şi companii care doresc doar să ocupe o poziţie în topul vânzărilor, oferind dispozitive smart 5G la preţuri accesibile. Printre acestea se numără Xiaomi, Honor, Sony, OnePlus, OPPO, Lenovo şi Motorola.

Poziţii internaţionale privind implementarea 5G

La nivelul Uniunii Europene nu există o politică unitară referitoare la integrarea tehnologiilor 5G dezvoltate de companii chineze. Germania, Franţa, Italia şi Ungaria s-au pronunţat împotriva interzicerii totale a echipamentelor 5G produse în R.P. Chineză, iar unele state din estul UE (Polonia, Cehia) au solicitat UE să excludă Huawei din lista furnizorilor de echipamente IT&C. În urma efectuării de expertize tehnice de către furnizorii de servicii de comunicaţii din UE asupra echipamentelor produse de cele două companii chinezeşti, nu au fost descoperite indicii care să probeze afirmaţiile oficialilor americani.

NATO are o abordare similară cu cea a UE, organizaţia nepronunţându-se încă cu privire la utilizarea produselor din R.P. Chineză. Secretarul General NATO, Jens STOLTENBERG, a declarat (în cadrul unei conferinţei desfăşurate la Institutul Lowy din Sidney/Australia, 07.08.2019), că structurile de specialitate din cadrul NATO sunt în proces de analizare şi revizuire a politicilor de securitate privind canalele de comunicaţii, urmând ca o decizie finală să fie luată ulterior.

SUA a fost primul stat care a interzis utilizarea în reţelele de comunicaţii destinate agenţiilor guvernamentale a soluţiilor 5G de provenienţă chinezească. Ulterior, această poziţie a fost adoptată şi de Australia, Noua Zeelandă, Japonia şi Taiwan. Deşi principalul motiv de îngrijorare exprimat de administraţia de la Washington îl reprezintă presupusele breşe de securitate destinate culegerii de informaţii şi acţiunilor cibernetice în favoarea R.P. Chineze, până în prezent instituţiile abilitate din SUA nu au prezentat public rapoarte care să aducă dovezi concrete, de natură tehnologică, cu privire la riscurile şi ameninţările echipamentelor IT produse de companiile chinezeşti Huawei şi ZTE.

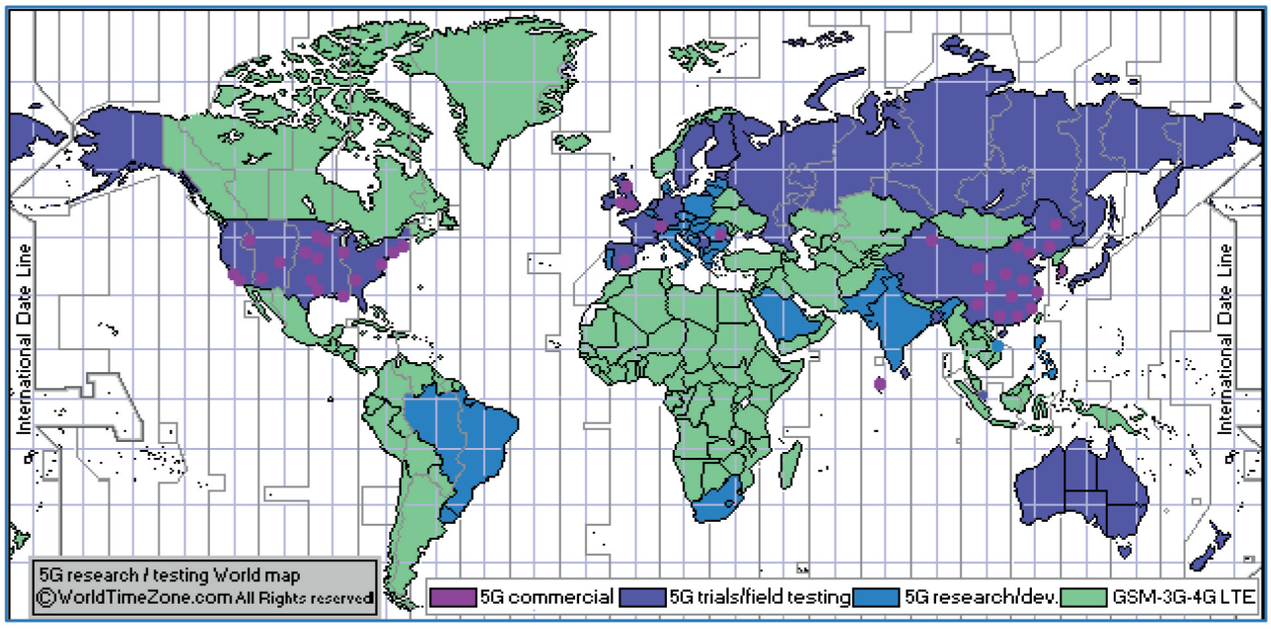


Figura 1 - Acoperirea 5G [17]

Autoritățile din Marea Britanie au aprobat (ianuarie 2019) dezvoltarea infrastructurii 5G şi cu ajutorul unor echipamente ale companiei Huawei. Acestea nu vor fi utilizate în construirea unor elemente esențiale (din cadrul unor obiective militare sau de infrastructură critică), compania fiind limitată la o cotă de piață de 35%. Cu toate acestea este posibil ca relațiile cu SUA (în contextul Brexitului) să fie afectate de această decizie.

Federația Rusă a dezvoltat relațiile în domeniu cu R.P. Chineză prin sprijinirea directă a companiei Huawei, oferindu-i acces (sub incidența unor condiții) la piața internă 5G. Astfel, au fost dezvoltate două centre de cercetare şi dezvoltare în domeniul tehnologiilor disruptive (5G, IA), a fost demarată dezvoltarea rețelei 5G începând cu zona centrală a Moscovei, iar compania aeronautică MiG a utilizat în premieră echipamentele Huawei (servere şi procesoare) pentru retehnologizarea infrastructurii, deşi prevederile interne impun utilizarea tehnologiei produse în Federația Rusă.

Este posibil ca Federația Rusă să apeleze în continuare la tehnologia 5G chineză, precum şi la dezvoltările din domeniul inteligenței artificiale şi comunicațiilor cuantice, în lipsa know-how-ului şi a sistemelor proprii naționale, ca urmare a menținerii sancțiunilor internaționale din partea SUA şi a statelor UE referitoare la importul de tehnologie şi sisteme avansate.

R.P. Chineză este, în prezent, evaluată ca fiind lider de piață în ceea ce priveşte tehnologiile care acoperă spectrul de frecvențe de până la 6 GHz (sub-6) şi va fi cel mai probabil prima țară care va reuşi să implementeze tehnologia 5G pe scară largă utilizând resurse proprii. De asemenea, companiile chineze, care foarte probabil au beneficiat anterior de anumite facilități din partea guvernului de la Beijing, sunt în acest moment cele mai bine poziționate din perspectiva furnizării sistemelor necesare implementării noii tehnologii[22].

Argentina şi Brazilia intenționează să nu limiteze implicarea companiilor chineze în dezvoltarea infrastructurii 5G. În pofida unor reticențe inițiale, Coreea de Sud, Filipine, Tailanda şi alte state din sud-estul Asiei au început testarea şi implementarea echipamentelor Huawei în infrastructura 5G proprie.

Riscuri asociate implementării tehnologiei 5G

Principalele posibile amenințări la adresa securității, evidențiate de evaluarea coordonată la nivelul UE a riscurilor [21], sunt legate de inovațiile-cheie (factori tehnici) în domeniul tehnologiei 5G (în special rolul important al programelor informatice şi gama largă de servicii şi aplicații pe care le va oferi tehnologia 5G) şi de rolul furnizorilor în implementarea şi operarea

rețelelor 5G, dar şi de gradul de dependență de anumiți furnizori. Alte riscuri identificate, care pot avea implicații asupra securității naționale, pot fi generate de factori de natură umană, economică şi juridică.

Riscuri generate de factori tehnici

La începutul anului 2018, M. Dehnel-Wild şi colab. prezentau [12] vulnerabilități descoperite în noul standard de telecomunicații. Un atac reuşit ar fi afectat confidențialitatea, integritatea şi autenticitatea datelor tranzitate prin canalul de comunicații compromis. Vulnerabilitățile identificate au fost remediate, însă este aproape cert faptul că noi vulnerabilități vor fi descoperite şi exploatate.

Mai mult decât atât, vulnerabilitățile cunoscute care afectează protocolul actual, LTE, sunt aplicabile şi pentru noua tehnologie, având efecte similare sau de întrerupere a serviciului [13].

Un grup de cercetători din SUA a descoperit trei vulnerabilități noi în tehnologiile 4G şi 5G, acestea fiind făcute cunoscute publicului în luna februarie a anului 2019. Aceste vulnerabilități permit unui atacator să intercepteze un apel telefonic şi să urmărească locația unui utilizator de telefon mobil [14]. Pe lângă aceste vulnerabilități, atacatorii pot scădea în mod controlat şi insesizabil standardul de comunicații la GSM (pentru a derula atacuri de tip MITM[6]) sau întrerupe serviciile oferite prin rețeaua 5G. În acest context, reprezentanți ai serviciilor de securitate din 30 de state membre ale Uniunii Europene şi NATO au agreat, în luna mai 2019 (la Praga), un set de recomandări pentru viitoarele rețele 5G.

Rolul jucat de tehnologia 5G în contextul securității este unul major, prin prisma dispozitivelor care vor fi conectate la Internet şi vor influența categoric viețile utilizatorilor. Implementarea 5G poate conduce la riscul amplificării capacităților de atac cibernetic pentru vectorii de atac prin creşterea capacităților de bandă, a suprafeței de atac şi prin diminuarea latenței canalelor de comunicații. De asemenea, prin extinderea IoT şi a comunicațiilor M2M, suprafața atacurilor cibernetice va creşte direct proporțional cu noile puncte de intrare create.

O atenție deosebită trebuie acordată acelor servicii 5G care facilitează sau deservesc activități care sunt sau ar putea fi necesare pentru a asigura un standard minim de trai şi bunăstare al societății şi a căror degradare sau întrerupere a furnizării, ca urmare a perturbării sau distrugerii sistemului fizic de bază, ar afecta semnificativ siguranța sau securitatea populației şi funcționarea instituțiilor de stat.

Sistemele informatice prin care sunt operate elemente din infrastructura critică sunt vizate de atacatori bine pregătiți şi finanțați. Schimbarea arhitecturii de rețea, de la echipamente care utilizează linii de cupru sau fibră optică la sisteme moderne ce angrenează mii de transmisii wireless, nu modifică problematica securității rețelei respective.

Apare necesitatea adaptării tehnologiilor actuale de securitate cibernetică la o nouă infrastructură şi arhitectură de rețea - implementarea conceptului „politică de securitate cibernetică dinamică". Direcția de evoluție se impune datorită implementării inovațiilor tehnice, precum şi a conceptelor SDN, SDR şi NVF. Introducerea inovațiilor 5G va conduce la apariția unor noi vectori de atac şi oportunități de atac cibernetic în mediul digital global.

Suplimentar, rețelele de tip 5G vor interconecta echipamente utilizate în serviciile de siguranță publică şi intervenție în caz de dezastru, parte a infrastructurii critice, alături de sectoarele energetic, transporturi, bancar şi sănătate. Atacuri conduse de actori statali la adresa acestor sectoare au determinat în trecut crize dificil de gestionat (Ucraina 2015, Venezuela 2019, SUA 2019, Georgia 2019).

Problemele pot fi evitate prin verificarea atentă a lanțului de aprovizionare cu tehnologie, de la faza de fabricare a integratelor utilizate şi respectarea standardelor şi a măsurilor de securitate impuse până la distribuirea acestor sisteme către consumatori. Codul sursă utilizat trebuie, de asemenea, auditat şi modul de funcționare verificat periodic prin teste specifice fiecărui echipament.

Cu toate acestea, atacurile asupra sistemelor naționale, publice sau private care interacționează

cu infrastructura critică sunt foarte dificil de prevenit fără un organism eficient de protecție și răspuns în caz de incident.

Soluțiile consacrate de protecție, precum echipamentele IDS/IPS[7] sau NGFW[8], vor constitui în continuare fundația pentru securitatea rețelelor 5G. Riscul va fi dat de implementarea noilor standarde care vor implica, foarte probabil, vulnerabilități specifice necunoscute și vor face ca recunoașterea atacurilor în noile rețele să fie foarte dificilă.

Totodată, volumul mai mare de date procesate va presupune un volum mai mare de alerte și evenimente de securitate de analizat, utilizând soluții de monitorizare (de exemplu, SIEM[9]). În acest context, pentru implementarea adecvată a oricărui program 5G, vor trebui luate în considerare soluții emergente de monitorizare și detecție, care utilizează tehnici avansate de *machine learning* (ML).

Securitatea informației reprezintă o problemă fundamentală pentru infrastructura IT, soluțiile de protecție cu ML oferind un avantaj considerabil în fața amenințărilor avansate. Comunitățile care prezintă interes în acest domeniu încearcă, pe de o parte, să țină pasul cu noile tehnologii care apar în mod accelerat, iar pe de altă parte, să dezvolte soluții specializate.

Vulnerabilitățile prezentate mai sus sunt confirmate de raportul întocmit de Agenția Uniunii Europene pentru Securitate Cibernetică, în colaborare cu Comisia Europeană și statele membre, potrivit căruia riscurile de securitate principale decurg din inovațiile aduse de noua tehnologie [18].

Pe lângă amenințările la adresa confidențialității, dat fiind faptul că rețelele 5G urmează să devină coloana vertebrală a numeroase aplicații informatice esențiale, integritatea și disponibilitatea acestor rețele vor deveni preocupări majore în materie de securitate națională și o provocare esențială în materie de securitate din perspectiva UE [20].

Având în vedere faptul că rețelele 5G se bazează din ce în ce mai mult pe programe informatice, devin tot mai importante riscurile legate de deficiențele majore în materie de securitate, cum ar fi cele generate de procesele necorespunzătoare de dezvoltare a programelor informatice de către furnizori. Aceste deficiențe ar putea, de asemenea, să faciliteze introducerea cu rea-intenție de către factorii de amenințare a unor tehnologii de tip „*backdoor*” în produse și să îngreuneze detectarea lor.

Riscuri generate prin dependența de furnizori

O dependență majoră de un singur furnizor sporește expunerea la o potențială întrerupere a aprovizionării, rezultată, de exemplu, din eșecul comercial, și la consecințele acesteia. De asemenea, aceasta agravează eventualul impact al deficiențelor sau al vulnerabilităților, precum și posibila lor exploatare de către factorii de amenințare, în special în cazul dependenței de un furnizor care prezintă un grad ridicat de risc.

O expunere sporită la riscurile legate de dependența operatorilor de rețele mobile de furnizori va conduce la creșterea numărului de căi utilizate pentru atacuri care ar putea fi exploatate de factorii de amenințare și la eventuala agravare a impactului unor astfel de atacuri. Printre diverșii actori potențiali, statele terțe sau actorii sprijiniți de stat sunt considerați a fi cei mai periculoși și cei mai susceptibili să vizeze rețelele 5G [20].

De asemenea, din perspectiva securității naționale, creșterea dependenței infrastructurilor critice de producătorii majori de tehnologie de la nivel global (Nokia, Ericsson, Huawei și ZTE) poate reprezenta un risc major, mai ales în contextul în care companiile chinezești (jucătorii principali din piață) au fost suspectate, în ultimii, ani, că își folosesc echipamentele pentru spionaj cibernetic direcționat de guvernul de la Beijing.

În acest context, de expunere sporită la amenințări facilitate de furnizori, profilul de risc al fiecărui furnizor va deveni deosebit de important, inclusiv probabilitatea ca o țară terță să se implice în activitatea furnizorului.

Alte riscuri relevante pentru securitatea națională

Riscuri generate de componenta umană. Fondatorul companiei Huawei, Ren ZHENGFEI,

este un fost inginer militar care a lucrat în Armata Populară de Eliberare. Până în anul 2018, funcția de preşedinte executiv al companiei a fost ocupată de un fost ofițer al Ministerului Securității Statului, care a asigurat stabilirea unor legături strânse între companie şi serviciile de securitate chineze. De asemenea, cea mai mare parte a angajaților Huawei şi ZTE sunt cetățeni chinezi care au obligații patriotice față de statul chinez, statuate prin lege.

Riscuri economice. Potrivit datelor publice, companiile Huawei şi ZTE au beneficiat de un sprijin financiar consistent din partea guvernului de la Beijing, care este unul din cei mai importanți clienți ai celor două companii, astfel că acestea sunt dependente de menținerea unor bune relații cu guvernul chinez.

Riscuri de natură juridică. Legislația chineză obligă atât persoanele fizice, cât şi persoanele juridice private să coopereze cu structurile guvernamentale în probleme de securitate națională [19], de unde suspiciunea că, la cerere, Huawei şi ZTE ar putea oferi guvernului de la Beijing informații confidențiale conexe funcționării rețelelor 5G proprii în alte state.

Concluzii

A cincea generație de rețea de comunicații în spectrul radio va putea oferi comunicații rapide, în timp real, acoperire extinsă şi conexiuni stabile între sisteme de comunicații integrate civile şi militare. Implementarea acestei tehnologii se va concentra şi pe mijloacele de asigurare a securității infrastructurii 5G care poate fi afectată de sisteme de război electronic şi cibernetic.

Securitatea şi reziliența noilor sisteme 5G trebuie să devină o prioritate pentru toate organismele implicate, fiind esențial pentru fiecare stat să identifice propriile elemente din industrie care pot contribui la dezvoltarea tehnologiei. Un alt aspect care trebuie avut în vedere este generat de provocările apărute în cadrul lanțului de aprovizionare cu tehnologie, inițiate de globalizare, evoluția rapidă a pieților de desfacere, calitate şi conformitate.

Legăturile existente între producătorii chinezi de sisteme 5G şi structuri ale guvernului chinez generează suspiciuni asupra posibilității ca cele două companii să pună la dispoziția acestora mijloacele tehnice care să le permită accesul la sistemele comercializate în țări membre NATO sau UE. Până în prezent, toate pozițiile exprimate împotriva contractării celor două companii pentru dezvoltarea rețelelor 5G au fost fundamentate pe aceste suspiciuni, fără a fi prezentate dovezi concrete, pur tehnice.

Complexitatea foarte ridicată a sistemelor care formează rețelele 5G ar putea permite implementarea unor vulnerabilități încă din faza de proiectare, ceea ce le va face aproape imposibil de detectat chiar şi prin utilizarea de tehnici şi instrumente avansate.

Se poate aprecia că tehnologia 5G va juca un rol important în viitorul apropiat, veniturile la nivel mondial generate de aceasta fiind estimate la 225 de miliarde euro în 2025. Beneficiile introducerii tehnologiei 5G în cele patru sectoare industriale esențiale, şi anume cel al autovehiculelor, cel al sănătății, cel al transporturilor şi cel al energiei, ar putea ajunge la 114 miliarde euro pe an.

În momentul de față, există proiecte majore privind transformarea societății într-o „societate inteligentă", care urmăresc aducerea tuturor avantajelor tehnologice în viața de zi cu zi, respectiv în calitatea serviciilor publice şi private. În consecință, există premisele unei societăți viitoare consolidate pe interconectarea inteligentă a tuturor dispozitivelor care ne înconjoară şi a tehnologiilor care stau la baza acestora.

În timp ce avantajele unei astfel de societăți sunt clare, suprafața de atac din perspectiva vulnerabilităților introduse creşte exponențial. Totodată, efectele atacurilor asupra infrastructurii IoT vor fi amplificate direct proporțional şi mult mai dificil de contracarat.

Garantarea introducerii în siguranță a tehnologiei 5G este în mare măsură responsabilitatea actorilor de pe piață, securitatea națională este responsabilitatea fiecărui stat, iar, în ansamblu, securitatea rețelelor 5G este o chestiune de importanță strategică pentru întreaga piață unică şi pentru suveranitatea tehnologică la nivel european.

Bibliografie:

1. Autoritatea Națională pentru Administrare și Reglementare în Comunicații, 2018. http://www.ancom.org.ro/uploads/links_files/Strategia_5G_pentru_Romania.pdf [Accesat 2019].
2. H.-R. You, „Key Parameters for 5G Mobile Communications", NETMANIAS, 2015.
3. ITU, „5G overview", Setting the Scene for 5G: Opportunities and Challenges, pp. 3-9, 2018.
4. UN, „The Sustainable Development Goals (SDGs)", UNDP, 2015. https://www.undp.org/content/undp/en/home/sustainable-development-goals.html [Accesat 2019].
5. „Ericsson expands its 5G portfolio", Ericsson, 05 Septembrie 2017. https://www.ericsson.com/en/press-releases/2017/9/ericsson-expands-its-5g-portfolio [Accesat 2019].
6. „Deutsche Telekom and Ericsson top lOOGbps over microwave link", Ericsson, 10 Mai 2019. https://www.ericsson.com/en/press-releases/2019/5/deutsche-telekom-and-ericsson-top-100gbps-over-microwave-link [Accesat 2019].
7. „The Top 5G Vendors Around the Globe", SDxCentral, 2017. https://www.sdxcentral.com/5g/definitions/5g-vendors-around-globe/ [Accesat 2019].
8. „With Intel's Help, 5G Pushes Toward 2020 Deployment", Intel, 07 Septembrie 2017. https://newsroom.intel.com/editorials/intels-help-5g-pushes-toward-2020-deployment/#gs.c0umls [Accesat 2019].
9. „ZTE 5G Going Beyond Reality", ZTE, 2017. https://www.zte.com.cn/china/topics/zte-5g-en/index.html [Accesat 2019].
10. „Nokia heralds 5G era with commercial end-to-end 5G FIRST #MWC17", Nokia, 26 Februarie 2017. https://www.nokia.com/about-us/news/releases/2017/02/26/nokia-heralds-5g-era-with-commercial-end-to-end-5g-first-mwcl7/ [Accesat 2019].
11. „Huawei Launches 5G Simplified Solution", Huawei, 26 Februarie 2019. https://www.huawei.com/en/press-events/news/2019/2/huawei-5g-simplified-solution [Accesat 2019].
12. M. Dehnel-Wild şi C. Cremers, „Security vulnerability in 5G-AKA draft", Department of Computer Science, University of Oxford, 2018.
13. R. P. Jover şi V. Marojevic, „Security and Protocol Exploit Analysis of the 5G Specifications", 2018.
14. Z. Whittaker, „New flaws in 4G, 5G allow attackers to intercept calls and track phone locations", Februarie 2019. https://techcrunch.com/2019/02/24/new-4g-5g-security-flaws/ [Accesat 2019].
15. R. Desai, „5G", 1 Decembrie 2019. http://drrajivdesaimd.com/2019/12/01/5g/ [Accesat 2019].
16. S. Mc Bride, „The 5G Revolution Starts Next Year, And This Stock Will Double As A Result", Forbes, 15 Octombrie 2018. https://www.forbes.com/sites/stephenmcbride1/2018/10/15/the-5g-revolution-starts-next-year-and-this-stock-will-double-as-a-result/#621de9b2343b [Accesat 2019].
17. „5G - World Time Zone", https://www.worldtimezone.com/5g.html [Accesat 2020].
18. „EU coordinated risk assessment of the cyber security of 5G networks", NIS Cooperation Group, octombrie 2019.
19. China's National Intelligence Law, Iunie 2017.
20. „Cyber security of 5G networks. EU Toolbox of risk mitigating measures", NIS Cooperation Group, CG Publication, ianuarie 2020.
21. John R. Hoehn, Kelley M. Sayler - National Security Implications of Fifth Generation (5G) Mobile Technologies, Congressional Research Service, 25 martie 2020.

[1]MIMO - Multiple Input, Multiple Output;
[2]FDD- Frequency Division Duplex;
[3]MTP - Mobile Trial Platform;
[4]FPGA - Field Programmable Gate Array, este un tip de circuit logic programabil;
[5] MUSA - Multi-UserShared Access;
[6] MITM - Man In The Middle.
[7]IDS/IPS - Intrusion Detection System/ Intrusion Prevention System;
[8] NGFW- Next-Generation Firewall;
[9] SIEM - Security information and event management.

GEOINT – DOMENIUL DE CONVERGENȚĂ AL DISCIPLINELOR DE INTELLIGENCE

Alexandru ZAMFIR
Cătălin CONDURACHE
*Ionuț MIHAI**

Abstract

In the current security context, due to the massive influx of information faced daily by intelligence services, GEOspatial INTelligence (GEOINT) capability offers the ability to collate and integrate data and raw information from other intelligence sources and disciplines, such as HUMan INTelligence (HUMINT), SIGnal INTelligence (SIGINT) and Open Source INTelligence (OSINT). In this manner, the multi-source analysis can be optimized by changing the classic intelligence paradigm, where the information collected is stored into a database and keywords are used for interrogation. GEOINT provides powerful and modern tools to the analysts, which can easily project the available data and information using a geospatial support, making in this way the collation process more fast and reliable. Moreover, GEOINT can support also the collection of information and the dissemination of intelligence products, contributing in this way to the optimization of the intelligence cycle.Given the aforementioned arguments, we can state that GEOINT represents the domain of convergence for all intelligence disciplines.

***Keywords**: GEOINT, geospatial support, imagery, intelligence, multi-source analysis.*

Introducere

În contextul actual de securitate, din cauza afluxului masiv de informații cu care se confruntă serviciile de informații (nivelul de veridicitate al informațiilor este dificil de stabilit/acestea își pierd rapid valoarea, se alterează şi pot conduce la decizii greşite), analiza GEOspatial INTelligence (GEOINT) oferă un instrument deosebit de util în elaborarea de produse informative cu grad ridicat de credibilitate în situații de criză şi oferă posibilitatea alegerii cursurilor de acțiune corespunzătoare.

Conform Agenției Naționale pentru Informații Geospațiale a SUA (National Geospatial Intelligence Agency – NGA), GEOINT constă în analiza şi exploatarea imaginilor şi informațiilor geospațiale pentru a descrie, evalua şi a evidenția vizual detaliile fizice şi activitățile referențiate geografic de pe suprafața Pământului[1].

În general, GEOINTpoate fi mai uşor definită ca fiind mulțimea de date, informații şi cunoştințe colectate despre entități care pot fi referențiate geografic, la o anumită locație de pe, deasupra, sau sub suprafața Pământului. Informațiile pot fi colectate prin senzori specifici GEOINT sau prin alte capabilități de intelligence de natură tehnică (SIGnal INTelligence – SIGINT sau Open Source INTelligence - OSINT) sau clasice (HUMan INTelligence - HUMINT).

Se remarcă necesitatea implementării în cadrul activității de intelligence a unor instrumente

Autorii sunt experți în cadrul Ministerului Apărării Naționale.

specifice GEOINT, materializate prin servicii şi aplicaţii GIS (Geographic Information System), care să permită furnizarea de date în timp real, cu o mare capacitate de procesare şi partajare a produselor rezultate în urma analizelor efectuate. Din această perspectivă, GEOINT reprezintă un element cheie care poate contribui la optimizarea ciclului informaţional.

În prezent, problema accesului la date şi informaţii s-a aplatizat, făcându-se trecerea de la era lipsei lor la era "BIG DATA". Astfel, abundenţa datelor şi informaţiilor din surse variate se poate transforma într-o problemă, iar validarea volumului mare de date şi informaţii a devenit una din principalele activităţi mari consumatoare de timp şi resurse. Culegerea de informaţii presupune monitorizarea unui set complex de ameninţări globale, de la zone în care sunt prezente conflicte militare până la activităţi politice sau economice. În acest context, domeniul GEOINT are capabilitatea de a gestiona informaţiile provenite din surse multiple şi de a oferi suportul necesar pentru realizarea în timp util şi diseminarea către beneficiari a unor produse informative precise, necesare luării deciziilor[2].

Câştigul operaţional adus de capabilitatea GEOINT

Dezvoltarea domeniului GEOINT depinde în mod direct de nivelul de ambiţie al instituţiei/serviciului de informaţii interesat, cu responsabilităţi în domeniul geospaţial, având în vedere faptul că această disciplină de intelligence reprezintă o capabilitate relativ recent apărută (spre deosebire de disciplinele clasice de intelligence), care necesită investiţii importante pentru implementare, operaţionalizare şi mentenanţă.

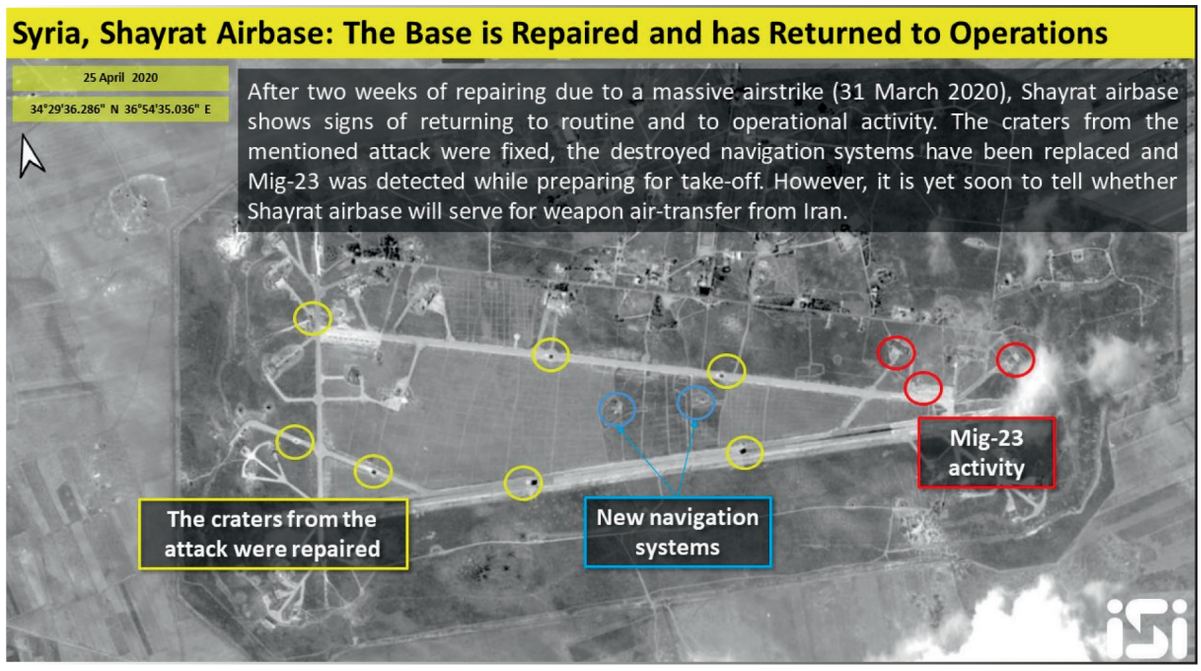
GEOINT face parte din efortul susţinut al oricărui serviciu de informaţii, civil sau militar, de a-şi moderniza capabilităţile, obiectivul final fiind creşterea capacităţii de a furniza avertizări timpurii cu privire la producerea unor evenimente cu impact major asupra securităţii statale sau a aliaţilor, în proximitatea teritoriului naţional sau în zonele unde forţele armate îşi desfăşoară activitatea[3].

GEOINT reprezintă mai mult decât informaţiile provenite din imagini aeriene sau satelitare. Este compus din totalitatea datelor spaţiale şi temporare georeferenţiate, provenite din orice tip de sursă[4], precum şi din produsele geospaţiale rezultate în urma analizei multisursă.

Principalul câştig operaţional adus de către această disciplină de intelligence este reprezentat de **accesul la date şi informaţii specifice**, oferit de către senzorii exploataţi de către capabilitatea GEOINT. Astfel, chiar dacă statul sau serviciul de informaţii în cauză nu beneficiează de platforme satelitare proprii pentru culegerea imaginilor şi datelor geospaţiale, multitudinea de companii comerciale care oferă imagini satelitare de foarte înaltă rezoluţie spaţială reprezintă o alternativă viabilă.

Spre deosebire de activitatea de culegere a imaginilor aeriene de pe platforme convenţionale - avioane sau UAV (Unmanned Aerial Vehicle) de recunoaştere - modalitatea de obţinere a datelor şi imaginilor satelitare este una neintruzivă, deoarece platformele satelitare nu sunt constrânse de reglementări specifice spaţiilor aeriene suverane ale altor state. Mai mult, prin intermediul traiectoriilor de orbitare ale platformelor satelitare, acoperirea globală cu imagini satelitare achiziţionate la o anumită frecvenţă de revizitare a zonelor de interes este posibilă prin procesul de tasking. Imaginile satelitare pot fi asigurate aproximativ în timp real, în funcţie de durata fluxului de procesare a datelor brute transmise de către satelit, prin intermediul staţiilor de control dispuse la sol.

Prin asigurarea accesului la o gamă vastă de senzori imagistici satelitari, influenţa unor limitări precum condiţiile atmosferice din zona de interes ce urmează a fi monitorizată sau condiţiile de iluminare (zi/noapte) poate fi redusă şi chiar eliminată. Pe lângă imaginile culese cu senzori electro-optici, GEOINT utilizează imagini SAR (Synthetic Aperture Radar), IR (Infra-Red) sau obţinute prin tehnologia LIDAR (LIght Detection And Ranging). În funcţie de particularităţile fiecărei analize, se pot achiziţiona imagini prin metode diferite pentru a satisface nevoile beneficiarilor. De exemplu, în cazul în



care un anumit obiectiv se doreşte a fi analizat pe timpul nopții se vor folosi imagini SAR, care nu sunt dependente de iluminarea solară[5].

O altă contribuție majoră adusă de către capabilitatea GEOINT este **determinarea cu precizie şi acuratețe ridicată a locației unor obiective de interes**. Aceasta este asigurată prin analiza imaginilor satelitare cu ajutorul fluxurilor de lucru specifice GEOINT. Pe lângă localizarea obiectivelor de interes, stabilirea dimensiunilor şi a altor caracteristici gabaritice este posibilă prin analiza imaginilor satelitare. Aceste date sunt utilizate de regulă în cadrul procesului de **targeting** sau pentru estimarea eficienței loviturilor aeriene (battle damage assessment).

Imaginea de mai sus prezintă un exemplu de produs informativ GEOINT, în care se pot observa atât distrugerile cauzate de către atacurile aeriene executate asupra unei baze aeriene din Siria, cât şi activitățile de reparare şi repunere în stare de funcționare a infrastructurii aeroportuare[6].

Mai mult, monitorizarea unei zone de interes cu scopul de a observa mişcările trupelor aparținând inamicului este posibilă prin **detectarea schimbărilor în cadrul unor serii temporale de imagini satelitare**. Pe baza acestora, coroborate cu informații provenite din surse colaterale, analistul de pe spațiul respectiv poate elabora estimări sau posibile cursuri de acțiune viitoare.

GEOINT - integrator al informațiilor provenite din surse de intelligence multiple

Pentru a face față noilor amenințări specifice secolului XXI, serviciile de informații trebuie să evolueze sau să se reinventeze. Necesitatea stabilirii de noi mijloace pretabile în cadrul analizei informațiilor este constantă. O posibilă cale prin care aceste mijloace pot fi obținute o reprezintă înlocuirea vechii paradigme[7], **de a colaționa informațiile** provenite din surse de intelligence multiple, prin stocarea acestora într-o bază de date şi interogarea pe baza cuvintelor cheie, **cu integrarea şi afişarea acestora pe o platformă de tip suport geospațial**, conectată la baza de date, şi filtrarea acestor date şi informații pe baza poziției lor geografice. Această nouă modalitate de colaționare pune la dispoziția analistului instrumente diverse, cu ajutorul cărora pot fi formulate aprecieri, concluzii, prognoze[8].

Abilitatea de integrare a informațiilor din surse precum HUMINT, SIGINT şi OSINT în sistemele de stocare şi prelucrare specifice GEOINT s-ar putea dovedi de o importanță vitală în rezolvarea provocărilor operaționale şi de securitate contemporane. Domeniul GEOINT oferă instrumentele necesare acestei integrări cu ajutorul unei platforme de tip „hartă digitală", interactivă şi dinamică. Efectele integrării informațiilor multisursă conferă procesului de analiză o dimensiune comprehensibilă prin

exploatarea concomitentă şi în totalitate a tuturor informațiilor disponibile. Un alt avantaj este reprezentat de reducerea riscului de omitere a anumitor date sau informații relevante. Astfel, analistul dispune **de întreaga "hartă" a evenimentelor dintr-o anumită zonă de interes** prin utilizarea instrumentelor furnizate de capabilitatea GEOINT. Procesul de corelare a datelor se reduce, la fel şi timpul necesar analistului pentru interogarea bazei de date. Analistul va dispune în acest mod de mai mult timp pentru crearea produsului informativ final.

Pentru implementarea acestei noi abordări în cadrul procesului de analiză sunt necesare **o serie de schimbări,** care se pot conceptualiza utilizând perspectiva factorilor critici („modelul celor 3P: Personal, Proces şi Produs")[9], astfel:

- **la nivelul personalului**:
  - este necesară instruirea personalului implicat în activitatea de culegere a informațiilor, astfel încât datele şi informațiile brute obținute prin metode specifice să fie însoțite de referințe geografice, cu ajutorul cărora infomația alfa-numerică[10] va putea deveni informație geospațială;
  - la nivelul personalului implicat în procesul de analiză este necesară instruirea în vederea familiarizării şi operării noilor platforme GIS şi a utilizării unor algoritmi spațiali pentru interogarea bazei de date, în scopul integrării şi coroborării datelor şi informațiilor.
- **la nivelul procesului**:
  - implementarea unei baze de date comună pentru stocarea informațiilor provenite din multiple surse de intelligence, având ataşate etichete geospațiale standardizate, pe baza referințelor geografice alocate de către structurile de culegere. Astfel, elementul comun central al datelor şi informațiilor brute va fi reprezentat de către poziționarea spațială, iar interfața de vizualizare şi exploatare a acestei baze de date va fi sub forma unei hărți digitale dinamice şi interactive;
  - având în vedere că GEOINT poate deveni factor accelerator în fuziunea INT-urilor[11], se remarcă posibilitatea realocării timpului „câştigat" de către analist datorită identificării mai rapide a informației relevante în soluționarea cererii de informații.
- **la nivelul produsului**:
  - GEOINT oferă posibilitatea elaborării unor produse de intelligence complexe, în care partea analitică a produsului final de intelligence este armonizată cu partea geospațială, prin includerea unor informații imagistice de tip „hartă" în care sunt surprinse evoluțiile contextului operațional sau de securitate;
  - GEOINT are capabilitatea de a oferi beneficiarilor un produs final de intelligence sub forma unei „hărți" actualizate permanent (de tip cvadri-dimensional), în care spațiul tridimensional şi timpul sunt înglobate prin abilitatea de detectare a schimbărilor (change detection), prezentată anterior.

Atenuarea limitărilor analizei multisursă prin integrarea informațiilor provenite din surse de intelligence multiple cu ajutorul instrumentelor GEOINT

În activitatea de intelligence, o singură categorie de surse nu este suficientă pentru a conferi procesului de analiză certitudinea că produsul informativ final transmite informația corectă şi, mai ales, completă către beneficiari. Se remarcă necesitatea unei fuziuni a mai multor informații, care să certifice veridicitatea aspectelor semnalate şi, eventual, să le completeze[12].

Spre deosebire de analiza bazată pe o singură categorie de informații, analiza multisursă relevă provocări majore în elaborarea produsului de intelligence, care pot fi diminuate prin intermediul capabilităților GEOINT prezentate în acest studiu. Totuşi, este necesară menționarea faptului că nu este vorba despre probleme indisolubile legate de acest tip de analiză, ci, în unele cazuri, despre probleme ale oricărui tip de proces analitic, dar care sunt mai evidente în cazul analizei multisursă.

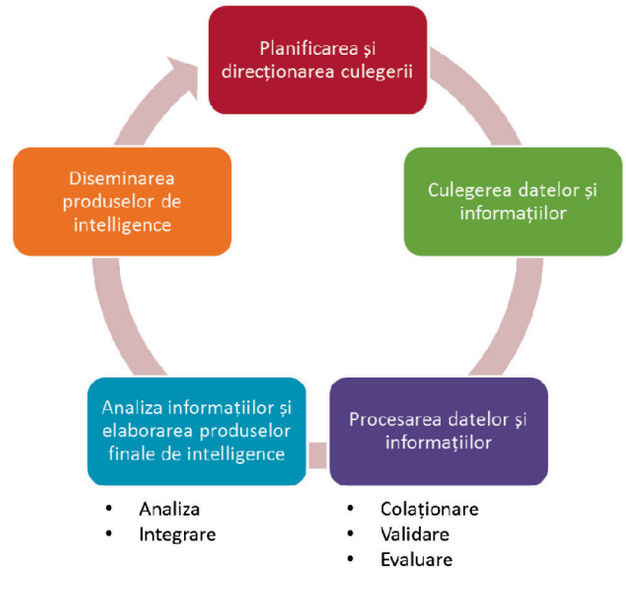
Prima provocare este legată de presiunea constantă a timpului exercitată asupra oricărui analist, care trebuie să livreze produsul informativ în timp util. În acest context, este conturată dilema procesului de analiză: mai multe informații din cât mai multe tipuri de surse versus necesitatea de a răspunde oportun diverselor solicitări. Astfel, analistul de informații se găseşte, de cele mai multe ori, în situația de a nu-şi permite „confortul" specific specialistului academic, de a înmagazina cât de multă informație consideră că este necesară şi de a-şi rafina cât de mult posibil produsul. Luând acestea în considerare, putem afirma că integrarea informațiilor provenite din multiple surse de intelligence reprezintă o „sabie cu două tăişuri". Din cauza unui timp limitat alocat întocmirii produsului de intelligence, analistul va trebui să lucreze într-un „disconfort" creat la nivel mental, ceea ce reprezintă un dezavantaj. Acest „disconfort" este cauzat de lipsa unui timp de lucru adecvat consultării întregului spectru de informații disponibile, specific analizei multisursă. Lipsa încrederii analistului în produsul informativ va fi amplificată din cauza multitudinii de informații care nu au fost consultate. GEOINT oferă o soluție acestei probleme prin afişarea informațiilor disponibile din zona de interes pe aceeaşi platformă de tip hartă digitală, în funcție de sortarea multi-criterială a tuturor seturilor de date, posibilă în urma procesului de clasificare a datelor în vederea extragerii informațiilor relevante[13]. Acest mod de prezentare a informațiilor conferă analistului o nouă perspectivă de vizualizare şi conceptualizare a evenimentelor din zona de interes.

A doua provocare o reprezintă coroborarea surselor, care, deşi în teorie pare simplă, în practică nu este la fel. Coroborarea surselor oferă multe avantaje, fiind în esență benefică şi extrem de utilă, însă, din cauza lipsei timpului (deseori insuficient) acordat realizării produsului, devine doar o altă problemă. În acest caz, coroborarea surselor cu ajutorul unei platforme geospațiale integratoare devine mai eficientă prin abilitatea conferită analistului de a observa cu uşurință şi exactitate locația descrisă de informație, momentul temporal descris de informație şi ce informații sunt diametral opuse, converg sau se confirmă unele pe celelalte. Astfel, analistul poate realiza cu uşurință armonizarea unor informații care, fără o locație sau o referință temporală precisă, ar putea părea că se infirmă unele pe celelalte. Mai mult, din punct de vedere al coroborării datelor şi informațiilor, integrarea multisursă evidențiază necesitatea partajării accesului la informații cu diferite niveluri de clasificare. Este cunoscut faptul că nu toți analiştii de informații au acces la toate informațiile disponibile. Acest lucru este de la sine înțeles având în vedere unul dintre principiile fundamentale ale activității de intelligence – "need to know" – conform căruia analistului trebuie să îi fie cunoscute informațiile necesare şi doar atât. Astfel, se impune identificarea unei soluții tehnice pentru partajarea eficientă a accesului la informații.

Cu toate acestea, nu putem afirma că GEOINT oferă o soluție de tip panaceu pentru provocările sus menționate, ci, mai degrabă, această capabilitate poate contribui la reducerea influenței acestor problematici asupra activității de analiză multisursă şi nu la eliminarea, în totalitate, a acestora.

GEOINT - contributor major la optimizarea ciclului informațional

Activitatea de informații este bazată pe un proces logic, de formă repetitivă, în care etapele sunt structurate sub forma unui ciclu



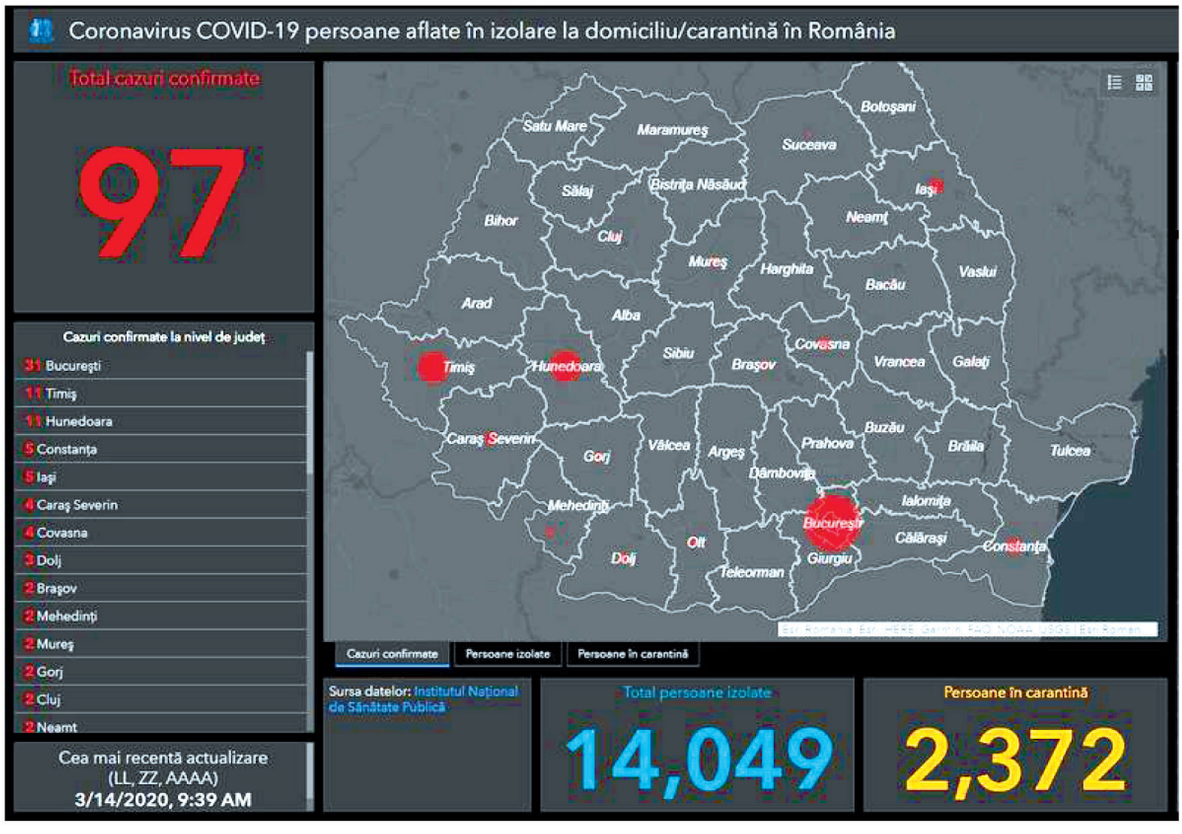
informațional. Pe scurt, acest proces cuprinde cinci activități importante: planificarea şi direcționarea culegerii, culegerea datelor şi informațiilor relevante, procesarea datelor şi informațiilor, analiza şi elaborarea pe baza acestora a unui produs informativ care să fie diseminat către beneficiari. Imaginea de mai jos prezintă o schematizare a ciclului informațional[14].

Capabilitatea GEOINT contribuie major la optimizarea ciclului informațional prin punerea la dispoziția structurilor de culegere şi a celor de analiză a unor instrumente specializate.

Pentru a evidenția modalitatea prin care **GEOINT contribuie la optimizarea şi îmbunătățirea activității de culegere a datelor şi informațiilor,** este exemplificată activitatea desfăşurată de către o structură HUMINT într-un teatru de operații. Culegerea informațiilor de către structurile specializate HUMINT nu se rezumă doar la interacțiunea cu surse umane[15]. Pe lângă această activitate principală, operatorii HUMINT trebuie să pregătească misiunile şi să se asigure că nu se află în atenția structurilor de contrainformații din zona unde operează, prin evitarea supravegherii operative. În cadrul acestor activități HUMINT în care nu sunt implicate surse umane, operatorii pot utiliza o aplicație mobilă de tip "collector"[16] pentru culegerea datelor din teren. Prin intermediul unui dispozitiv smartphone, care să asigure cu centrul o conexiune securizată, colectarea datelor şi distribuirea în mod real a informațiilor devine mult mai facilă. În cadrul aplicației se pot adăuga informații în timp real din teren, fie ele date scrise sau chiar fotografii, acestea fiind referențiate geospațial în mod automat. Astfel, structura HUMINT poate dispune de date în timp real pentru a le exploata în cadrul misiunilor specifice.

Modalitatea prin care etapa de procesare şi analiză a informațiilor poate fi îmbunătățită a fost prezentată în cadrul capitolului anterior, prin utilizarea unui instrument GEOINT de tip suport geospațial pentru colaționarea şi integrarea datelor şi informațiilor disponibile.

Diseminarea produsului de intelligence final către beneficiari poate fi realizată cu celeritate prin intermediul mediului de lucru colaborativ specific GEOINT, disponibil prin intermediul unui portal intern, din cadrul organizației. Serviciile GIS de tip "story map" sau „dashboard"oferă beneficiarilor acces în timp real la produsele de intelligence elaborate de către structurile



de analiză. GEOINT schimbă, astfel, percepția generală referitoare la produsele de intelligence, conform căreia acestea sunt doar o reprezentare statică a situației de interes.

Mai mult, prin intermediul unei aplicații web intuitive, în care informațiile sunt convertite şi structurate sub forma unor straturi tematice, decidenții militari şi politico-militari pot fi informați în permanență cu privire la evoluțiile de securitate, şi nu numai, dintr-o anumită zonă de interes. Analiştii au posibilitatea de a prezenta rezultatul analizei datelor (temporale şi geospațiale) utilizând un instrument foarte eficient, de tip "dashboard". Mai sus este prezentat un exemplu al acestui tip de hartă interactivă[17], care a fost utilizat recent de către agențiile de presă pentru a afişa evoluția pandemiei de coronavirus în lume sau în România.

Concluzii

În prezent, serviciile de informații se confruntă cu probleme legate de accesul la date şi informații, din perpectiva trecerii de la era lipsei lor la era "Big Data". Afluxul masiv de date şi informații din surse variate relevă necesitatea operaționalizării unor fluxuri de lucru performante pentru colaționarea şi procesarea acestui volum de informații culese.

Pe lângă câştigul operațional adus de capabilitatea GEOINT în cadrul activității de intelligence, se remarcă capabilitatea de a colaționa şi integra informații provenite din surse de intelligence multiple. Astfel, este necesară înlocuirea vechii paradigme de a colaționa informațiile provenite din surse de intelligence multiple prin stocarea acestora într-o bază de date şi interogarea pe baza cuvintelor cheie cu integrarea şi afişarea acestora pe o platformă de tip suport geospațial, conectată la baza de date, şi filtrarea acestor date şi informații pe baza poziției lor geografice. Această nouă modalitate de colaționare pune la dispoziția analistului de informații instrumente diverse, cu ajutorul cărora pot fi formulate aprecieri, concluzii, prognoze.

În vederea implementării acestei noi abordări în cadrul procesului de analiză sunt necesare schimbări atât la nivelul personalului implicat în activitatea de culegere şi analiză a informațiilor, la nivelul procesului şi fluxurilor de lucru, precum şi în cadrul modului de elaborare a produsului final de intelligence.

Pe lângă aportul la reducerea influenței limitărilor apărute în procesul de analiză multisursă, GEOINT îşi poate dovedi utilitatea şi în cadrul etapelor de culegere a informațiilor şi de diseminare a produsului de intelligence final, prin intermediul instrumentelor de tip aplicații web specifice, contribuind astfel major la optimizarea ciclului informațional.

Mediul colaborativ materializat prin servicii GIS este utilizat din ce în ce mai mult de către structurile de intelligence din cadrul NATO şi UE, domeniul GEOINT oferind astfel posibilitatea atât analiştilor, cât şi utilizatorilor finali de a beneficia de acces la informații şi produse de intelligence într-o manieră rapidă şi sigură din punct de vedere al securității rețelelor de comunicații.

Bibliografie*:*

1. FOCA, Marcel; BĂLOI, Aurel-Mihai, „GEOINT Analysis – suport decizional care poate face diferența", în *ARS ANALYTICA – Provocări şi tendințe în analiza de intelligence*, Editura Rao, Bucureşti, 2013;
2. COSTEA, Cătălina, „Analiza multisursă", în *ARS ANALYTICA – Provocări şi tendințe în analiza de intelligence*, Editura Rao, Bucureşti, 2013;
3. NIȚU, Ionel, *Analiza de intelligence*, ediția a II-a revăzută şi adăugită, Editura RAO;
4. ZAMFIR, Alexandru, „GEOINT – integrator şi platformă suport pentru analiza multisursă", în *INFOSFERA,* nr. 3/2018, DGIA, Bucureşti;
5. MIHAI, Aurel; ȚENEA, Florin; BĂJINARU, Mihai, „Tehnologii moderne de analiză a datelor geospațiale", *INFOSFERA,* nr. 3/2019 (anul XI), pg. 78;
6. *Geospatial Intelligence (GEOINT) Basic Doctrine*, Publication 1.0, 2018, p. 4, disponibil on-line la https://www.nga.mil/ProductsServices/Pages/GEOINT-Basic-Doctrine-Publication. aspx;
7. „Mesajul Directorului General al DGIA, cu prilejul sărbătoririi a 159 de ani de la înființarea primei structuri de informații militare", *INFOSFERA,* nr. 3/2018 (anul X);

8. https://intelligence.sri.ro/provocari-privind-implementarea-unei-reforme-unitare-si-comprehensive-analiza-de-intelligence-proiectul-3p/;
9. https://www.intelligencecareers.gov/icintelligence.html;
10. https://fas.org;
11. https://media.hotnews.ro;
12. https://en.wikipedia.org/wiki/Geospatial_intelligence;
13. https://www.esri.com/en-us/arcgis/products/apps-for-everyone/overview;
14. https://trajectorymagazine.com/nga-seeks-achieve-object-contextualization/.

---

[1] *Geospatial Intelligence (GEOINT) Basic Doctrine*, Publication 1.0, 2018, p. 4, disponibil on-line la https://www.nga.mil/ProductsServices/ Pages/GEOINT-Basic-Doctrine-Publication.aspx

[2] Aurel Mihai, Florin Țenea, Mihai Băjinaru, Tehnologii moderne de analiză a datelor geospațiale, în *INFOSFERA,* nr. 3/2019 (anul XI), pg. 78.

[3] „Mesajul Directorului General al DGIA, cu prilejul sărbătoririi a 159 de ani de la înființarea primei structuri de informații militare", în *INFOSFERA,* nr. 3/2018 (anul X), pg. 6.

[4]https://trajectorymagazine.com/nga-seeks-achieve-object-contextualization/

[5]Alexandru Zamfir, GEOINT – integrator şi platformă suport pentru analiza multisursă, în *INFOSFERA,* nr. 3/2018 (anul X), pg. 45

[6] https://www.imagesatintl.com/

[7] Ionel Nițu, *Analiza de intelligence*, ediția a II-a revăzută şi adăugită, Editura RAO, pg.204.

[8] George Maior şi Ionel Nițu, *ARS ANALYTICA,* 2013, Editura RAO, pg.184

[9]https://intelligence.sri.ro/provocari-privind-implementarea-unei-reforme-unitare-si-comprehensive-analiza-de-intelligence-proiectul-3p/

[10] Care este exprimată prin intermediul literelor şi cifrelor.

[11] GEOINT analysis – suportul decizional care poate face diferența, *ARS ANALYTICA,*2013, Editura RAO, pg. 189.

[12] Cătălina Costea, „Analiza multisursă", în *ARS ANALYTICA,* 2013, Editura RAO, pg. 201.

[13] „GEOINT analysis – suportul decizional care poate face diferența", *ARS ANALYTICA,* 2013, Editura RAO, pg. 192.

[14] https://www.intelligence careers.gov/icintelligence.html

[15] https://fas.org

[16] www.esri.com

[17] https://media.hotnews.ro

RELAȚIILE CIVIL - MILITARE ŞI CONTROLUL POLITIC (CIVIL) ASUPRA INSTITUȚIEI ARMATEI ÎN SOCIETĂȚILE CONTEMPORANE

Dan Laurențiu MOCANU*

Abstract

The role and place of the armed forces in the modern and contemporary society made the subject of extensive scientific research papers from a juridical, sociological and military perspective, referring to periods of political stability, social peace, war, internal conflict, political crisis and revolution. The political crisis and revolutions that took place at the end of the twentieth century and the beginning of the 21st century in the former socialist states from Eastern Europe, and especially the ones in Northern Africa, known as the "Arabic Spring" brought to the attention of both researchers (in varied fields, from history to sociology) and the public the problem of the relations between the military and the civilian factor (politicians) that runs the state; this is due to the importance of the role played by the army as an institution in society in predicting the political regime.

Keywords*: civil-military relations, civilian control, political transition, military organisation.*

Introducere

În lucrarea *Armata şi societatea*[1], un reper în abordarea temei relațiilor civil-militare în literatura ştiințifică românească, problematica este abordată pe trei paliere: (1) din perspectiva securității naționale, concept care a căpătat un caracter extins după sfârşitul Războiului Rece; (2) din perspectiva gândirii militare şi a modelului social militar; (3) relațiile civil-militare şi controlul politic civil asupra instituției armatei. Acest ultim aspect constituie subiectul studiului, tema relațiilor civil-militare în societatea contemporană fiind abordată în sens dinamic, cu interacțiuni reciproce, conflictuale sau de cooperare; de asemenea, noțiunea de control democratic civil reprezintă cea mai importantă aplicație practică a teoriei relațiilor civil-militare.

Relațiile civil-militare şi controlul politic (civil) asupra instituției armatei în societățile actuale

Relațiile civil-militare se referă, evident, la raporturile stabilite între componenta civilă şi componenta militară a unei societăți. Pentru delimitarea termenilor „civil" şi „militar" în contextul societății moderne, profesorul de ştiințe politice Daniel N. Nelson a propus o matrice cu două intrări, în cadrul căreia a definit cele două componente, în sens larg şi în sens restrâns (vezi figura 1). Acest model reprezintă o evoluție pornind de la „modelul Huntington", care lua în considerare cele două sfere (civilă şi militară) în sens restrâns, către analiza din prezent a celor două sfere, în sens larg. Astfel, conform lui Nelson, prin termenul de „militar" se înțelege, în sens restrâns, personalul militar al forțelor armate, iar în sens larg, orice categorie de personal din cadrul oricărei structuri de securitate națională. Prin termenul de „civil" se înțelege, în sens restrâns, un decident politic, iar în sens larg, întreaga societate. În baza acestor interpretări, Nelson concepe relația dintre cele două componente într-o cheie dinamică, trasată de interacțiuni atât de natură conflictuală, cât şi de cooperare[2].

***Doctorand, Universitatea Națională de Apărare „Carol I".**

Militar / Civil	**Definire în sens restrâns** Forțele armate, în special personalul militar de profesie.	**Definire în sens larg** Toate instituțiile de securitate națională, plus alte grupuri asociate.
Definire în sens restrâns Instituțiile guvernamentale şi ocupanții posturilor	I. Militarii şi elita politică interacționează fără a ține cont de procesul democratic şi de opinia publică.	II. Structurile de securitate interacționează cu elita politică prin pacte.
Definire în sens larg Toată sfera publică, inclusiv societatea civilă, mass-media	III. Sfera politică şi societatea civilă interacționează cu militarii – relații tensionate potențiale.	IV. Structurile de securitate interacționează cu publicul larg, pe baza unui dialog despre amenințările şi capacitatea națiunii.

În guvernările democratice, instituția militară este profesionalizată, neutră din punct de vedere politic şi controlată eficient de autoritățile civile. Controlul civil al armatei presupune o serie de concepte, proceduri, legi, standarde şi tradiții prin care se exercită autoritatea politică civilă asupra forțelor armate ale unei țări. Responsabilitatea controlului civil revine clasei politice, în timp ce responsabilitatea militarilor este aceea de execuție. Legitimitatea controlului civil este asigurată de legitimitatea procesului democratic (electoral), prin intermediul căruia „voința poporului" este delegată autorității politice.

Samuel Huntington, în lucrarea sa emblematică *„The Soldier and the State: The Theory and Politics of Civil-Military"* (1957), încă printre cele mai citate în literatura de specialitate, consideră că „the principal focus of civil-military relations is the relation of the officer corps to the state", deoarece „the modern officer corps is a professional body and the modern military officer a professional man"[3].

Analizând societățile moderne, Huntington face distincție între controlul civil subiectiv şi cel obiectiv asupra armatei. Controlul subiectiv înseamnă că puterea factorului politic (civil) este maximizată în raport cu instituția armatei (are tendința de a-i „civili" pe militari, de a-i transforma într-o oglindă a statului). Scopul controlului civil obiectiv este acela de a minimiza puterea armatei, profesionalizând-o şi făcând-o neutră politic[4]. Controlul civil obiectiv presupune maximizarea profesionalizării militare, în sensul că relația elita militară - conducerea politică duce către adoptarea unor atitudini şi comportamente reprezentative pentru întreaga profesie militară şi nu doar pentru „elita generalilor"[5].

Aşadar, pentru realizarea unui control civil obiectiv „perfect" este nevoie de o separare clară a responsabilităților între civili şi militari, militarii alcătuind un corp profesional ce se ocupă de managementul forței în stat, iar civilii din sfera politică conduc statul având legitimitatea oferită de alegerile democratice[6]. Aducem în discuție, pentru delimitarea etică şi practică a profesiei militarilor şi concepția lui Carl von Clausewitz despre supremația, în statul modern, a politicului asupra sistemului militar: „Războiul este o continuare a politicii cu alte mijloace"[7].

Nu există un model prestabilit care să ne arate cum trebuie organizate forțele armate într-o societate democratică şi cum să se exercite controlul asupra instituției militare. Există, totuşi, un număr de principii comune aplicabile într-un regim politic democratic. Acestea includ premise indispensabile pentru organizarea şi garantarea atât a unei conduceri civile corespunzătoare, cât şi pentru controlul asupra forțelor armate.

Concepția NATO referitoare la controlul civil asupra instituției militare într-un stat democratic a fost expusă de generalul german Harald Kujat, cu ocazia unui seminar organizat de Alianță la Sarajevo (iulie 1998)[8]:

- existența unei baze legale şi constituționale democratice care să definească relația dintre stat şi armată;
- un rol semnificativ al Parlamentului în legiferarea problemelor de securitate şi apărare şi în structurarea unei strategii naționale în domeniu;

- responsabilitatea ierarhică a armatei față de guvern, printr-un organ civil public de administrație - un Minister al Apărării - care este însărcinat, în general, cu supervizarea şi conducerea activității instituției militare;
- existența unei armate pregătite şi experimentate, respectată şi asigurată cu fonduri echilibrate de autoritatea civilă;
- neutralitate politică şi nepartizanat al forțelor armate;
- existența unei societăți civile evoluate, cu o înțelegere clară a instituțiilor şi valorilor democratice; şi ca parte a culturii politice, un consens național asupra rolului şi misiunii armatei;
- prezența unei componente nonguvernamentale rezonabile în comunitatea de apărare, capabilă să participe în dezbateri publice legate de politica de securitate şi apărare, prezentând viziuni şi programe alternative.

Ideea centrală a lucrării lui Huntington (1957) despre profesiunea militară şi relațiile civil- militare[9] este aceea potrivit căreia „corpul modern de ofițeri este un organism profesional, iar ofițerul modern este un profesionist". Profesionalismul diferențiază ofițerul modern de luptătorul de odinioară, iar profesionalizarea face distincția dintre armata de masă („armata întregului popor") şi armata actuală. Soldatul de rând este profesionist în aplicarea violenței (privită ca ocupație), însă numai ofițerul este manager al violenței (considerată ca fiind o profesie), adică un individ profesional, socialmente definit. Astfel, managementul violenței (profesia războiului) nu este acelaşi lucru cu aplicarea violenței (profesionistul războiului)[10].

Potrivit lui Huntington (1957), profesionalismul militar constă în trei aspecte definitorii: expertiză, responsabilitate şi corporatism. Expertiza se referă la educația şi experiența personalului militar, iar responsabilitatea are în vedere rolul militarului ca apărător legal al statului (pentru ca acesta din urmă să existe ca entitate distinctă în relațiile internaționale). Corporatismul se referă la împărtăşirea aceluiaşi sentiment de unitate de către personalul militar[11]. La rândul său, Samuel Finer adaugă noi aspecte, precum o comandă centralizată, o ierarhie cu reguli precise, disciplină, intercomunicare, spirit de echipă şi monopolul utilizării legitime a mijloacelor de forță[12]. Dacă, în ciuda acestor atu-uri evidente, militarii intervin rar din punct de vedere politic, aceasta se datorează unor slăbiciuni instituționale, şi anume: incapacitatea tehnică de gestionare (de către militari) a structurilor civile organizaționale complexe şi lipsa de legitimitate pentru a guverna pe termen lung[13].

Îndeplinirea obiectivului - „restrângerea puterii generalilor prin autoritatea politicienilor" - se poate realiza, aşadar, pe două căi: *obiectiv*, prin profesionalizarea forțelor armate şi impunerea, în acest fel, a unei atitudini neutre față de politică, şi *subiectiv,* prin atragerea militarilor în interiorul unei opțiuni politice. Eficiența controlului civil se măsoară prin capacitatea clasei politice de a controla forțele armate în situații „delicate": dezangajarea armatei după încheierea unui conflict de amploare sau cu ocazia unor decizii majore care afectează instituția (reduceri de personal, restructurări şi scăderi ale fondurilor alocate etc.).

Stanislav Andrewski a creat, în 1968, un sistem de evaluare a relațiilor civil-militare cu trei variabile standard: *military participation ratio (MRP),* adică numărul de militari raportați la ansamblul populației; gradul de subordonare a armatei autorităților civile şi gradul de coeziune internă a structurii militare. Morris Janowitz (1971) distinge patru modele istorice de relații civil-militare: aristocratic-feudal, statul garnizoană, totalitarist şi democratic[14].

Charles Moskos Jr. formula, în plin Război Rece, modelul „pluralist" de relații civil-militare. Teza lui Moskos afirmă că transformarea armatei trebuie judecată în evoluția sa dialectică, cea în care sfera militară parcurge atât faza divergenței, cât şi a convergenței cu sfera civilă[15]. Armata nu este o instituție omogenă, ci un organism pluralist în care coexistă sectoare asimilate de societatea civilă cu sectoare care prezervă gândirea şi acțiunea militară tradițională. În acel context istoric, pluralismul lui Moskos

oferea cea mai bună soluție organizațională, de combinare a celor două sfere, pentru realizarea unor deziderate esențiale: eficiența operațională şi controlul eficient de către autorități. Pe această bază teoretică, Charles Moskos Jr. a construit modelul cunoscut în sociologia militară ca „Modelul Interpretativ/Ocupație”[16].

Mandatul „standard” al unei armate este să-şi apere țara împotriva amenințărilor externe la adresa securității naționale. Pe lângă apărarea țării sale, obiectivul instituției militare este acela de a menține securitatea şi ordinea internă şi să promoveze propriul interes instituțional. Aceste interese instituționale, în concordanță cu cadrul legal, se referă la menținerea coeziunii interne ca structură coerentă şi solidă pentru a-şi proteja imaginea în raport cu societatea şi a asigura legitimitatea națională şi, foarte important, pentru a-şi promova, în raporturile cu factorul politic, interesele economice. Armata are interese atât instituționale, cât şi individuale dacă ne gândim la nevoia unui buget echilibrat şi suficient care să asigure nevoia de echipamente moderne şi pregătire de specialitate, dar şi o salarizare atractivă şi oportunități profesionale, vitale într-o lume în care se pune din ce în ce mai mult accent pe specializare[17].

În regimurile autoritare militarizate, mandatul armatei este extins în zone extra-militare, cum ar fi guvernarea şi controlul asupra unor sectoare economice cu mari beneficii pentru elita militară. Samuel Finer aprecia că intervenția Armatei în viața socială se produce atunci când instituțiile politice sunt slabe şi lipsite de legitimitate, când există pericolul unei dezagregări a statului.

Diferă considerabil măsura şi modul în care militarii sunt implicați la nivelul de decizie al regimurilor politice autoritare[18]. În general, cu cât este mai puțin dezvoltat un sistem politic şi cu cât legitimitatea sa în societate este mai mică, cu atât este mai probabil ca militarii să se angajeze în asumarea, mai mult sau mai puțin „discretă”, a deciziei politice[19]. O dictatură militară, din experiența istoriei, nu are şanse de a se menține la putere prea mult timp, de aceea este mult mai avantajos ca elita militară să exercite puterea „din umbră”. Conform lui Alfred Stepan, „militarii politicieni” se caracterizează prin faptul că dețin anumite prerogative: „dreptul sau privilegiul militarilor, dobândit formal sau informal, să exercite controlul efectiv asupra guvernanței interne, pentru a juca un rol determinant în zonele extramilitare, precum în interiorul aparatului de stat sau chiar pentru a structura relațiile dintre stat - politic - societatea civilă”[20].

În regimurile autoritare militarizate, conducătorii armatei decid deseori cu privire la legislație, Constituție şi alegerea persoanei în funcția de şef al executivului. De-a lungul anilor au existat diferite forme de regimuri autoritare militarizate. Samuel Finer diferențiază regimurile pe baza structurilor lor politice şi a rolului constituțional atribuit fiecăreia. Acesta distinge cinci structuri politice pe baza gradului în care armata controlează principalele politici şi a gradului de deschidere al regimului: conducere militară directă, conducere directă cvasi-civilă, conducere continuă indirectă, conducere indirectă intermitentă şi conducere dual[21].

Dictatura militară din Argentina (1966–1973) este un exemplu clasic de conducere militară directă, în timp ce intervenția politică a armatei în Turcia pentru „a îndrepta situația” este un exemplu de conducere militară directă, urmată de conducere indirectă intermitentă, în sensul de „apărătoare din umbră a legalității”[22].

De asemenea, se poate face distincție între militarii ce intenționează să rămână la putere sau să rămână sub controlul elitei politice aflate la putere şi cei care intenționează să exercite un control temporar asupra statului (supervizarea acestuia) pentru a menține lucrurile „aşa cum trebuie”[23].

Nivelul de instituționalizare a regimului politic în care militarii intenționează să rămână la putere ia diferite forme. Acesta implică stabilirea unor reguli formale, cum ar fi o Constituție care reglementează structura de putere în cadrul regimului, funcțiile guvernamentale şi succesiunea conducerii (adesea critice în regimurile nedemocratice).

Instituționalizarea conduce, de obicei, la o separare între Armată, ca instituție, şi militari, ca factor de guvernare. În Argentina, Peru şi

Uruguay nivelul ingerinței militarilor în stat a fost la un nivel mai redus decât în Chile sau Brazilia[24].

O distincție este necesar să se realizeze între nivelele de guvernanță în care militarii sunt factor determinant şi parametrii puterii guvernamentale pentru a se asigura controlul real, direcția general stabilită sectoarelor şi organizațiilor respective şi administrarea departamentelor guvernamentale, a corporațiilor de afaceri şi a sindicatelor. Măsura în care armata deține puterea guvernamentală depinde de scopul acestui control, de baza de resurse şi de eficiența actului de guvernare[25].

Conform Evei Bellin, militarii sunt în măsură să-şi mențină rolul politic atât timp cât pot asigura finanțe sănătoase, au o imagine externă cel puțin neutră, nu fac obiectul unui embargo economic şi politic internațional şi nu coagulează împotriva lor largi segmente sociale pe care nu le pot controla eficient[26].

Alături de diferitele forme de guvernare militară şi de implicare politică a acesteia, o distincție poate fi făcută între instituționalizare (nu trebuie confundat cu cele descrise mai sus, respectiv instituționalizarea armatei într-un regim autoritar) şi armata implicată în politică într-un mod patrimonial.

Un aparat militar instituționalizat are o identitate corporativă separată de stat, în timp ce identitatea armatei implicată patrimonial se confundă cu cea a regimului autoritar. Definim instituționalismul prin principiile birocratice enunțate de Max Weber: predictibilitatea guvernării, meritocrație, criterii clare de avansare în carieră şi recrutare a aparatului birocratic, promovare bazată pe performanță, corupție „controlabilă", etică etc.[27]

O organizație militară patrimonială este grevată de o corupție generalizată şi cronică, abuz de putere, îngrădirea puternică a forțelor de opoziție şi eliminarea distincției între misiunile publice asumate prin legislație şi cele ce țin de interesele particulare ale elitei conducătoare. O organizație militară patrimonială este, în mod particular, rezistentă la reforme democratice şi, conform lui O'Donnell şi Schmitter (1986), revolta armată pare să fie singura cale de înlăturare de la putere. O organizație militară instituționalizată va fi mai dispusă să se retragă de la putere şi să permită reforme politice care să deschidă calea spre democrație, ca urmare a unui proces negociat şi asumat împreună cu partenerii civili (conceptul interacțiunii „celor patru actori")[28].

Aşadar, militarii au capacitatea de a veghea la securitatea societății, elita militară are posibilitatea de a genera concepte alternative gândirii civile şi, în anumite circumstanțe, să preia efectiv controlul societății, aşa cum avem o multitudine de exemple în America Latină şi de Sud sau în Africa, după anul 1945.

Armata este un instrument de consolidare, protejare şi prezervare a realităților societale, prin urmare, ca şi instituție modernă de referință, armata nu are un caracter revoluționar; dar poate căpăta un „caracter revoluționar" în anumite situații socio-politice. Conform lui Gianfranco Pasquino (1974), relația armată-societate în epoca contemporană îşi are cheia explicativă în raportul dintre ritmul modernizării socio-economice şi gradul de instituționalizare (de maturitate) al procedurilor şi organizării politice. Dacă ritmul este prea rapid şi provoacă o expansiune accelerată şi/sau o improvizație a participării politice în absența procedurilor şi organizațiilor capabile să-l absoarbă şi să-l canalizeze în sens constructiv, se ajunge la instituții politice de tip „forme fără fond", incapabile să-şi îndeplinească eficient atribuțiile şi atunci militarii vor interveni pentru a împiedica dezagregarea societății[29].

Concluzii

Relațiile civil (politic)-militare constituie un sistem complex de factori. Profesorul Jon Rahbek-Clemmensen aprecia că există cinci variabile-cheie esențiale pentru modul în care funcționează sistemul: prioritățile guvernului civil, încrederea civililor în armată, încrederea militarilor în civili, instituțiile externe care definesc interacțiunea lor şi abilitățile reale ale elitelor/conducătorilor militari şi civili. Scopul sistemului este de a maximiza legitimitatea şi eficacitatea statului[30].

Numărul în scădere al regimurilor militare şi al loviturilor de stat înregistrate în ultimele decenii nu conduce la eliminarea influenței

instituției militare asupra regimurilor politice. În dezvoltarea statelor actuale, militarii rămân actori puternici, putând influența, în diverse spații ale planetei, atât modernizarea, cât şi eşecul democratic. Totodată, forțele armate din secolul XXI folosesc canale mai discrete pentru a exercita influență şi a-şi atinge obiectivele proprii în raport cu factorul politic conducător.

Bibliografie:

1. AGUERO, Felipe, *Chile's lingering authoritanian legacy*, în "Current History", No. 616, February 1998.
2. BELLIN, Eva, *Reconsidering the Robustness of Authoritarianism in the Middle East: Lessons from the Arab Spring*, în "Comparative Politics", Vol. 44, No. 2 (January 2012).
3. BELLIN, Eva, *The Robustness of Authoritarianism in the Middle East: Exceptionalism Comparative Perspective,* în "Comparative Politics", Vol. 36, No. 2 (Jan., 2004).
4. FINER, Samuel, *The Man on Horseback: The Role of the Military in Politics*, Pall Mall Press, London, 1962.
5. FINER, Samuel, *Comparative Government: An Introduction to the Study of Politics*, (Pelican books) Paperback – 25 Apr. 1974.
6. HUNTINGTON, Samuel P., *The Soldier and the State: The Theory and Politics of Civil-Military Relations*, Harvard University Press, 1957.
7. HUNTINGTON, Samuel P., *The Military Mind: Conservative Realism of the Professional Military Ethic*, Oxford, New Delhi. 1993.
8. KOONINGS, Kees; Dirk KRUIJT, *Political Armies: Military Politics and the Mission of Nation-Building in the Age of Democracy*, Publisher: Zed Books, 2002.
9. LINZ J. Juan, *Totalitarian and Authoritarian Regimes*, Lynne Rienner Publishers, London, 2000.
10. MEIJER Rozetta, *The Role of the Military in Political Transitions. Egypt: a Case Study*, July 2014, https://openaccess.leidenuniv.nl/bitstream/handle/1887/31895/MilitaryEgypt.pdf?sequence=1
11. MOSKOS Jr. Charles, "*From Institution to Occupation: Trends in Military Orgaization"*, în *Armed Forces and Society,* Vol. 4, No. 1/1977.
12. NATO, *The Role of the Military in a Democracy*, Address by Major General H. Kujat, GEAF, Assistant Director Plans & Policy Division, International Military Staff, https://www.nato.int/docu/speech/1998/s980702h.htm
13. NELSON N. Daniel, "Definition, Diagnosis, Therapy – A Civil-Military Critique", *Defense&Security Analysis*, vol. 18, No. 2, 2002.
14. O'DONNELL Guillermo, Schmitter C. Philippe, *Transitions from Authoritarian Rule: Tentative Conclusions about Uncertain Democracies*, Baltimore/London, Johns Hopkins University Press, 1986.
15. RAHBEK-Clemmensen Jon, *Beyond 'The Soldier and the State' -The Theoretical Framework of Elite Civil-Military Relations*, London School of Economics and Political Science, August 2013.
16. SAVA Ionel Nicu, Gheorghe Tibil, Marian Zulean, *Armata şi societatea*, Editura INFO-TEAM, Bucureşti, 1998.
17. STEPAN Alfred, *Re-Thinking Military Politics: Brazil and the Southern Cone*, Princeton: Princeton University Press, 1988.
18. Von CLAUSEWITZ Carl, *Despre război*, Editura ANTET, Bucureşti, 2012.
19. ZULEAN Marian, *Militarul şi Societatea*, Editura Militară, Bucureşti, 2008.

[1] Ionel Nicu Sava, Gheorghe Tibil, Marian Zulean, *Armata şi Societatea,* Editura INFO-TEAM, Bucureşti, 1998.

[2] Daniel N. Nelson, *Definition, Diagnosis, Therapy – A Civil-Military Critique*, Defense&Security Analysis, vol. 18, 2002, nr. 2, pp. 157-170, apud Marian Zulean, *Militarul şi societatea*, Editura Militară, Bucureşti, 2008, p. 16.

[3] Samuel P. Huntington, *The Soldier and the State: The Theory and Politics of Civil-Military*, Cambridge: Harvard University Press, 1957, p. 3 and p. 7.

[4] Rozetta Meijer, *The Role of the Military in Political Transitions. Egypt: a Case Study*, July 2014, p. 14, https://openaccess.leidenuniv.nl/bitstream/handle/1887/31895/MilitaryEgypt.pdf?sequence=1

[5] „Subjective civilian control achieves its end by civilianizing the military, making them the mirror of the state. Objective civilian control achieves its end by militarizing the military, making them the tool of the state. Subjective civilian control

exists in a variety of forms, objective civilian control in only one. The antithesis of objective civilian control is military participation in politics: civilian control decreases as the military become progressively involved in institutional, class, and constitutional politics. Subjective civilian control, on the other hand, presupposes this involvement. The essence of objective civilian control is the recognition of autonomous military professionalism; the essence of subjective civilian control is the denial of an independent military sphere. Historically, the demand for objective control has come from the military profession, the demand for subjective control from the multifarious civilian groups anxious to maximize their power in military affairs", Samuel P. Huntington, *The Soldier and the State: The Theory and Politics of Civil-Military*, Cambridge: Harvard University Press, 1957, pp. 83-84.

[6] Marian Zulean, *Militarul şi societatea*, Editura Militară, Bucureşti, 2008, p. 9.

[7] A se vedea, pe larg, Carl von Clausewitz, *Despre război*, Editura: ANTET, Bucureşti, 2012.

[8] NATO, *„The Role of the Military in a Democracy"*, Address by Major General H. Kujat, GEAF, Assistant Director Plans & Policy Division, International Military Staff, https://www.nato.int/docu/speech/1998/s980702h.htm

[9] Samuel P. Huntington, *The Soldier and the State: The Theory and Politics of Civil-Military*, p. 7.

[10] Ionel Nicu Sava, Gheorghe Tibil, Marian Zulean, op. cit., p. 31.

[11] Samuel P. Huntington, *The Soldier and the State: The Theory and Politics of Civil-Military*, pp. 8-10.

[12] Samuel Finer, *The Man on Horseback: The Role of the Military in Politics*, Pall Mall Press, London, 1962, p. 7.

[13]Samuel Finer, op. cit., p. 14.

[14] Ionel Nicu Sava, Gheorghe Tibil, Marian Zulean, op. cit., p. 34.

[15] Charles Moskos Jr., *From Institution to Occupation: Trends in Military Organization*, în „Armed Forces and Society", Vol. 4, No. 1/1977.

[16] Marian Zulean, *Militarul şi Societatea*, Editura Militară, 2008, Bucureşti, p. 11; Moskos defineşte modelul instituțional ca fiind acel model în care militarul intră în armată pe baza unei vocații, caută mai mult stimulente morale, identificându-se cu colectivitatea pentru care este gata să se jertfească. Armata, ca ocupație, este definită în termenii economiei de piață, individul fiind mai preocupat de bunăstarea sa decât de cea a colectivității, obligațiile sale fiind de tip contractual.

[17] Eva Bellin, *Reconsidering the Robustness of Authoritarianism in the Middle East: Lessons from the Arab Spring*, în „Comparative Politics", Vol. 44, No. 2 (January 2012), p. 131.

[18] Regimul autoritar nu este nici democratic, dar nici totalitar, ci unul în care puterea este ferm controlată de către organele centrale de guvernământ, iar libertățile cetățenești sunt limitate. Juan Linz, în cartea sa *Totalitarian and Authoritarian Regimes* (2000), indica patru caracteristici ale regimului autoritar: pluralism politic limitat, legitimizarea regimului prin necesitatea ca acesta să conducă lupta întregii societăți pentru o cauză anume, mobilizare minimă din partea societății pentru a se opune regimului şi configurarea foarte vagă a relațiilor de putere şi autoritate între instituțiile statului. Astfel, se face posibilă exercitarea autoritară a puterii în stat de către un individ, de regulă prin intermediul unui grup de apropiați constituiți ca elită a unui partid.

[19]Samuel Finer, *The Man on Horseback*...., pp. 164-204; Kees Koonings and Dirk Kruijt, *Political Armies: Military Politics and the Mission of Nation-Building in the Age of Democracy*, Publisher: Zed Books, 2002, p. 17.

[20] Alfred Stepan, *Re-Thinking Military Politics: Brazil and the Southern Cone*, Princeton: Princeton University Press, 1988, p. 9.

[21] Samuel Finer, *The Man on Horseback*...., 1962, pp. 200-204; *Comparative Government: An Introduction to the Study of Politics*, (Pelican books) Paperback – 25 Apr 1974, pp. 25-27.

[22]Samuel Finer, op. cit., 1974, pp. 11-13.

[23]Samuel Finer, op. cit., 1974, pp. 6-8.

[24] Felipe Aguero, *Chile's lingering authoritanian legacy*, în „Current History", No. 616, February 1998, pp. 396-400.

[25]Samuel Finer, *Comparative Government: An Introduction to the Study of Politics*, (Pelican books) Paperback – 25 Apr. 1974, p. 11.

[26] Eva Bellin, *The Robustness of Authoritarianism in the Middle East: Exceptionalism in Comparative Politics*, Vol. 36, No. 2 (Jan., 2004), pp. 148-149.

[27] Eva Bellin, op. cit., 2004, pp. 145-149.

[28] Guillermo O'Donnell, Philippe C. Schmitter, *Transitions from Authoritarian Rule: Tentative Conclusions about Uncertain Democracies*, 1986, p. 33.

[29] Gianfranco Pasquino, *Military e potere in America Latina*, 1974, pp. 242-243, apud Ionel Nicu Sava, Gheorghe Tibil, Marian Zulean, op. cit., p. 30.

[30] Jon Rahbek-Clemmensen, *Beyond 'The Soldier and the State' - The Theoretical Framework of Elite Civil-Military Relations*, London School of Economics and Political Science, August 2013, p. 9.

AGENTUL SECRET, PERSONAJUL NEVĂZUT AL SCENEI SOCIALE

Ioana Andreea MIHĂILĂ*

Abstract

Many times, humans have been the main tool in initiation and development of espionage and counterespionage acts. If this tool meets certain requirements and is craftily and professionally used, then success is ensured anywhere and anytime.

Humans have been used as a direct combat tool against enemy or just to prepare conditions for reaching specific goals, but only after thorough and adequate training according to the objective pursued, concurrently indicating him the benefits that he could personally enjoy, if successful.

Keywords: *spy, woman, sparrow, intelligence, sex-agents.*

Motto: „Jocul este o artă a relației cu rolul.”
Georg Simmel,
Zur Philosophie des Schauspielers

Operația *Honey Trap*

Ca agent secret, femeia are anumite particularități. Femeile care lucrează pentru serviciile secrete sunt învăluite de mister în ochii publicului larg. Este, însă, firesc să fie astfel deoarece, pentru ele, nu există primejdie mai mare decât să se afle în centrul atenției. Agenții trăiesc periculos, duc o viață plină de suspans, însă când vine vorba de femei fantezia oamenilor pare nelimitată. Imaginea spioanei din cultura populară implică de obicei aventura, obținerea de informații în paturi străine, este încărcată de romantism şi fascinația fructului interzis.

Deşi cunoaştem multe cazuri de femei spion din istoria recentă, ne aducem cu siguranță aminte de două nume care provoacă şi acum un fior plăcut: Mata Hari şi Christine Keeler. Ele reprezintă prototipul femeii imorale şi periculoase din mediul ultrasecret al serviciilor de informații. Nu s-a pierdut oare un război mondial din cauza uneia, iar cealaltă nu a trădat ruşilor secretele militare ale Angliei? Niciuna din aceste afirmații nu este adevărată. În ambele cazuri s-a exagerat şi s-a denaturat adevărul. Mata Hari şi Christine Keeler se înscriau în tiparul femeii spion, ce implică sex, romantism şi imoralitate, iar mai departe oamenii erau liberi să-şi dea frâu liber imaginației[1].

Perioada Războiului Rece a fost cea în care se poate spune că femeile au „invadat” „frontul secret”, aportul lor fiind nu numai cantitativ, ci şi în ceea ce priveşte valoarea informațiilor pe care le-au obținut. Afirmația este valabilă, în primul rând, pentru agentele care au activat pentru URSS şi care au avut preponderență față de cele recrutate pentru serviciile occidentale. În acea perioadă, în confruntările informative au apărut noi „mari puteri”. Este vorba, în primul rând, de spioanele

***Expert în cadrul Ministerului Apărării Naționale.**

STASI, agenția de informații a R.D. Germane, despre care se poate spune că a perfecționat metodele legate de așa-numita„metodă Romeo”, după cum vom avea ocazia să subliniem, dar și cele din alte state socialiste care au folosit „spionajul feminin”, adesea în colaborare cu agențiile sovietice. De asemenea, Israelul, motivat de „asediul” la care era supus de statele arabe, a folosit intens agente operative implicate în complicate acțiuni de răpire și pedepsire.

„Capcana cu miere” era o operație de obținere de informații prin intermediul folosirii prostituatelor. Ofițeri KGB, denumiți „unchi”, erau însărcinați să instruiască aceste „sex-agents” („agente sexuale”, denumite și „rândunici”) pentru a obține informații folosindu-și farmecele sexuale.

Unele dintre aceste femei acționau voluntar sau în schimbul unor avantaje materiale, dar se întâmpla ca altele să fie obligate la asemenea relații prin diferite mijloace, de exemplu prin șantaj, atunci când erau identificate ca având relații cu străini. Unele dintre ele au declarat că, la capătul unui „antrenament” adecvat, își însușeau mijloace corporale și psihice sofisticate. Primele contacte erau „regizate” ca să pară întâmplătoare, dar ulterior relația era susținută, astfel încât victimei îi era deosebit de dificil să scape din această „capcană cu miere”[2].

Într-un interviu acordat presei românești în 2009, I.C. Smith, fost agent FBI, care a participat la numeroase acțiuni informative peste hotare și a deținut funcții de conducere în această agenție, afirma următoarele: „Am avut atunci, și acum poate și mai mult, o mare admirație pentru STASI. Cred că a fost cel mai important serviciu de informații din cadrul blocului sovietic, superior chiar KGB-ului. Cred că una dintre marile enigme ale Războiului Rece a fost lipsa relativă de succes a Occidentului împotriva celor din STASI... Preocuparea principală a est-germanilor era Germania federală, unde au avut succese mari...”.

Așa cum am văzut, KGB-ul pusese la punct un sistem de seducere și de exploatare informativă a unor reprezentante ale „sexului slab” prin agenți proprii. Dar cel care a extins și a perfecționat acest sistem, sub numele de „metoda Romeo”, ducând la constituirea și funcționarea unei rețele, ce poate purta aceeași denumire, a fost serviciul est-german de spionaj, STASI, sub conducerea lui Markus Wolf. Acesta a mărturisit că nici el nu a bănuit, de la început, ce câștiguri informative va aduce această operațiune. A fost format un „corp” de agenți specializați care acționau de-a lungul unor perioade îndelungate, iar vizate erau mai ales femei (de cele mai multe ori nu la prima tinerețe!) care lucrau în ministere, instituții guvernamentale de prim rang din R.F. Germania. În opinia lui Wolf, care și-a intitulat un capitol din memoriile sale *„Spionaj din dragoste”*, o „femeie bine plasată era mai productivă decât zece diplomați”. Un fost ofițer în „armata străină” a STASI, Gotthold Schramm, recunoaște că informațiile obținute prin „metoda Romeo” erau rezultatul unor acțiuni imorale, dar ele ar fi contribuit la „prevenirea” unui nou război mondial.

În ceea ce privește motivația care le făcea pe aceste femei să devină agente, acceptând contacte cu bărbați arătoși și afectuoși, cu posibilități materiale, în realitate agenți STASI, era, cum arăta chiar una din femeile recrutate în cadrul „rețelei Romeo”, Gabriele Kliem, singurătatea, „concurența” care se născuse în mica capitală a R.F. Germania, Bonn, posibilitatea de a scăpa de singurătatea apăsătoare, pentru a-și „găsi o pereche” care să le ofere companie și, eventual, un trai decent.

Aceeași problemă a preocupat-o și pe Marianne Quoirin, autoarea volumului *Agentinnen aus Liebe (Agente din dragoste)*. Cele mai multe din aceste „victime” ale „agenților Romeo” erau vulnerabile din anumite motive (situație familială, izolare, situație materială). Bineînțeles, agenții STASI se informau amănunțit, în prealabil, asupra acestor situații și „atacau” la momentul potrivit. Este de reținut că cele mai multe persoane vizate nu erau la prima tinerețe și nici deosebit de atractive, ceea ce le făcea să fie amatoare de o relație „romantică”, înscenată cu abilitate, după rețete bine studiate de agenții STASI, după care nu atracția sexuală, ci cea sentimentală trebuia să primeze. Nu este

mai puțin adevărat că și „argumentele” materiale, cadourile și, mai târziu, o retribuție nu cine știe ce substanțială, au jucat un anumit rol.

Nici serviciile de contraspionaj din R.F. Germania nu au rămas fără replică la această „ofensivă” informativă prin „metoda Romeo”. Într-un document de avertizare redactat de BND, serviciul de contrainformații, se arăta, în legătură cu „metoda Romeo”, că „multe cazuri de spionaj au început în acest fel. Agenții știu că dragostea e oarbă”. Într-un document redactat de Comisia specială pentru controlul dizolvării organelor de spionaj din R.D. Germania după 1989, condusă de pastorul Joachim Gauck, se evidenția că Procuratura generală a incriminat 500 de persoane pentru activități de spionaj împotriva R.F. Germania, dintre care 110 erau femei. Șapte dintre ele au fost recrutate, în mod evident, prin „metoda Romeo”, dar câte nu vor fi rămas neidentificate...[3]

Relațiile dintre „spionajul feminin” și serviciile de informații ale SUA au fost abordate, în ultima vreme, într-o serie de articole apărute în presă sau chiar în volume. Sunt reproduse unele din punctele de vedere ale oficialilor CIA, care, la întrebarea dacă utilizarea „armei sexului” s-a aflat printre mijloacele importante utilizate de agenție, au răspuns că, în general, aceasta „nu s-a întâmplat des”, în recrutarea agenților străini preferându-se cointeresarea materială, deci banii. De asemenea, se acreditează ideea că „promiscuitatea sexuală” nu a fost o problemă în cadrul agenției.

De altfel, cel care a condus multă vreme spionajul american, Allan Dulles, afirma că „sexul niciodată nu va fi utilizat într-o operațiune atâta vreme cât el este director”.

În același timp, se admite că au fost destul de dese cazurile în care agenții CIA au făcut obiectul unor „asalturi” sexuale întreprinse de KGB, dar și de STASI, care porneau de la premiza că americanii, în general, sunt niște „materialiști obsedați sexual”. De aceea, agenții CIA erau avertizați de șefii lor asupra acestui pericol reprezentat de așa-numitele „lebede”, agentele care încercau seducerea și exploatarea informativă a personalului agenției, mai ales în străinătate. Totuși, se admite că, în special, KGB a repurtat, din perspectiva „spionajului feminin”, „câteva succese modeste”.

Unul dintre cei mai importanți specialiști din istoria CIA, Eric Frattini, admite că în terminologia CIA există și termenul „sexspionaj”.

Unele dintre problemele legate de activitatea femeilor în CIA după încheierea Războiului Rece au fost abordate în diferite intervenții ale unor factori din conducerea agenției, inclusiv în declarația directorului său executiv în fața „Chicago Council on Foreign Relations” din 1996, ale cărei puncte principale sunt încă actuale. Mai întâi, este negată opinia conform căreia CIA este doar „un bastion” al bărbaților. Sunt desființate o serie de „stereotipuri” ilustrate mai ales de tipul de spioane prezente în literatura și filmele „James Bond”. De fapt, nu există prea multe lucruri spectaculoase în activitatea agentelor CIA, a căror activitate presupune mari dificultăți, uneori acestea fiind confruntate cu situații „teribile”.

De fapt, încă în OSS, organism care a premers CIA, a existat preocuparea, mai ales a lui William Donovan, de atragere a femeilor în activitățile informative. Cazul Virginiei Hall, agentă OSS în timpul celui de-al Doilea Război Mondial, iar apoi angajată în CIA, este edificator în acest sens.

Această preocupare a făcut ca, la mijlocul anilor 1990, femeile să reprezinte 15% din posturile superioare din CIA. Există numeroase femei care îndeplinesc funcții de conducător de stații (rezidenturi) și de ofițer de caz. De asemenea, agente ale CIA au fost implicate în operații secrete de mare importanță, au abordat ambasadori, președinți, personalități politice, contribuind la obținerea de informații prețioase, inclusiv cele privind noile tehnologii[4].

Problemele legate de activitatea femeilor în CIA au continuat să-i preocupe pe analiști. În 2007, David E. Kaplan publică articolul *Sexismul în CIA*, în care actualizează unele date și interpretări ale acestei probleme. Astfel, se subliniază că, de-a lungul vremii, au fost destul de numeroase cazurile în care angajate ale CIA și-au pierdut posturile din cauza complicațiilor ivite atunci când au întreținut relații sentimentale. Au existat

asemenea „complicații” şi în interiorul Agenției, fiind citat cazul unui agent care a descoperit că soția sa întreținea relații cu agenturi din țara în cadrul căreia îşi desfăşura activitatea. Dacă, până în anii 1990, principala vulnerabilitate de natură sexuală era considerată homosexualitatea, în perioada următoare pe prim-plan au trecut relațiile heterosexuale.

În acelaşi timp, studiul subliniază că femeile au fost printre cei mai capabili şi mai experimentați „ofițeri de caz”, fiind în dese cazuri recompensate cu ordine şi medalii. În momentul redactării articolului (2007), femeile reprezentau 39% din personalul departamentului însărcinat cu operațiuni de spionaj („National Clandestine Service”). La nivelul Agenției, ponderea femeilor a crescut de la 14%, în 1996, la 25% în 2006.

Nu este trecută cu vederea nici presiunea exercitată de KGB. A existat chiar cazul primului şef al postului CIA din Moscova care a fost corupt de o agentă „lebădă” în terminologia KGB, astfel încât a trebuit să fie retras.

Una dintre prioritățile KGB şi GRU, în contextul Războiului Rece, a constituit-o cea referitoare la ataşații militari[5].

În ciuda unor dezbateri intense, CIA a fost destul de „zgârcită” în a face publică activitatea concretă şi numele unora dintre agentele sale care au fost implicate în acțiuni de spionaj sau au căzut victime „ripostei” contramăsurilor întreprinse de agenții străine. Unul din cazurile asimilate acestei categorii este cel legat de cel mai tânăr agent CIA mort într-o acțiune, Barbara Anette Robbins, secretară la Ambasada Statelor Unite la Saigon, în Vietnamul de Sud. Ea a fost asasinată la 30 martie 1965, când o maşină capcană a explodat pe o stradă apropiată de misiunea diplomatică[6].

Încă din 1924, profesorul-instructor Charles Russel, la cursurile sale pentru pregătirea ofițerilor în rezervă din armata S.U.A., atrăgea în mod repetat atenția asupra potențialului informativ pe care îl reprezentau femeile, dar şi asupra necazurilor ce pot apărea în munca cu acestea, a pericolelor ce se pot ivi dacă nu se sesizează din timp fisurile de natură contrainformativă existente[7].

Toate cursurile lui Charles Russel au fost presărate cu îndemnul la prudență şi de a se manifesta maximum de atenție când este vorba de femei angajate în munca de spionaj sau contraspionaj. Undeva, ca o chintesență a ideilor referitoare la pericolul pe care-l prezintă femeia în munca de informații, dar şi la eficacitatea acestui „instrument” în cazul în care se recurge la folosirea lui, instructorul militar american spunea: „Dacă vreți să prindeți un bărbat, trimiteți pentru aceasta o fată frumoasă”.

Iată alte îndemnuri, în formularea instructorului american, care merită toată atenția, oriunde şi oricând: „Evitați femeile: cu ajutorul acestora au fost prinşi mulți spioni, chiar dintre cei mai buni”, „Nu vă încredeți în femei când lucrați pe teritoriul inamicului”; „Când aveți de-a face cu femei, nu uitați niciodată să jucați rolul pe care l-ați ales”; „Aproape fiecare serviciu de spionaj are printre agenții săi şi femei: de obicei, femeile sunt folosite pentru misiuni speciale, iar în timp de război au de îndeplinit misiuni dintre cele mai grele şi neprevăzute”; „Se crede că femeile spion sunt întotdeauna bine îmbrăcate, frumoase şi culte, dar aceasta este departe de realitate; veți întâlni femei spion peste tot, începând de la cele mai bune hoteluri şi terminând cu casele de toleranță cele mai infecte”; „Femeile spion sunt inamicul cel mai periculos şi, în acelaşi timp, cel mai greu de demascat; când întâlniți astfel de femei, nu trebuie să admiteți ca simpatia sau antipatia să influențeze asupra hotărârii voastre - o astfel

de slăbiciune poate avea urmări fatale asupra voastră"; „Deseori veți întâlni agenți femei: de regulă, strângerea dovezilor împotriva femeilor agenți este o treabă deosebit de dificilă, care cere mult timp; femeile lucrează mai întotdeauna în apropierea hotelurilor sau cafenelelor frecventate de militari - aici veți observa de multe ori una sau mai multe femei atrăgătoare înconjurate de ofițeri (cavalerismul față de femei constituie, în timp de pace, o frumoasă calitate, însă multe femei inteligente au folosit această înclinație a bărbaților pentru a prelua informații şi secrete prețioase de la victima lor, care nu bănuia nimic)"; „Când suspectați o femeie, fiți de două ori mai prudenți: țineți minte că femeile agent sunt cei mai periculoşi inamici/pe de altă parte, unul dintre cele mai bune procedee de a demasca o femeie agent este de a trezi în ea gelozia; „Există diferite categorii de spioni de profesie: cu această activitate se ocupă femeile şi bărbații din diferite pături sociale: spion poate fi şi o femeie din înalta societate, care organizează în casa ei serate pentru ofițeri, precum şi o prostituată care vă acostează pe stradă, în văzul tuturor".

Arta informațiilor

Una dintre cele mai mari acțiuni de spionaj ale sovieticilor înainte şi după al Doilea Război Mondial a fost crearea rețelei din Orientul Îndepărtat, sub conducerea lui Richard Sorge, cetățean german care lucra la Tokio în calitate de corespondent al ziarului *Frankfurter Zeitung*. Vederile de stânga ale lui Sorge i-au adus probleme cu poliția şi, de aceea, în 1924, a fugit din Germania şi s-a refugiat în Rusia Sovietică.

În 1929, a început să lucreze ca ofițer de informații militare şi a fost trimis în prima misiune în China. După trei ani de spionaj în China, Sorge s-a întors la Moscova în 1933. Următoarea misiune a lui Sorge a fost în Japonia, unde trebuia să formeze o rețea de informații în folosul Uniunii Sovietice. În 1932, Japonia a cucerit Manciuria, iar Moscova se temea că următoarea țintă a japonezilor va fi Estul Îndepărtat al Rusiei Sovietice. Ca să îşi construiască acoperirea de jurnalist, Sorge a mers în Germania, iar un editor de la un ziar german a acceptat să îi publice câteva articole şi i-a dat o scrisoare de recomandare către colonelul Eugen Ott, noul ofițer trimis de Germania la Tokyo. Sorge a ajuns în Tokyo în septembrie 1933. Articolele publicate în ziarul nazist şi scrisoarea de recomandare din partea editorului german i-au adus recunoaşterea ca expert în Japonia.

În plus, el s-a alăturat Partidului Nazist. În acest fel, a dobândit acces la Ambasada Germaniei, unde se reuneau toți diplomații, inclusiv ambasadorul din Japonia, la acel moment Herbert von Dirksen. Sorge nu a pretins că este un nazist înfocat şi de multe ori şi-a exprimat disprețul față de excesele naziste şi prostia unor lideri de partid. În mod surprinzător, această atitudine i-a adus credibilitate, fiind considerat un savant patriot. Cele două vicii ale lui Sorge, băutura şi femeile, au contribuit, de asemenea, la „acoperirea" lui. Un prieten de pahar al lui Sorge, jurnalist american, a scris mai târziu despre el: „Sorge lăsa impresia că este un *playboy*, un pierde-vară, opusul unui spion periculos".

Sorge nu încerca să se ascundă. Locuia într-un cartier rezidențial liniştit, nu departe de secția de poliție, călătorea prin oraşul aglomerat pe o motocicletă, de multe ori sub influența alcoolului.

Articolele lui au fost însă foarte apreciate de diplomații germani şi curând a reuşit să câştige încrederea colonelului Eugen Ott şi a devenit consilierul acestuia. Ott l-a primit pe spionul rus în casa lui şi chiar în patul său. Sorge a avut o scurtă aventură cu soția ambasadorului, Helma, pe care Eugen Ott a decis să o ignore. Ambasadorul prețuia foarte mult sfaturile lui Sorge şi nu voia să îşi piardă consilierul din cauza acestei „indiscreții".

Rețeaua din Tokyo condusă de Sorge includea alți doi agenți trimişi de Moscova: Branko Vukelic, un comunist iugoslav, care lucra ca jurnalist pentru o agenție de ştiri franceză, şi Max Clausen, un comunist german, care se ocupa de transmisiunile radio către Uniunea Sovietică. Autoritățile japoneze au descoperit transmisiunile radio neautorizate, dar nu au reuşit să depisteze sursa sau să descifreze codul folosit de Clausen.

Un alt membru important al rețelei era Hotsumi Ozaki, un ziarist japonez, cu orientare de

stânga, care avea multe contacte influente. Unul dintre prietenii lui era şeful cabinetului primului ministru, prinţul Fumimaro Konoye. Ulterior, Konoye l-a angajat pe Ozaki ca şi consultant, acesta primind acces la documente secrete, rapoarte de politică externă şi recomandări din partea guvernului.

Ozaki îi furniza informaţii lui Sorge, pe care acesta le trimitea la Moscova. Spionul rus folosea informaţiile şi pentru a-şi consolida poziţia de expert printre diplomaţii de la ambasada germană.

În primăvara anului 1936, munca lui Sorge în Tokyo a început să dea roade. Eugen Ott a aflat de la contactele sale din armată despre o serie de negocieri secrete care au avut loc la Berlin între Germania şi Japonia (Pactul Anticomintern, aşa cum a devenit cunoscut ulterior). Ott a împărtăşit aceste informaţii doar cu ambasadorul Dirksen şi cu Sorge, aşa că spionul rus a putut să furnizeze către GRU toate noutăţile despre negocieri. În 1938, colonelul Ott a fost promovat şi a devenit ambasadorul Germaniei în Japonia. Astfel, Sorge a obţinut o poziţie privilegiată în cadrul ambasadei germane. Noul ambasador german la Tokyo îi arăta lui Sorge toate rapoartele şi proiectele sale şi îi cerea părerea înainte de a le trimite la Berlin. Toţi angajaţii ambasadei au observat relaţia apropiată dintre Ott şi Sorge şi, de aceea, mulţi dintre ei îi împărtăşeau spionului rus toate informaţiile pe care le aveau. În octombrie, poliţia japoneză l-a prins pe unul dintre colaboratorii lui Ozaki, pe nume Yotoku Miyagi. Acesta a încercat să se sinucidă ca să nu îşi trădeze colegii şi, într-un moment de neatenţie din partea gardienilor, s-a aruncat pe o fereastră. Căderea nu i-a fost însă fatală şi, supus unui interogatoriu agresiv, el le-a dezvăluit japonezilor numele lui Ozaki şi a lui Sorge. Pe 18 octombrie, Sorge a fost arestat. După o săptămână de tortură, el a povestit toate detaliile despre activitatea sa în Japonia în schimbul eliberării soţiei sale, Hanako Iishi, şi a soţiilor colaboratorilor săi, care erau nevinovate. Sorge şi-a petrecut următorii trei ani în închisoarea Sugamo din Tokyo, condamnat ca agent sovietic ale cărui activităţi de spionaj au avut ca scop răsturnarea regimului din Japonia şi distrugerea proprietăţii private. În septembrie 1943, Sorge a fost condamnat la moarte. El a sperat, însă, că autorităţile de la Tokyo îl vor elibera în schimbul unui prizonier japonez capturat de sovietici. De altfel, Japonia a încercat de trei ori să aranjeze acest schimb de prizonieri, dar, de fiecare dată, răspunsul de la Moscova a fost acelaşi: „Omul numit Richard Sorge este necunoscut pentru noi”.

În avanposturi informative

Harold Adrian Russell „Kim” Philby a avut parte de o reuşită fantastică în acţiunile întreprinse de el pentru sovietici, el fiind foarte bine integrat în Secret Intelligence Service (SIS), având o reţea de agenţi foarte diversificată, infiltraţi în foarte multe locuri de interes pentru el şi serviciile ruse. A reuşit foarte uşor să se infiltreze de la SOE la SIS cu ajutorul tatălui său, un om influent cu foarte multe relaţii, care l-a recomandat adjunctului SIS, col. Valentine Vivian. Acesta din urmă, în urma discuţiilor cu Kim, şi-a dat seama de valoarea băiatului; un lucru foarte important a fost pregătirea acestuia şi cunoştinţele pe care le-a acumulat, reuşind să-l facă pe Vivian să-l transfere imediat la SIS, secţia contraspionaj, un lucru fantastic pentru sovietici. „Kim” Philby lucra la două capete, deşi, fiind agent sovietic, avea în subordine doi oameni, Foote şi Rado, care dădeau informaţii posibil false către SIS, în scopul creşterii încrederii sale la nivelul SIS. Acesta a avut parte şi de mult sprijin din partea serviciului sovietic, care îl punea în legătură şi îl ajuta în anumite situaţii (contactarea lui Rado, realizarea de permise de liberă trecere în Franţa pentru Rado şi Foote, pentru ca aceştia să scape odată cu demascarea lor).

Cu ajutorul reţelei sale şi instruirea foarte bună a agenţilor săi, Kim Philby a reuşit să demaşte 6 spioni nazişti în Spania. De asemenea, a reuşit să demaşte, cu ajutorul agenţilor săi, un alt spion, Rogerio Menezes, de la ambasada portugheză, lucrul care l-a făcut pe Kim să-l suspecteze fiind cunoştinţele mult prea mari pe care le avea în comparaţie cu funcţia ocupată. Prin intermediul reţelei sale de agenţi a putut afla că este spion nazist, ce coresponda printr-un cod şi cerneală simpatică; acesta i-a interceptat corespondenţa şi a putut descifra tot ce portughezul trimitea şi primea. Astfel, infiltrarea lui Menezes a fost foarte slab calculată, întrucât s-a putut afla foarte uşor trecutul şi legăturile acestuia; mai mult, sistemul de corespondenţă era inadecvat, criptarea a fost

precară, cunoştinţele acestuia erau neadaptate la poziţia pe care o deţinea în ambasadă. Un agent infiltrat prins de un alt agent infiltrat, dar mult mai instruit.

Kim Philby avea un partener foarte priceput şi de încredere, Guy Burgess, de asemenea infiltrat foarte bine în SIS, pe care îl chema când avea nevoie de ajutor pentru o sarcină importantă, făcând toate demersurile pentru a-l aduce. Avea un rol foarte important în dezinformarea decidenţilor, reuşind să-l inducă în eroare pe preşedintele american Harry S. Truman cu privire la faptul că nu există niciun pericol din partea chinezilor, lucru neadevărat. De asemenea, a avut un rol foarte important în înfrângerile suferite de americani şi sud-coreeni, informaţiile sale ajungând la Moscova, implicit la chinezi şi nord-coreeni.

Concluzii

Articulaţie dinamică a economiei sociale a politicii secrete, agentul secret poartă în el slăbiciunile, conflictele, clivajele, ambiguităţile şi impasurile acesteia.

Pentru profesionişti, suprema plăcere a riscului final şi, în acelaşi timp, sursa ireductibilă de tensiuni, agentul secret este figura unei alterităţi inaccesibile şi foarte apropiate, totodată.

Bibliografie

1. *** - „Spionii Romeo folosiţi pentru a seduce secretarele germane în timpul Războiului Rece” Ziua, 20.03.2009;
2. http://www2.fiu.edu/~fcf/ray.washingtonpost.cia91897.html;
3. DIETL, Wilhelm, *Femei spion*, Bucureşti, Editura Litera, 2010;
4. David E. KAPLAN, „Sexism in CIA”, U.S. News& World Report în „Foreign Affairs”, 22.04.2007;
5. Eric FRATTINI, *CIA. Ferma lui Langley,* Editura Tritonic, Bucureşti, 2009;
6. FULGER, Vasile Dumitru, *Secţia amazoanelor*, Bucureşti, Editura Aldo Press;
7. NOVAC, Adrian, „I.C., SMITH: fost agent FBI: Spionul perfect nu e James Bond, ci vecinul tăcut şi modest de alături”, Hotnews, 21.08.2009;
8. QUOIRIN, Marianne, *Agentinnen aus Liebe,* Eichborn, 1999;
9. IVANOV, Lucian-Marius, *Lumea reală: spionaj şi spioni*, Editura Academiei Forţelor Terestre „Nicolae Bălcescu”, Sibiu, 2013;
10. POPESCU, Alexandru, *Dicţionarul universal al spionilor*, Bucureşti, Editura Meronia, 2010;
11. POPESCU, Alexandru, *Frumoasele agente. Femeile şi spionajul, O istorie universală*, Tîrgovişte, Editura Cetatea de Scaun, 2010.
12. Seth HETTENA, *Feasting on the Spoils: The Life and Times of Randy „Duke” Cunningham, History’s Most Corrupt Congressman*, St. Martin’s Press, 2007;
13. SILVERSTEIN, Ken, *Sex and the CIA,* în „Harper’s Magazine”, 17.04.2007;
14. TRAHAIR, Richard C.S., *Encyclopedia of Cold War Espionage, Spies, and Operations,* Westport, 2004;
15. WOLF, Markus, *Spionagechef im geheimen Krieg: Erinnerungen*, Editura Econ&List, München, 1997.

[1] Wilhelm Dietl, *Femei spion*, Bucureşti, Editura Litera, 2010.

[2]Richard C.S. Trahair, *Encyclopedia of Cold War Espionage, Spies, and Operations,*Westport, 2004.

[3]Markus Wolf, *Spionagechef im geheimen Krieg: Erinnerungen*, Editura Econ&List, München, 1997; Marianne Quoirin, *Agentinnen aus Liebe,* Eichborn, 1999; I.C. Smith, fost agent FBI: *Spionul perfect nu e James Bond, ci vecinul tăcut şi modest de alături*, Hotnews, 21.08.2009; *Spionii „Romeo” folosiţi pentru a seduce secretarele germane în timpul Războiului Rece,* în „Ziua”, 20.03.2009.

[4]Seth Hettena, *Feasting on the Spoils: The Life and Times of Randy „Duke” Cunningham, History’s Most Corrupt Congressman*, St. Martin’s Press, 2007; Eric Frattini, *CIA. Ferma lui Langley,* Editura Tritonic, Bucureşti, 2009, pag. 46, 55.

[5]David E. Kaplan, *Sexism in CIA,* U.S. News& World Report în „Foreign Affairs” 22.04.2007; Ken Silverstein, *Sex and the CIA,* în „Harper’s Magatine”, 17.04.2007.

[6]http://www2.fiu.edu/~fcf/ray.washingtonpost.cia91897.html.

[7] Vasile Dumitru Fulger, *Secţia amazoanelor*, Bucureşti, Editura Aldo Press.

ROLUL SERVICIILOR DE INFORMAȚII ÎN VREME DE PANDEMIE

Mădălin-Cosmin DĂNGUȚ*

Abstract

The uncertain nature of threats that we face in our days, makes it extremely difficult to be identified, which leads to the impossibility of implementation concrete military and political measures by the legal authorities. In this context it is mandatory the state actors, through their specialized institutions, to identify the most effective ways to respond to the actual security environment challenges.

Keywords: *pandemic, security environment, intelligence hybrid measures, fake news, security culture.*

Trăim într-un secol al *„schimbărilor fulger”*, unde imprevizibilitatea mediului de securitate nu încetează să ne uimească, iar complexitatea amenințărilor capătă noi dimensiuni.

Astăzi, mai mult ca oricând, statul este pus în situația de a-şi apăra integritatea şi securitatea, luptând pe fronturi multiple, împotriva unor agresori care pot fi sau nu definiți, care acționează sau nu într-un efort comun asupra aceleiaşi ținte şi a căror strategie de exploatare a succesului se bazează pe lansarea de atacuri perfide, de tip cal troian, ingenios concepute şi care au efecte pe termen lung. Este limpede de înțeles că rata de succes a acestor agresori creşte exponențial cu cât statul sau entitatea țintă se află în proces de gestionare a altor crize sau situații consumatoare de resurse, întregul său „*efort de apărare*” fiind orientat pentru neutralizarea acestora şi înlăturarea efectelor conexe.

Odată cu începutul anului 2020 statele au devenit mult mai vulnerabile. Răspândirea virusului SARS-CoV-2 a schimbat optica asupra situației de securitate la nivel global, iar evoluția acestei pandemii, care acționează disproporționat, produce pe zi ce trece efecte care pot influența ierarhia mondială.

Departe de a avea o imagine completă a cauzelor, implicațiilor şi a efectelor finale ale pandemiei de COVID-19 şi la fel de departe de a deține o soluție pentru stoparea definitivă a acestuia, actorii statali acționează pentru limitarea extinderii coronavirusului. Acest lucru este posibil doar prin implicarea într-un efort unitar a tuturor instituțiilor de care actorii statali dispun şi, totodată, prin menținerea unei comunicări permanente cu populația.

Dacă întreg efortul instituțiilor statului şi majoritatea resurselor de care acesta dispune sunt utilizate pentru a gestiona criza pandemică menționată, cine va proteja statul împotriva agresorilor clasici şi a amenințărilor cunoscute, fie ele convenționale sau neconvenționale?

Scenariul izbucnirii unor noi conflicte armate clasice devine puțin probabil, însă nu trebuie să uităm că lupta pentru putere rămâne interesul principal al statelor lumii. Întrucât viitorul este o necunoscută, a cărei predictibilitate, în situația dată, nu are fundament, actorii statali se vor folosi de toate mijloacele şi resursele de care dispun pentru a se menține în clasamentul puterii, pentru a câştiga credit şi pentru a pregăti terenul pentru acțiuni viitoare.

***Expert în cadrul Ministerului Apărării Naționale.**

În acest sens, toate instituțiile actorilor statali au fost nevoite să își configureze traseul în funcție de noile amenințări, majoritatea implicându-se pe deplin în prevenirea şi combaterea răspândirii coronavirusului. Serviciile de informații, pe lângă noile atribuții însuşite ca urmare a adaptării la cerințele actuale ale mediului de securitate, continuă să acționeze, după caz, ofensiv sau defensiv împotriva inamicilor.

Pe lângă puterea sa distructivă, pandemia de COVID-19 a deschis noi uşi care oferă actorilor statali posibilitatea de a-şi clădi sau consolida o nouă imagine la nivel mondial.

Acțiunile hibride au devenit arma ideală şi favorită de care marile puteri uzitează, în principal prin intermediul serviciilor de informații, pentru a-şi impune voința politică. Prin natura lor, acestea sunt greu de anticipat şi, prin urmare, greu de prevenit, producând efecte pe termen lung şi foarte lung.

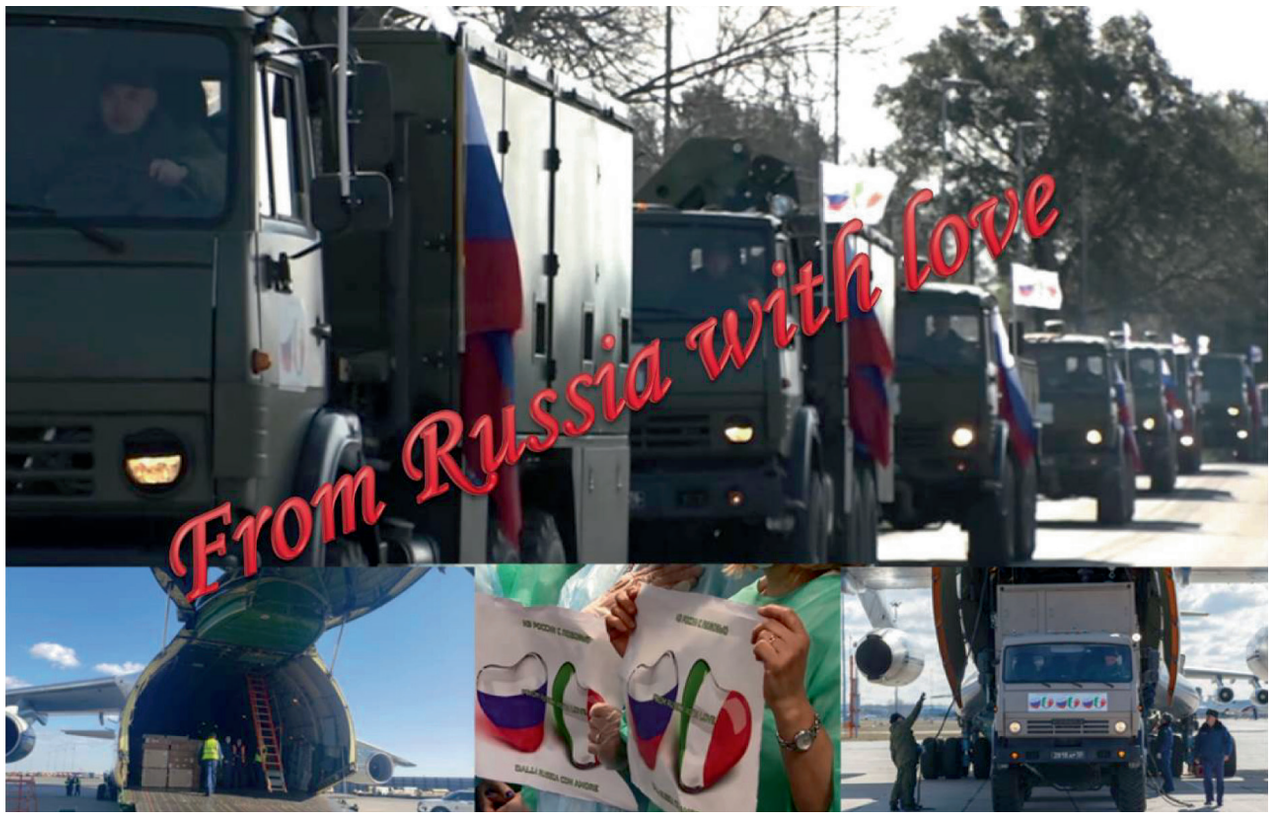
Pe timpul crizei sanitare**,** *Fakenews-ul* a căpătat valențe de neimaginat până în prezent. Pandemia a generat asaltarea de către populație a platformelor online atât din motive administrative, întrucât majoritatea activităților din diferite sectoare au fost mutate în mediul online, cât şi din dorința oamenilor, mai mult ca niciodată, de a se menține informați din motive de teamă sau din dorința de a afla când îşi vor recăpăta „*libertatea*". Conform unor statistici, în această perioadă traficul global de Internet a crescut cu 50 de procente[1].

Potrivit[2] şefului Agenției suedeze de informații interne şi contraterorism (SAPO), Klas Friberg, pe timpul pandemiei s-a constatat intensificarea activităților vizând slăbirea statului, o serie de puteri străine înmulțindu-şi încercările de a influența opiniile publicului. Totodată, acesta a atras atenția că este necesară sporirea vigilenței şi întărirea securității informatice pentru a împiedica puterile străine să obțină acces la informații sensibile.

Aşadar, în plan ofensiv serviciile de informații, precum şi alte entități ostile interesate, exploatează oportunitatea de a se adresa unui auditoriu nemaiîntâlnit ca volum, în încercarea de a manipula convingerile şi percepția acestuia, utilizând la scară largă metode precum:

- **desfăşurarea unor operații psihologice**, cu scopul de a deruta şi împărți opinia publică, referitoare la instituțiile statului, la modul de gestionare a crizei apărute;
- **publicarea unor materiale propagandistice** în publicații/reviste de prestigiu, prin interpuşi sau jurnalişti cumpărați;
- **utilizarea unor formatori de opinie** plătiți pentru pentru a promova interesele dorite: întrucât informațiile sunt percepute în mod diferit de persoane, în funcție de mediul din care provin şi categoria de vârstă pe care o reprezintă, formatorii de opinie utilizați de către serviciile de informații fac parte din categorii sociale diverse şi activează în toate mediile de referință considerate vocale de către publicul larg (publicații/emisiuni cu caracter religios, politic, care abordează elemente din domeniul sănătății publice, elemente cotidiene sau de cancan, acțiuni de *vlogging*);
- **folosirea boților**, programați cu scopul de a se înscrie în diferite grupuri create în cadrul platformelor de socializare şi pentru a distribui informații elaborate de serviciile de informații strict cu scopul de a crea anumite percepții.

Sub protecția oferită de imaginea de bun samaritean, unii actori statali trimit, odată cu materiale sanitare, echipamente de protecție şi personal medical, adevărați „cai troieni" în țările de interes, cu scopul de a culege informații greu de obținut în vreme de pace despre anumite obiective militare sau pentru a câştiga credit din punct de vedere al relațiilor diplomatice. Spre exemplu, ajutorul umanitar trimis Italiei de către F.Rusă, dublat de o amplă campanie de relații publice derulată sub sloganul *From Russia with Love*, a generat numeroase controverse şi acuze. Deşi Kremlinul a negat faptul că oferind ajutor a încercat să facă lobby pentru anularea sancțiunilor europene împotriva sa, unii specialişti consideră că ajutorul a fost oferit pentru ca ministerul rus de externe şi alte câteva site-uri media asociate acestuia să facă o propagandă ieftină, publicând mai multe imagini şi materiale video cu camioanele şi aeronavele militare care au



livrat Italiei ajutorul umanitar[3] şi că fără îndoială printre medicii şi militarii ruşi au fost infiltraţi şi ofiţeri GRU[4].

Criza provocată de COVID-19 a dat startul unei curse a mapamondului pentru dezvoltarea unui vaccin împotriva noului coronavirus, unde miza o constituie faptul că „ţara care descoperă prima formula cea mai eficientă şi mai sigură se va asigura că cetăţenii ei sunt primii care beneficiază de vaccin", iar capitalul politic, diplomatic şi economic nu va întârzia să apară[5]. Aşadar, serviciile de informaţii sunt direct interesate să obţină cât mai multe date despre progresul cercetărilor efectuate în acest domeniu. Bill Evanina, directorul Centrului pentru Securitate şi Contrainformaţii din SUA, a susţinut că „în această perioadă nimic nu este mai valoros decât cercetarea biomedicală care ar putea să ne ajute cu dezvoltarea unui vaccin împotriva coronavirusului", declarând totodată că guvernul american a avertizat organizaţiile care se ocupă de cercetare medicală în privinţa riscurilor care pot să apară[6].

Nu în ultimul rând, din punct de vedere ofensiv, **campaniile de atacuri cibernetice** provenite din partea unor grupări de criminalitate cibernetică, independente sau coordonate din umbră de servicii de informaţii sau de entităţi nonguvernamentale, şi-au intensificat activitatea. Limitarea liberei circulaţii şi a funcţionării fizice a unor instituţii de utilitate publică, ajutate de transferarea majorităţii activităţilor în mediul online, a obligat publicul larg să utilizeze aplicaţii de internet banking pentru a efectua diferite plăţi. Bazându-se pe pregătirea precară a populaţiei referitoare la riscurile asociate domeniului cyber, precum şi pe nefamiliarizarea noilor utilizatori cu operarea spaţiului virtual atacurile vizează în principal domeniul financiar-bancar, însă nu se limitează la acesta. Deşi la nivel internaţional este aplicată cu strictеţe legislaţia referitoare la protecţia datelor cu caracter personal, supraaglomerarea reţelei globale de Internet şi desfăşurarea unor activităţi în mediul online pe perioada pandemiei, folosind reţele nesecurizate sau slab securizate, oferă atacatorilor oportunitatea de a intra în posesia datelor referitoare la persoane sau organizaţii, pe care le pot folosi în perioada post-pandemie pentru a obţine diferite avantaje.

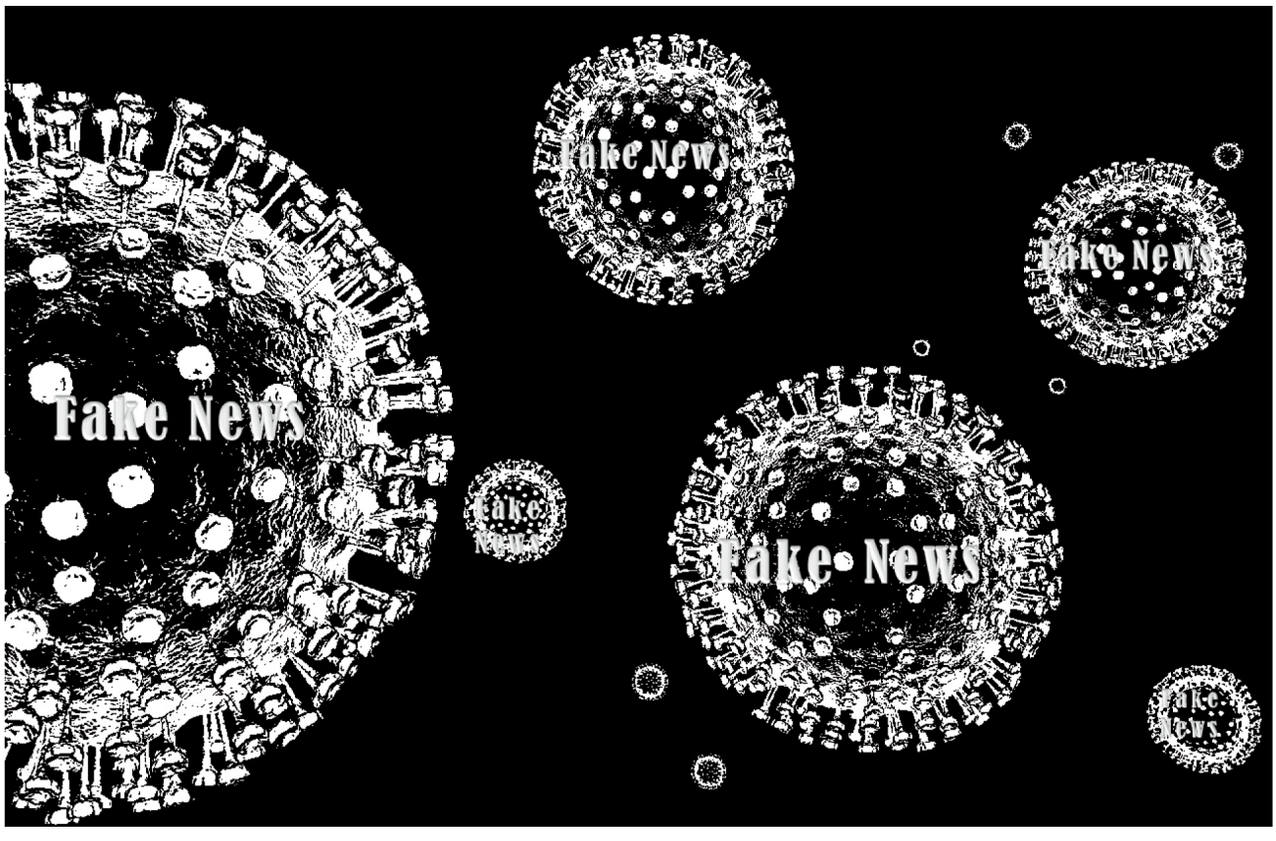
Din punct de vedere defensiv, actorii statali, în frunte cu serviciile de informaţii, culeg roadele a ceea ce au semănat. Pentru stat cea mai importantă resursă este omul, sănătos din punct de vedere fizic şi cu o gândire clară.

Direct implicați în luptă, pentru a stopa răspândirea noului coronavirus şi pentru a înlătura cât mai repede efectele provocate de acest virus, actorii statali, prin instituțiile de care dispun, au înțeles că succesul poate fi atins, pe lângă depunerea unui efort medical substanțial, doar dacă populația este responsabilă şi că dialogul permanent cu aceasta este esențial. Totuşi, majoritatea actorilor statali au întâmpinat probleme, fie din cauza lipsei de încredere a populației în clasa politică, fie din cauza fluxului sufocant al campaniilor agresive de dezinformare, conduse din umbră de servicii de informații ostile, care a creat panică şi a reuşit să mențină opinia publică confuză.

Neîncrederea şi suspiciunea cetățenilor pot genera breşe de securitate, care nu fac decât să vulnerabilizeze suplimentar un stat, având implicații, uneori ireversibile, asupra securității şi intereselor sale strategice[7].

Astfel, în vreme de pandemie, apărarea securității statului, prin menținerea unei populații informate corect, rămâne rolul principal al serviciilor de informații. Acestea au obligația de a adopta măsurile necesare în vederea decantării informațiilor false transmise prin intermediul new-media şi mass-media şi, totodată, să identifice şi să demaşte *„pionii”* folosiți drept formatori de opinie de către entitățile ostile pentru a le reprezenta interesele. În lupta împotriva acțiunilor subversive este esențial ca populația unui stat să înțeleagă modul de acțiune al amenințărilor şi să cunoască modele viabile de răspuns pentru a se proteja împotriva acestora. Acest grad de pregătire al populației se regăseşte în conceptul de „cultură de securitate“.

Odată cu apariția războiului informațional, statele dezvoltate au înțeles necesitatea educării populației în acest sens, tocmai pentru ca în vreme de criză să îşi poată concentra resurselor asupra rezolvării eficiente a situațiilor apărute, iar populația să fie în măsură să răspundă amenințărilor perfide care în *„mod clasic atacă prada vulnerabilă”*. Dezvoltarea culturii de securitate rămâne atributul serviciilor de informații, într-un efort unitar cu instituțiile statului, în vederea alinierii legislației în acest sens şi pentru a educa populația prin intermediul programelor de informare şi învățământ de care dispun. Totodată, fiecare cetățean trebuie să se autoeduce în acest sens pentru a contribui activ la realizarea securității naționale.



Un alt sprijin oferit de serviciile de informații pe timpul pandemiei este reprezentat de susținerea conducerii politico-militare cu produse informative care să permită adoptarea unor decizii fundamentate corect, de utilitate imediată şi aplicabile în timp oportun, în scop preventiv sau care să poată corecta anumite deficiențe existente. Structurile de apărare cibernetică joacă un rol esențial în timp de pandemie, efortul principal al acestora fiind depus pentru apărarea structurilor critice ale statului în fața atacurilor informatice, al căror scop principal îl reprezintă furtul de date, de proprietate intelectuală sau chiar sabotarea unor instalații vitale pentru menținerea unui climat de securitate optim.

În ciuda faptului că a generat multiple efecte negative la adresa populației, pandemia a scos la iveală noi fațete ale amenințărilor cunoscute şi ale modului de manifestare al acestora pe timp de criză, care, coroborate cu gradul de eficiență rezultat în urma aplicării deciziilor adoptate de către reprezentanții statelor şi organizațiilor internaționale, oferă perspective noi de analiză atât asupra amenințărilor şi a surselor acestora, precum şi asupra deficiențelor interne ale instituțiilor şi actorilor statali.

Având în vedere efectele produse de acțiunile hibride pe timpul pandemiei, este necesar ca instituțiile de profil să efectueze analize complexe asupra implicațiilor fenomenului menționat şi să înainteze factorilor decidenți politico-militari propuneri pentru îmbunătățirea metodelor de răspuns împotriva unor astfel de amenințări.

Una dintre cele mai eficiente metode de răspuns împotriva acțiunilor de tip hibrid, rămâne creşterea culturii de securitate în rândul populației. În acest sens, pot fi aplicate următoarele recomandări:

- introducerea la nivel național în unitățile de învățământ, în funcție de nivelul de studii, module de pregătire referitoare la utilizarea mass-media, new-media, a unor criterii de selectare a informațiilor, precum şi a unor metode de răspuns împotriva altor amenințări îndreptate asupra securității statului;
- crearea unor platforme interactive în mediul online în scop educativ, care să permită utilizatorilor efectuarea unor dezbateri pe diferite subiecte de securitate;
- stabilirea unor canale de comunicare şi a unor surse de informare securizate care să poată fi utilizate de către toți cetățenii statului, precum şi crearea unor platforme online în care utilizatorii să poată semnala ştirile false apărute în mediul online sau în diferite publicații tipărite.

În plan internațional, este necesar ca serviciile de informații să creeze şi să mențină legături strânse de cooperare cu structurile partenere, în vederea efectuării schimbului de informații de necesitate imediată, pentru a putea lua decizii oportune. Transmiterea „lecțiilor învățate“ referitoare la modul de materializare a noilor amenințări, în timp util către parteneri, ajută la economisirea alocării unor resurse importante şi, totodată, la adoptarea unor măsuri preventive eficiente.

La nivel național, serviciile de informații trebuie să manifeste tot mai multă transparență față de cetățeni şi să vină în sprijinul acestora atât cu avertizări de securitate care îi vizează în mod direct, precum şi cu campanii de informare referitoare la amenințările generale de securitate.

[1] Marc Scott, Laurens Cerulus, Janosch Delcker, „Coronavirus is forcing people to work from home. Will it break the internet?”, *Politico*, 17.03.2020, politico. eu/article/coronavirus-covid19-internet-data-work-home-mobile-internet/.

[2] S.I. Cătălin, „Agenția suedeză de informații: Pandemia, exemplu clasic al modului în care puteri străine încearcă să influențeze cetățenii”, *defenseromania.ro*, 26.03.2020, https://www.defenseromania.ro/agentia-suedeza-de-informatii-pandemia-exemplu-clasic-al-modului-in-care-puteri-straine-incearca-sa-influenteze-cetatenii_602283.html

[3] S.I. Cătălin, „Presa italiană: Aproximativ 80% din ajutorul umanitar trimis de Rusia este inutil”, *defenseromania.ro*, 26.03.2020, https://www.defenseromania.ro/presa-italiana-ajutorul-din-partea-rusiei-este-inutil_602276.html

[4] Andrei Jipa, „Rusia a infiltrat spioni pe post de doctori trimişi să trateze bolnavii de coronavirus. Reacția Kremlinului după afirmația din La Stampa”, *Mediafax.ro*, 04.04.2020, link

[5] Gordon Corera, „Coronavirus: Cyber-spies seek coronavirus vaccine secrets”, *BBC*, 1 May 2020, bbc.com/news/technology-54490432.

[6] Idem

[7] Andrei Maftei, „Tentaculele războiului hibrid. Rafinarea dezinformării”, *INTELLIGENCE*, 24 octombrie 2018, https://intelligence.sri.ro/tentaculele-razboiului-hibrid-rafinarea-dezinformarii/

Direcția Generală de Informații a Apărării