Revista Română de Studii de Intelligence

Nr. 6/decembrie 2011
București

Cristina POSAȘTIUC — Reengineering Intelligence

Tudor RAȚ, Raluca GALAON — Crowdsourcing în intelligence

Adrian POPESCU — Managementul modern în cadrul organizațiilor de intelligence

Ionel NIȚU, Felicia RĂDOI — Despre necesitatea unui brand al analistului de intelligence

Gheorghe-Costinel ANUȚA — Intelligence și foresight: repere ale utilizării studiilor prospective în fundamentarea deciziilor în domeniul securității naționale

Adrian LESENCIUC, Cosmina DRĂGHICI, Oana-Andreea PÎRNUȚĂ — Rolul contextului comunicațional în analiza de intelligence: către un intelligence al redundanței

Florin DIACONU — Evaluarea implicării NATO în Afganistan: o provocare pentru activitatea de intelligence strategic a comunității academice

Ella CIUPERCĂ — A missing link: Education for security dimension of the corporate social responsibility

Aurora-Elena BARĂU — Cooperarea în intelligence. Mutații generate de noul context de securitate

Vlăduț BRÎNZĂ — Aport de intelligence românesc la securitatea europeană

Gabriela TRANCIUC — Uniunea Europeană – către un serviciu de informații european?

Viorel BUȚA — Securitate națională, surse de putere și intelligence

Daniela SPÎNU — Internetul și radicalizarea migranților musulmani din vestul Europei. Riscuri ale societății cunoașterii.

Dumitru DUMBRAVĂ — Agresiunile în spațiul cibernetic

Alexandru IOAN — Războiul din Georgia pe fluxurile de știri

Ana Ligia LEAUA — O viziune strategică a securității mediului în era globalizării

REVISTA ROMÂNĂ
DE STUDII DE INTELLIGENCE

Nr. 6
Decembrie
2011

Bucureşti
- 2011 -

Colegiul Editorial:

George Cristian MAIOR
- director al Serviciului Român de Informații, conf. univ. dr. Academia Națională de Informații *„Mihai Viteazul”* și Școala Națională de Studii Politice și Administrative

Christopher DONNELLY
- senior fellow la Defence Academy din Regatul Unit și director al Institute for Statecraft and Governance, Oxford

Ioan Mircea PAȘCU
- deputat Parlamentul European, prof. univ. dr. Școala Națională de Studii Politice și Administrative

Vasile DÂNCU
- prof. univ. dr. Universitatea din București, Universitatea Babeș-Bolyai și Academia Națională de Informații *„Mihai Viteazul”*

Gheorghe TOMA
- prof. univ. dr. Academia Națională de Informații *„Mihai Viteazul”*

Cristiana MATEI
- lecturer Center for Civil-Military Relations din Monterey, SUA

Marius SEBE
- conf. univ. dr. Academia Națională de Informații *„Mihai Viteazul”*

Cristian BARNA
- conf. univ. dr. Academia Națională de Informații *„Mihai Viteazul”*

Irena DUMITRU
- conf. univ. dr. Academia Națională de Informații *„Mihai Viteazul”*

Ella CIUPERCĂ
- conf. univ. dr. Academia Națională de Informații *„Mihai Viteazul”*

Valentin Fernand FILIP
- lector univ. drd. Academia Națională de Informații *„Mihai Viteazul”*

Alina PĂUN
- expert

Colectivul de redacție:

Redactor-șef: *dr. Cristian NIȚĂ*
Redactori: *George IANCU*
Cristian CIUPERCĂ
Aitana BOGDAN
Oana SPRÎNCENATU
Mihaela STOICA
Tehnoredactori: *Alexandra Mihaela VIZITIU*
Lucian COROI
Coperta: *Mihai MANEA*

CUPRINS

Cristina POSAŞTIUC	**Reengineering Intelligence**	5
Tudor RAŢ Raluca GALAON	**Crowdsourcing în intelligence**	14
Adrian POPESCU	**Managementul modern în cadrul organizaţiilor de intelligence**	24
Ionel NIŢU Felicia RĂDOI	**Despre necesitatea unui brand al analistului de intelligence**	36
Gheorghe-Costinel ANUŢA	**Intelligence şi foresight: repere ale utilizării studiilor prospective în fundamentarea deciziilor în domeniul securităţii naţionale**	46
Adrian LESENCIUC Cosmina DRĂGHICI Oana-Andreea PÎRNUŢĂ	**Rolul contextului comunicaţional în analiza de intelligence: către un intelligence al redundanţei**	59
Florin DIACONU	**Evaluarea implicării NATO în Afganistan: o provocare pentru activitatea de intelligence strategic a comunităţii academice**	74
Ella CIUPERCĂ	**A missing link: Education for security dimension of the corporate social responsibility**	85
Aurora-Elena BARĂU	**Cooperarea în intelligence. Mutaţii generate de noul context de securitate**	94
Vlăduţ BRÎNZĂ	**Aport de intelligence românesc la securitatea europeană**	110
Gabriela TRANCIUC	**Uniunea Europeană – către un serviciu de informaţii european?**	126
Viorel BUŢA	**Securitate naţională, surse de putere şi intelligence**	140
Daniela SPÎNU	**Internetul şi radicalizarea migranţilor musulmani din vestul Europei. Riscuri ale societăţii cunoaşterii.**	153
Dumitru DUMBRAVĂ	**Agresiunile în spaţiul cibernetic**	164
Alexandru IOAN	**Războiul din Georgia pe fluxurile de ştiri**	179
Ana Ligia LEAUA	**O viziune strategică a securităţii mediului în era globalizării**	197

CONTENT

Cristina POSAŞTIUC	**Reengineering Intelligence**	5
Tudor RAŢ Raluca GALAON	**Crowdsourcing în intelligence**	14
Adrian POPESCU	**Modern Management in Intelligence Organizations**	24
Ionel NIŢU Felicia RĂDOI	**Considerations on the Necessity of Haring an Intelligence Analyst's brand.**	36
Gheorghe-Costinel ANUŢA	**Intelligence and foresight: landmarks of the usage of foresight in supporting the decision-making process in the field of national security**	46
Adrian LESENCIUC Cosmina DRĂGHICI Oana-Andreea PÎRNUŢĂ	**The role of the communication context in intelligence analysis: towards an intelligence of redundancy**	59
Florin DIACONU	**The assessment of NATO's involved in Afghanistan: a challenge for the strategic intelligence activity of the academic community**	74
Ella CIUPERCĂ	**A missing link: Education for security dimension of the corporate social responsibility**	85
Aurora-Elena BARĂU	**Cooperation in intelligence. Mutations generated by the new security environment**	94
Vlăduț BRÎNZĂ	**Contribution of Romanian Intelligence to European Security**	110
Gabriela TRANCIUC	**The European Union - towards an European Intelligence Service?**	126
Viorel BUŢA	**National security, sources of power and intelligence**	140
Daniela SPÎNU	**The Internet and the radicalization of Muslim migrants from Western Europe. Risks associated to the knowledge society.**	153
Dumitru DUMBRAVĂ	**Cyber-Agressions**	164
Alexandru IOAN	**The war in Georgia reflected in the news stream**	179
Ana Ligia LEAUA	**Strategic vision on environmental security in the age of globalization**	197

Reengineering *Intelligence*

Ph D. Cristina POSAŞTIUC
Romanian Intelligence Service
e-mail:**pcristina@dcti.ro**

Abstract

Unlike the business environment, where successful management models are characterized by the ability to make profits and orient all available resources to satisfy the demands of the end-user, in the field of social organizations and public institutions, the efficiency measurement can hardly be quantified. Among the specific indicators of any modern intelligence organization, the following elements should be mentioned: the early warning capabilities, the strategic value of the products, the focus on collaborative activities, the emphasis on open source exploitation, and the academic expertise. Although intelligence services have had a major role in the information age which has ruled over the society, as soon as the need for information has been replaced by a more sophisticated demand, known as the need-to-know principle, intelligence organizations have been forced to turn themselves into knowledge agencies.

Keywords: reengineering, collaborative, network-centric, knowledge society.

Antropological Reasons of Change

Several specialized assessments highlight that despite the profound changes the intelligence environment witnessed in the last two decades, many *intelligence* services still have cumbersome entities, structured and run according to Adam Smith' principles dating back to the 18th century: division, specialization and technological progress capitalization.

Experts' opinions are mainly based on the fact that those organizations are, like most modern institutions, creations of the 19th century; with all adjustments they have been subject to over time, they generally revolved around the bureaucratic model derived from the legal/ rational authority concept as defined by Max Weber[1].

[1] Max Weber identifies six key elements of the model of the modern bureaucratic system: clear regulations, the formal hierarchy, inflexibility in vertical communication, the big size of the organization, unipersonal leadership, the promotion system.

A remark having as a reference point the end of the Cold War and 9/11 attacks is that *intelligence* services reform has occurred *post factum*, as a result of several syncopes in carrying out their key mission.

However, a constant preoccupation for preventing major gaps between threats and risks dynamics, on the one hand, and intelligence services' adjustment to these developments, on the other hand, has lately been noticed.

The idea that the pace of institutional adjustments in *intelligence* is rather slow could originate in the social and institutional change, namely in the fact that, macrosocially, the transition from the industrial society to the knowledge society has been made gradually.

Considering what Braudel[2] called *"long duration",* the adjustments of mentalities underlying social and cultural practices fueling structural norms have been made smoothly enough to avoid a dramatic outphasing in terms of institutions' adjustment to new realities.

The situation is completely different if we consider current changes. In a research conducted by the University of Bucharest[3], the new social configuration, defined either as the 'postindustrial'[4], 'postcapitalist'[5], 'technological'[6], 'information' and 'network'[7], 'risk' or 'knowledge' society, is characterized by 'a flow of causal determination from knowledge to social processes of organization, management, identity structures etc. or from technologies, especially information and communication, to macrosocial

---

[2] Braudel, Fernand, *The Mediterranean and the Mediterranean World in the Age of Philip II*, Meridiane Publishing House, 1985-1986. The author introduces the concept of *long duration* to better express the difference between visible historical stages (history of events) and the profound ones (history of mentalities).

[3] http://www.stisoc.ro – *Public and Science*, 2010.

[4] Daniel Bell, *The Coming of Post-Industrial Society: A Venture in Social Forecasting*, New York, Basic Books, 1973. J. Hage and C.H.Powers, Post-Industrial Lives: Roles and Relationships in the 21st Century, Newbury Park, CA:Sage, 1992, in the *Public and Science S*tudy, available, on October 20, 2011, at http://www.stisoc.ro

[5] P.F.Drucker, *Post-Capitalist Society, New York*, HarperCollins, 1993, in the *Public and Science S*tudy, available, on October 20, 2011, at http://www.stisoc.ro

[6] P.L.Berger, B.Berger and H.Kellner, *The Homeless Mind: Modernization and Consciousness*, New York, Vintage Books, 1974, in the *Public and Science S*tudy, available, on October 20, 2011, at http://www.stisoc.ro

[7] J.R.Beniger, *The Control Revolution*, Cambridge, MA: Harvard University Press, 1986. M. Castells, The Rise of the Network Society, New York, Harper and Row, 1996, in the *Public and Science S*tudy, available, on October 20, 2011, at http://www.stisoc.ro

configurations like 'technology-based globalized societies', 'economies, and information and knowledge societies' or 'network-based societies''.

The knowledge society is therefore, par excellence, a society compressing the development cycles determined by the technological and globalization progress, as well as one in which the old patterns of the social architecture are totally reversed in favour of a 'network' world[8]. Nowadays, people and institutions are more than ever products of information exchange connections established within networks among persons, organizations or national states during the social time, in the real geographic area or in the virtual space.

Any analysis of institutional changes should therefore start by realizing that the main difference from the industrial society, which ended in late 20th century, is individualization: "the individual's emancipation from the constraints imposed by the social structures and categories and his stand-out as an architect of his own identity on several networks"[9].

Reengineering Intelligence

The knowledge society and the coming one, the conscience society, are so much different from any other form of previous social organization, that the *intelligence* strategic thinking needs deep changes, from the almost Victorian traditionalism of organization and values, to the promotion of a revolutionary concept based on competitivity, innovation and knowledge.

Introducing, as an argument, the *reengineering* concept, specific to economic sciences, may seem surprising, but the prospective may be different if we consider that relevant experts have been the first to understand that 'the factory pattern, based on the pyramidal hierarchical organization is obsolete; the workers are now highly specialized and qualified, all they need is information and the authority to act in order to be successful"[10].

The main idea conveyed by the *reengineering* theoreticians, Michael Hammer and James Champy[11], professors at the Massachusetts Institute

---

[8] The term network society was introduced by Manuel Castells (1996), researcher in the communication field. His study – The Space of Flow, published in The Rise of the Network Society, 2000 (available at http://socacis.ubbcluj.ro) is very eloquent.

[9] The study *System for Social Networks Analysis,* conducted by University of Bucharest, 2010.

[10] Stan, Silviu, *Reengeenering – a new philosophy of management*, Expert Publishing House, 2007.

[11] Hammer, Michael, Champy, James, *Reengineering the Corporation: A Manifesto for Business Revolution,* Harper Collins, New York, 1993.

of Technology, is that the radical redesign of the organization's *processes* should prevail against the reorganization. As compared to the fundamental Taylorist principles, relying on the efficiency of the repetitive tasks carried out by different structures, the *reengineering* concept brings the tasks together into work units designed to operate this way.

Major problems faced by private companies were solved by placing *processes* before *function,* as the shortcomings did not necessarily lie within the compartments, but in intercompartmental relationships.

Reengineering solves a challenge faced by many companies: while developing, they are prone to excessively focus on the organization's internal problems and needs, neglecting the clients' needs.

Mutatis mutandis, the US, British or Spanish intelligence agencies were taken by surprise by the waves of terrorist attacks that emerged at the end of the Cold War not because they lacked resources, appropriate technology or freedom of action, but because they focused on internal problems and on the need to reassess their missions and roles.

The assessment of the intelligence communities, including the Report issued by the US Congressional 9/11 Commission[12], proved that the most serious flaws were not found at the level of various departments or activity profiles, but at the level of information sharing and cooperation within the intelligence community.

One could notice that the most common error triggering operational failures of the intelligence services is linked to the way in which the *intelligence* process is built – the path from *input* (planning and data collection) to *output* (dissemination) –, more precisely its erroneous design starting from the organization's and not customer's requirements.

Not accidentally, the lack of feedback is considered an indication of the wrong implementation of the *intelligence* process: either the decision-maker's silence is caused by the failure to understand the information value, or the information lacks intrinsic value, the lack of reaction shows clearly that the customer was not involved in the process aimed at setting priorities and major goals.

---

[12] The 9-11 Commission Report, *The Final Report of the National Commission on Terrorist Attacks Upon the United States*, Official Government Edition, available at http://www.gpoaccess.gov/911, on October 13, 2011.

Reengineering Essence*: *Moving Power to the Edge

According to the *reengineering* theory, the first step towards rethinking the intelligence consists in replacing the security services' practice of information *feudalization* with consistent interdisciplinary cooperation, interagency partnerships under the umbrella of the national intelligence communities.

Moreover, fostering cooperation with partner agencies and encouraging information sharing have become an *imperative* condition[13].

Network-centric intelligence[14] is the formula defining the involvement of various actors inside or outside the institution, it entails cooperation with the civil society and the important universities and research institutes, recognizing, implicitly, the fact that *intelligence* agencies cannot cope by themselves with the challenges posed by the new security environment.

Robert David Steele pointed that the underlying threat to peace and prosperity – the so-called "cause of causes" – derives from the chasm between policymakers with power, and private sector experts and participants with knowledge, ignoring thus a vast amount of knowledge.[15]

Asymmetric threats require asymmetric responses. In order to be able to *scan* the area of interest and to fulfill the early-warning task, the *intelligence* agencies should no longer rely on a pyramidal architecture, on cumbersome regulations, the encouragement of horizontal teamwork being an imperative.[16]

Thus, the creation of an efficient system requires a new organizational management philosophy, which provides for the transformation of the institutions dominated by a powerful core structure

---

[13] http://www.sri.ro, Online Library, Strategic *Documents, Strategic Vision 2007-2010* – "Enhancing cooperation with other national intelligence services and strengthening SRI's profile within the intelligence community as well as broadening international cooperation in bilateral and multilateral formats (...)" are mentioned among SRI's priorities.

[14] Sharfman, Peter, *Network-Centric Intelligence: An Approach to a Strategic Framework*, The Command and Control Research Program (CCRP) Publication Series, available at http://www.dodccrp.org, on October 22, 2011.

[15] Robert David Steele, "Fixing the White House and National Intelligence", International Journal of Intelligence and Counter Intelligence, 2010.

[16] Idem.

into a *cluster*[17] entity, where many decisions are made at the intermediate levels or even in the operational theater[18].

Steele[19] asserted that the "*central intelligence*" syntagm was an oxymoron, making a harsh analysis of the US intelligence community's working principles, especially in terms of the lack of dialog between politicians and government policy-makers (power factors) and the experts with vast knowledge. He assessed that the US leadership operates on only 2% of the relevant information.

Director of the Romanian Intelligence Service George Cristian Maior also noticed that, in the current security environment, 'the actors and processes have experienced a fundamental change, and the power is not longer exercised by individual entities, but by networks, which relay on information sharing, civic action and supranational integration', and the answer of the intelligence should take the form of 'assimilation by 'internalizing' those changes'.[20]

The modern services effectively apply those principles by setting up flexible working units with specific tasks permanently oriented towards consulting the regional factors, sharing information with other entities and participating in numerous interdisciplinary and inter-institutional meetings.

The collaborative work is primarily focused on prediction, strategic value of the products, and assimilation of open source information and expertise of the experts outside the intelligence agencies.[21]

The secret tends to lose its supremacy in the globalization and Internet era, the stake shifting towards joining efforts with top scientific researchers, with business representatives, in order to achieve the early-warning function over some social, economic, demographic, and geopolitical developments.

---

[17] Alberts, David; Hayes, Richard, Power to the Edge, The Comand and Control Research Program (CCRP) Publication Series, available at http://www.dodccrp.org, on October 20, 2011.

[18] http://www.sri.ro, Online Library, *Strategic Documents* – This philosophy was explicitly stated in the first programmatic document approaching SRI's institutional reform process – Strategic Vision 2007-2010 –, asserting the need to "increase the flexibility of the Service structure by: mitigating bureaucracy, raising the autonomy level and structural decision-making decentralization; balancing responsibilities by an equal assignment at the decision-making level; rethinking internal practices and rules and supporting horizontal cooperation among structures (...)."

[19] Robert David Steele, idem.

[20] Maior, George Cristian, Message of the Director of the Romanian Intelligence Service in the 2011-2015 Strategic Vision. SRI in the Information Age, available at htttp://sri.ro

[21] Schreier, Fred, *Transforming Intelligence Services*, National Defense Academy, 2010.

In future, the analysis will mainly revolve around global developments, the challenge faced being the approach on the core worrying problems and the way in which strategic advantage over the enemy is achieved.

This is actually the essence of the collaborative work, which makes the transition from *cooperation* to the *integration of the actors* outside the intelligence agencies in a complex system that produces superior knowledge.

An Operational Concept

In my opinion, *Reengineering Intelligence* should become a reality in managing the intelligence services, an ad hoc definition revealing a significant potential of this type of approach: *fundamental re-thinking and radical re-design of the intelligence processes, in order to considerably improve the performance indicators in the field, especially the early-warning one.*

This proposal observes the principles found in the complex process of SRI's institutional reform process, more precisely exceeding the vision focused on *structure*, and adopting an orientation favoring working *strategies*, *policies,* and *practices*.

To that end, probably the most important lesson learned in the modernization process of the Romanian Intelligence Service is that the institutions make real progress not when they search for solutions to topical problems (a significant activity, which is actually related to the management logic), but when they design the future, when they have a strategic vision on the role they have to play in a context completely different from the present one (*The 2007-2010 Strategic Vision* on 'Service transforming' and *The 2011-2015 Strategic Vision* on 'career transforming'[22]).

As the matter of fact, the Romanian experts debate on the fundamental values of *reengineering*:

o "The reform is often used as a catch-all phrase, including all efforts already taken in order to operate significant changes in the intelligence services. Actually, the reform is an answer to certain gaps in the system. (...) The failures in the intelligence activity do not necessarily depend on the organizational gaps, and the reorganization is unlikely to settle organizational problems. The reorganization as such is a predictable, slow process. Before completing the process, the old causes of the shortcomings will be replaced with new ones. (...) In order to tackle

[22] *2011-2015 Strategic Vision. SRI in the Information Age*, available at htttp://sri.ro

the future security changes, the intelligence services should look ahead towards the constant transformation of the activity and not in the past, towards reform. If the reform is a static process, reactive, oriented towards mending the mistakes of the past, the transformation ensures the anticipative dimension, focused on preventing the future mistakes, based on a continuous dynamic".[23]

Considering the defining parameters of the knowledge society, as previously described, we assess that the intelligence services face a crucial decision for their future and the international security, and for preserving the democracy values as a last resort. The problem is not *if*, but *when* they will realize their impossibility to face today's enemy with structures conceived for another historical period. Dealing with secrets, the collaborative philosophy is a *discreet revolution*, but there is also hope that, at a certain moment, the intelligence services will turn into *knowledge services*.

Bibliography

1. Alberts, David; Hayes, Richard, Power to the Edge, *The Comand and Control Research Program* (CCRP) Publication Series, available, on October 20, 2011, at http://www.dodccrp.org.

2. Bell, Daniel, *The Coming of Post-industrial Society: A Venture in Social Forecasting*, New York, Basic Books, 1973, in the *Public and Science S*tudy, available on October 20, 2011, at http://www.stisoc.ro

3. Berger, P. L., B. Berger, H. Kellner, *The Homeless Mind: Modernization and Consciousness*, New York, Vintage Books, 1974, in the *Public and Science S*tudy, available on October 20, 2011, la http://www.stisoc.ro

4. Beniger, J. R. *The Control Revolution*, Cambridge, MA: Harvard University Press, 1986. M. Castells, The Rise of the Network Society, New York, Harper and Row, 1996, in the *Public and Science S*tudy, available on October 20, 2011, la http://www.stisoc.ro

5. Braudel, Fernand, *The Mediterranean and the Mediterranean World in the Age of Philip II*, Meridiane Publisjing House, 1985-1986.

6. Drucker, P.F., *Post-Capitalist Society*, New York, Harper Collins, 1993, in the *Public and Science S*tudy, available on October 20, 2011, la http://www.stisoc.ro

[23] Grosu, Ion, "Intelligence Services: Reform or Transformation?", *Intelligence*, no.16, July 2009.

7. Grosu, Ion, *Intelligence Services: Reform or Transformation?*, Intelligence Magazine, no.16, July 2009.

8. Hammer, Michael, *Reengineering the Corporation: A Manifesto for Business revolution*, Harper Collins, New York, 1933.

9. Maior, George Cristian, *Uncertainty. Strategic Thinking and International Relations in the 21st Century*, RAO Publishing House, Bucharest, 2009.

10. Maior, George Cristian, *The New Ally – Rethinking Romania's Defence Policy at the Beginning of the 21st Century*, RAO Publishing House, Bucharest, 2009.

11. Maior, George Cristian, *A War of Mind*, RAO Publishing House, Bucharest, 2010.

12. *Public and Science*, 2010 http://www.stisoc.ro

13. Schreier, Fred, *Transforming Intelligence Services*, National Defence Academy, 2010.

14. Sharfman, Peter, *Network-Centric Intelligence: An Approach to a Strategic Framework, The Comand and Control Research Program* (CCRP) Publication Series, available on October 22, 2011, on http://www.dodccrp.org.

15. Stan, Silviu, *Reengeenering – A New Philosophy of Management*, Expert Publishing House, 2007.

16. Steele, Robert – David, *Fixing the White House and National Intelligence*, International Journal of Intelligence and CounterIntelligence, 2010.

17. *2011-2015 Strategic Vision. SRI in the Information Age*, the Message of the Director of the Romanian Intelligence Service, available on http://www.sri.ro

18. *Analysis System of Social Networking*, a study conducted by the University of Bucharest, 2010.

19. *The 9/11 Commission Report, The Final Report of the National Commission on Terrorist Attacks Upon the United States*, Official Government Edition, available on October 13, 2011, on http://ebooks.unibuc.ro

20. http://ebooks.unibuc.ro

21. http://www.gpoaccess.gov/911

22. http://www.sri.ro

Crowdsourcing în intelligence

Tudor RAȚ, Raluca GALAON
Serviciul Român de Informații
e-mail: **ratudor@dcti.ro, graluca@dcti.ro**

Abstract

Nowadays, the complex development of the security environment plays an important role to the emergence of a new perspective regarding security, seen as "a common good" - the shaping of the concept is the responsibility of the entire society and its effects influence everybody. The vulnerabilities, risks and threats to the national security have a multidimensional structure, the intelligence services face difficulties in operating, by themselves, the amount of challenges to protect and promote the national interests. Crowdsourcing can be a solution to surpass the limits imposed by the proliferation of information, especially open sources, in the twenty-first century. The term defines, basically, the practice of "externalizing" some dimensions of the intelligence cycle to social actors, in order to create a symbiotic relationship between the intelligence community and the civil society.

Keywords: crowdsourcing, intelligence, predictions, smart nation, web 2.0.

I. De la *for personal profit* la *all profit*

Termenul *crowdsourcing* a fost introdus – relativ recent – în limbajul de specialitate de către Jeff Howe (2006), care a creat acest *portmanteau* prin alăturarea particulelor *crowd* şi *outsourcing*. *Crowdsourcing* desemnează astfel practica unei organizații de a externaliza (*outsourcing*) anumite sarcini către o comunitate (*crowd*) cu scopul de a folosi, spre beneficiul comun, fondul de resurse (cognitive sau materiale) de care dispun grupurile umane.

Dacă ***outsourcing*-ul este un model economic** ce presupune încheierea unei înțelegeri contractuale între două părți (un actor economic prestează un serviciu pentru alt actor economic, cedând, în schimbul remunerației, drepturile intelectuale şi de folosință asupra produsului creat), ***crowdsourcing*-ul reprezintă un model social,** ce ia forma unei invitații deschise, lansată de o organizație către publicul interesat şi capabil să contribuie la rezolvarea unei probleme ale cărei implicații vizează întreaga comunitate. Binomul organizație – comunitate este construit cu aportul

ambelor părți: indivizii pun la dispoziție resurse amorfe, neorientate ca scop şi nestructurate (timp, cunoştințe, bani, capacitate de efort etc.), pe care organizația le orientează, structurează şi le angrenează efortului de atingere a unui scop comun.

Pe fondul creşterii exponențiale a complexității mediului de securitate (datorată unor fenomene sociale, politice, tehnologice, economice şi culturale specifice secolului al XXI-lea precum: globalizarea, avalanşa informațională etc.), serviciile de informații – organizații pe care societatea le însărcinează cu protejarea şi promovarea intereselor naționale – întâmpină dificultăți tot mai mari în administrarea portofoliului de problematici ce le revine din punct de vedere legal.

În acest sens, o inițiativă de tip ***crowdsourcing*** **poate contribui semnificativ la conturarea unei comunități de intelligence la nivel național, în sensul incluziv al conceptului**[1]: distribuția cunoaşterii, a informației şi a expertizei într-o lume interconectată şi avansată tehnologic precum cea a secolului al XXI-lea face ca imaginea unei structuri de intelligence închisă în sine, necomunicativă cu societatea, să fie una vetustă. Angrenarea tuturor actorilor sociali (organizații guvernamentale şi nonguvernamentale, medii academice, grupuri profesionale, experți sau simpli cetățeni) ce pot şi vor să contribuie la realizarea securității naționale, privită ca o premisă *sine qua non* a dezvoltării şi prosperității sociale şi individuale, va deveni mai mult decât un deziderat utopic: o necesitate de supraviețuire a națiunilor într-un sistem global tot mai interconectat, dar şi mai vulnerabil în fața şocurilor.

II. Mecanisme de funcționare

Un ***smart mob*** (Rheingold, 2002) este un grup mare, eterogen şi nestructurat de oameni ce acționează inteligent şi eficient datorită unei premise (inteligența de grup) şi a unui catalizator tehnologic (mijloacele de comunicare moderne ce facilitează schimbul de informații de tip *one-to-many* şi *many-to-many*).

Prin *crowdsourcing*, aceste *smart mobs* devin ceea ce John Henry Holland (2006) numea **sistem complex adaptativ**: arhitecturi ce incumbă „un număr mare de componente, denumite adeseori ‹‹agenți››, ce interacționează, învață şi se adaptează”.

[1] Asemănător viziunii promovate de Stevan Dedijer (2002).

II.1. Inteligența de grup

Istoria ne învață că grupurile mari de oameni sunt periculoase: pot deveni violente şi au tendința de a încuraja comportamente anti-sociale. Huliganismul, vandalismul, linşajul sunt formele degenerate ale comportamentului colectiv. În grupuri mari, care încurajează anonimitatea şi facilitează ceea ce sociologii numesc „difuzia responsabilității", indivizii converg adeseori spre o stare exaltată a mentalului colectiv – fenomen denumit „contagiune" de către Gustave Le Bon, în a sa „Psihologie a mulțimilor" (Gustave Le Bon, 1895).

Totuşi, comunitățile umane, indiferent de formă şi context, sunt sisteme ce tind spre armonie colectivă – altfel, nu am trăi în societăți complexe, bazate pe reguli şi prescripții de comportament. Şi asta datorită faptului că societățile nu sunt constructe umane modulare, ce însumează aportul individual al membrilor – ele reprezintă *ceva* ce este mai mult decât suma părților. Oamenii de ştiință (din matematică, economie, biologie), gânditorii din domenii umaniste (filosofii, sociologii, psihologii) şi scriitorii (din domeniul *science fiction*, cu precădere) s-au preocupat de aspectele pozitive ale agregării sociale, **inteligența colectivă** fiind un domeniu central de interes.

Deşi pare contraintuitiv, după depăşirea unui prag[2] (atunci când grupul devine suficient de mare şi suficient de eterogen), mărimea unui grup corelează pozitiv cu capacitatea conjugată a membrilor de a acționa inteligent şi spre binele colectiv în situații caracterizate de risc ridicat şi / sau incertitudine:

• La concursurile de tip „Vrei sa fii miliardar?" (*Who Wants to Be A Millionaire?)* concurenții au trei opțiuni de sprijin dacă nu ştiu răspunsul la o întrebare: înjumătățirea răspunsurilor posibile, apelarea unui prieten (considerat de respondent „expert" în domeniu) sau interogarea publicului (alcătuit din non-experți). James Surowiecki (2005) a analizat modul în care răspunsurile „experților" se compară cu cele ale publicului. Dacă prietenii concurenților au răspuns corect la 65% dintre întrebări, publicul a intuit răspunsul bun în 91% din cazuri. Mai mult, autorul invocă un experiment în care

Game-shows.chris-place.com

[2] Membrii grupurilor mici, formate din oameni cu opinii similare, au tendința de a gândi la fel şi de a lua decizii proaste în situații-limită: acest fenomen poartă numele de *groupthink* (gândire de grup).

participanții au fost rugați să aproximeze numărul de jeleuri dintr-un borcan. Unii au avansat o cifră foarte scăzută, unii un număr foarte mare: media predicțiilor a fost de 871 de jeleuri în borcan, cu doar 21 mai multe decât numărul real.

• Foldit este un joc de tip *crowdsourcing* ce a reușit rezolvarea unui „puzzle" molecular a unui retrovirus ce a nedumerit comunitatea științifică timp de 10 ani. Cei aproximativ 260.000 de jucători au descifrat secvențele moleculare în mai puțin de 10 zile, manipulând și îmbinând diverse secvențe tridimensionale generate pe calculator ale ADN-ului retrovirusului (Khatib et. al., 2011).

www.harapnik.org

• The Office of Naval Research din cadrul US Navy a inițiat un program ambițios de studiu al modului în care indivizii pot crea strategii militare ofensive și defensive (Jensen, 2011). Proiectul MMOWGLI (Massive Multiplayer Online WarGame Leveraging the Internet) este un joc-simulator, în care o tabără joacă rolul piraților din Cornul Africii și cealaltă pe cel al *task-force*-ului însărcinat să protejeze navele și să salveze pasagerii dacă aceștia sunt capturați. Jocul este extrem de realist: „pirații" elaborează tactici și strategii de atac, negociază răscumpărarea captivilor etc., iar tabăra *task-force*-ului operează cu calcule ce privesc logistica necesară înarmării vasului, probabilități de atac și alte aspecte juridice, financiare, operaționale ce se întâlnesc și în realitate. The Office of Naval Research speră ca jucătorii să genereze tactici de război specifice cu totul inovative, care să ajute ofițerii însărcinați cu protecția vaselor ce tranzitează Golful Aden în conturarea unor măsuri de prevenție și contracarare eficiente.

www.iftf.org/mmowgl

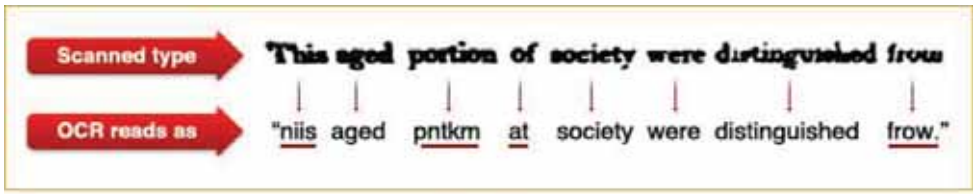
II.2. Tehnologia secolului al XXI-lea

Tehnologia modernă nu reprezintă o simplă umbrelă conceptuală pentru multitudinea de instrumente (computere, smartphone-uri şi alte *gadget*-uri) şi software-uri (reţele de socializare, aplicaţii web 2.0 etc.) pe care le folosim pentru a comunica, lucra, a ne petrece timpul liber ş.a.m.d., ci o realitate socială redefinită de capacitatea hipertrofiată de a interacţiona cu semenii şi cu informaţia.

Facebook, Ticketmaster, Twitter, 4chan, CNN.com, StumbleUpon, Craigslist şi alte câteva mii de site-uri din întreaga lume folosesc una dintre cele mai simple şi utile forme de *crowdsourcing* pentru a ajuta gigantul Google în demersul său de a scana, traduce şi face publice documente vechi, ce riscă să se piardă din cauza perisabilităţii hârtiei pe care sunt scrise.

Începând cu anul 2009, site-urile menţionate folosesc o formă derivată a programului CAPTCHA - soft ce nu permite accesul programelor automate de tip *spambot* pe site-uri prin adresarea cerinţei către utilizatori de a transcrie câteva cuvinte scrise într-o formă greu lizibilă. Programul, intitulat reCAPTCHA, foloseşte cuvinte pe care soft-ul Google nu a reuşit să le traducă.

www.captcha.net



www.google.com/recaptcha/learnmore

În doar câteva luni, cu un minim de efort, utilizatorii site-urilor ce folosesc reCAPTCHA au tradus peste 7.300 de ediţii ale „New York Times" (numerele apărute zilnic timp de 20 de ani). Google estimează că zilnic sunt afişate aproximativ 200 de milioane de bucăţi de text reCAPTCHA.

Smart mob-urile despre care discuta Rheingold sunt forme de agregare a grupului: fără tehnologia modernă (al cărei punct pivotal îl reprezintă Internetul şi tehnologiile derivate de comunicare *one-to-many* şi *many-to-many*), comunitățile nu ar fi putut genera inteligență colectivă la scară mare, din cauza limitărilor inerente, atât cele obiective (spațiu, timp), cât şi cele subiective (capacitățile mental-cognitive[3] ale indivizilor).

en.paperblog.com

Sub denumirea de *smart mob* se ascund multe tipuri de grupuri eterogene: pot fi protestatarii egipteni şi tunisieni ce au folosit Facebook şi Twitter în cursul revoltelor din țările MENA („Middle East and North Africa" – n. b. – acronim care desemnează o regiune ce se întinde din Maroc în Iran, care include majoritatea țărilor din Orientul Mijlociu şi Maghreb) în 2011, pentru a-şi coordona acțiunile de stradă sau a evita represaliile instituțiilor de forță sau pot fi *flash-mob*-uri ce comemorează moartea cântărețului pop Michael Jackson, prin dansuri sincronizate.

Astfel**, tehnologia este atât o cauză** a creşterii complexității mediului de securitate (din prisma facilitării şi accelerării procesului de globalizare şi a fenomenului avalanşei informaționale), **cât şi o soluție** de depăşire a limitelor vechilor modele de adaptare la realitățile politice, economice, sociale, culturale şi de securitate (acționând ca mijloc de augmentare a potențialului individual prin crearea unor rețele supra-individuale, ce creează şi mobilizează cunoaştere).

III. Utilizarea *crowdsourcing*-ului în organizațiile de intelligence

Robert Steele (1992a, 1992b, 1996, 2002 ş.a.m.d.) este principalul promotor al utilizării comunităților inteligente în construcția a ceea ce el numeşte arhitectura de „intelligence public" – un model de cooperare în care

[3] Antropologul britanic Robert Dunbar a teoretizat că numărul de relații sociale stabile face-to-face pe care un individ le poate întreține este între 100-230, fapt ce rezultă din limitările de volum ale neocortexului uman.

indivizii şi organizațiile (guvernamentale, neguvernamentale, academice etc.) folosesc informații obținute etic şi legal (în special OSINT) pentru beneficiul comun şi colectiv al unei națiuni „smart". *Crowdsourcing*-ul poate contribui la realizarea acestei arhitecturi în mai multe modalități:

• **Ameliorarea calitativă a ciclului de intelligence, în special pe palierul analitic-predictiv**.

Problemele complexe, multifațetate şi dificil de administrat mental, cu care se confruntă experții în intelligence în mod regulat, sunt supuse riscului unei interpretări analitice greşite. Cauzele sunt numeroase: bias-uri şi limite cognitive ale analistului, existența unor date contradictorii sau a unui bagaj voluminos de informații brute, în limbi şi formate greu accesibile etc. Predicțiile analiştilor au rolul orientării deciziei strategice a beneficiarilor – o miză importantă a muncii de intelligence, cu costuri asociate în caz de eşec extrem de mari. Pornind de la fundamente greşite (acuratețea, calitatea sau profunzimea analizei), predicțiile devin vulnerabile sub aspectul calității. Folosirea comunităților de indivizi interesați să participe anonim la interpretarea evenimentelor, discriminarea informațiilor nerelevante, sintetizarea datelor importante sau conturarea unor predicții (prin intermediul unei platforme web ce foloseşte un script bazat pe metoda Delphi, de exemplu) poate ajuta structurile analitice ale unui serviciu de informații în validarea sau modificarea analizelor şi predicțiilor proprii.

De exemplu, în 1986, naveta spațială Challenger a explodat la 73 de secunde de la lansare. Bursa a reacționat imediat: cei 4 contractori care au furnizat piese de construcție pentru racheta americană au cunoscut fluctuații ale prețului acțiunilor. 3 dintre cele 4 firme menționate au înregistrat pierderi minore, dar cea de-a patra companie, Morton Thiokol, a suferit o scădere de 12 puncte procentuale în decursul unei singure sesiuni. Nimeni nu formulase public vreo acuzație asupra contractorilor, dar milioanele de traderi au intuit, colectiv, că piesele provenite de la Morton Thiokol sunt cele responsabile de catastrofă. Abia după 6 luni, o comisie guvernamentală de experți a conchis că, într-adevăr, piesele celui de-al patrulea contractor au dus la explozia navetei Challenger.

Astăzi, în mediul business, există numeroase firme ce folosesc capacitatea predictivă a grupurilor mari, eterogene şi nestructurate pentru a lua decizii strategice: Motorola, Hewlett-Packard, Renault, Pfizer, Siemens, Arcelor Mittal, Microsoft, France Telecom, Google şi General Electric sunt doar câteva dintre organizațiile ce întrețin sau uzitează rezultate generate de platforme de predicție.

• **Armonizarea strategiilor organizațiilor de intelligence la nevoile şi aşteptările comunității**.

Deşi pare o mişcare îndrăzneață, poate chiar utopică pentru un serviciu de intelligence ce foloseşte secretul ca resursă pivotală a activității, externalizarea către comunitate poate reprezenta o componentă de strategie de comunicare publică a instituției. Integrarea comunității în elaborarea întregului plan de activitate a unui serviciu de informații nu este nici dezirabilă, nici eficientă - motivele sunt de la sine înțelese. Totuşi, definirea liniilor mari de orientare strategică a intelligence-ului național prin includerea părerii colective este o datorie în principal etică a instituțiilor însărcinate cu asigurarea protecției şi promovării intereselor colectivității.

Spre exemplificare, Wikimedia Foundation, organizația care administrează proiectul Wikipedia şi cele derivate, a întreprins un exercițiu de *crowdsourcing* ce a conturat strategia companiei pentru perioada 2011-2016 (Newstead, Lanzerotti, 2010). Utilizatorii au creat o mare parte din documentul strategic, definind coerent, coeziv şi inteligibil direcțiile de dezvoltare pe care Wikimedia s-a angajat să le urmeze timp de 5 ani. Au existat, bineînțeles, zone de decizie internă: prioritizarea direcțiilor şi transpunerea lor într-un business-plan a rămas în sarcina forurilor decizionale ale companiei.

Numărul mare de contributori şi formula participativă perfect democratică de luare a deciziei au garantat faptul că niciun potențial terț cu rele intenții nu a avut puterea de a orienta strategia Wikimedia pe un făgaş greşit.

III.1. Avantaje şi riscuri ale utilizării *crowdsourcing* în intelligence

Crowdsourcing-ul nu este un panaceu, ci o soluție punctuală pentru depăşirea unor limite ale activității de intelligence. Nu trebuie pierdut din vedere faptul că, dincolo de avantaje, o astfel de inițiativă incumbă riscuri – elaborarea unei asemenea inițiative trebuind să pornească de la o evaluare lucidă a zonelor de utilitate şi a ecuației „beneficii – pericole" asociată cu fiecare din aceste zone. Trebuie precizat că avantajele şi riscurile avansate în schema următoare nu se află în corelație.

Avantaje	Riscuri
Rapiditate – S*mart mobs* reacționează imediat la evenimente semnificative.	**Folosirea inadecvată a analizelor / predicțiilor** – Grupul devine viabil ca resursă doar dacă îndeplineşte anumite condiții de mărime, eterogenitate etc. Folosirea comunității înainte de atingerea acestor praguri poate duce la obținerea unor rezultate nesatisfăcătoare şi la decredibilizarea metodei.
Stabilitate – Ecologia grupului face ca individualitățile să ocupe un loc secund în influențarea calității unui material: pierderile sunt înlocuibile.	**„Soluția miracol / panaceu"** – Nu toate domeniile de intelligence sunt pretabile la *crowdsourcing*.
Cost redus – Pregătirea unui analist este un proces costisitor şi cronofag: comparativ, folosirea resurselor comunității costă puțin.	**Disiparea responsabilității analistului** – *crowdsourcing*-ul nu oferă soluții „la cheie", ci doar un mijloc de ajustare a analizelor / predicțiilor realizate de experți în cadrul organizației de intelligence.
Abordare holistică – Grupurile mari, de persoane care nu se cunosc face-to-face încurajează circulația ideilor noi, a abordărilor insolite şi a gândirii *out of the box*.	„**Efecte perverse**" – o astfel de inițiativă poate fi privită cu suspiciune sau într-o cheie tendențioasă de către opinia publică, mai ales în spațiile care au cunoscut o perioadă de dictatură (serviciile de informații ca organe de represiune politică).
„**Aurea mediocritas**" – În grupuri suficient de mari, orice abatere / deviație, indiferent de magnitudine, nu influențează semnificativ din punct de vedere statistic media şi mediana populației de referință.	**Rezultate inacceptabile moral** – comunitatea, neangajată legal, poate propune căi de acțiune neconforme cu dreptul internațional (comunitatea poate resimți ostilitate față de o minoritate pe care o vrea suprimată).
Construirea comunității – Prin exerciții de transparență şi de apropiere onestă de comunitate se creează premisele apariției unei culturi de securitate asumată la nivel național.	**Aşteptări înşelate** – un serviciu de informații nu poate garanta utilizarea informației transmisă beneficiarului conform intențiilor emitentului. Totuşi, prin prisma formulării inițiativei, instituțiile de intelligence pot fi considerate responsabile de către comunitate pentru lipsa rezultatele palpabile.
Recrutarea performerilor – Tehnologiile web permit evaluarea în timp a calității sintezelor, analizelor, predicțiilor: cei mai buni ies în evidență.	

Bibliografie

1. **Dedijer**, Stevan, *Development & Intelligence 2003-2053* în *National Security and The Future Journal,* 2002.

2. **Holland**, John, *Studying Complex Adaptive Systems* în *Journal of Systems Science and Complexity,* nr. 19, pp. 1-8, 2006, articol disponibil la adresa: http://hdl.handle.net/2027.42/41486.

3. **Howe**, Jeff, *The Rise of Crowdsourcing* în *Wired Magazine*, 2006, articol disponibil la adresa: http://tinyurl.com/6fl5h52.

4. **Jensen**, Garth, *MMOWGLI: An Experiment in Generating Collective Intelligence,* 2011, în *Armed with Science,* articol disponibil la adresa: http://tinyurl.com/6ybp97c

5. **Khatib,** Firas et. al., *Crystal structure of a monomeric retroviral protease solved by protein folding game players* în *Nature Structural & Molecular Biology*, 2011, articol disponibil la adresa: http://tinyurl.com/3df5gqd

6. **Le Bon,** Gustave, *Psihologia mulțimilor*, Filipeştii de Târg, Editura Antet XX Press, 1895 (2007).

7. **Newstead**, Barry şi **Lanzerotti**, Laura, *Can You Open-Source Your Strategy?* în *Harvard Business Review*, 2010, articol disponibil la adresa: http://tinyurl.com/6e3h8cb.

8. **Rheingold**, Howard, *Smart Mobs: The Next Social Revolution*, New York, Editura Basic Books, 2002.

9. **Steele**, Robert, *E3I: Ethics, Ecology, Evolution and Intelligence,* 1992a, în Whole Earth Review, fall edition.

10. **Steele**, Robert*, Open Source Intelligence Clarifies Global Threats*, 1992b, în AFCEA International, fall edition.

11. **Steele**, Robert, *Creating a Smart Nation: Strategy, Policy, Intelligence and Information* în Government Information Quarterly, Volume 13, Number 2, pp. 159-173, 1996.

12. **Steele**, Robert, *The New Craft of Intelligence*, New York, OSS Publishing Company, 2002.

13. **Surowiecki,** James, *The wisdom of crowds*, New York, Anchor Books – Random House, 2005.

Managementul modern în cadrul organizațiilor de intelligence

Adrian POPESCU
Serviciul Român de Informații
e-mail: **adrianpopescu@sri.ro**

Abstract

The transformation and reorganization process of national security structures requires, inevitably, a change of the organizational culture.

Within these structures there is a tendency to create a strong organizational culture, quality-oriented, involving the existence of values, beliefs, perceptions and representations based on this principle. Developing a quality-oriented organizational culture determined for all groups in the organization (regardless of the hierarchical level, training or complexity of specific tasks) a consistent approach to activities within the organization and in relation to the environments in which it operates.

Keywords: intelligence, organizational culture, knowledge, evolution, management.

Introducere

Intrat în vocabularul managementului în a doua jumătate a anilor 1990, cu ocazia primei conferințe internaționale dedicate managementului, inițiată de profesorul Igor Ansiff, în cadrul Universității Vanderbilt, **managementul strategic** reprezintă un proces dinamic de aliniere a strategiilor, performanțelor şi rezultatelor, aplicabil oricărui domeniu de activitate. Managementul strategic presupune combinația a patru elemente: oameni (resursa umană), leadership, tehnologii şi procese.

Procesul de transformare şi reorganizare a structurilor din domeniul securității naționale determină inevitabil şi transformarea („îmbunătățirea", „perfecționarea") culturii organizaționale, în scopul orientării către calitate şi eficientizare printr-un leadership performant, prin sporirea gradului de profesionalizare a personalului, şi printr-un management eficient al resurselor umane, asigurând astfel un un management al calității totale.

Dezvoltarea unei culturi organizaționale orientate spre calitate determină pentru toate grupurile din organizație (indiferent de nivelul ierarhic, de pregătire sau de complexitatea misiunilor specifice) un mod de abordare unitară a activităților din interiorul organizației, precum şi în relație cu mediile în care aceasta funcționează.

Această abordare omogenă a realității din interiorul şi exteriorul organizației este realizată datorită valorilor şi normelor de conduită impuse prin promovarea în cadrul acesteia a principiilor managementului calității.

Provocările noului mileniu

Modificarea dramatica a contextului de securitate şi a modelelor funcționale organizaționale, cu cauzalitate multiplă (globalizarea, progresul asimptotic al tehnologiei, decredibilizarea unor modele de conducere clasice ca urmare a crizei economice profunde) impun o reevaluare a modului în care trebuie abordat managementul organizațional. Din această perspectivă, se impune şi o analiză atentă şi, dacă este cazul, o reevaluarea modului în raspund structurile de intelligence la noile provocări.

Astfel, globalizarea are un impact major asupra activității de intelligence, în sensul că lansează provocări la adresa comunităților de informații pe linia creşterii capabilităților proprii de exploatare a surselor deschise şi de accesare a expertizei externe, concomitent cu „reducerea" distanței dintre producătorul şi consumatorul de intelligence.

Din această perspectivă, evaluarea complexă a stării de securitate şi a modului în care organismele competente răspund acestor circumstanțe scoate în evidență următoarele:

- Amenințările devin mai complexe şi mai extinse, atât în interiorul statelor, cât şi în plan internațional. Statele-națiune şi actorii non-statali, activând împreună sau separat, au un acces sporit la informația acționabilă, mecanismele financiare globale şi capabilități distructive, inclusiv la arme de distrugere în masă. Noile problematici de intelligence, multe dintre ele conexate dezvoltării tehnologice şi ştiințifice, determină formarea de noi experți, respectiv de noi beneficiari, pe toate segmentele de guvernare.
- Cerințele analitice depăşesc frecvent capacitățile interne ale comunităților de intelligence, obligând factorii de decizie la măsuri dure în direcția dezvoltării acestora.

- Interconectivitatea istorică dintre intelligence, strategie şi politică este din ce în ce mai dificil de manageriat într-un mediu în care informaţia circulă din ce în ce mai rapid, marcat de o relaţie mai strânsă ca niciodată între membrii comunităţii de intelligence, decidenţii politici şi experţi externi. În paralel, sunt tot mai greu de contracarat tendinţele de birocratizare a intelligence-ului, tehnicile eficiente de lucru fiind esenţiale inclusiv pentru contracararea politizării. Cu toate acestea, un leadership solid este garanţia menţinerii obiectivităţii analitice.
- Beneficiarii interconectaţi în reţea utilizează la scară din ce în ce mai mare surse alternative pe care le consideră mai utile şi oportune decât produsele de intelligence – sau sunt, pur şi simplu, suficient de bune – în respectarea termenelor vizate. În acelaşi timp, analiştii pierd, în continuare, avantajul competitiv în privinţa problemelor complexe de securitate naţională şi devin din ce în ce mai dependenţi de informaţiile din surse deschise şi de cooperarea cu partenerii externi.
- Opţiunile analiştilor privind carierele proprii devin din ce în ce mai numeroase şi atractive în afara comunităţii de informaţii. Managerii se văd obligaţi să motiveze şi să reţină o forţă de muncă ce tinde să opteze în favoarea exploatării acestor opţiuni, în detrimentul celor din interiorul comunităţii, considerate mai puţin atractive, fapt repercutat asupra exploatării tehnologiilor colaborative de ultimă generaţie, accesării celor mai bune surse deschise de informare şi colaborării cu omologi aparţinând organizaţiilor externe din domeniul intelligence.
- Managerii au nevoie de training de calitate în vederea ridicării standardelor de management, necesare pregătirii şi perfecţionării resurselor umane din cadrul comunităţii de intelligence. Într-un mediu de lucru tensionat, managementul eficient pe fiecare segment de activitate este esenţial în buna orientare a analiştilor, în prezervarea subiectivităţii şi a integrităţii procesului de intelligence. Managerii vor trebui să îndeplinească inclusiv rolul de lider.
- Instituţiile specializate în pregătire profesională şi training, care dispun de toate resursele necesare, sunt foarte importante în conetxtul globalizării. Comunitatea care nu dispune de structuri de profil nu poate avea pretenţia că îşi profesionalizează resursele umane în conformitate cu principiile erei informatizate.
- O „Universitate Naţională de Intelligence" ar avea misiunea de a încorpora, prezerva şi creşte vastul segment al cunoaşterii profesionale asociate intelligence-ului. De asemenea, ar contribui la educarea actanţilor în intelligence – furnizori şi beneficiari – întrucât reformarea comunităţii

de informații nu poate reuşi decât dacă respectiva comunitate şi principalele instituții politice de conducere a ei au obiective şi strategii comune în îndeplinirea lor.

- Mesajul de bază pentru nucleul analitic al unei comunități de intelligence care îşi pierde competitivitatea în era informațională este să nu „sune retragerea", să-şi sporească capabilitățile şi să exploateze cât mai agresiv noile tehnologii, investind în expertiza resurselor umane şi în parteneriate, în special în lumea ştiințifică (Gannon, 2008)[1].

Mai mult, raportându-se la evenimentele din 11 septembrie 2001 şi la problematica armelor de distrugere în masă din Irak, Gregory F. Treverton (2003) accentuează necesitatea „*instituționalizării lecțiilor învățate*" *(the institutionalized "lessons learned"* capacity), asociind sub această formulă nevoia de a valorifica, atât eşecurile, cât şi reuşitele, mai ales acele reuşite „*care nu au rezultat ca urmare a unor doctrine prestabilite*"[2]. Aspectul este sintetizat de Mark Lowenthal (2008) în „Analyzing Intelligence: Origins, obstacles, and innovations" sub forma a patru întrebări:

- Ce am învățat (sau ce credem că am învățat)?
- Ce este diferit?
- Ce anume trebuie să facem în continuare?
- Încotro ne îndreptăm?[3]

Procese de intelligence

Procesul de intelligence, aşa cum este cunoscut în orice prezentare clasică, dar şi în foarte multe site-uri de specialitate pe Internet, urmează un flux de tratare a informațiilor format din cinci etape, cunoscut ca ciclul de intelligence.

Producția de intelligence urmează un **proces ciclic**, o serie de măsuri repetate şi interdependente care adaugă valoare datelor primare stocate în bazele de date şi creează un produs transformat în mod substanțial.

---

[1] John C. Gannon, Managing Analysis in the Information Age în GEORGE, Roger Z. şi BRUCE, James B., Analyzing Intelligence: Origins, obstacles and innovations, 2008, p. 215

[2]Gregory F. Treverton, Reshaping National Intelligence for an Age of Information, Cambridge, Cambridge University Press, 2003, p. 11-13

[3]Mark M. Lowenthal – „Intelligence in Transition: Analysis after September 11 and Iraq", în George, Roger z. şi Bruce, James B., „Analyzing Intelligence: Origins, obstacles, and innovations", 2008, p. 226

Deşi procesul de intelligence este complex şi dinamic, mai multe funcţii / componente pot fi distinse de ansamblu. Din această perspectivă, **procesul intelligence clasic** cuprinde următoarele etape**: planificarea**, **colectarea**, **procesarea**, **analiza** şi **diseminarea** produselor intelligence.

Acest model păstrează o particularitate obligatorie de compartimentare a oricărei activităţi intelligence, cerinţă necesară şi astăzi pentru protejarea metodelor şi, în special, a surselor de informaţii care utilizează şi surse închise (secrete) (Sebe, 2010)[4].

Planificare, stabilire cerinţe şi direcţionare reprezintă definirea de către decident, la un nivel înalt de abstractizare, a cunoştinţelor necesare pentru a lua decizii. Cerinţele sunt traduse în termeni de informaţii solicitate, apoi în date care trebuie să fie colectate.

Colectare: sursele tehnice şi umane sunt adresate pentru a se colecta datele brute cerute. Surse pot fi disponibile în mod deschis sau închis, fiind accesate prin diverse metode. Aceste surse şi metode sunt cele mai fragile şi protejate elemente ale procesului.

Surse de inteligenţă pot fi: ***human intelligence*** (HUMINT), ***imagery intelligence*** (IMINT), ***signals intelligence*** (SIGINT), ***electromagnetic signals monitoring*** (ELINT), ***open source intelligence*** (OSINT) etc..

Procesare: datele colectate sunt procesate (ex. traduceri din alte limbi, decriptări), indexate şi organizate. Progresul în atingerea cerinţelor planului de colectare este monitorizat, iar modul de abordare poate fi rafinat pe baza datelor primite.

Analiza: baza de informaţii este procesată folosindu-se tehnici de estimare sau inferenţiale care combină datele surselor în încercarea de a da răspuns la întrebarea solicitatorului. Datele sunt analizate (descompuse pe componente şi studiate) şi soluţiile sunt sintetizate (construite plecând de la evidenţele acumulate). Subiectele analizelor sunt modelate şi se pot face noi cerinţe pentru colectări şi procesări adiţionale.

Analiza în domeniul intelligence a fost mereu importantă deoarece prin aceasta se generează înţelegerea. Importanţa înţelegerii „concurenţei" a fost recunoscută de strategul militar Sun Tzu[5] încă din sec. VI I.H.. Această necesitate de a-şi cunoaşte adversarul era afirmată prin folosirea spionilor: „*cunoaşterea aprofundată nu poate fi obţinută prin fantome*

[4] Sebe Marius, *Despre intelligence*, Bucureşti, Revista Română de Studii de Intelligence nr. 3, octombrie 2010

[5] Sun Tze, *Arta războiului*, Editura Antet, 2004

şi spirite, dedusă din fenomene, sau prin raportare la standardele Raiului, ci trebuie dobândită de la oameni deoarece reprezintă cunoaştere adevăratei situații a duşmanului".

Diseminarea: în cele din urmă, informația este diseminată către consumatori în formate diverse, plecând de la imagini dinamice ale sistemelor militare de război şi până la rapoarte formale către politicieni. Se pot distinge trei categorii de rapoarte de inteligență tactică şi strategică formale: ***current intelligence reports*** sunt rapoarte tip ştiri, care descriu evenimente recente sau indicatori şi avertismente; ***basic intelligence reports*** furnizează descrieri complete ale unei situații specifice (ex. ordinea de luptă sau situații politice) şi ***intelligence estimates***, rapoarte care încearcă să prevadă posibile situații viitoare ca rezultat a stării şi constrângerilor curente.

Produsele de intelligence sunt diseminate către utilizator, furnizând răspunsuri la interogări şi estimări ale acurateței produsului livrat.

Noi abordări în secolul 21

Producerea intelligence-ului guvernamental în Era Informațională a suferit o schimbare paradigmatică, astfel încât procesul intelligence să se desfăşoare sub imperiul condițiilor impuse de *paradigma diamant* (Steele, 1998)[6].

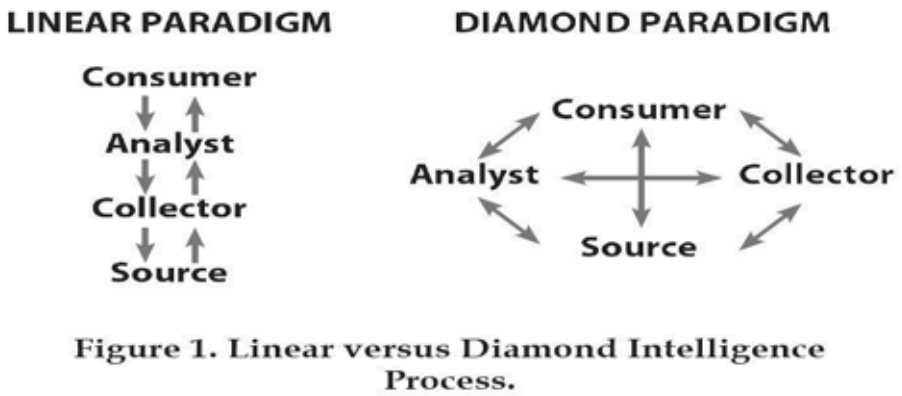


Figura 1. Procesul de intelligence liniar vs. diamant (sursa: http://www.phibetaiota.net /wp-content/uploads/2009/08/Linear-versus-Diamond-Paradigm1.jpg)

[6] Steele, Robert David, *New craft of intelligence,* 2002

Vechea paradigmă, cea liniară, se bazează pe un model de intelligence, specific secolelor 19 şi 20, prin care consumatorul discuta cu planificatorii intelligence, aceştia cu cei ce colectează informațiile, care ajung la surse, obțin informațiile pentru analişti, care închid ciclul prin diseminarea produsului de intelligence către consumator.

Acest model nu numai că era prea încet şi greoi, dar nu poate fi funcțional când în jurul sistemului există un mediu cu o agendă în continuă schimbare, plină de subiecte şi nuanțe care sunt dificil de comunicat prin intermediari.

Paradigma diamant impune un model prin care consumatorul contactează direct analistul şi colectorul, iar în multe ocazii ajunge chiar la sursă (atunci când este posibil prin nivelele de clasificare intelligence).

În acelaşi timp, jucătorii de pe piața intelligence, indiferent că acesta este intelligence politic, economic, de afaceri, militar, cultural, etnic-religios etc., au fost obligați să treacă de la arhitectura „înaintării" – „push" la arhitectura „tragerii" – „pull", datorită dezvoltării fără precedent a diseminării electronice.

În secolul 20, diseminarea intelligence-ului se desfăşura conform arhitecturii „push", când mediul informativ referitor la derularea evenimentelor utiliza spațiul transmisiilor Erei Industriale, în care analistul de intelligence selecta dintr-o cantitate de informații ceea ce el credea că utilizatorii ar trebui cel mai mult să cunoască. De cele mai multe ori, aceste produse de intelligence erau „înaintate" (push) în cadrul unor termene fixe ori după un program dictat de capacitatea de lucru a analistului.

În secolul 21, mediul informativ funcționează sub imperiul şi în spațiul transmisiilor Erei Informaționale, în care diseminarea electronică schimbă complet arhitectura, în sensul că utilizatorii produselor de intelligence au la dispoziție mari cantități de informații, iar deciziile privind tipul de informații care ajunge la aceştia, nivelul de detaliere, formatul documentelor, iar mai presus de orice momentul când trebuie să ajungă, revin utilizatorilor.

Fluxuri şi sisteme informaționale

Managementul oricărei companii care se respectă se bazează, într-o măsură mai mare sau mai mică, pe intelligence-ul privat, iar capacitatea acestuia de a recunoaşte valoarea noului în fluxul informațional, de a-l asimila şi de a-l aplica în funcție de necesitățile derulării afacerilor asigură

eficacitatea procesului decizional la acest nivel. Abilitatea unei companii de a obține şi utiliza intelligence-ul privat devine tot mai importantă pe măsură ce debitul informațional referitor la dinamica pieței sporeşte, iar incertitudinile privind oportunităților viitoare se intensifică (Purcărea, Constantinescu, 2003)[7].

Formarea culturii de intelligence reprezintă o prioritate a oricărui demers educativ prin cunoaştere, iar coordonarea factorilor implicați ONG-uri, medii academice, instituții cu atribuții în domeniu ar trebui să devină o nouă responsabilitate a Comunității Naționale de Informații.

Conceptul de informație este un concept de mare generalitate, întâlnindu-se în absolut toate activitățile umane şi în natură. Nu este posibil nici un sistem natural sau social fără schimb de informații, atât între sistemul respectiv şi alte sisteme, cât şi în interiorul sistemului propriu, între componentele acestuia.

Între componentele (elementele) oricărui sistem şi/sau între sisteme, informațiile iau naştere, în mod aleator sau determinist, locul de emitere a informației numindu-se „**sursă**", iar locul de destinație „**receptor**". Între sursă şi receptor informația circulă printr-un canal de comunicație.

Pentru realizarea unor produse materiale sunt necesare transmiterea şi utilizarea unor informații.

Fluxul informațional reprezintă totalitatea informațiilor transmise într-un interval de timp determinat, de la o sursă de informații la un receptor printr-o mulțime de canale informaționale (Vădana, 2011)[8]. Este caracterizat prin anumite caracteristici - lungime, viteză de deplasare, fiabilitate, cost etc.

Configurația fluxului informațional este determinată, în principal de:

- conținutul informației;
- scopul informațiilor vehiculate;
- poziția în structura organizatorică a centrelor emițătoare şi receptoare, respectiv natura relațiilor dintre acestea;
- viteza de prelucrare;
- lungimea şi capacitatea de transport a canalelor de comunicare.

Fluxurile sunt ascendente, descendente şi orizontale.

Printre elementele acestuia se numără conținutul, volumul, sensul, frecvența (ritmicitatea cu care sunt transmise informațiile), fiabilitatea (caracteristica prin care conținutul unei informații nu este denaturat prin prelucrările suferite), calitatea (totalitatea însuşirilor şi laturilor esențiale ale

[7] Purcărea, Anca & Niculescu, Cristian & Constantinescu, Doina – *Curs Management,* 2003
[8] Vădana, Ioan Iustin - *Managementul informațional,* 2011

datelor şi informaţiilor. Definitorie în acest caz este capacitatea fluxului de a asigura date, informaţii şi produse disponibile în timp), procesul de obţinere şi costul (cheltuieli operate pentru asigurarea resurselor informaţionale necesare realizării obiectivelor stabilite).

Un sistem informaţional cuprinde mai multe fluxuri informaţionale, precum şi o mulţime de conexiuni ce se stabilesc între diferite componente ale acestora.

Sistemul informaţional poate fi definit drept ansamblul integrat şi ierarhizat de procese informaţionale, procedee, mijloace, metode, echipamente, programe şi relaţii care asigură cadrul de realizare a resurselor informaţionale şi posibilitatea transformării lor în produse informaţionale necesare fundamentării deciziilor, în vederea realizării obiectivelor organizaţiei.

Un sistem informaţional specific activităţii de intelligence reprezintă „itinerariul" unei informaţii de la obţinere până la clasare ori distrugerea acesteia sau traiectul pe care îl parcurge informaţia respectivă ori o categorie de informaţii similare, de la sursă şi până la beneficiar sau utilizator.

Funcţionalitatea oricărui sistem informaţional este condiţionată într-o proporţie semnificativă de existenţa unor circuite şi **fluxuri informaţionale**.

Sistemul informatic are obiective similare şi îndeplineşte în mare măsură aceleaşi funcţii ca şi sistemul informaţional. Acesta poate fi definit drept ansamblul integrat şi ierarhizat de procese informaţionale, procedee, mijloace, metode, echipamente şi relaţii care asigură cadrul de realizare a resurselor informaţionale şi posibilitatea transformării lor în produse informaţionale necesare fundamentării deciziilor, în vederea realizării obiectivelor organizaţiei.

Evaluarea performanţelor

Organizaţia trebuie să dezvolte proceduri clare cu privire la evaluarea performanţelor (Loch, Johnson, 2010)[9]. În acest sens trebuie avute în vedere:

1. feedback-ul beneficiarilor;
2. uşurinţa accesării şi utilizării surselor deschise şi a instrumentelor oferite analiştilor din cadrul comunităţii de informaţii;
3. viteza de reacţie;

[9] Loch K. Johnson - The Oxford Handbook of National Security Intelligence, Oxford University Press, 2010, Cap. VI Assessing Intelligence Performance - John A. Gentry

4. acurateţea analizelor tactice şi strategice;
5. gradul de colaborare la realizarea acestora.

Opinia majorităţii specialiştilor este că nu există o teorie generală a performanţei în intelligence, însemnând identificarea criteriilor după care se poate realiza o analiză pertinentă a activităţii serviciilor: ce fac serviciile secrete în general, dacă performanţa lor este bună, proastă sau mediocră, cum sunt eşecurile rare, dar proeminente în comparaţie cu performanţele şi cum ignorarea performanţei diferitelor tipuri de activităţi de intelligence afectează evaluarea tuturor serviciilor de informaţii.

Deşi intelligence-ul de succes depinde de activităţile organizaţiilor de informaţii, de asemenea, aceasta are la bază politici eficiente şi controlul liderilor în ceea ce priveşte implementarea politicii de către agenţiile de informaţii nonguvernamentale, ministerele de apărare ministerele de externe şi deciziile luate pe câmpul de luptă şi acţiunile în afara controlului serviciilor de informaţii.

Consecinţele strategice ale folosirii intelligence-ului de către state depind în mod special de structurile de intelligence care se ocupă de culegerea şi analiza informaţiilor, în acest sens fiind identificate patru misiuni de substanţă ale serviciilor de informaţii: (1) monitorizarea (2) identificarea ameninţării (3) identificarea oportunităţilor şi (4) prognoze.

Succesul performanţei fiecăreia dintre cele patru direcţii implică sarcini subordonate, doar unele dintre acestea fiind în responsabilitatea iniţială a serviciilor de informaţii.

Concluzii

Începutul acestui mileniu va rămâne în istorie nu prin conflictele militare care l-au marcat şi nici prin evenimentele politice, ci prin intrarea într-o nouă fază a revoluţiei informaţiilor. Domeniul intelligence impune derularea, pe de o parte, a unui proces de integrare intrinsecă, menit să asigure sinergia sistemului (gradul de integrare poate fi consecinţa dominantă a politicilor de management informaţional), iar – pe de altă parte – a unui proces de integrare prin informatizare, de fapt, o strategie globală, care pleacă de la premisa unui management integrat, orientat pe proces.

Strategia de integrare prin informatizare a organizaţiilor de intelligence are la bază două obiective, puternic corelate: optimizarea procesului managerial şi de execuţie, prin utilizarea unui sistem avansat de management informaţional, şi – respectiv – construirea unei strategii

şi a unui sistem de instruire destinate atât dezvoltării, cât şi antrenării factorilor decizionali, indiferent de nivelul la care se află.

Optimizarea proceselor manageriale şi de execuţie printr-un sistem avansat de management informaţional poate avea la bază următoarele elemente conceptuale:

• utilizarea tehnicilor de tip flux de activităţi integrat, care conectează etapele specifice, operaţionale, la procesele manageriale şi de execuţie ale sistemului global;

• operaţiile integrate (management pe proces), care previn o fundamentare a activităţii bazate pe funcţii şi garantează un flux continuu de informaţie între structurile funcţionale şi celelalte segmente componente ale sistemului militar. În mod evident, operaţiile integrate induc în toate procesele manageriale calitate şi eficienţă;

• informaţia executivă, special pregătită, la care se adaugă sistemele de avertizare timpurie, care măresc transparenţa informaţiei atât pentru control (indiferent de nivelul decizional), cât şi pentru procesele de luare a deciziei.

Aceste aspecte sunt integrate organic managementului acţiunii militare, concept care presupune, într-o succesiune de etape, planificarea acţiunii respective prin formularea de obiective (strategice sau operative/operaţionale), conducerea procesului (organizarea procesului condus), în care scop se determină o strategie corespunzătoare (care se implementează), impunându-se totodată asigurarea resurselor necesare, controlul realizării strategiei pentru care s-a optat, la care se adaugă ajustarea acesteia în vederea atingerii obiectivelor propuse şi evaluarea performanţelor.

Asigurarea capacităţii de pregătire şi fundamentare a deciziei la nivelul sistemului informaţional-decizional, precum şi optimizarea mecanismelor decizionale reprezintă probleme deosebit de importante, care se soluţionează prin utilizarea unor instrumente specifice diferite, dintre care pot fi menţionate managementul riscurilor (riscurile asociate obiectivelor pe care şi le propune sistemul informaţional-decizional respectiv); elaborarea şi analiza de scenarii pentru evaluare şi prognoză, prin identificarea celor mai importanţi factori care pot influenţa fenomenul analizat; planificarea strategică în condiţii de incertitudine, luându-se în considerare posibilele strategii de răspuns la acestea, pe baza unor scenarii proiectate; simulări şi jocuri strategice (politico-militare, economice, de intelligence), destinate analizei şi fundamentării deciziei, având rolul de a preveni eventuale situaţii critice care pot apărea în mediul informaţional-decizional.

Bibliografie

1. John C. Gannon, *Managing Analysis in the Information Age* în George, Roger Z. & Bruce, James B., *Analyzing Intelligence: Origins, obstacles, and innovations*, Georgetown University Press, Washington DC, 2008.

2. Gregory F. Treverton, *Reshaping National Intelligence for an Age of Information*, Cambridge, Cambridge University Press, 2003.

3. Mark M. Lowenthal, *Intelligence in Transition: Analysis after September 11 and Iraq*, în George, Roger z. & Bruce, James B., *Analyzing Intelligence: Origins, obstacles, and innovations*, Georgetown University Press, Washington DC, 2008.

4. Sebe Marius, *Despre intelligence*, Bucureşti, Revista Română de Studii de Intelligence nr. 3, octombrie 2010.

5. Sun Tze, *Arta războiului*, Editura Antet, 2004

6. Steele, Robert David, *New craft of intelligence,* februarie 2002.

7. Purcărea, Anca & Niculescu, Cristian & Constantinescu, Doina – *Curs Management*, 2003 Universitatea din Bucureşti accesibil la adresa http://ebooks.unibuc.ro/StiinteADM/management/cuprins.htm

8. Vădana, Ioan Iustin - *Managementul informațional*, 2011, accesibil la adresa http://academiclink.ro/ Management/ managementul- informational- informatia- sistemul- informational-i- fluxurile- informationale.html

9. Johnson, Loch K. - *The Oxford Handbook of National Security Intelligence* - Gentry, John A. - *Cap. VI Assessing Intelligence Performance*, Oxford University Press, 2010.

Despre necesitatea unui brand al analistului de intelligence

Ionel NIȚU
Lector universitar drd., Serviciul Român de Informații
e-mail: **ionelnitu@sri.ro**
Felicia RĂDOI
Serviciul Român de Informații
e-mail: **feliciara2@yahoo.com**

„Intelligence services employ intelligence analysts to do just that – transforming accurate and relevant information into meaningful insights, in a form consumers can use at a time they need them. If intelligence fails to do this, it fails altogether".
(Fred Schreier)

Résumé

Face au déluge d'informations, le renseignement est contraint à reconsidérer la place d'analyste – le principal responsable pour la sélection, l'organisation et l'interprétation des données disponibles à un certain moment. Sa présence est, par la suite, une condition absolument nécessaire du processus de renseignement, sur lequel l'analyste agit de manière active, lui superposant une valeur supplémentaire en termes de connaissance et décision.

En tant qu'arbitre des jugements, l'analyste est doué d'habiletés et aptitudes mentales particulières. Le système doit être lui aussi flexible, afin d'assurer la meilleure intégration des capacités analytiques.

De telles provocations exigent de constituer et faire largement reconnaître l'identité professionnelle de l'analyste de renseignement.

C'est justement ce que l'auteur se propose, c'est-à-dire d'apporter la nécessité d'un brand de l'analyste de renseignement à l'attention publique. La raison en est dictée par un double impératif : d'un côté, par l'exigence interne, et de l'autre par l'opportunité de projeter à l'extérieur l'image de l'institution en utilisant l'analyste.

C'est tout à fait légitime, par conséquent, de prendre en considération l'opportunité d'inclure l'analyste de renseignement dans le nomenclateur professionnel.

Mots-clés: renseignement, processus de renseignement, analyste de renseignement, brand.

▪ În loc de argument

Mai întâi câteva paradoxuri, care, în esență, reprezintă şi argumentul pentru care ne-am propus să abordăm acest subiect:

- în spațiul public românesc sunt prezente numeroase categorii de analişti (în Clasificarea Ocupațiilor din România sunt definite 27 de tipuri de analişti, iar la posturile de televiziune puteam vedea încă 3-4 categorii), dar analistul de intelligence (sau analistul de informații) nu este recunoscut drept o ocupație / profesie în țara noastră;

- există departamente de analiză în toate serviciile de informații, în unele ministere, ONG şi firme private, dar analiza de intelligence nu este definită / conceptualizată.

Mai mult, Facultatea de Sociologie şi Asistență Socială din cadrul Universității Bucureşti (în parteneriat cu Serviciul Român de Informații) a lansat (în urmă cu 3 ani) masterul de Analiza Informației, iar la Academia Națională de Informații „Mihai Viteazul" au fost inițiate, din toamna acestui an, o licență (*Studii de Securitate şi Informații)* şi un master (*Analiza de Intelligence)* dedicate analizei de informații.

Şi totuşi, nu putem să nu ne întrebăm: Unde sunt analiştii de intelligence? Cine sunt ei? Cu ce se ocupă?

Acestea sunt numai câteva din motivele pentru care considerăm că se impune crearea unui standard ocupațional care să confere identitate profesională distinctă analistului de intelligence şi profesiei acestuia: analiza de intelligence. Aceasta din urmă trebuie să parcurgă şi un proces de firească teoretizare, sens în care autorii au contribuit la redactarea „Ghidului analistului de intelligence. Compendiu pentru analiştii debutanți", editat de Academia Națională de Informații „Mihai Viteazul" şi lansat cu numai câteva zile în urmă.

1. Cine este analistul de intelligence

▪ Locul şi rolul analistului în fluxul de intelligence

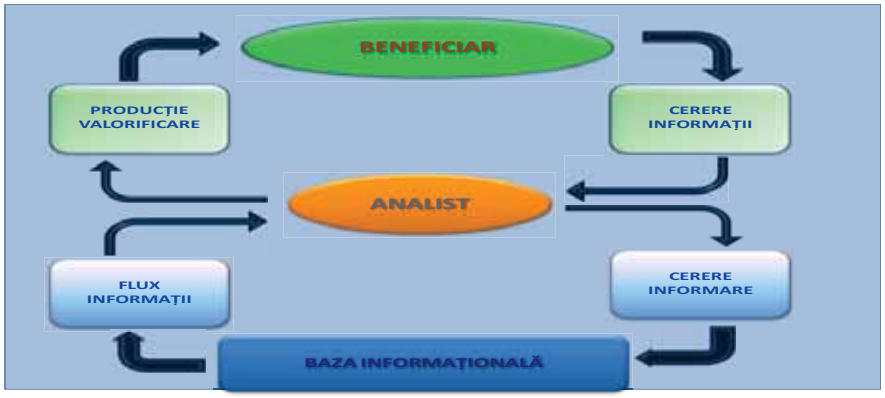
Confruntată cu necesitatea de a gestiona un flux din ce în ce mai mare de informații, activitatea de intelligence este constrânsă la reconsiderarea proceselor de selecție, organizare, evaluare şi interpretare a datelor – ceea ce se identifică, fundamental, cu procesul de analiză a informațiilor. În special în actualul context, definit de societatea informațională, instanța analitică reprezintă o condiție *sine qua non* a activității de intelligence.

O primă remarcă, elementară, este că softurile dezvoltate pentru analiza de intelligence pot realiza filtrarea şi organizarea datelor, însă nu pot înlocui

factorul uman, mai ales în ceea ce priveşte atribuirea valorii şi a semnificaţiilor datelor obţinute / disponibile la un moment dat. Ca urmare, analistul de intelligence trebuie privit ca factor-cheie al acestui proces complex, generând plus-valoare în planul cunoaşterii şi utilitate în plan decizional.

Analistul ce activează în alte domenii (social, economic, financiar) are, de asemenea, ca domenii de competenţă şi sarcini culegerea de date, selecţia şi evaluarea lor şi redactarea unui raport destinat managementului instituţiei / organizaţiei, menit să întemeieze deciziile privind activitatea acesteia. **Diferenţa specifică** o reprezintă, în cazul analistului de intelligence, operarea cu elemente de cunoaştere de o largă diversitate tematică, atât din surse deschise, cât mai ales **secrete,** şi faptul că produsele activităţii sale (documente de informare, evaluări, prognoze) au **incidenţă nemijlocită asupra problematicii de securitate naţională**, fiind menite **să fundamenteze decizia politică** în stat.

Rolul analistului în fluxul de *intelligence* (**Schema nr. 1**) derivă din situarea sa ca interfaţă cu dublu sens între nivelul informativ-operativ şi beneficiari, respectiv între structura de securitate în care activează şi decizionalii statului. Din această perspectivă, departamentelor de analiză le revine, pe de o parte, sarcina de a gestiona informaţiile obţinute de zonele operaţionale şi cele disponibile din surse deschise şi de a elabora documentele de informare pentru responsabilii guvernamentali, şi, pe de altă parte, aceea de a orienta demersurile informative pentru a răspunde solicitărilor beneficiarilor, cu respectarea cadrului legal.



Schema nr. 1 – Analistul în fluxul de *intelligence.*
Sursa: Niţu Ionel (coord.), Ghidul analistului de intelligence: compendiu pentru analiştii debutanţi, Editura ANI „MV", 2011, pag. 31

În consecință, atribuțiile ce le revin analiştilor de informații acoperă un registru vast de activități, respectiv:

- trierea informațiilor disponibile referitoare la un anumit subiect, prin raportarea acestora la criterii de veridicitate şi relevanță şi decelarea elementelor esențiale. Aceasta presupune, de cele mai multe ori, o atentă şi constantă monitorizare a evoluțiilor în problematica de interes şi în domeniile conexe şi chiar o specializare de nişă a analistului.

Sunt avute în vedere atât baza de date disponibilă din input, sursele deschise, evaluările şi punctele de vedere ale altor specialişti, precum şi experiența personală a analistului;

- organizarea datelor în forma cea mai potrivită, cu respectarea scalei cronologice sau determinist, în scopul relevării adecvate a schimbărilor;
- fundamentarea şi dezvoltarea unui raționament corect, care să permită identificarea cauzelor şi a efectelor probabile. Sunt aplicate metode specifice menite să asigure validitatea şi obiectivitatea demersului rațional (mai ales în condițiile în care sunt disponibile informații contradictorii), evitarea erorilor de analiză, cu apel consecvent la gândire critică. Analistul de intelligence trebuie să aplice justa măsură în valorificarea experienței deținute şi a clişeelor personale, pentru a putea interpreta corect elementele de noutate şi a remodela proiecțiile de natură predictivă. În egală măsură, se află în postura de a identifica elementele de cunoaştere suplimentare necesare pentru fundamentarea unei evaluări valide;
- elaborarea şi redactarea documentului de informare, cu respectarea normelor gramaticale şi de exprimare, precum şi a procedurilor de formă şi fond instituționale. Stilul trebuie să fie adecvat comunicării inter-instituționale, cu formulări clare şi concise;
- transpunerea feed-back-ului în termeni de solicitări de noi informații.

Dincolo de toate acestea, activitatea curentă a analistului de intelligence presupune, în esență, procesarea unor baze mari de date (de multe ori în termene scurte) ori furnizarea unor evaluări în condiții de deficit informațional (înainte de sau la scurt timp după producerea unui eveniment), sub imperativul de a oferi explicații ori scenarii valide.

Analistului de intelligence i se cere să deceleze şi să comunice în timp util decizionalilor schimbările semnificative în privința vulnerabilităților / amenințărilor la adresa securității naționale, încât să fundamenteze atât măsuri de prevenire, contracarare sau de limitare a efectelor negative, cât şi politici şi strategii naționale pe termen lung.

Ca specificități, care individualizează activitatea curentă a analistului de intelligence, ar mai fi de menționat: setul de rigori derivate din

chestiunile de ordin normativ dar şi din codul deontologic aplicabil domeniului analizei, aplicarea anumitor metode analitice, restricţiile (date de caracterul secret al activităţii sale, stresul şi condiţionalităţile specifice carierei oricărui militar), anonimatul (produsele sale sunt remise beneficiarilor în numele instituţiei) şi multe altele. Lăsăm cititorului posibilitatea de a identifica noi dimensiuni ale activităţii de analiză şi de a reflecta asupra modului în care acestea conferă individualitate profesiei de analist de intelligence.

▪ Repere ale profilului psiho-profesional al analistului de intelligence

A corespunde unor asemenea expectaţii / exigenţe profesionale implică existenţa unor însuşiri psiho-intelectuale şi a unor abilităţi şi deprinderi specifice (prezentate sintetic în **Schema nr. 2**). Pot fi considerate premise ale performanţei analitice următoarele:

• *aptitudini*:

- un grad de inteligenţă peste medie;

- capacitatea de accesare a tuturor tipurilor de gândire – algoritmică / euristică, reproductivă / productivă, divergentă / convergentă, inductivă / deductivă;

- aptitudini cognitive dezvoltate, respectiv: rapiditate perceptivă, atenţie distributivă, capacitate de concentrare, capacitate de structurare eficientă a informaţiilor, flexibilitate categorială, originalitate, coerenţa şi flexibilitatea ideilor, înţelegere şi exprimare fluentă şi facilă verbală şi în scris;

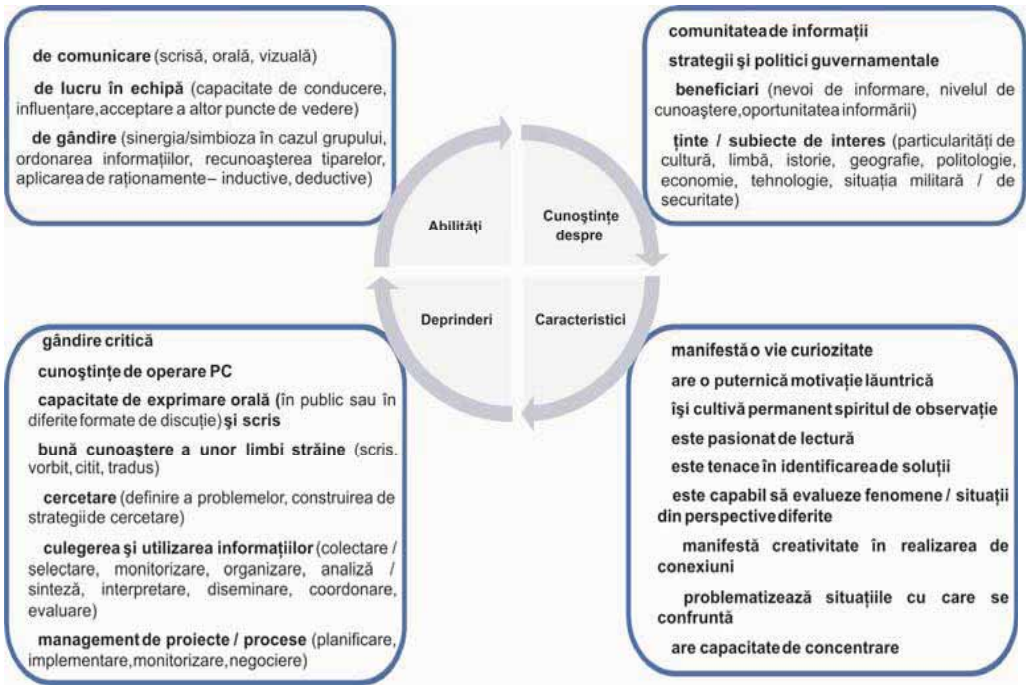
• *deprinderi*:

- formative (manifestate în învăţare activă);

- rezolutive (capacitate de soluţionare rapidă, de gestionare a unor probleme complexe, ascultare activă);

- reglatorii (analiza controlului, monitorizarea şi managementul timpului);

• *trăsături de personalitate şi elemente psiho-caracteriale*: responsabilitate, conformism social, perseverenţă, controlul tendinţei de a lua decizii pripite, obţinerea de informaţii prin conversaţie, autocontrolul, deschiderea către experienţe, capacitatea de coordonare, receptivitatea socială, dorinţa de realizare, asertivitatea, încrederea socială, flexibilitatea comportamentală, argumentarea verbală, independenţa, amabilitatea, capacitatea de refacere a tonusului, sociabilitatea, capacitatea de negociere, persuasiunea.



Schema nr. 2 – Competenţe de bază ale analistului de *intelligence*
Sursa: Niţu Ionel (coord.), Ghidul analistului de intelligence: compendiu pentru analiştii debutanţi, Editura ANI „MV", 2011, pag. 37

Pe lângă aptitudinile înnăscute şi cele dezvoltate în procesul de formare, eficienţa activităţii analistului se află în corelaţie directă cu:

- un grad ridicat de cultură generală, respectiv deţinerea unui bagaj de cunoştinţe structurat, organizat din cât mai multe domenii (economic, juridic, administrativ, cultural, religios, istoric etc.), care să permită evidenţierea unor elemente definitorii aflate în conexiune - uneori aparent inexplicabil – cu fenomene, reacţii, situaţii etc. din actualitate, cu relevanţă pentru securitatea naţională;
- o experienţă profesională relevantă, reprezentând acumulare de elemente de cunoaştere şi de norme / proceduri, care să favorizeaze soluţionarea cu operativitate a sarcinilor;
- utilizarea unui aparat metodologic adecvat, fiind privilegiate, în principiu, acele metode şi tehnici analitice cu un pronunţat caracter inductiv (raţionament de la particular la general) şi predictiv (estimări cu privire la „viitorul" posibil).

Metodele de analiză utilizate de analiştii de intelligence nu se revendică neapărat din spectrul ştiinţific – după cum evidenţiază şi Jeffrey R. Cooper – întrucât privilegiază mai curând intuiţia şi imaginaţia şi nu comportă planul imediat, concret, verificabil şi cuantificabil. Judecăţile de valoare la care analiştii ajung nu se datorează doar operării cu planul factual, ci se întemeiază în bună măsură pe conexiuni şi procese cognitive individuale (în care experienţa personală deţine un rol important) – tocmai pentru a putea compensa ceea ce este incomplet, contradictoriu, ambiguu[1].

În acest context, o importanţă deosebită revine apelului constant la gândirea critică, respectiv la tehnicile de evitare a erorilor cognitive (ceea ce Mark Lowenthal denumea „triplu joc mintal": a ne gândi la modul nostru de gândire în timp ce gândim)[2]. Analiştii de intelligence dispun de o capacitate aparte de a-şi monitoriza raţionamentele, eliminând poziţionările pur personale ori clişeele mentale, fiind capabili să construiască scenarii alternative şi să ia în considerare ipoteze şi puncte de vedere diferite.

Conturându-se în această manieră, profilul psiho-profesional al analistului de intelligence evidenţiază importanţa majoră a existenţei unor capacităţi cognitive superioare înnăscute, cărora li se adaugă un proces continuu de cultivare programatică – de cele mai multe ori prin mentorat şi lucru efectiv – ce include gestionarea / asumarea aspectelor specifice „delicate" (secret, ierarhie ori eşec).

2. Cine poate fi analistul de intelligence – despre asumarea unei imagini publice

Pe de altă parte, însă, *analistul este un element al unui mecanism instituţional* complex, nevoit să se adapteze constant la solicitările unui context de securitate din ce în ce mai dinamic.

Adaptarea componentei analitice a procesului de intelligence la schimbările mediului de securitate impune **dezvoltarea unei culturi analitice** atât *la nivel individual* (prin configurarea unor programe specifice de formare şi valorificare a potenţialului analiştilor), cât şi *instituţional* (prin crearea mecanismelor şi asimilarea rezultatelor unor procese de lecţii învăţate, prin dezvoltarea programelor de mentorat ca manieră eficientă de transmitere a experienţei şi integrarea superioară a segmentelor analitic şi operaţional).

[1] Cooper, Jeffrey R. – *Curing Analytic Pathologies*, CSI, 2005.
[2] Lowenthal, Mark M. – *Intelligence from Secret to Policy*, CQPRESS.

În egală măsură, însă, tocmai rolul şi importanţa analistului în ecuaţia activităţii de intelligence recomandă şi reclamă simultan dezvoltarea unei culturi analitice *la nivelul societăţii* – deziderat pentru a cărui materializare este esenţială ***asumarea şi promovarea unei imagini publice a analistului / analizei de intelligence.*** **Scopul** unui astfel de demers îl constituie aducerea în lumină a unei dimensiuni de înaltă performanţă, mai puţin cunoscute a activităţii structurilor de intelligence, care să fie plasată / recunoscută public ca aparţinând (şi) registrului intelectual, cu evidenţierea utilităţii procesului analitic din perspectiva fundamentării deciziilor privind interese naţionale.

Adiacent, pot fi identificate ca **scopuri subsidiare** ale acestui proces:

- promovarea publică a cooperării în domeniul analizei de intelligence cu instituţii omologe relevante din spaţiul euro-atlantic, precum şi cu mediul academic şi societatea civilă;

- mediatizarea eforturilor constante pentru profesionalizarea resursei umane implicate în activitatea de analiză şi creşterea interesului pentru o carieră în acest domeniu.

Din perspectiva conturării unui brand al analistului de intelligence, primul pas ar trebui să îl reprezinte realizarea unei analize SWOT care să reliefeze punctele tari ale comunităţii de analişti de intelligence pe care s-ar putea sprijini un asemenea demers, în contrapondere cu eventualele puncte slabe. Acestea sunt, în principiu, generate fie de lipsa unor referinţe conceptuale în privinţa profesiei de analist de informaţii şi de dificultatea - dat fiind specificul activităţii - de a promova public persoane identificate ca analişti, fie de asocierea imagologică a activităţii structurilor de intelligence cu spectrul „ocult" sau intrusiv.

Publicul vizat de promovarea unui brand al analistului de intelligence îl reprezintă, în principal, *liderii şi formatorii de opinie* - reprezentanţi ai instituţiilor din sistemul de securitate şi apărare, instituţiile publice din administraţia centrală şi locală, beneficiare de produse de intelligence, dar şi analişti din mediul internaţional, reprezentanţi ai comunităţilor de informaţii din alte state. În aceeaşi categorie pot fi incluşi membri activi ai mediului academic, jurnalişti de prestigiu, reprezentanţi ai ONG-urilor cu profil conectat domeniului securităţii naţionale, agenţii de consultanţă politică, economică sau de securitate. **Publicul secundar** îl constituie publicul general – indirect, prin reflectarea mesajelor promovate de formatorii de opinie.

Mesajul esenţial al unui brand al analistului de intelligence ar trebui să evidenţieze faptul că activitatea acestuia, caracterizată prin profesionalism şi competenţă, contribuie la decizii importante în politica de securitate a unui stat, reprezentând o necesitate şi o plus-valoare în folosul binelui public.

Configurarea unei identităţi de brand reprezintă principala provocare a unei asemenea iniţiative, fiind necesară găsirea unui suport vizual şi verbal care să susţină performanţa şi utilitatea profesiei. De altfel, însuşi personajul analistului de intelligence se profilează în mod adecvat prin *accentuarea valorilor asociate procesului şi produsului analizei de intelligence* (complexitate, caracter integrat, ştiinţific şi performant, legal, obiectiv şi corect, important pentru decizia strategică, apărarea intereselor naţionale şi ale drepturilor cetăţeanului).

Analistul de intelligence se conturează, astfel, ca personaj generic - un specialist în intelligence creativ, capabil de gândire critică şi iniţiativă, un profesionist integru, imparţial care cercetează în profunzime, cu metode ştiinţifice, un reprezentant de elită aflat în serviciul naţiunii care filtrează cu acurateţe o cantitate enormă de informaţii şi deţine astfel arta de a extrage cunoaşterea esenţială, utilă deciziei.

O variantă eficientă ar fi preluarea vizuală unor elemente de imagine naţională (tricolor, stemă) şi includerea în slogan a unor termeni-forţă, precum: patrie, securitate, adevăr, specialist, profesionalism, intelligence, cunoaştere, gândire.

Obiectivele de comunicare identitară ar putea fi:

Valorile brandului:

● analist;

- inteligenţă, perspicacitate, capacitate de prognoză;
- expertiză, profesionalism;
- intuiţie, flexibilitate, creativitate, operativitate;
- obiectivitate;
- mândrie profesională;
- abnegaţie, spirit de echipă, anduranţă;
- munca anonimă versus vizibilitatea / importanţa rezultatelor anonimatul muncii;
- în slujba interesului naţional.

● Procesul şi produsul de analiză:

- complex şi integrat;
- ştiinţific şi performant;
- legal, obiectiv, corect.
- important pentru decizia strategică, apărarea intereselor naţionale şi a drepturilor cetăţenilor

Mesajul brandului: Expertiza şi profesionalismul analiştilor sunt în serviciul naţiunii.

În concluzie, considerăm că un astfel de proiect ar putea completa imaginea instituțională a serviciilor de informații din România (ori chiar a comunității naționale de informații, în ansamblul său), prin promovarea publică a componentei analitice a activității de intelligence ca domeniu de performanță.

Un obiectiv implicit constă în definirea unui standard ocupațional care să aibă drept finalitate introducerea analizei de informații (analizei de intelligence) în Clasificarea Ocupațiilor din România şi, implicit, recunoaşterea acestei ocupații / profesii în țara noastră.

Bibliografie

1. Cooper, Jeffrey R. – *Curing Analytic Pathologies*, CSI, Washington DC, 2005.

2. Davis, Jack – *Tensions in Analyst-Policymaker Relations: Opinions, Facts, and Evidence*, in The Sherman Kent Center for Intelligence Analysis Occasional Papers: Vol.2, No. 2.

3. Johnston, Rob – *Analytic Culture in the U.S. Intelligence Community,* The Center for the Study of Intelligence (CSI), Washington DC, 2005.

4. Lowenthal M. Mark – *Intelligence: From Secrets to Policy*, CQ Press, Washinton DC, 2000.

5. Schreier, Fred – *Transforming Intelligence Services*, National Defence Academy & Austrian Ministry of Defence and Sports, in co-operation with Geneva Centre for the Democratic Control and Armed Forces, 2010.

Intelligence şi *foresight*: repere ale utilizării studiilor prospective în fundamentarea deciziilor în domeniul securității naționale

Gheorghe-Costinel ANUȚA
Serviciul Român de Informații
e-mail: **costinel.anuta@dcti.ro**

Abstract

The paper explores the potential role of foresight in supporting the decision-making process in the field of security, starting mainly from the hypothesis that in an environment dominated by incertitude and engaged in a fast transformation, the focus of the decision-making process on the future becomes imperative (taking into consideration at least a 4-5 years horizon).

In addition to the elements characteristic for foresight, respectively the characteristics or the elaboration/capitalization of these types of products, the study addresses the specific elements for foresight in other countries (Singapore, Great Britain, Holland or Finland).

Moreover, the paper analyzes the necessary premises for capitalization of such an approach for Romania: ***a new paradigm of security*** *(a 3D mix – Development, Diplomacy and Defense and resilience),* ***a "whole of society" network-type mechanism*** *(an analogy with the expression "whole of society" but which focuses on more than the governmental sector) with a significant early-warning dimension and* ***a new format of interaction with the decision-makers****: the strategic debate.*

Keywords: foresight, whole-of-society, intelligence.

Cei douăzeci de ani trecuți de la sfârşitul Războiului Rece au fost marcați de evenimente care au depăşit capacitatea noastră de a le gestiona oportun. Succesiunile de lebede negre sau gri[1] nu au făcut decât să ne

[1] Concepte dezvoltate de către Nassim Taleb în „*Lebăda Neagră. Impactul foarte puțin probabilului*", pentru a evidenția evenimentele care întrunesc anumite caracteristici, cum ar fi raritatea, impactul extrem şi predictabilitate retrospectivă.

deschidă ochii asupra necesității de dezvoltare a abilităților noastre de a anticipa şi de a ne pregăti pentru cel puțin o parte din evenimentele majore care ne vor marca viitorul.

Totodată, transformarea factorilor care determină evenimentele de tipul lebedelor negre sau gri (capacitatea computerului, banda de Internet, miniaturizarea, interdependența globală) înregistrează o accelerare exponențială, necesitând dezvoltarea unor perspective pe termen lung pentru factorii decizionali. În contextul unor asemenea evoluții, dezvoltarea şi utilizarea studiilor asupra viitorului în analiza şi implementarea politicilor de orice natură a devenit o cerință fundamentală.

În acelaşi timp, o analiză empirică a politicilor României, indiferent de domeniu, evidențiază lipsa / tratarea incoerentă a două „puncte de sprijin" în procesul dezvoltării şi implementării acestora: un input consolidat asupra a ceea ce preconizăm că ne va aduce viitorul, precum şi un instrumentar de analiză pentru verificarea progreselor înregistrate şi asigurarea corecțiilor procesului menționat. Prezenta lucrare tratează doar unul din cele două „puncte de sprijin" menționate, şi anume „incursiunea" în viitor.

1. Considerații generale privind studiile prospective

Studiile asupra viitorului, a căror dezvoltare a înregistrat o amploare semnificativă în ultimii ani, oferă posibilitatea creionării inputului consolidat menționat anterior.

Totuşi, dată fiind complexitatea modului de raportare la viitor a studiilor menționate, se impune o delimitare sumară a tipurilor acestora, cel puțin din perspectiva limitelor în creionarea stărilor viitoare.

Astfel, ne putem raporta la viitor probabil, plauzibil, respectiv posibil, precum şi despre viitor ne/preferabil (Figura 1), cu accent pe natura impactului pe care acesta l-ar avea asupra mediului sau organizației. Din această perspectivă, am putea face următoarea distincție:

- ***forecasting***-ul are în vedere proiectarea unui VIITOR PROBABIL (*likely to happen*), şi produsele de acest tip au la bază extrapolarea tendințelor evidențiate de date statistice);

- ***foresight***-ul proiectează un VIITOR PLAUZIBIL (*could happen*), produsele de acest tip având la bază toate cunoştințele noastre referitoare la starea de fapt / modul de manifestare al evenimentelor analizate);

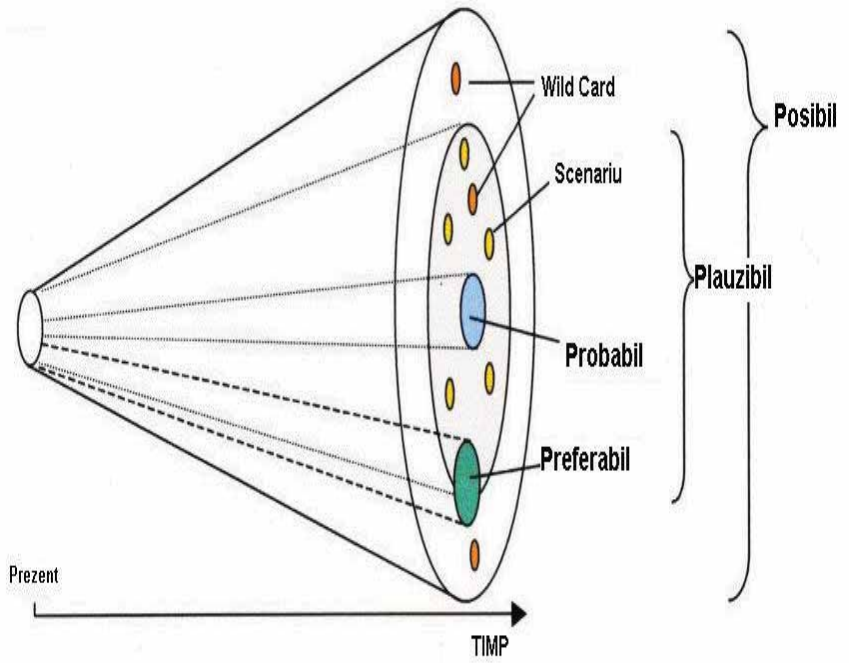


Figura 1. Conul viitorului

Adaptare după Joseph Voros, *A Primer on Futures Studies, Foresight and Use of Scenario*, www.thinkingfutures.net.

- ***normative futures*** vizează variantele ne/preferate ale STĂRILOR VIITOARE POSIBILE (*might happen*), produsele de acest tip explorând toate stările viitoare imaginabile.

Există o întreagă gamă de produse disponibile pe Internet pentru toate cele trei tipuri:

- în cazul *forecasting*-ului putem menționa *Future of Mobility Roadmap*, creată de *Smith School for Enterprise and Environment*, sau produsele *Intergovernmental Panel on Climate Change*,

- în ceea ce priveşte *foresight*-ul sunt deja arhicunoscute *Shell Energy Scenarios to 2050*, produs care a permis companiei olandeze să obțină un important avantaj strategic pe piața pe care acționează, iar

- pentru *normative futures* reține atenția *Vision 2050*, raport elaborat de către *World Business Council for Sustainable Development*.

Produsele sunt diferențiate atât din perspectiva **complexității structurale** (mai mare, pe măsură ce produsul încorporează / analizează mai multe scenarii) cât şi din cea a **conflictului de valori** asociat acestora (mai mare, pe măsură ce produsul ia în considerare toate scenariile imaginabile).

Având în vedere că elementul central al lucrării îl constituie conceptul de *foresight*, am considerat necesară identificarea unui corespondent al acestuia în limba română. Identificând un corespondent al conceptului deja adoptat, în cadrul proiectelor româneşti pe această temă, în domeniile cercetării şi inovării[2], respectiv învățământului superior[3], am preluat respectiva expresie – **studii prospective** – şi pentru studiul de față.

În ceea ce priveşte asocierea studiilor prospective cu domeniul securității ne putem raporta la două demersuri destul de familiare specialiştilor: rapoartele periodice *Global Trends* ale *National Intelligence Council*, respectiv *Multiple Futures Project (MFP)*, un proiect inițiat în cadrul NATO pentru stimularea dezbaterilor asupra Conceptului Strategic adoptat în 2010.

Ceea ce reține atenția în cazul MFP este că, în contextul identificării tendințelor / potențialelor evoluții ale mediului de securitate pentru orizontul 2030, a fost realizată şi o proiecție viitoare a organizației (Figura 2), având ca repere gradul de implicare / poziția dominantă a SUA şi UE în NATO, respectiv percepția asupra amenințărilor pe ambele țărmuri ale Oceanului Atlantic.

Astfel, proiectul MFP a adus în atenție **dubla utilitate** a studiilor prospective: anticiparea dinamicii mediului de securitate permite realizarea unor proiecții ale organizației în viitor şi, implicit, facilitează adaptarea acesteia atât conceptual, cât şi structural.

De altfel, am putea aprecia că abordarea inovativă menționată, respectiv de utilizare a studiilor prospective a facilitat obținerea de către NATO a unui document strategic destul de diferit de edițiile anterioare post Război Rece, datorită orientării către o abordare proiectiv-anticipativă în gestionarea amenințărilor emergente.

---

[2] www.strategie-cdi.ro.
[3] www.edu2025.ro.

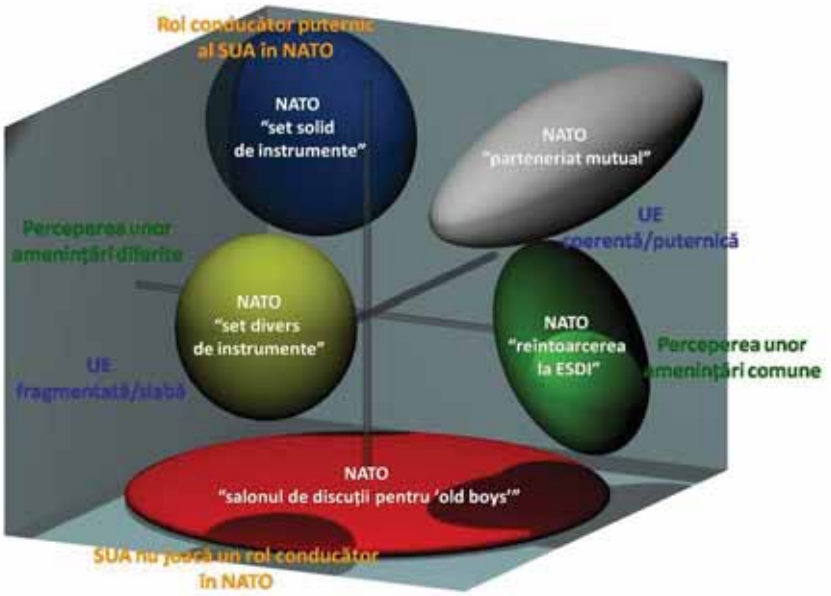


Figura 2. Viitoarele NATO

Preluată din NATO Review, http://www.nato.int/docu/review/2006/issue2/english/military.html.

2. Implicaţiile „instituţionale" ale utilizării studiilor prospective

După cum am menţionat în introducerea prezentei lucrări, politicile de orice natură promovate de către instituţiile româneşti sunt lipsite de un input consolidat asupra a ceea ce preconizăm că ne va aduce viitorul. Studiile prospective nu înseamnă planificare strategică, ci ar trebui să reprezinte **elementul care iniţiază procesul de planificare strategică**. În acest sens, un proces de scanare a orizontului (care să includă atât semnale / oportunităţi interne ale organizaţiei, cât şi tendinţe de evoluţie a mediului extern) ar trebui să orienteze formularea scenariilor / prognozelor (Figura 3).

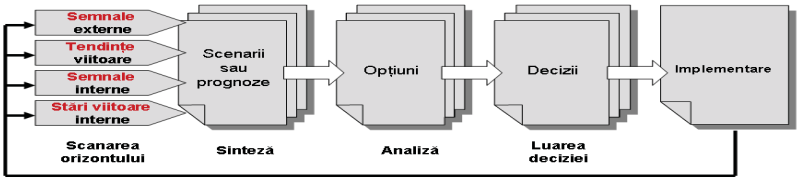


Figura 3. Conexiunea studii prospective – planificare strategică

Adaptare după Reynolds, John, Duckworth, Martin, Strategic Foresight Course, Bucureşti, 4-5 martie 2011

Deşi produsele de tipul studiilor prospective sunt percepute ca generatoare de preocupări suplimentare pentru decidenţi, concretețea şi evidențierea oportunităților ar putea conduce la angajarea acestora în conversațiile strategice necesare depăşirii cadrului formal al planificării. Conversațiile strategice ar presupune transmiterea elementelor esențiale prin intermediul unor briefinguri / conversații, în special în cazul situațiilor de criză. Principala problemă în aceste situații ar putea-o constitui nivelul de pregătire al decidentului (pericolul principal îl constituie „analfabetismul" strategic), necesar pentru a „susține" conversația strategică, respectiv pentru a lua o decizie fundamentată.

De altfel, un rol important în promovarea produsului îl are construirea unei relații adecvate cu decidenții, analiştii trebuind să aibă în vedere creşterea receptivității celor din urmă prin „construirea" unui viitor credibil, pornind - în măsura în care este posibil - de la un eveniment care a avut loc în altă zonă a globului. Un alt mod de creştere a receptivității vizează implicarea decidentului într-un mediu de simulare, în cadrul unor exerciții de tip *policy gaming* (similare „jocurilor de război", dar dincolo de sfera apărării). Totodată, analistul trebuie să aibă în vedere contextul operațional în care se va adopta decizia, un potențial model de raportare a decidentului la contextul operațional constituindu-l *Cynefin*[4] (Figura 4).

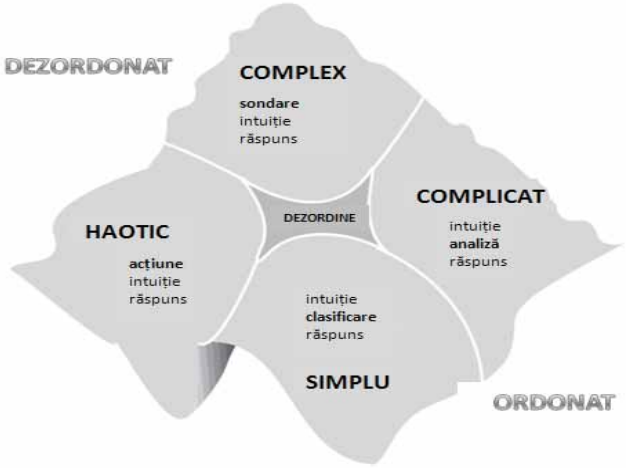


Figura 4. Modelul Cynefin

Prezentat de David J. Snowden şi Mary E. Boone în A Leader's Framework for Decision Making, Harvard Business Review, noiembrie 2007.

[4] Cuvânt de origine galică, ce descrie existența unor factori multipli în mediul extern care ne influențează în moduri pe care nu le putem înțelege.

Modelul *Cynefin* serveşte la determinarea, de către decident, a contextului operațional în vederea adoptării unei decizii adecvate (fiecare domeniu implicând decizii diferite). Contextele simple şi complicate pornesc de la premisa unui univers ordonat, unde relațiile cauză-efect sunt perceptibile şi răspunsurile pot fi determinate în baza faptelor. Contextele complexe şi haotice sunt dezordonate, nu există o relație cauză-efect vizibilă şi modul de acțiune este determinat pe baza unor modele emergente.

Majoritatea analizelor evidențiază faptul că instituționalizarea procesului de elaborare / utilizare a studiilor prospective ar putea constitui o premisă pentru gestionarea provocărilor viitorului, inclusiv de către sectorul de securitate, prin elaborarea unor noi politici (Australia, Finlanda), modificarea structurilor (Singapore) sau dezvoltarea de noi capabilități (Olanda)[5].

Procesul trebuie să fie structurat riguros, pe etape clar delimitate, dar – în acelaşi timp – să înglobeze un mecanism de „măsurare" a eficienței şi corectare a activității pentru a fi continuu adaptabil la evoluțiile mediului de securitate – fapt evidențiat atât de abordarea guvernamentală, cât şi de cea privată.

În acelaşi timp, procesul de elaborare / utilizare a studiilor prospective poate fi facilitat de transferul de *know-how* şi bune practici, prin constituirea de rețele / comunități de interes la nivel ne- / guvernamental, național şi internațional. Relevant în acest sens este exemplul Singapore-ului, unde, pentru îmbunătățirea relaționării – în special cu decidenții la nivel înalt – în cadrul guvernului a fost constituită *Rețeaua pentru Foresight Strategic* (*Strategic Futures Network*), formată din adjuncții secretarilor care conduc diversele agenții din zona guvernamentală şi care se întruneşte, de regulă, la interval de două luni. Se intenționează ca rețeaua guvernamentală (structurile specializate din diverse agenții) să fie conectată atât la o rețea națională (care să includă *think-tank*-urile din Singapore, zona de afaceri etc.), cât şi la una globală (conectată în special la sfera anglo-saxonă) pe această temă.

Translatarea concluziilor / recomandărilor studiilor prospective în sfera politicilor s-ar putea realiza prin includerea scenariilor în planificarea strategică şi distribuția resurselor (ciclurile de bugetare).

Având în vedere rolul serviciilor de informații de a „*a informa pentru a fundamenta procesul decizional al factorilor de autoritate*"[6],

---

[5] Lavoix, Helene, ed., *Strategic Foresight and Warning: Navigating the Unknown*, S. Rajaratnam School of International Studies, Singapore, November 2010.

[6] Nițu, Ionel, coord., Ghidul analistului de intelligence, Editura Academiei Naționale de Informații „Mihai Viteazul", Bucureşti, 2011, pag. 17.

studiile prospective ar putea constitui un instrument util din această perspectivă. În acelaşi timp, deşi sursele deschise oferă o multitudine de produse pe această temă, în sfera *intelligence*, studiile prospective ar putea căpăta mai multă consistență, având în vedere accesul la date / informații secrete care ar permite anticiparea anumitor evoluții cu un grad ridicat de acuratețe.

Totuşi, deşi serviciile de informații ar putea juca un rol important în implementarea studiilor prospective pe dimensiunea securității, eficiența procesului la nivel național necesită o serie de premise ce depăşesc sfera *intelligence*: o nouă alfabetizare în domeniul securității (pornind de la un mix *3D – Development, Diplomacy and Defence* şi reziliență) şi dezvoltarea unui mecanism de tip rețea „*whole-of-society / WhoS* (în analogie cu sintagma „*whole-of-government*", dar care vizează mai mult decât sectorul guvernamental) cu o dimensiune semnificativă de avertizare timpurie (Figura 5).

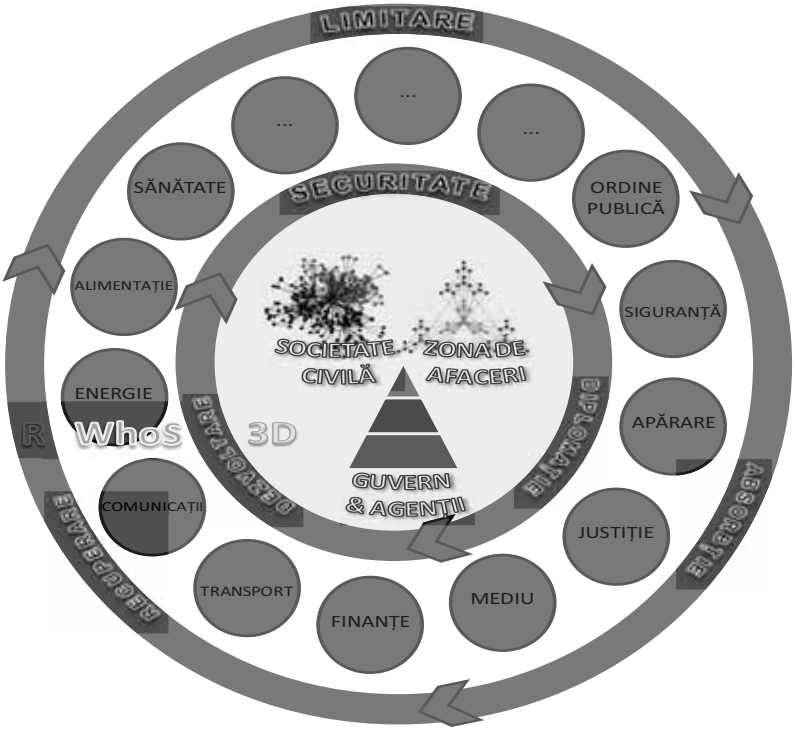


Figura 5. 3D + WhoS + R

Concret, în contextul abordării 3D, dezvoltarea ar viza „*construirea bazei economice, sociale şi politice a unui stat şi stabilizarea comunităţilor / societăţilor*", diplomaţia, „*activităţile de comunicare sau negociere pentru gestionarea conflictelor, care utilizează canale oficiale sau neoficiale în acest scop*", iar apărarea, „*o gamă largă de acţiuni cu specific preponderent militar*", de la ajutor umanitar la ducerea unui război[7]. Totuşi, în fapt, ideea de apărare în sintagma 3D este mai mult circumscrisă securităţii în sens larg, decât acţiunilor militare în sine.

Mecanismul de tip WhoS ar viza conectarea sferelor guvernamentale, a societăţii civile, respectiv a comunităţii de afaceri pentru o abordare coerentă a diferitelor domenii de activitate la nivel statal (sănătate, energie, etc.). În ceea ce priveşte ideea de avertizare timpurie, ar putea fi preluat modelul unor structuri / construcţii deja existente, cum ar fi *NATO Intelligence Warning System*, şi adaptat la un potenţial sistem naţional de management al crizelor[8].

În acelaşi timp, putem utiliza termenul de reziliență cu sensul conferit de SUA în abordarea securităţii interne – limitarea potenţialului ameninţării[9], absorbţia şocului (managementul consecinţelor) şi recuperarea[10] (revenirea la funcţionalitatea iniţială).

Conectarea conceptelor descrise (3D + WhoS + R) s-ar desfăşura având ca element central următorul algoritm: conectarea tuturor actorilor (guvern, societate civilă, afaceri) în vederea atingerii / realizării unor obiective stabilite (inclusiv pe dimensiunea securităţii naţionale), subsumate domeniilor 3D, într-un mod care să asigure rezilienţa întregului sistem. Acţiunile actorilor pot însă căpăta coerenţă şi consistenţa numai în cazul existenţei unei viziuni clare

---

[7] *A New Vision for U.S. and Global Security*, The 3D Security Initiative, Eastern Mennonite University, www.3Dsecurity.org.

[8] Kriendler, John, *NATO Intelligence and Early Warning*, Conflict Studies Research Centre, 2006, http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?id=39988&lng=en.

[9] Am „combinat" viziunea israeliană asupra rezilienţei (Meir Elron, *Israel's Homeland Security Concept: From Civil Defense to National Resilience*, briefing presented to Homeland Security Studies and Analysis Institute, August 4, 2009), cu cea americană, întrucât am considerat că ideea de a opune rezistenţă ameninţării (prezentă în conceptul american) nu exprimă într-un mod adecvat ideea de limitare a potenţialului de manifestare a ameninţării.

[10] Kahan, Jerome H., Allen, Andrew C., and George, Justin K. (2009), *An Operational Framework for Resilience*, Journal of Homeland Security and Emergency Management: Vol. 6: Issue 1, Article 83.

asupra stării viitoare (implicit obiectivelor), care poate fi formulată prin intermediul studiilor prospective. În acelaşi timp, această conectare evidenţiază necesitatea abordării / implementării studiilor prospective de o manieră integrată, prin organizarea de exerciţii dedicate, la nivel naţional.

3. Repere pentru un exerciţiu de *foresight* pe dimensiunea securităţii naţionale

În privinţa posibilităţilor curente în domeniul studiilor prospective, pe dimensiunea securităţii naţionale, am putea avea în vedere:

1. Utilizarea **posibilităţii de conectare la fluxurile naţionale şi internaţionale** existente.

La nivel internaţional ne putem raporta la proiecte NATO (*Multiple Futures*), SUA (*Global Trends*) sau UE (*European Foresight Monitoring Network*). La nivel naţional avem în vedere iniţiativele în derulare în spaţiul public românesc, menţionate anterior;

2. Valorificarea **posibilităţii de transfer de expertiză** din spaţiul public naţional.

Exerciţiul de foresight care a stat la baza elaborării Strategiei de cercetare, dezvoltare şi inovare 2007-2013, precum şi cel în derulare privind învăţământul superior (implicit experţii implicaţi în aceste proiecte), constituie surse extraordinare de cunoaştere în domeniu.

Transferul de expertiză este relevant atât din perspectiva **„algoritmului" de implementare** a unui asemenea demers, cât şi a **resurselor** implicate. Un alt avantaj al valorificării l-ar constitui conectarea – prin intermediul experţilor – a eforturilor guvernamentale cu cele din sfera societăţii civile;

3. Explorarea **instrumentarului disponibil** pe „piaţă" şi identificarea **metodelor / tehnicilor adecvate** pentru o abordare guvernamentală.

Pe lângă utilizarea motoarelor web de căutare, menţionăm două surse care concentrează demersuri consistente în domeniu:

- **platforma online dedicată comunităţii experţilor în studii prospective** – FORWIKI (www.forwiki.ro), lansată în contextul iniţiativei privind învăţământul superior din România, cu acces liber;
- volumul **Futures Research Methodology** (Metodologia pentru cercetare prospectivă), elaborat de către fundaţia *Millennium Project*.

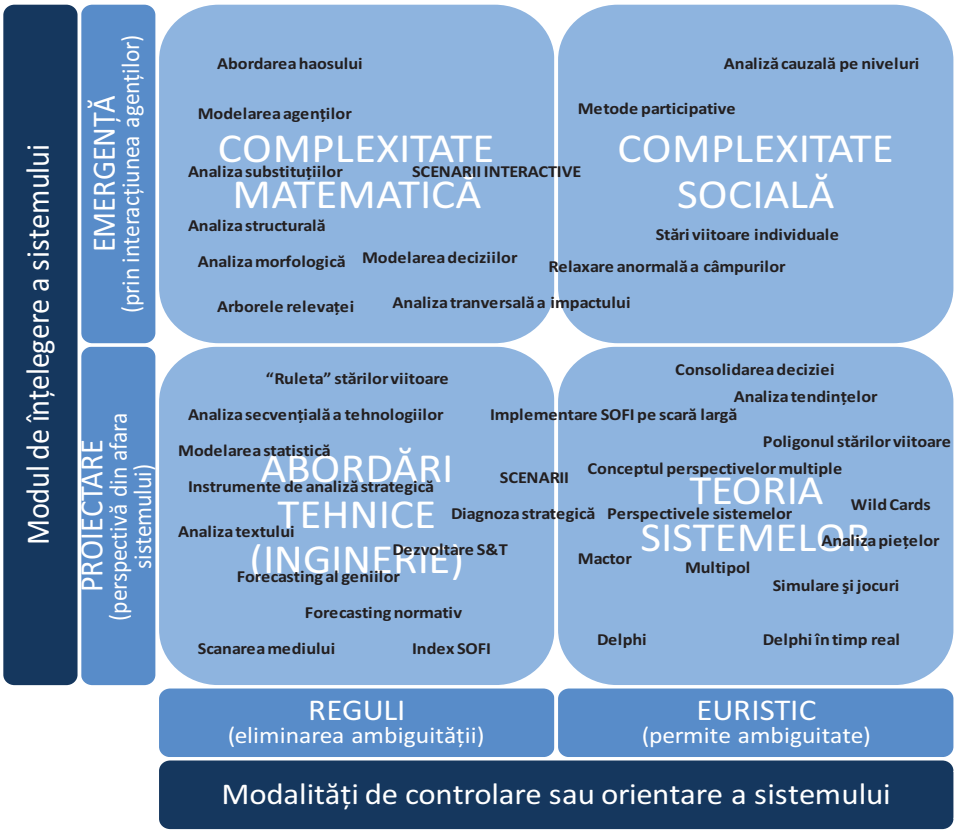


Figura 6. Matricea de analiză a metodelor prospective

Adaptare după *Futures Research Methodology*, Millennium Project

Demersurile curente pentru delimitarea unor metode / instrumente adecvate pentru derularea studiilor prospective ne oferă, de altfel, o perspectivă organizată a acestora, pornind chiar de la o taxonomie în raport cu modul de controlare a sistemului (gradul de ambiguitate), respectiv cu modul de percepere a sistemului, direct sau prin interacțiunea agenților (Figura 6).

Una din cele mai cunoscute metode de această natură o constituie scenariile. Metoda scenariilor este utilizată, în general, pentru explorarea posibilelor condiții de manifestare a unei situații, plecând de la un set de propuneri / ipoteze de lucru, fiecare scenariu reprezentând un viitor plauzibil distinct.

În vederea unei **potențiale implementări a *foresight*-ului** în sectorul guvernamental de securitate națională, am putea explora:

1. Constituirea unei **rețele naționale** (formale, sau chiar informale în stadiul inițial) care să gestioneze / analizeze problematica, dar să aibă la bază o **abordare extinsă a securității** (chiar cu o potențială reprezentare a think-tank-urilor / ONG-urilor relevante din spațiul public) şi crearea unei **platforme colaborative** având ca suport Internetul pentru o mai bună relaționare;

2. Asigurarea unui **input în fundamentarea documentelor programatice** – şi aici ne referim în special la strategia de securitate națională şi cele sectoriale subsidiare – **care să rezulte în urma unui exercițiu de *foresight*** (desfăşurat, în măsura în care este posibil, la nivel național).

*

Necesitatea şi oportunitatea inserării studiilor prospective în spațiul guvernamental merită o atenție deosebită. Există provocări a căror evoluție poate genera probleme de securitate (de exemplu evoluția demografică, atât prin prisma natalității, cât şi a exodului de creiere, sau securitatea energetică, care ar putea deveni o problemă pentru România în orizontul a 15-20 ani), dacă nu sunt abordate încă de pe acum. Studiile prospective pot oferi această perspectivă care ne lipseşte pentru a lua decizii pentru viitor începând de astăzi, în vederea gestionării adecvate a provocărilor a căror manifestare s-ar putea accentua chiar în viitorul apropiat.

Bibliografie

1. Glenn, Jerome C., Gordon, Theodore J., eds., *Futures Research Methodology*, Millennium Project.

2. Habegger, Beat, *Horizon Scanning in Government*, ETH Center for Security Studies, Zurich, 2009.

3. Kahan, Jerome H., Allen, Andrew C., George, Justin K. (2009), *An Operational Framework for Resilience*, Journal of Homeland Security and Emergency Management: Vol. 6: Issue 1, Article 83.

4. Kriendler, John, *NATO Intelligence and Early Warning*, Conflict Studies Research Centre, 2006, http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?id=39988&lng=en.

5. Lavoix, Helene, ed., *Strategic Foresight and Warning: Navigating the Unknown*, S. Rajaratnam School of International Studies, Singapore, 2010.

6. Low, Aaron, ed., *Decisions in a Complex World. Building Foresight Capabilities*, National Security Coordination Secretariat, Singapore, 2010.

7. Meir Elron, *Israel's Homeland Security Concept: From Civil Defense to National Resilience*, briefing presented to Homeland Security Studies and Analysis Institute, August 4, 2009.

8. Nițu, Ionel, coord., *Ghidul analistului de intelligence*, Editura Academiei Naționale de Informații „Mihai Viteazul", Bucureşti, 2011.

9. Popper, Rafael, *Mapping Foresight*, European Commission, Bruxelles, 2009.

10. Reynolds, John, Duckworth, Martin, *Strategic Foresight Course*, Bucureşti, 4-5 martie 2011;

11. Snowden, David J., Boone, Mary E., *A Leader's Framework for Decision Making*, Harvard Business Review, November 2007;

12. Taleb, Nassim, *Lebăda Neagră. Impactul foarte puțin probabilului*, Editura Curtea Veche, Bucureşti, 2008;

13. Voros, Joseph, *A Primer on Futures Studies, Foresight and Use of Scenario*, *A New Vision for U.S. and Global Security*, The 3D Security Initiative, Eastern Mennonite University.

Surse internet

1. http://forlearn.jrc.ec.europa.eu;
2. www.strategie-cdi.ro;
3. www.edu2025.ro;
4. www.nato.int/docu/review/2006/issue2/english/military.html.
5. www.thinkingfutures.net;
6. www.3Dsecurity.org.

Rolul contextului comunicațional în analiza de intelligence: către un *intelligence al redundanței*

Ph. D. Adrian LESENCIUC
„Henri Coandă" Air Force Academy Braşov
e-mail: **a.lesenciuc@yahoo.fr**
Cosmina DRĂGHICI
„Henri Coandă" Air Force Academy Braşov
e-mail: **cosminadr@yahoo.com**
Ph. D. Oana-Andreea PÎRNUȚĂ
„Transilvania" University of Braşov
e-mail: **andreea.pirnuta@gmail.com**

Abstract

The aims of the article is to present and evaluate the concept of intelligence of redundancy in accordance with the procedural directions of communication theories. It is analyzed the potential of the intelligence of redundancy related to the communication content and the accountability of facts.

Keywords: information, redundancy, redundancy management, intelligence of redundancy

1. Introducere

În concordanță cu direcțiile procedurale ale teoriilor comunicării, termenul de informație, folosit ca măsurare a imprevizibilității mesajului trimis, se referă la conținutul livrat.

Folosind diferite aparate conceptuale, informația de intelligence ținteşte spre cunoaşterea avansată complexă şi spre abilitatea de-a lua decizii obiective, care depăşesc limitele de raportare ale studiilor de comunicare. În termeni de comunicare, în cadrul modelelor procedurale, informația de intelligence subsumează un posibil intelligence al designului redundant. Aparent paradoxal exprimarea de redundanță a intelligence-ului ne trimite la principiile lui Sun Tzu cu privire la comportamentul opus. Această expresie îşi găseşte valoarea ştiințifică atunci când este dezvăluită în analizele şcolii de comunicare etnmetodologică a lui Garfinkel. Această

potențială redundanță a intelligence-ului se poate focaliza pe conținutul comunicației şi pe responsabilitatea faptelor (în limitele notabilității şi responsabilității), dovedind mai mult prin informație decât conceptul de bază înțeles în limitele imprevizibilității mesajului.

2. Redundanța. Abordare informațională

Redundanța, înțeleasă drept surplus informațional în telecomunicații, abundență inutilă de expresii în comunicare, este de regulă conotată negativ nu doar în ştiințele alimentate de teoria informației. Excepție face doar cazul creşterii stabilității canalului de comunicație față de acțiunile perturbatoare externe, situație în care redundanța joacă rolul important de recuperare a informației alterate, erorile putând fi corectate şi nefiind necesară re-transmiterea: „*Cu toate acestea, în multe situații din lumea reală, redundanța este utilă. În primul rând, dacă informația apare în două baze de date şi una dintre ele este alterată, putem reconstrui informația uşor. Astfel, redundanța acționează ca un mecanism de asigurare a validității datelor dintr-un domeniu anume.*" (Sauter, 2010:80). Prin urmare, un mesaj cu un grad ridicat de redundanță este mai uşor de transmis în condițiile în care în procesul comunicațional intervin perturbații de natură tehnică sau semantică. În câmpul psiho-social, redundanța păstrează nota perceptivă negativă, fiind asociată lipsei de relevanță, lestului, construcțiilor pleonastice, comunicării tautiste (Sfez, 2002:28)[1].

În teoria informației, născută din dorința de compresie a datelor şi transmitere corespunzătoare a acestora, termenii informație şi redundanță au fost direct şi indivizibil asociați. Termenul *informație* a fost utilizat cu privire la măsura impredictibilității semnalului emis, un semnal fiind înțeles ca având un conținut mai ridicat de informație cu cât gradul de predictibilitate a producerii acestuia este mai scăzut. Informația, în acest sens[2], nu se referă la probabilitatea evenimentului despre care relatează

[1] „*Într-un univers unde totul comunică, fără să se ştie originea emisiunii, fără să poți determina cine vorbeşte, în acest univers fără ierarhii, decât încâlcite, unde baza este vârful, comunicarea moare prin exces de comunicare şi sfârşeşte printr-o interminabilă agonie de spirale. Asta numesc eu ‹tautism›, neologism care îmbină autism şi tehnologie, evocând totalitatea, totalitarismul*".

[2] La modul general, înțelesul termenului *informație* este asociat noului, indiferent de domeniul de cunoaştere; cuvântul este polisemantic, având înțelesuri uneori chiar contradictorii, de aceea fiind necesară identificarea ariei de proveniență a sensului restrâns şi şcoala în baza căreia s-a realizat analiza, în ciuda tentativelor de „unificare" conceptuală, de aducere sub

mesajul, ci la probabilitatea apariției semnalului în cadrul mesajului. Astfel, informația devine măsurabilă şi se calculează ca funcție a inversului probabilității de apariție a semnului: $H = f(1/p)$, în care H este cantitatea de informație, iar p probabilitatea. Necesitatea măsurării informației a rezultat ca urmare a constatării că, pe parcursul transmiterii ei, aceasta se degradează în mod ireversibil. La modul general, informația se calculează pe baza următoarei formule elaborate de inginerul american Hartley:

$$H = \log_2(1/p). \tag{1}$$

Spre exemplu, cantitatea de informație furnizată de un semn cu probabilitate de apariție ½ este $H = \log_2(1/½) = \log_2 2 = 1$, caz particular din care derivă şi unitatea de măsură, *bit*-ul (prescurtare de la *binary digit*), termen propus de J.W. Tukey şi valorizat de Cl.E. Shannon (Shannon, Weaver, 1963:33).

În cazul unui repertoriu în care semnele au probabilitate de apariție diferită, informația medie se calculează după formula:

$$H_{med} = [p_1.\log(1/p_1)+ p_2.\log(1/p_2)+...+ p_n.\log(1/p_n)]/(p_1+p_2+...p_n)= [p_1.(-\log p_1)+ p_2.(-\log p_2)+...+ p_n.(-\log p_n)]/ (p_1+p_2+...p_n). \tag{2}$$

Dar suma probabilității de apariție a tuturor semnelor este egală cu 1, ceea ce înseamnă că formula generală a lui Shannon devine:

$$H = - \Sigma_{i=1,n} p_i.\log p_i. \tag{3}$$

Informația, în acest înțeles priveşte reflectarea fidelă, obiectivă, indiferent de interpretant, a realității, dar devine relevantă abia după ce a fost percepută ca fenomen de cunoaştere, adică abia după ce a fost supusă contactului cu interpretantul subiectiv, recepționată şi decodificată.

În baza aceleiaşi teorii a informației, *redundanța* este un concept strâns legat de cel de informație, adică se referă la ceea ce este predictibil într-un mesaj. Un mesaj cu un grad ridicat de predictibilitate este redundant,

aceeaşi umbrelă semantică şi de nuanțare ulterioară în funcție de aria de aplicabilitate;

în timp ce un mesaj cu un grad scăzut de predictibilitate este informativ. Pentru prima dată, termenul „redundanță" a fost utilizat de Harry Nyquist în 1920, care se referea la *componenta de semnal sinusoidal "inutil", care „nu transmite nicio informație", ca fiind redundantă* (*apud* Haraszti, 2002:369). Redundanța trimite la convenție, ceea ce înseamnă că presupune şi îndeplinirea unei funcții sociale. Totodată, comunicarea redundantă are şi rolul de a menține canalele de comunicare deschise. Prin urmare, redundanța priveşte tot informație, dar informație deja procesată şi stocată, care nu mai este necesară a fi supusă unor procese similare. Redundanța ține mai degrabă de interpretantul subiectiv, care o cataloghează astfel în funcție de background-ul raportării sale la mediul din care este culeasă informația. Aşadar, redundanța nu presupune non-informația, ci informația care deja a fost percepută ca fenomen de cunoaştere. Redundanța este, mai degrabă, o informație fără conținut informațional adițional la cunoaşterea anterioară, care nu implică plus cunoaştere. Dar plus cunoaşterea poate fi înțeleasă doar în raport cu un sistem individual sau organizațional de cunoaştere, subiectiv sau intersubiectiv, ceea ce presupune o notă importantă de subiectivitate alocată acestui termen. În aceste condiții, a considera redundanța ca fiind inutilă înseamnă a asocia sistemul subiectiv sau intersubiectiv de referință a fi obiectiv.

În termenii teoriei lui Shannon, redundanța este măsurabilă. Privitor la măsurarea redundanței unui mesaj, de exemplu, în cazul în care acesta este transmis printr-un repertoriu de semne nonechiprobabile (având probabilitate de apariție diferită), redundanța distribuțională, sau dimensiunea de informație cauzată de inegalitatea probabilității semnelor poate fi calculată în baza formulei:

$$R = H_{max} - H_{med}, \tag{4}$$

în care H_{max} este cantitatea de informație/semn, iar H_{med} este informația medie/repertoriul de semne.

Această redundanță, înțeleasă în termenii teoriei informației, poate îmbrăca trei forme distincte: redundanță necesară, privitoare la volumul informațional minim pentru menținerea comunicării, redundanță acceptată, vizând volumul informațional optim şi redundanță superfluă (o expresie în sine redundantă!), presupunând un volum informațional atât de mare, încât blochează comunicarea (Marian, 2008:40). Ultima dintre aceste forme este

larg întâlnită în sistemul mediatic contemporan, caracterizat prin exces comunicațional venit de pretutindeni, aparent fără țintă şi mesaj, interferând în preajma individului incapabil să aleagă, să discearnă. Redundanța superfluă a comunicării de masă, caracterizată de Sfez prin apel la mixonimul tautism, presupune transmiterea informației structurate pe orizontală, fără adâncime, fără intensitate, fără analiză calitativă, fără interpretare, caz în care comunicarea se realizează într-o „*rețea turnantă*", fără scop şi fără sfârşit, lărgindu-se cu fiecare tur şi lăsând individului audio / videospectator impresia realizării unui întreg sincron, ecosistemic şi autogestionar, în condițiile în care în realitate se produce autoînsingurarea (Sfez, 2002:100).

3. Utilitatea redundanței

Redundanța este utilă, aşa cum am văzut anterior, în cazul recuperării informațiilor alterate. Dar această utilitate, văzută mai degrabă ca fiind o rezervă de siguranță luată în limitele unei disponibilități de spațiu de stocare, de consum energetic suplimentar etc., nu este singulară. Plecând de la teoria informației, Schmidhuber (2000:694) rezumă câştigurile directe şi evidente ale reducerii redundanței, care*"*(...) *poate ajuta la reducerea spațiului de căutare pentru proceduri de învățare orientate către obiectiv"*, *"*(...) *permite comprimarea datelor"* şi*"*(...) *promite simplificarea clasificatorilor statistici"*. Dincolo de aceste beneficii directe, redundanța, înțeleasă drept pattern informațional[3], trebuie privită cu rezerve deoarece se referă la cunoaşterea comună, necesară în reducerea eforturilor de culegere a datelor prin apel la schema inductivă/deductivă imprimată de pattern, dar nu priveşte implicit şi convențiile referitoare la interpretarea şi utilizarea acesteia. Neînțelegerea utilității redundanței pleacă de la aplicarea unor scheme simplificatoare, generalizatoare în alocarea de sens informației redundante. Redundanța este privită ca fiind un proces de banalizare în raport cu memoria structurii care procesează informația: *"Redundanța, pe de altă parte, este procesul de banalizare ce are loc în strictă concordanță cu memoria sistemului. Se aşteaptă ca sistemul să echilibreze ambele funcții fără a compromite nici abilitatea sa de deschidere cognitivă către inovație, nici unitatea sa structurală."* (Philippopoulos-Mihalopoulos, 2004:86). Dar tocmai inconsistența acestei memorii este cea care transformă

[3] *Redundanța înseamnă că părți ale modelului utilizează informații commune. Înseamnă că, atâta vreme cât cunoaştem anumite componente ale modelului, ştim deja câte ceva despre alte componente.*" (Schmidhuber, 2000:693).

informația redundantă într-o informație importantă în reconstruirea dinamică a întregului de analizat.

Redundanța este o realitate cotidiană, face parte din viața socială. Orice sistem social este în mare măsură redundant şi rezistent la schimbare, la fel cum orice sistem biologic este redundant şi trăieşte din redundanță. De altfel, ca şi în cazul redundanței în limitele înțelegerii în conformitate cu teoria informației, redundanța în limitele biologicului poate oferi suportul recuperării pierderilor şi refacerii: *"Sistemele biologice în general tind să fie extrem de redundante, deoarece redundanța le face mai adaptabile: dacă o parte a proiectului dă greş, alta, parte similară a procesului, o poate prelua. Creierul continuă să funcționeze chiar dacă părți din el sunt distruse"*, dar are consturile sale metabolice, care nu sunt de neglijat: *„Oricum, redundanța şi adaptivitatea au, de asemenea, prețul lor: părți suplimentare trebuie să fie reprezentate genetic, acestea consumă energie, au greutate, ocupă spațiu din organism şi aşa mai departe."* (Pfeifer *et al.*, 2011:33). În sistemele sociale, redundanța poate fi privită ca fiind o forță constantă, gravitațională, îngreunând schimbarea şi favorizând raportarea conservatoare la valorile culturii naționale şi / sau organizaționale. Astfel privind problematica redundanței, utilitatea acesteia nu se rezumă la înlocuirea datelor alterate, aşa cum o descrie Sauter[4], de exemplu, ci priveşte şi aspecte funcționale ale vieții organizaționale. Spre exemplu, remarca emeritului profesor de ştiințe politice Martin Landau (1969:350), cunoscut pentru aplicarea conceptului redundanței în studiul organizațiilor publice, conform căreia redundanța *"acceptă limitările inerente ale oricărei organizații prin tratarea fiecărei părți, indiferent de gradul de perfecțiune, precum actor de risc"*, este ilustrativă pentru posibilitatea punerii în discuție a unui management al redundanței. Eliminarea redundanței poate conduce, în înțelesul lui Landau, la apariția mesajelor false, distorsionate, înşelătoare tocmai datorită lipsei de raportare la un sistem de referință stabil. Focalizarea asupra perspectivei lui Landau este fundamentală în reproiectarea raporturilor informație-redundanță, în afara înțelesurilor circumscrise de teoria

[4] *„Pe măsură ce mediul organizațional şi decidenții se schimbă, ei vor găsi tipuri de căutare care vor produce schimbarea. Dacă aceste schimbări nu au fost anticipate, bazele de date existente în mod normal nu vor putea să îndeplinească cerințele. Oricum, puțină redundanță permite acestor căutări neanticipate să fie procesate eficient. Prin urmare, este nevoie să se gândească anticipativ atunci când se evaluează beneficiile redundanței pentru o anume aplicație."* (Sauter, 2010:80)

informației. Cu alte cuvinte, întrebându-ne asemenea profesorului american dacă am putea proiecta o organizație mai fiabilă decât oricare dintre subsistemele componente ale acesteia, vom ajunge la răspunsul pozitiv doar dacă vom înțelege că aceasta se poate realiza în condițiile unui grad ridicat de redundanță, ceea ce se poate traduce prin faptul că teoria redundanței şi teoria fiabilității sunt convergente (esența studiilor lui Landau[5]).

4. Spre un intelligence al redundanței

Dată fiind utilitatea redundanței, nu doar menținerea / cultivarea acesteia în mediul organizațional este necesară. Atâta timp cât informația şi redundanța nu trebuie priviți ca doi poli opuşi şi ireductibili, ca doi termeni contrari, ci, ambii fiind purtători de informație, în primul caz neprocesată, în cel de-al doilea procesată parțial şi superficial, se poate vorbi şi despre un *intelligence al redundanței*, în aceeaşi măsură în care expresia *intelligence al informației* este deja consacrată. Ideea nu este complet nouă sau neatacată. Privitor la *intelligence-ul informației*, simpla mențiune a faptului că vectorii informaționali pot fi purtători direcți sau indirecți de informație este suficientă pentru a înțelege că informația provenită din surse redundante nu este complet abandonată. Dar de la abandonul reducerii redundanței – direcția imprimată de managementul vizând rezultate imediate – până la utilizarea eficientă a redundanței ca informație care mai poate fi încă procesată şi interpretată este cale lungă. Utilizarea redundanței ca structură-balast, necesară reconfigurării informației redundante, se găseşte undeva între cele două extreme anterior menționate. Pentru a putea vorbi de fiabilitatea organizațională proiectată de Landau, structurile de intelligence nu trebuie să abandoneze calea exploatării maximale a redundanței (bineînțeles, în limitele consumului energetic şi financiar prevăzut).

---

[5] Manuel Angel Morales (2010) sintetiza esența studiilor lui Landau asupra rolului redundanței în organizație astfel: *„Martin Landau a fost cel care a afirmat că redundanța este un dispozitiv puternic pentru înlăturarea erorii şi pentru asigurarea fiabilității în comunicare. Uneori, simpla repetare este cel mai simplu mod de a introduce redundanța pentru asigurarea perfomanțelor solicitate. Organizațiile funcționează ca sisteme ce se auto-organizează şi tind să îşi dezvolte propriile circuite paralele: nu în ultimul rând, dintre acestea face parte şi transformarea acestor părți reziduale precum grupurile informale, în redundanțe constructive. Redundanța are mai multor funcții vitale în managementul organizațiilor. Acesta furnizează factori de siguranță, oferă răspunsuri flexibile la situații anormale şi asigură un potențial creativ pentru cei care sunt capabili să-l vadă."*

Intelligence-ul redundanței, chiar dacă nu a existat sub această denumire, a cunoscut rudimente aplicative sau a fost pus în discuție în lipsa luării în considerație a elementelor care îl propun. Spre exemplu, privitor la impunerea legii, a fost propusă o strategie de utilizare în limitele HUMINT, SIGINT, IMINT etc. bazată exclusiv pe redundanța informațională, presupunând contactarea jucătorilor cheie, constrângere / impunere în limitele mediului electronic (e-enforcement) etc. (de Bruin *et al.*, 2007:41-42). În primul caz, al culegerii datelor prin apel la sursele umane, spre exemplu, utilizarea redundanței implică un număr mare de surse, incapabile să ofere, individual, informație cu un grad ridicat de impredictibilitate (informație *hard*). Însă, informația culeasă de la acest număr mare de surse, deşi tinzând spre predictibilitate maximă (infomație *soft*), se verifică reciproc şi contribuie, ca într-un joc de puzzle, la construirea unui întreg complex. Mai mult, utilizarea redundanței în activitatea de intelligence a fost necesară deoarece nici o structură de culegere de informații nu poate fi garantată necondiționat. Culegerea nu se poate rezuma la sursele deschise, oficiale, datorită dezinformării. Mai mult, sursele tehnice nu pot fi garantate necondiționat datorită transmisiunilor „fabricate" şi bruiajelor, informațiile foto-video putând fi uşor trucate.

Invocând principiul fiabilității enunțat de Landau, informația culeasă de foarte multe surse redundante nu poate fi înlocuită nici măcar cu informația culeasă de la principala sursă purtătoare de informație *hard*. În acest caz,"*îmbinarea aceste informații fragmentate cu altă informație ce o face mai valoroasă*", ceea ce presupune necesitatea focalizării asupra acestei forme particulare de *intelligence* nu din dorința de reconstrucție organică a întregului organizațional aflat în vizor (structuri, rețele, organizații), ci din dorința de elimina posibilele „pitfalls of the defector", ca în cazul informațiilor eronate furnizate despre programul nuclear al Irakului (Massing, 2004). Avantajele unei strategii a redundanței, aşa cum reiese din studiul lui de Bruin *et al.* (2007:43-44), pot fi rezumate la: prevenirea dependenței de o sursă de informații sau doar de câteva, cuplarea diferitelor tipuri de informații (cuplarea tipurilor de tehnologii ale informației, cuplarea fluxurilor fizice cu cele financiare), strategia „*not showing your hands*" (redundanța contribuind, în acest caz, la creşterea impredictibilității, deoarece sursele, neştiind exact ce se cunoaşte şi care sunt posibilitățile de verificare, vor oferi informație puțină, dar corectă), folosirea formelor alternative de culegere de informații etc.

Limitele utilizării redundanței în culegerea şi analiza informațiilor țin mai degrabă de natura resurselor temporale şi bugetare aflate la dispoziție, decât de altă natură. De altfel, inclusiv aparatele doctrinare definesc cadrul raportării la redundanță, respectiv modul de valorificare a informațiilor redundante; spre exemplu, în limitele direcției anterior amintite, a HUMINT, manualul FM 2-22.3 (2006:4-12) stabileşte: „*Redundanța bunurilor utilizează o combinație a aceluiaşi tip de bunuri împotriva unui obiectiv de colectare de înaltă clasă. Acest lucru este vital în culegerea HUMINT, deoarece, în relațiile cu sursele umane, informațiile culese sunt de multe ori o parte dintr-o imagine de ansamblu sau sunt influențate de percepția şi preconceperea sursei. Culegerea cu acelaşi scop de la un număr diferit de furnizori de informație oferă o imagine a culegerii de date mai precisă şi este o metodă de validare a sursei.*" (FM 2-22.3: 4-12). Mai mult, utilizarea formelor alternative de intelligence în scopul compensării datelor şi verificării acestora, direcție propusă în strategia privitoare la managementul redundanței în limitele intelligence-ului nu constituie o noutate. Şi în acest caz se recomandă construirea de planuri care să asigure colectarea multiplă de date şi implementarea acestora ca soluții adecvate de raportare la un mediu informațional complex şi dinamic: "*Un plan bun de culegere va presupune asigurarea că există redundanță construită în interiorul procesului astfel încât să poată apărea încrucişări adecvate între discipline*" (Armistead, 2004). Dacă sursele tehnologice prezintă vulnerabilități şi nesiguranță în obținerea unor elemente cu grad ridicat de certitudine, mijlocul utilizat este cel al "încrucişării surselor", respectiv, a celor tehnice cu cele umane. Chiar dacă sursele umane au limitele lor determinate de subiectivism, de motivație, de gradul de instruire, etc., acestea rămân totuşi cele mai potrivite, adesea singurele care pot furniza informații valide. Culegerea de informații presupune apelul la redundanță deoarece este aproape exclus ca o singură persoană să dețină o informație în totalitate. De aceea, este necesar să fie luat în calcul un număr relativ mare de persoane pentru a întregi o informație cu grad ridicat de credibilitate şi adevăr. Acest fapt presupune însă riscuri, mai ales în domeniul informațiilor clasificate. Mai exact, cu cât se apelează la un număr mai mare de persoane în înțelegerea unei informații, cu atât creşte riscul deconspirării acesteia. De aceea, între intelligence şi redundanță există o legătură cu efecte benefice dar şi mai puțin benefice. Astfel, dacă analiza de intelligence este bine organizată şi pregătită, atunci informația şi redundanța

nu trebuie privite ca doi poli opuşi ci, în limitele logicii terţului inclus, ca simpli purtători de informaţie.

Nu trebuie făcută însă confuzie, între informaţia redundantă culeasă, indiferent de forma de intelligence, şi informaţia neclasificată, descoperită deliberat, dar supusă ulterior selecţiei, filtrării etc. (OSINT). În ciuda faptului că OSINT constituie un domeniu în continuă expansiune, fiind asimilat temeliei intelligence-ului (Mitu, Mitu, 2010:44), *intelligence-ul redundanţei* nu se fundamentează pe aprecierea faţă de sursele deschise de informaţii, ci pe culegerea de informaţie redundantă indiferent de raportarea la / situarea pe axa secret-public. Prin urmare, intelligence-ul redundanţei priveşte mai mult decât utilizarea surselor deschise, deşi OSINT oferă o cale fundamentală de punere în rol a culegerii de informaţie redundantă: înfiinţarea de reţele colaborative furnizoare de informaţii (cu grad mai ridicat sau mai scăzut de probabilitate de producere), care scutesc din efortul de energie şi resurse umane, finaciare, materiale şi de timp ale structurilor de intelligence şi care, funcţional, sunt necesare „*să integreze OSINT şi să conţină experţi atât în sectorul privat, cât şi în structurile de intelligence*" (Mitu, Mitu, 2010:49). *Intelligence-ul redundanţei* implică şi se realizează doar în paralel cu promovarea culturii de securitate, adică în paralel cu participarea societăţii în ansamblul la asigurarea securităţii.

Propunerea noastră, de a pune în discuţie posibilul *intelligence al redundanţei* nu se limitează, aşadar, la includerea în planurile de culegere şi analiză a datelor a măsurilor privitoare la fragmentele de informaţii cu un grad aparent nul de noutate (informaţii *soft*), dar care să constituie fundamentul unui puzzle refăcut, al imaginii de ansamblu a activităţii organizaţiei aflate în vizor, şi nici măcar discutarea despre utilizarea formelor alternative de intelligence sau creionarea şi implementarea unor strategii având în prim plan redundanţa. Direcţiile şi aspectele anterior amintite privesc măsuri, metode, paşi tactici, eventual strategii menite să valorifice întregul organic, reconstituit, al obiectivului de analizat. Însă măsurile, metodele şi paşii tactici se limitează la a contribui la reconstruirea în poză statică a unui întreg dinamic, la momentul analizei, în timp ce strategia priveşte luarea în calcul a întregului dinamic pe o perioadă delimitată. Strategia redundanţei în limitele intelligence-ului priveşte mai degrabă o adiţie (sau chiar o juxtapunere) de informaţii culese în limitele deja proiectatului *intelligence al informaţiei*, în timp ce compoziţia finală ar trebui să fie dinamică şi relevantă la momentul analizei şi acţiunii, nu la

momentul culegerii datelor (caz în care reducerea la minimum a intervalului temporal dintre culegerea datelor şi prelucrarea acestora/acţiunea impusă este mai degrabă o cerinţă decât o realitate). Scopul fundamental al unui *intelligence al redundanţei* nu este construirea tabloului de ansamblu (*overall picture*), ci reconfigurarea organizaţiei vizate ca organism viu şi funcţional, bazat pe o cultură organizaţională proprie. Pentru aceasta nu este suficientă proiectarea de metode şi strategii bazate pe valorificarea redundanţei, ci este necesară integrarea în limitele comportamentului comunicaţional redundant al surselor.

Propunerea de *intelligence al redundanţei* pleacă de la aserţiunea de provenienţă paloaltistă, conform căreia orice fenomen rămâne inexplicabil atâta timp cât observaţia nu include contextul în care are loc fenomenul. Chiar dacă aserţiunea are rădăcini în antropologie şi în ştiinţele comunicării, avându-l drept „părinte" pe Gregory Bateson (1979), ea este aplicabilă indiferent de domeniul de activitate. Problematica *intelligence-ului redundanţei* devine, în câmp teoretic, o problematică a raporturilor dintre modelele comunicaţionale procesuale (de sorginte matematică, cibernetică) şi modelele interacţioniste. Prin urmare, esenţa *intelligence-ului redundanţei* (proiectat în manieră interacţionistă) excede limitele intelligence-ului tradiţional (proiectat în manieră procesuală) şi se impune a fi statuată în afara acestui câmp al aplicabilităţii. Ea se originează în cerinţa firească, în termenii interacţionismului, de studiere a funcţionalităţii fără decupajul din întreg. *Pattern*-ul care face posibilă analiza întregului este comunicarea, în înţelesul dat de Bateson, în cadrul şi cu ajutorul căruia totul se modelează în baza unei semantici care excede limbajul verbal: o semantică a contextului. Propunerea de *intelligence al redundanţei* pleacă de la înţelesurile batesoniene alocate contextului şi de la rolul prefigurat: „Contextul *fixează înţelesul şi trebuie neîndoielnic să fie contextual receptării, care oferă înţelesuri pentru instrucţiuni genetice*" (Bateson, 1979:15). În acest cadru al designului, comunicarea încetează a fi privită drept schimb de informaţie, iar intelligence-ul tradiţional îşi pierde esenţa cantonându-se în limitele informativităţii. Esenţa intelligence-ului, reconfigurat, priveşte actul comunicaţional, care înseamnă mai degrabă relaţie decât informaţie: o relaţie redundantă, abundând de informaţie *soft* şi nu de informaţie *hard.* În noul cadru teoretic comunicaţional de redefinire a intelligence-ului prin raportare la redundanţă, indiferent de scopurile observaţiei, „*observatorul comportamentului uman se întoarce atunci de la*

stadiul inferențial al manifestărilor observabile ale relației" (Watzlawick *et al.*, 1967:21).

Plecând de la semnificația redundanței, aceea de surplus nejustificat de informație la transmiterea unui mesaj, sau abundența inutilă de cuvinte şi expresii la redarea unei idei sau introducerea de dispozitive suplimentare față de cel de bază, care să asigure funcționarea unui sistem în cazul în care primul sau altul din dispozitive cu aceeaşi funcție a ieşit din uz întâmplător, se pot analiza limitele sau impedimentele, precum şi beneficiile în activitatea de intelligence. Ecuația este relativ simplă în activitatea de intelligence, fiind realizată în 4 etape: culegerea de informații, verificarea acestora, transmiterea şi valorificarea de către decident. În aceste patru etape, redundanța are roluri diferite. În primele două etape, culegerea de informații şi verificarea acestora poate avea un rol benefic. Astfel, surplusul de comunicare, de expresii, şi, de ce nu, surplusul de idei, păreri despre acelaşi fenomen, vine în sprijinul analistului de intelligence pentru a ajunge la informația *soft.* Informația pentru intelligence este „un produs" rezultat din culegerea, evaluarea, analiza, integrarea şi interpretarea tuturor datelor, faptelor disponibile care privesc unul sau mai multe aspecte despre fapte, locuri, stări, care sunt importante pentru atingerea unui obiectiv. Redundanța oferă această plajă pentru specialistul în intelligence. În acelaşi timp, multitudinea de expresii, idei, păreri, etc., precum şi gradul de imprecizie sau generalizare, îngreunează procesul de analiză, de separare a aspectelor precise, reale de pure invenții sau zvonuri. Pe de altă parte, redundanța este cu siguranță un impediment serios pentru ceea ce înseamnă transmiterea informației şi evaluarea de către consumatorul de informație. Pentru a fi transmisă prin canalele de comunicații către consumator şi pentru a se putea lua decizii de către acesta, informația trebuie să fie scurtă, concisă, să aibă un grad redus de incertitudine, adică, să cuprindă ceea ce este semnificativ, esențial chiar şi să aibă sens logic, ceea ce înseamnă să se înlăture o anumită formă de redundanța. Astfel, un stil defectuos constând în abundența de cuvinte şi expresii la redarea informației poate genera luarea de către decident, care nu este specialist în intelligence, a unor decizii eronate cu consecințe nedorite.

O modalitate de „aplicare" în domeniul culegerii de informație redundantă constă în luarea în considerație a etnometodelor – proceduri utilizate de actorul social obişnuit în activitatea cotidiană, rutine, comportamente familiare, venite de la sine (*taken for granted*), înțelese de oricare dintre membrii societății, fără însă a fi conştientizat şi sensul acțiunii. Această cale a etnometodelor, identificabile prin inducerea unor

situații diferite de cotidian, a fost propusă de Garfinkel (1967) şi denumită etnometodologie. Constatând că sociologia clasică – unul dintre pilonii intelligence-ului tradițional – consideră rutina ca fiind o condiție necesară a acțiunii raționale şi alocă raționalitate actelor rutiniere, Garfinkel punctează incongruența rutină – raționalitate şi propune studierea (nu neapărat în baza unei ipoteze de lucru preliminare) a situațiilor imediate, observabile şi descriptibile, atâta timp cât interacțiunea are loc la nivelurile elementare, fiind o interacțiune fundamentată intersubiectiv şi furnizoare de informație privitoare la sensuri. În baza acestei descrieri, realitatea socială este reconstruită continuu, iar informația *hard* îşi pierde actualitatea şi validitatea odată cu reconstruirea realității sociale. În manieră similară, putem constata că redundanța este privită, actualmente, mai degrabă ca structură balast, raționalizată, posibilă de redus într-un diferențiator care să prelucreze minimum de informație nouă necesară. Din nefericire, redundanța – asociată rutinei, nu este superpozabilă fundamentării raționale, iar culegerea de informații rutiniere nu trebuie continuată de trierea noului, ci de construirea întregului prin luarea în considerație o singură dată, ca termen în puzzle-ul de construit. Etnometodologia poate furniza date importante despre organizarea observației, focalizată pe limbaj, care posedă trei proprietăți fundamentale: indexicalitate (*indexicality*), reflexivitate (*reflexivity*) şi descriptibilitate (*accountability*), furnizând informații despre moduri de utilizare mai degrabă decât despre sensuri asociate, despre integrarea socială a alocării de sens şi construirea, în baza acesteia, a ordinii sociale aferente, respectiv despre modalitatea de organizare a faptelor descriptibile de limbaj (Garfinkel, Sacks, 1986:160). Toate aceste proprietăți amintesc de necesitatea luării în considerare a redundanței, capabilă să conducă la construirea de grile interpretative personale pertinente. Esența informației este păstrată tocmai prin redundanță, iar interpretarea devine mult mai funcțională: „*Procedeele interpretative sugerează informațiile ca fiind cunoştințe distribuite social, care-i permit actorului să asocieze reguli informative generale cu scene de interacțiune trăite. Procedeele interpretative şi regulile de suprafață (normative) furnizează actorului o structură cu ajutorul căreia îşi poate compartimenta mediul în domenii de semnificații*" (Cicourel, *apud* Lallement, 1998:234). În lipsa redundanței, domeniile de semnificații devin simple deziderate, procesul interpretativ fiind îngreunat sau chiar suspendat.

5. Concluzii

În esența sa, conceptul de *intelligence al redundanței* este unul paradoxal şi departe de suscitarea interesului, legat de judecățile simplificatoare asociate redundanței: banalizare, informație de mâna a doua etc. Spre deosebire de primul termen al expresiei, *intelligence*, insuficient conceptualizat şi insuficient recunoscut, dar păstrând un potențial de atractivitate ridicat tocmai datorită faptului că persistă nota de empirism, constructul întreg pierde din strălucirea interesului, dar câştigă în planul aplicabilității şi utilității. Informația brută, ca măsură a impredictibilității semnalului emis, este insuficientă în proiectarea cunoaşterii prin această formă specială, a intelligence-ului. Rămâne doar să eliminăm înțelesurile generalizatoare, cum ar fi cel de suprainformare – supraîncărcare a canalelor de comunicare cu informație inutilă, asociate unui concept precum cel de redundanță care, în profunzimea înțelesurilor, presupune deschidere, nou, continuitate şi contextualizare. Redundanța se poate constitui într-o cale care să asigure funcționalitatea şi vitalitatea intelligence-ului, în paralel cu punerea bazelor unei culturi a securității.

Bibliografie

1. ARMISTEAD, Leigh (ed.) (2004). *Information Operations. Warfare and the Hard Reality of Soft Power.* A textbook produced in conjunction with the Joint Forces Staff College and zhe National Security Agency. Dulles, Virginia: Potomac Books.

2. BATESON, Gregory. (1979). *Mind and Nature: A Necessary Unity.* London: WilwoodHouse Ltd.

3. de BRUIN, Hans, ten HEUVELHOF, Ernst, KOOPMANS, Marieke. (2007). *Law Enforcement: The Game between Inspectors and Inspectees.* Boca Baton, Florida: Universal Publishers.

4. GARFINKEL, Harold. (1967). *Studies in Ethnomethodology.* Englewood Cliffs, NJ: Prentice-Hall.

5. GARFINKEL, Harold, SACKS, Harry. (1986). On formal structures of practical actions. În Harold Garfinkel (ed.). *Ethnomethodological Studies of Work.* London, New York: Routledge & Kegan Paul.

6. HARASZTI, Tegze P. (2002). *CMOS memory circuits*. New York: Kluwer Academic Publisher.

7. LALLEMENT, Michel. (1998). *Istoria ideilor sociologice. Vol.II. DE la Parsons la contemporani.* Bucureşti: Antet.

8. LANDAU, Martin. (1969). Redundancy, Rationality, and the Problem of Dupplication and Overlap. *Public Administration Review.* 29 (4): 346-358.

9. MARIAN, Liliana. (2008). *Etica profesională şi bazele comunicării. Ciclu de prelegeri.* Chişinău: Universitatea Tehnică a Moldovei.

10. MASSING, Michael. (2004). *Bnow they tell us: the American Press and Iraq.* New York: new York Review Books.

11. MITU, Teodor, MITU, Daniela. (2010). OSINT – la granița dintre secret şi public. *Revista Română de Studii de Intelligence*. 4: 42-52.

12. MORALES, Manuel Angel. (2010). The Management of Redundancy, Duplication and Overlap. [online]. *Intelligence Forecasting, Corp.* URL: http://intelligenceforecasting.com/english/articles/2010/The%20Management%20of%20Redundancy.pdf. [accesat în octombrie 2011].

13. PFEIFER, Rolf, BONGARD, Josh, BERRY, Don. (2011). *Designing Intelligence. Why Brains Aren't Enough.* Anthology. Munchen: GRIN Verlag.

14. PHILIPPOPOULOS-MIHALOPOULOS, Andreas. (2004) Boundaries of Exclusion Past: The Memory of Waste. În Ronnie Lippens (ed.). *Imaginary Boundaries of Justice. Social and Legal Justice across Disciplines.* Oxford, Portland, Orlando: Hart Publishing. 69-96.

15. SAUTER, Vicky L. (2010). *Decision Support Systems for Business Intelligence.* Hoboken, NJ: John Wiley & Sons, Inc.

16. SCHMIDHUBER, Jürgen. (2000). Neural Predictors for Detecting and Removing Redundant Information. În Helge Ritter, Holk Cruse, Jeffrey Dean (eds.) *Preoperational intelligence: Adaptive Behavior and Itelligent Systems wihout Symbols and Logic.* Volume 2. Dordrecht: Kluwer Academic Publishers.

17. SFEZ, Lucien. (2002). *Comunicarea*. Iaşi: Institutul European.

18. WATZLAWICK, Paul, BEAVIN BAVELAS, Janet, JACKSON, Don. (1967). *Pragmatics of Human Communication: A Study of Interactional Patterns, Pathologies, and Paradoxes.* New York: W.W. Norton & Company, Inc.

19. ***. (2006). *Human Intelligence Collector Operations. FM 2-22.3 (FM 34-52).* Washington DC: Headquarters, Department of the Army.

Evaluarea implicării NATO în Afganistan: o provocare pentru activitatea de intelligence strategic a comunității academice

Conf. univ. dr. Florin DIACONU
Institutul Diplomatic Român
e-mail: **florin.diaconu@fspub.unibuc.ro**

Abstract

Ten years ago, only a few days after the terrorist attacks which hit US on September 11, 2001, small units of the US Special Forces, plus several CIA teams were already operating in Afghanistan, starting – and later on boosting and coordinating – a quick and decisive campaign which, in less than three months, led to the complete collapse of the Taliban regime. At this very moment, more than ten years after the beginning of the Global War on Terror (GWOT), United States of America, together with the other NATO member states and other allies and partners are deeply involved, at political and military level, in Afghanistan. This massive involvement generates both a significant number of successes and a complex set of problems and worries. The study evaluates the way in which civilian academic think-tanks (mainly universities, faculties and research institutes) can offer the decision-makers (including here the Romanian ones) final product belonging, in a way or another to the category we usually call strategic intelligence. Such intellectual products, if and when are available and are really sound evaluations, can be the solid foundation used to successfully stage an analytical and predictive effort, potentially decisive for both policy making and implementing – at different levels – policies able to cope with the very complex and very fluid situation in Afghanistan.

Keywords: Strategic intelligence; Afghanistan; NATO, USA, Romania, grand (superior) strategy, victory (with its several meanings); the Talibans; Al Qaeda.

Introducere: câteva precizări conceptuale absolut necesare

În acest studiu[1] voi folosi conceptul de *strategic intelligence* pentru a desemna un tip cu totul special de proces (şi de produs) intelectual: unul care, utilizând (respectiv identificând, analizând şi asamblând) în special

[1] Punctele de vedere exprimate în continuare nu angajează, în nici un fel, nici Universitatea din Bucureşti, nici Institutul Diplomatic Român sau MAE. Ele reprezintă opinii profesionale pentru care responsabilitatea integrală revine exclusiv autorului.

elemente de informație deschisă, să fundamenteze în chip cât mai solid (oferind, la nevoie, inclusiv mai multe variante alternative de acțiune, împreună cu o analiză detaliată cost / rezultate) activitatea şi hotărârile decidenților politici (inclusiv cei din România) în contextul general al efortului de mare amploare, de intensitate cel mai adesea variabilă şi de foarte lungă durată pe care îl numim în mod uzual Războiul Global Contra Terorismului (Global War On Terror – GWOT). E nevoie, cred, să precizez încă din acest moment că tipul de produs intelectual pe care îl numesc aici *strategic intelligence* nu întemeiază *orice* tip de acțiune a decidenților, ci doar activitățile şi hotărârile luate în interiorul sistemului de referință pe care îl numim, prin raportare la solida tradiție anglo-saxonă, folosind conceptul de *mare strategie*. Readuc aminte onoratului auditoriu, cât şi viitorilor cititori ai acestui studiu, că – în viziunea unui autor clasic şi extrem de influent, de tipul lui B. H. Liddell Hart – stratul realității politice pe care îl numim mare strategie (grand strategy sau superior strategy) este substanțial diferit de acela al strategiei militare. Mai precis, dacă *strategia militară* – sau strategia pură – este „arta comandantului de oşti" şi are ca element principal, de natură să pregătească (sau chiar să garanteze) succesul „în primul rând... calculul şi coordonarea judicioasă a scopului cu mijloacele"[2], *marea strategie* – respectiv acel strat al realității politice care trebuie alimentat în chip constant (sau măcar în momente-cheie) cu produse din categoria pe care am numit-o *strategic intelligence* – este „practic sinonimă cu politica militară, care dirijează conducerea războiului, dar distinctă de politica fundamentală care îi guvernează scopul[3]". Acelaşi Liddell Hart preciza şi că „rolul marii strategii sau al strategiei superioare constă în a coordona şi îndrepta toate resursele națiunii sau ale unui grup de națiuni spre atingerea scopului politic al războiului, scopului definit de politica fundamentală", în sensul în care „marea strategie trebuie să evidențieze şi să mobilizeze resursele economice şi umane ale națiunii pentru a susține efortul militar. La fel stau lucrurile şi cu resursele morale, deoarece ridicarea moralului poporului este adeseori tot atât de importantă ca şi a poseda cele mai concrete forme ale puterii[4]".

Am simțit nevoia să fac, de la bun început, această precizare conceptuală din motive, cred, lesne de înțeles. Nu este deloc clar – atunci când urmărim literatura de specialitate cu toate nuanțele şi detaliile sale –

[2] B. H. LIDDELL HART, *Strategia: Acțiunile indirecte*, Editura Militară, Bucureşti, 1973, p. 335.
[3] *Ibidem*, p. 334.
[4] *Ibidem*, p. 334.

care ar putea fi încărcătura *exactă* de sens a termenului intelligence. Destule dintre definițiile cu care operăm în mod curent rămân, de fapt, departe de a fi realmente precise. Aşa de exemplu, definiția generală, ne spune că intelligence înseamnă „informație despre o entitate străină", dar „şi structuri / agenții care se îndeletnicesc cu colectarea de asemenea informații", precum şi că acelaşi termen desemnează – sau este „intim" legat de „ciclul de intelligence", un proces în mai multe etape prin care se ajunge de la informația brută la accesul decidenților la produsul intens prelucrat al muncii de intelligence (pasajul la care fac trimitere arată în original astel: „Intelligence is information concerning a foreign entity, usually (although not always) an adversary, as well as agencies concerned with collection of such information. It is intimately tied with the intelligence cycle, a process whereby raw information is acquired, converted into intelligence, and disseminated to the appropriate consumers[5]"). La fel, nu e deloc clar nici ce denumim prin intermediul conceptului strategie / strategic. Şi, în mod predictibil, din însumarea a două concepte care nu au deloc conținuturi foarte rigide / pe de-a-ntregul stabilizate / foarte bine – şi definitiv – precizate, nu se poate naşte, în mod firesc, decât o zonă de incertitudine şi mai pronunțată, care ar fi complet contraproductivă, cred, în termenii oricărei preocupări pentru un nivel acceptabil de eficiență a politicului[6].

O listă de chestiuni realmente importante pentru efortul de *strategic intelligence*

Cel puțin două straturi ale realității politice cu relevanță geostrategică fac obiectul efortului de *intelligence strategic*, atunci când vorbim despre implicarea NATO (trecută, prezentă şi viitoare) în

[5] K. LEE LERNER, BRENDA WILMOTH LERNER (editors), *Encyclopedia of Espionage, Intelligence, and Security*, volume 2 (F-Q), Thomson Gale, Detroit, New York, San Diego, San Francisco, Cleveland, 2004, p. 117.

[6] Există numeroşi autori care discută în termeni extrem de interesanți chestiunea eficienței generale a politicului. Unul dintre aceştia este părintele şcolii realiste clasice, Hans J. Morgenthau, care afirma – într-unul din principiile realismului politic – nu numai că „realismul politic este conştient de semnificația morală a acțiunii politice", ci şi că acelaşi realism „este conştient şi de inevitabila tensiune între cerințele morale şi necesitățile acțiunii politice de succes", nefiind deloc „dispus să mascheze şi să elimine această tensiune" – pentru toate acestea vezi Hans J. MORGENTHAU, *Politica între națiuni: Lupta pentru putere şi lupta pentru pace*, Editura Polirom, Iaşi, 2007, p. 51.

Afganistan. Pe de o parte putem lua în calcul *maniera în care Alianța interacționează, la fața locului, cu diverşi actori politici prezenți, într-un fel sau altul, pe teatrul de operațiuni sau în vecinătatea acestuia*. Din această perspectivă există, în mod limpede, cel puțin trei tipuri mari de interacțiuni lesne decelabile:

- relații de tip conflictual, dominate de un nivel înalt al interacțiunii directe negative (vezi, de exemplu, relațiile între segmentele diverse din cadrul ISAF, pe de o parte şi tandemul talibani / Al Qaeda);
- relații de cooperare, dominate de un nivel înalt al interacțiunii pozitive (vezi, de exemplu, relațiile între ISAF / NATO, pe de o parte, şi autoritățile centrale de la Kabul, care sunt – dincolo de sistemul axiologic pe care îl reprezintă – unul dintre beneficiarii majori ai prezenței NATO în regiune);
- relații dominate de un nivel scăzut al interacțiunii directe pozitive.

Dacă luăm în calcul, dintr-o altă perspectivă (complementară cu cea deja prezentată), tipul interacțiunilor pe care le regăsim, între NATO / ISAF şi alți actori de diverse tipuri în zona Afganistanului (această arie geografică fiind privită fie în sens restrâns, fie în sens ceva mai larg), operăm cu cel puțin două tipuri distincte de situații:

- acelea în care agenda declarațiilor politice (indiferent de nivelul sau rangul celor care le fac) se suprapune peste / coincide cu aceea a acțiunilor practice (ceea ce este măcar cazul relațiilor conflictuale între prezența ISAF / NATO pe de o parte şi tandemul talibani / al Qaeda);
- şi acela în care declarațiile politice (în special cele oficiale / la nivel guvernamental) par să indice un anume tip de realitate, iar acțiunile practice cu relevanță geostrategică par să indice *un cu totul alt* tip de realitate (adesea în coliziune directă – sau cel puțin aproape directă – cu stratul deja amintit al declarațiilor politice oficiale făcute la nivel înalt sau foarte înalt). Este, de exemplu, cazul relației extrem de complexe a NATO (de fapt, în special a SUA) cu Pakistanul. Mai multe segmente ale relativ recentului episod constituit de raidul întreprins de forțele speciale americane împotriva ascunzătorii în care se afla Osama bin Laden, ca şi câteva dintre episoadele conexe (vezi, de exemplu, serioasa cantitate de relatări de presă de foarte bună calitate profesională cu privire la ceea ce s-a întâmplat cu rămăşițele elicopterului *stealth* care s-a prăbuşit cu ocazia deja amintitului raid) pun în chip serios sub semnul întrebării cooperarea Pakistanului cu Occidentul / NATO / SUA.

Un al doilea strat al realității cu relevanță geostrategică serioasă, despre care de asemenea trebuie să discutăm atunci când evaluăm prezența / implicarea NATO în Afganistan este acela constituit de *relațiile din interiorul NATO* (strat substanțial diferit de cel deja trecut în revistă, în chip sumar, şi care cuprindea relațiile NATO cu actori din exteriorul Alianței). În legătură cu pachetul de chestiuni legate de ceea ce se întâmplă, legat de Afganistan, în interiorul NATO, putem (sau, de fapt, *trebuie*) să luăm în calcul cel puțin trei elemente / segmente / straturi distincte:

- segmentul *relațiilor de cooperare* (reflectat inclusiv în misiuni comune de diverse tipuri);
- segmentul *divergențelor* (care merg de la simple – şi oarecum benigne – diferențe de opinii privind evaluarea unor momente şi trenduri şi până la nivelul unor diferențe majore legate de maniera în care elitele decidente din țările membre ale NATO se raportează la ceea ce se întâmplă în Afganistan, ca şi la miza geostrategică pe termen mediu şi lung constituită de confruntarea din Afganistan;
- segmentul raporturilor dinamice dintre acțiunile NATO ca entitate (sau a țărilor membre ale Alianței) şi documentele oficiale ale Alianței (ca ipoteză de lucru, cu cel puțin două tipuri de corelații posibile: în unele cazuri am putea constata că experiența istorică semnificativă a elementelor care compun segmentul GWOT purtat în Afganistan este corect înțeleasă şi transferată / înglobată în documente oficiale ale NATO care sunt de natură să consolideze, într-un fel sau altul, şansele Alianței de a acționa eficient; în alte cazuri, dimpotrivă, am putea avea de-a face cu situații în care tonalitatea şi conținutul unor documente / formulări ale diferitelor segmente instituționale ale Alianței pare să nu înglobeze suficient din experiența practică a segmentului GWOT derulat în ultimii 10 ani în Afganistan.

Dintre aceste trei straturi, acela care îmi atrage în mod constant atenția este acela al *divergențelor de opinii / percepții din interiorul NATO cu privire la importanța relativă şi / sau absolută a evoluțiilor din Afganistan, divergențe care explică dramaticele contraste pe care le constatăm adesea între rangul real al puterii unor țări membre ale Alianței şi ponderea implicării lor în Afganistan*. Pentru a înțelege mai bine această problemă, este suficient să citim, cu atenție – şi în corelație cu orice sursă de bună calitate care ne oferă date referitoare la mărimea populației şi la puterea economică

(exprimată în cifre sintetice semnificative, de tipul PIB / GDP) – datele referitoare la mărimea contingentelor naționale care compun ISAF. În tabelul care urmează (vezi Tabelul 1: Date principale referitoare la câteva contingente naționale şi / sau regionale din cadrul ISAF, corelate cu date economice şi demografice semnificative pentru puterea națională a statelor (sau puterea totală / însumată a grupurilor de state) luate în calcul), am folosit cifre preluate din documente oficiale ale ISAF, făcute publice la 13 iulie 2007[7] şi respectiv 18 octombrie 2011[8] , iar pentru datele statistice relevante în ceea ce priveşte potențialul demografic şi militar al țărilor (fie ele membre ale NATO sau nu) cu contingente în cadrul ISAF am utilizat date din volumul anual intitulat *Military Balance*, editat de către Institutul Internațional pentru Studii Strategice de la Londra (ediția pentru 2005-2006, publicată în octombrie 2005[9]).

Oricât de incomplete / fragmentare ar fi, datele utilizate aici sunt reale şi, în plus, sunt semnificative, precum şi absolut suficiente pentru a formula *nişte întrebări*. Desigur, percepția curentă este că „fişa postului" analistului de informații (acela care este implicat *inclusiv* în activitatea de *strategic intelligence*), fie el civil sau militar, are ca element principal obligația *profesională* de a formula răspunsuri, iar nu capacitatea de a pune întrebări (fiindcă, nu-i aşa, decidenții de rang înalt şi mijlociu sunt aceia care pun în mod natural întrebări, iar analiştii sunt cei care răspund la ele). Dincolo de această percepție curentă – cu sau fără o serioasă legătură cu realitatea – merită făcută următoarea observație: în orice societate aflată realmente în stare de funcționare, cei care cu adevărat dau răspunsuri cu *consecințe perene* sunt decidenții (în sensul în care diverse segmente ale realității generează / conțin probleme, iar decidenții *trebuie* să rezolve, într-un fel sau altul, respectivele probleme).

---

[7] International Security Assistance Force (ISAF), *Troop Contributing Nations (TCN)*, current as of 13 July 2007, document de pe site-ul ISAF (www.isaf.nato.int) care preciza că mărimea efectivelor întabelate „nu reflectă numărul exact al militarilor aflați în misiune în vreun moment dat".

[8] International Security Assistance Force (ISAF), Troop Contributing Nations (TCN), 18 October 2011, document de pe site-ul ISAF care precizează că „numărul militarilor trebuie interpretat ca fiind orientativ, întrucât el se schimbă zilnic".

[9] The International Institute for Strategic Studies, *The Military Balance 2005-2006*, Routledge Taylor & Francis Group, October 2005, London, pp. 18-106, 266.

TABEL 1: Date principale referitoare la câteva contingente naționale şi / sau regionale din cadrul ISAF, corelate cu date economice şi demografice semnificative pentru puterea națională a statelor (sau puterea totală / însumată a grupurilor de state) luate în calcul

Nr.	Numele statului (sau ce reprezintă actorul evaluat)	Mărimea contingentului militar în cadrul ISAF, în iulie-oct. 2007	Mărimea contingentului militar în cadrul ISAF, în octombrie 2011	Populația totală (milioane oameni) în 2004	PIB (GDP), pentru anul 2004 (miliarde USD)
1	SUA	14.750	90.000	293	11.700
2	Germania	3.000	5.000	82,43	2.670
3	Marea Britanie	6.500	9.500	60,44	2.100
4	Franța	800	3.932	60,65	2.000
5	Italia	2.500	3.952	58,10	1.660
6	Spania	650	1.526	40,34	986
7	Primele cinci mari puteri europene ale NATO luate la un loc (5 E M)	13.450	23.910	301,96	9.416
8	SUA / 5 E M	14,7 / 13,4 (110%)	90 / 23,9 (aprox. 370 %)	97-98%	112-114 %
9	România	500	1.873	22,32	72,1
10	Bulgaria	400	597	7,45	23,8
11	Ungaria	180	415	10,00	99,5
12	Cehia	220	623	10,24	106
13	Slovacia	60	309	5,43	41.0
14	Cinci puteri mici şi / sau mijlocii din Europa Centrală şi de Est luate la un loc (5 E m)	1.360	3.817	55,44	342,40
15	Australia	700	1.550	20,09	598
16	Canada	2.500	529	32,50	980

17	**Două puteri mijlocii extraeuropene luate la un loc (2 nonE)**	**3.200**	**2.079**	**52,59**	**1.578**
18	**Belgia**	**295**	**520**	**10,36**	**282**
19	**Danemarca**	**400**	**750**	**5,43**	**239**
20	**Olanda**	**1.300**	**183**	**16,40**	**575**
21	**Norvegia**	**500**	**429**	**4,59**	**243**
22	**Portugalia**	**150**	**140**	**10,56**	**166**
23	**Cinci mici puteri vest-europene din NATO luate la un loc (5VE m)**	**2.645**	**2.022**	**35,34**	**1.505**
24	**Estonia**	**110**	**159**	**1,33**	**10,9**
25	**Letonia**	**35**	**174**	**2,29**	**13**
26	**Lituania**	**130**	**236**	**3,59**	**22,1**
27	**Țările baltice, luate la un loc (B 3)**	**275**	**569**	**7,22**	**46,0**

O tare spinoasă întrebare: cât de consistentă e voința politică a NATO legată de Afganistan?

Pentru a răspunde la o astfel de întrebare (sau măcar pentru a o propune ca element central – sau măcar suficient de important – al agendei de preocupări a decidenților), este suficient, cred, să citim cu o anumită atenție tabelul anterior. El ne spune, într-o manieră *aproape* incontestabilă, următoarele:

- implicarea SUA este, în mod clar, *net superioară* celei a restului statelor cu contingente în cadrul ISAF. Cele cinci mari puteri membre NATO din Europa Occidentală (respectiv Germania, Marea Britanie, Franța, Italia şi Spania) au, împreună, un potențial demografic şi economic vădit comparabil cu acela al SUA. Dar, în ciuda potențialului extrem de consistent de *putere*[10], ele au acum în Afganistan un număr total de *doar* aproximativ

[10] În acest studiu conceptul de putere este folosit în cheie teoretică realistă, într-o manieră deliberat compatibilă cu definiția dată de Morgenthau, părintele şcolii realiste clasice. Acesta afirma că puterea înseamnă, în orice context politic (deci *şi* în relațiile internaționale), „controlul omului asupra minții şi acțiunilor altor oameni" – vezi HANS J. MORGENTHAU, *op. cit*., p. 68.

24.000 de militari, adică o fracțiune mai mult decât modestă din numărul total de 90.000 de militari – cât au SUA pe acelaşi teatru de operațiuni;

- dar nu vorbim *doar* despre un important contrast între o *masivă* prezență americană şi o *modestă* prezență europeană în cadrul misiunii NATO din Afganistan, ci şi despre contraste *importante* – sau falii, dacă preferăm acest termen – *în interiorul efortului făcut de statele europene membre ale NATO*. Cele trei minuscule republici baltice, cu doar în jur de 7 milioane locuitori (pe cifrele valabile pentru anul 2004) au acum în Afganistan 569 de militari, ceea ce înseamnă în jur de 81 de militari pentru fiecare milion de locuitori). Şi aceasta în timp ce, de exemplu, Germania – țară care are acum peste 80 de milioane de oameni, are pe acelaşi teatru de operațiuni militare doar în jur de 5.000 de militari (respectiv *doar* în jur de 62 de militari pentru fiecare milion de locuitori);

- astfel de diferențe – de fapt de contraste care măsoară voințe politice *extrem de diferit* profilate ale statelor europene membre ale NATO – sunt şi mai mari dacă luăm în calcul componenta *economică* a puterii actorilor politici de tip statal despre care discutăm. Pe datele din 2004, produsul intern brut (PIB) însumat al celor trei state baltice este de doar 46 de miliarde de USD (ceea ce înseamnă câte un militar pentru fiecare 80,843 milioane USD din PIB-ul însumat al celor trei țări). Dacă un stat realmente puternic, de tipul Germaniei, de exemplu, ar trimite în Afganistan câte un militar pentru fiecare 80,843 milioane USD din uriaşul său PIB, de 2.670 miliarde USD (vezi cifrele din Tabelul 1, valabile pentru 2004), ar însemna că la eforturile contra talibanilor şi ale al Qaeda ar trebui să participe nu mai puțin de 33.027 militari germani, adică de peste 6 ori şi jumătate mai mulți decât are acum Berlinul pe teatrul de operațiuni afgan;

- puteri europene mijlocii (din punct de vedere al potențialului demografic) sau mici (dacă luăm în calcul puterea economică măsurată de indicatorul economic numit Produs Intern Brut / PIB), de tipul *României*, fac şi ele un *efort disproporționat de mare în raport cu acela făcut acum în Afganistan de unii dintre marii actori de tip statal din zona vest-europeană a NATO*. Mai precis, *România* are acum în Afganistan, conform datelor *oficiale* ale ISAF, un efectiv total de 1.873 de militari. Aceasta înseamnă, raportat la resursele demografice totale, câte un militar care serveşte interesul național (privit aici ca *parte* integrantă a intereselor geostrategice ale NATO) în Afganistan, pentru fiecare 11.917 locuitori ai României. Din nou, *dacă* marile puteri din zona vest-europeană a NATO ar face un efort de aceeaşi intensitate, un stat ca Germania, de exemplu, ar trebui să aibă în Afganistan nu 5.000,

ci în jur de 6.917 militari. La fel, un stat cu ambiții, tradiții şi potențial de mare putere cum este Franța ar trebui să aibă pe acelaşi teatru de operațiuni militare în jur de 5.089 militari, adică cu mai bine de 25 % mai mulți decât cei sub 4.000 pe care îi are acum în Afganistan;

- în sfârşit, dincolo de astfel de calcule – care măsoară, de altfel, *foarte* exact faptul că unele state europene fac eforturi *mari* (iau uneori chiar *foarte* mari) în raport cu resursele de putere pe care le au, în timp ce alte state fac eforturi semnificativ mai mici, proporțional – putem privi cu atenție şi *dinamica generală* a efectivelor contingentelor naționale care compun prezența NATO pe teatrul de operațiuni din Afganistan. În intervalul ultimilor patru ani, efectivele *americane* din cadrul ISAF au crescut de la nici 15.000 de militari la 90.000 de oameni (deci de 6 ori). Cele *româneşti* au crescut de la 500 de militari la 1.873 de oameni (de 3,75 ori). Cele ale *Cehiei* au crescut, şi ele, de la 220 la peste 600 de militari (deci de aproape trei ori). Cele *slovace* au crescut de la 60 la peste 300 de oameni (deci de peste 5 ori). Cele ale *Letoniei* au crescut, şi ele, de la 35 la 174 militari (deci de aproape 5 ori). Există însă şi creşteri mult mai modeste: prezența militară *bulgară* în Afganistan, în cadrul ISAF, de exemplu, a crescut doar de la 400 la ceva mai puțin de 600 de oameni, deci cu mai puțin de 50 %; la fel, *estonienii* şi-au amplificat prezența de la 110 la 159 militari (din nou cu ceva mai puțin de 50 %). Dar cel mai *îngrijorător* aspect este cel constituit de faptul că *unele* state din cadrul NATO au decis deja – *indiferent* de motivele care le-au îndemnat şi le-au determinat să facă aceasta – să-şi reducă masiv prezența. Dintre statele vest-europene, cazul cel mai semnificativ este, fără nici o îndoială, acela al *Olandei*: 1.300 de oameni în 2007 şi doar 183 astăzi (respectiv o scădere de peste 7 ori în patru ani!). La fel au procedat şi actori statali noneuropeni: *Canada*, de exemplu, şi-a redus, în ultimii patru ani, efectivele din Afganistan de aproape 5 ori, de la 2.500 la cu puțin peste 500 de militari.

Toate aceste cifre pun în fața celui implicat într-un efort *analitic* făcut în domeniul de *strategic intelligence* o sarcină intelectuală *interesantă*, dar şi *extrem* de *dificilă*: aceea de a prospecta istoria (fie ea mai recentă sau, dimpotrivă, episoade plasate ceva mai departe în timp) pentru a înțelege mai bine ce şanse are, în general, o alianță politico-militară (în cazul concret despre care discutăm este vorba, desigur, despre NATO) să-şi îndeplinească *în mod eficient* şi *în timp util* obiective *importante* în planul *marii strategii*, atâta timp cât entitățile statale componente *nu dau dovadă de o voință politică realmente constantă, puternică şi mai ales omogenă*.

Alte două teme importante pentru munca de *strategic intelligence*: scurte remarci finale

În condițiile descrise mai sus – cu suficient de multe date, cred – rămâne ca persoanele, grupurile şi instituțiile (fie ele civile sau militare) implicate în efortul de *strategic intelligence*, ca şi decidenții în mâna cărora ajung analizele şi estimările cercetătorilor să-şi concentreze *măcar* o parte din atenție înspre arii tematice cu un *numitor comun* clar: încercarea de a înlocui, în cazul NATO, voința politică realmente puternică, omogenă şi constantă (voință politică despre care am afirmat deja că *nu* funcționează bine) cu formule *eficiente* de substituție.

Dintre aceste formule de substituție listez aici, *fără* a intra în amănunte, două despre care cred că sunt nu numai *teoretic* interesante, ci şi *practic* aplicabile / utilizabile:

- încercarea de *a augmenta puterea NATO* prin identificarea şi mobilizarea de *aliați locali / regionali*, fie aceştia conjuncturali sau nu;
- şi încercarea de a aplica, în raport cu adversarii NATO prezenți în contextul concret din Afganistan, dictonul latin *divide et impera* (respectiv prospectarea măsurii în care pot fi *exploatate* sau chiar *create* fisuri care să segmenteze, de exemplu, blocul etnic pashtun, cel care susține insurgența talibană, sau falii care să-i separe tot mai mult pe talibani şi pe cei din al Qaeda).

Bibliografie

1. International Security Assistance Force (ISAF), *Troop Contributing Nations (TCN)*, current as of 13 July 2007, la adresa de Internet www.isaf.nato.int

2. International Security Assistance Force (ISAF), *Troop Contributing Nations (TCN)*, 18 October 2011, la adresa de Internet www.isaf.nato.int

3. K. LEE LERNER, BRENDA WILMOTH LERNER (editors), *Encyclopedia of Espionage, Intelligence, and Security*, volume 2 (F-Q), Thomson Gale, Detroit, New York, San Diego, San Francisco, Cleveland, 2004.

4. B. H. LIDDELL HART, *Strategia: Acțiunile indirecte*, Editura Militară, Bucureşti, 1973.

5. HANS J. MORGENTHAU, *Politica între națiuni: Lupta pentru putere şi lupta pentru pace*, Editura Polirom, Iaşi, 2007.

6. The International Institute for Strategic Studies, *The Military Balance 2005-2006*, Routledge Taylor & Francis Group, October 2005, London.

A missing link: Education for security dimension of the corporate social responsibility[1]

Assoc. prof. Ph. D. Ella CIUPERCĂ
„Mihai Viteazul", National Intelligence Academy
e-mail: **ellaciuperca@yahoo.com**

Abstract

The continuous change of our world determined the reduction of the role of the state in economy. Assuming that the survival and welfare of the community greatly depend of the involvement of every economic company in corporate social responsibility (CSR) actions, in this paper I will propose and argue for a new adaptive strategy to the contemporary social conditions: the inclusion of security issues in the field of CSR actions undertaken by firms. An important step in this direction is to change their own behaviors and attitudes by generalized hiring of security experts and by creating a security culture among the employees.

Keywords: corporate social responsibility, intelligence culture, security culture, economic performance, community welfare

1. Introduction

Corporate Social Responsibility (CSR) has become a priority in the contemporary world, primarily because of the way society has evolved. The present globalization implies the interdependence of individuals, communities, and ideas. All these changes had as a natural consequence the reduction of the role of the state in economy, trade liberalization, international financial transactions, and the emergence of transnational corporations.

In this context, the social involvement of economic corporate is an effective way to compensate the logistic inability of the state to solve the problems of society. The emergence of the notion of "corporate social responsibility" was facilitated by the social pact between the community

[1] This work was supported by CNCSIS-UEFISCSU, project number PN II-RU 64/2010

and businesses, based mainly on mutual trust, cooperation and mutual dependency (Wartick & Cochran, 1985). Therefore, according to modern approaches the company is equated with a citizen. The same way a citizen has his rights and obligations, each company acquires corporate citizenship and therefore has, in turn, benefits and responsibilities.

Although I am not in a complete agreement with the idea that the economic environment has the capacity to solve the major social problems of humanity as poverty, conflicts, population growth and so on, I agree with the contemporary idea that firms have significant human and material resources that should be directed to the community and used by its members.

2. Corporate social responsibility: a definition

Social responsibility is a relatively recent issue studied by social sciences, but the interest in this subject is growing. However, to date there is still no agreement on what constitutes CSR. The literature highlighs sometimes dissonant positions among specialists.

Broadly speaking, CSR objective is to solve social problems, i.e. those situations which represent a gap between reality and an imagined ideal society (Pounds, 1969). According to G. Hardin (1968), social problems are caused by selfish behavior of individuals, which is repeated on the long term, and such behavioures create problems for the community (community tragedy).

The European Commission has tried to answer the question "What is CSR?". Using the answers to a questionnaire applied to a group which consists of over 250 associations, organizations and private companies, unions and civil society, they conclude that CSR is the way a company operates within its legal system and regulations established by the society in accordance with universal human rights. A. Carroll (1979) argues that corporate social responsibility is measured by the degree to which management decisions conform to the needs of the community in which they operate.

In a publication of the World Business Council for Sustainable Development (WBCSD) CSR is definied as follows: "corporate social responsibility is assumed by the continuing commitment of companies to behave ethically and to contribute to economic development while improving the quality of life of employees and their families, local communities and society in general." (*apud* Holme&Watts, 2000).

Critics highlight the dimension of the concept of CSR, but also some negative aspects of its implementation. Among the most important are the diminution of shareholders power, of their property rights over their own business, the weakening of the overall corporate strength and on the long term – the changing of the very essence of capitalism. CSR has been criticized from the perspective that being exported to foreign communities by multinational companies it can legitimate values and approaches that are not in the interest of the poor and marginalized people.

The discussion about the limits of CSR cannot ignore a famous statement of Milton Friedman (1970): "Social responsibility of business is to increase their profit. According to the author, the only economic entities' responsibilities are to pay state taxes and their salaries." The supporters of these ideas have as their main argument the fact that studies have failed to identify a correlation between CSR activities and the performance indicators of firms.

Beyond the regular European discourse regarding CSR, its practices evolve differently from country to country, depending on the economic and social specificity of each region. The literature include "the Scandinavian model of CSR" which is characterized by the fact that the state plays the role of welfare provider, harmoniously combining the development based on capital items with a generous social security system. A representative country in this regard is Norway, thanks to its commitment of giving evidence in the struggle for peace, poverty and environmental destruction. Recent research shows that, for instance, the United Kingdom, too, attaches importance to ethical issues and moral conflicts arising from the practice of CSR. In the Nordic countries, CSR programs are particularly targeted by environmental problems, while in southern Europe there is a greater interest in diminishing social problems.

3. Corporate social responsibility and economical performance

The degree to which social expectations regarding business ethics resonate with the ethic of the economic environment depends on the comparison of social norms of firms and their conduct and also from the comparison between society's expectations and what corporate managers consider to be legitimate social demands. On the other hand, the connecting of personal interests with moral principles allows long-term development of the company, because, although an immediate profit leads to a lower capital, on the long term it produces a durable capital: reputation.

The literature includes antithetical ideas on this topic. Some (Low&Yeats, 1992; Lucas et al., 1992) are appalled by the manner in which multinational companies exploit lenient laws of some foreign countries, while others emphasize the existence of a strong correlation between internationalization and social responsibility (Bansal&Roth, 2000, Christmann, 2004).

In time, social responsibility has shown positive effects in the socioeconomic field of individual actors engaged in certain activities and the community at large. For example, in countries that encourage cooperation and trust between the actors and that emphasize the human and social capital there is the highest prosperity (Waddock&Graves, 1997).

The difficulty to distinguish positive from negative effects of CSR explaines why the studies regarding the relationship between CSR and financial performance are both contradictory and inconclusive. Recent studies have identified a strong correlation of these variables (Waddock& Graves, 1997), no correlation (McWilliams& Siegel, 2000) or a negative correlation (Wright&Ferris, 1997). For example, Margolis and Walsh (2003) monitored over 95 studies and found that 42% did not indicate any correlation. They also noted that the economic usefulness of CSR occurs when consumers are especially interested in social issues. It was also shown empirically that corporate CSR activities are not sufficiently well known (Sen, Bhattacharya&Korschun, 2006).

Ellen, Webb and Mohr (2006) found that, when choosing a company, 34% of people say they would avoid buying a product or service from a company perceived as being unethical, 16% seek information about its business practices and 50% did not intend to purchase a product or service from a company that is not considered socially responsible. In general, consumers have positive attitudes towards the company if it is involved in CSR activities.

Of course, the existence or inexistence of a correlation between social responsibility and various economic indicators can be determined by many variables. Beliveau, Cottrill and O'Neill (1994) showed that the relationship between CSR and profit varies both from an industry to another but also according to the organizational performance indicators.

Although there are many arguments that favor the hypothesis that CSR covers its own costs (Carroll, 1991) because it eliminates the reasons that lead skeptics to seek the approval of a more drastic legislation,

eliminates disputes or reduces their costs and facilitates easier access to funds from NGOs and other governmental agencies, the literature reflects a lot of contradictions within results of empirical research in this field.

4. Social responsibility of Romanian bussiness and the need for security culture

Compliance with ethical principles in business has led to the shaping of the concept of "moral capitalism" based on values such as respect for human dignity, respect for consumer's choice, elimination of immoral activities. Moreover, the corporate citizenship entails a moral obligation of companies to behave according to the ethical principles of the community they belong to, to fight against social degradation, to protect the culture of the community and to encourage education.

After the Revolution of December 1989, Romanian business was in a position to adopt the market economy model, and companies had to become more competitive and more interested in achieving profit in the context of economic hardship: serious problems inherited from the communist infrastructure, pollution, obsolescence of outdated industrial machinery and equipment especially in energy, mining and metallurgy. In such a context, the Romanian managers, still influenced by the mentality of the past, were in a difficult situation: should they spend money to gain profit or to be socially responsible?

The concern of Romanian business environment for the multiplication of such CSR initiatives is notable. Government statistics show that investment firms in corporate social responsibility activities were over 10 million euros each year. However, most of the money is spent for donations or sponsorships in the fields of social assistance support for charitable associations, the financing of scientific projects or research, in education or environmental protection and not for real CSR programs.

In 1973, Daniel Bell warned that the principal driver of change towards a "new techno-economic order" would be information and knowledge. We all agree now with this statement. In addition, everybody supports the growth of quality education so that people's training to be more suited to community needs.

As a proof of maturity of Romanian society in this regard and in full agreement with the changes occurring in the international security

environment and the commitments assumed by Romania in the perspective of European integration some institutions of higher education have introduced in their curricula topics that address frontal or tangential the problem of community survival, especilly security issues.

Michael Goodman and Sir David Omand (2008) consider that academic knowledge is hard to convey in the governamental area. Disciplines such as military history, history of intelligence, international relations, social sciences, and critical thinking is part of the required education of every security practitioner, but also of any common member of the community. On the other hand, such a transmission of strictly specialized knowledge from professionals to beginners can be an obstacle to interagency cooperation as it doesn't allow the establishment of common standards.

Hence, to discuss security issues related to running the analysis of education in the context of CSR should not seem so unusual. Unfortunately, the previous analysis of CSR concept made clear that security issues is rarely included in the list of socially responsible activities.

Therefore, along with meeting the need for accurate information, the possibility of specialization in security studies and intelligence is at least as important because it represents the foundation of the culture of intelligence for the civil society. An efficient civil society must be innovative and ready to adjust itself so as to ensure a correct balance between public interests and the sphere of private interests.

From this perspective, I consider that the worldwide realignment regarding the importance of intelligence services reflected in new strategies national and international security is not random. The issues of security and intelligence, as areas that provide tools to collect relevant information and tailored intelligence products, already enjoy new dimensions, which is the contribution of the civil society.

The present need for security becomes more acute in the context of an unmanageable information bombing in the modern era. Providing security is very difficult to achieve in the absence of a social framework that allows the contribution of each social actor (individual or organization). Because of this reality a new type of individual and community behavior has appeared on the social scene – the one that is characterized by social responsibility.

Based on Allesandro Politi's ideas, Leslie Donovan (2005) referred to the concept of "intelligence volunteering", considering that to encourage citizens to be cautious and attentive to issues of national security becomes

a public good of a democracy. Of course such efforts should be designed to protect citizens and not to get political or social control. The author also underlines the fact that people are influenced by the preconceived idea that cooperating with authorities in providing information is equal to denunciation, betrayal, espionage or subversive action. In his opinion this is the most important barrier for intelligence volunteering. Therefore, this barrier is located primarily in the individual psyche of citizens and is determined by their value system. In many countries, ordinary people do not grant security the same value politics does. Milton Rokeach has empirically shown that Americans, Canadians, Australians tend to grant a minimum value to national security. Having in mind Maslow's theory regarding the hierarchy of needs and also the widespread perception that people greatly value their security, such a finding is highly counterintuitive. According to Abraham Maslow (1943) people want to meet primarily the needs of food, water, shelter and, subsequently, of security. Only the fulfillment of these needs will enable the individual to feel as belonging to a community. Therefore this lack of theoretical concordance should be considered additionally.

Also Stuart Surlin and Barry Berlin (1991) found that Americans and Canadians put national security on the 18th place in their hierarchy of values. Similar values were found among American and Japanese pilots and among the employees of the National Aeronautics and Space Administration. In these circumstances the question is why national intelligence agencies and policy makers do not set up an educational program to change the idea that ordinary citizens can live their lives without having to look after the security of the community they live in.

As long as people feel unable to influence national security, they will not be able to take appropriate actions when needed. In this regard, psychologists have emphasized the importance of self-efficiency, namely of the belief that one is able of an adaptive response to danger according to his capacity to achieve his own objectives. As Louis Pasteur said "chance favors the prepared mind". A population that lack security self-efficiency is composed of poorly trained individuals in terms of enhancing the value of relevant information they encounter and of acting in accordance with that information (Donovan, 2005).

5. Conclusions

The evolution of the last two decades has decisively shaped the contemporary society with major effects on the security of individuals. Its consequences and costs have been frequently considered to be above the thresholds of acceptance and adaptation of a contemporary man who is set to expect more and tolerate low costs.

The identification of the problem and its remodeling through proactive measures must be a priority for everyone. Therefore every bussinessman should be aware of security threats and include such issues in their proactive actions, especially in the corporate social responsibility sphere. Also I believe that the growth of expertise in research, development and innovation of the national security sector respond to the needs of Romanian society and constitutes one of the greatest challenges of our contemporary society.

References

1. Bansal, P.& Roth, K. (2000). Why companies go green: a model of ecological responsiveness. *Academy of Management Journal*, 43(4), p. 717-736.

2. Beliveau, B., Cottrill, M.&O'Neill, H.M. (1994). Predicting corporate social resposiveness. A model drawn from three perspectives. *Journal of Business Ethics*, 13, p. 731-738.

3. Carroll, A. (1979). A three dimensional model of corporate performance. *Academy of Management Review*, 4, p. 497-505.

4. Carroll, A. B. (1991). The pyramid of corporate social responsibility: Toward the moral management of organizational stakeholders. *Business Horizons*, 34(4), p. 39-48.

5. Christmann, P. (2004). Multinational companies and the natural environment: determinants of global environmental policy standardization. *Academy of Management Journal*, 47(5), 747-760.

6. Donovan, L.A. (2005). Citizens as intelligence volunteers: the impact of value structures. *International Journal of Intelligence and Counterintelligence*, 18, p. 239-245.

7. Ellen, P.S., Webb, D.J.&Mohr, L.A. (2006). Building corporate associations: Consumer attributions for corporate socially responsible programs. *Journal of the Academy of Marketing Science*, 34, p. 147-157.

8. Friedman, M. (1970). The Social Responsibility of Business is to Increase Its Profits. *The New York Times Magazine,* 13 septembrie.

9. Goodman, M.S. & Omand, D. (2008). What analysts need to understand: the King′s intelligence studies program. *Studies in Intelligence*, 52 (4), (extracts, december 2008).

10. Hardin, G. (1968). The Tragedy of the Commons. *Science*, 162, p. 1243-1248.

11. Holme, R. & Watts, P. (2000). *Corporate Social Responsibility*: *Making Good Business Sense*. Geneva: WBCSD.

12. Low, P. & Yeats, A. (1992). Do 'Dirty' Industries Migrate? În P. Low (ed.) *International Trade and the Environment*, pp. 89-104, World Bank: Washington, DC.

13. Lucas, R.E.B., Wheeler, D. & Hettige, H. (1992). Economic Development, Environmental Regulation and the International Migration of Toxic Industrial Pollution, 1960-1988. În P. Low (ed.) *International Trade and the Environment*, pp: 67-88, World Bank: Washington.

14. Margolis, J.D. & Walsh, J.P. (2003). Misery loves companies: Rethinking social initiatives by business. *Administrative Science Quarterly*, 48, p. 268-305.

15. Maslow, A.H. (1943). A Theory of Human Motivation, *Psychological Review*, 50(4), p. 370-96.

16. McWilliams, A. & Siegel, D. (2000). Corporate social responsibility and financial performance: Correlation or misspecification? *Strategic Management Journal*, 21 (5), p. 603-609.

17. McWilliams, A. & Siegel, D. (2001). Corporate Social Responsibility: A Theory of the Firm Perspective. *The Academy of Management Review*, 26 (1), p. 117-127.

18. Politi, A. (2003). The Citizen as 'Intelligence Minuteman.' *International Journal of Intelligence and Counterintelligence*, 16 (1), p. 34-38.

19. Pounds, W. (1969). The Process of Problem Finding. *Industrial Management Review*, 11(1), p. 1-19.

20. Sen, S., Bhattacharya, C. B. & Korschun, D. (2006). The role of corporate social responsibility in strengthening multiple stakeholder relationships: A field experiment. Journal of the Academy of Marketing Science, 34, 158-166.

21. Waddock, S. & Graves, S. (1997). The corporate social performance-financial performance link. Strategic Management Journal, 18, 303-319.

22. Wartick, S. L. & Cochran, P. L. (1985). The evolution of the corporate social performance model. Academy of Management Review , 4, 758-769.

23. Wright, P. & Ferris, S. (1997). Agency conflict and corporate strategy: The effect of divestment on corporate value. Strategic Management Journal, 18, 77-83.

Cooperarea în intelligence. Mutații generate de noul context de securitate

Aurora-Elena BARĂU
Serviciul Român de Informații
e-mail: **aura_22_88@yahoo.com**

Abstract
The present paper tackles upon one of the highly classified fields within the intelligence sphere, the current cooperation relationships between the intelligence services, putting great emphasis on the major transformations and mutations generated by the 9/11 events. The so-called asymmetrical threats, as well as the new warfare that intelligence agencies have to deal with, imposed a considerably different approach of the international cooperation activity, which has evolved from an auxiliary sector to a priority one.

Keywords: intelligence services**,** asymmetrical threats, need to share, need to know.

După două decenii de la încheierea oficială a confruntării clasice, specifice Războiului Rece, dintre cele două blocuri oponente, structurile de securitate se confruntă cu o nouă provocare – o luptă generalizată împotriva terorismului islamic şi a altor amenințări neconvenționale, ceea ce impune noi eforturi de adaptare. În acest context, s-a conturat din ce în ce mai clar necesitatea formulării unor răspunsuri conjugate la provocările noului mediu de securitate, ceea ce implică dezvoltarea capacității de adaptabilitate, flexibilitate şi reacție rapidă. Coordonatele actuale de securitate, determinate pe de o parte de dispariția dihotomiei create de ideologia comunistă, iar pe de altă parte de amplificarea amenințărilor neconvenționale, au condus la înregistrarea unei deschideri către cooperare şi la extinderea domeniilor de colaborare între nucleele care compun „rețeaua globală de securitate".

În prezent, se remarcă nu doar o creştere cantitativă a schimbului informațional dintre servicii aparținând unor state diferite, ci şi transformări de factură calitativă. State despre care altădată s-ar fi considerat că este imposibil să încheie un parteneriat sunt astăzi angajate în relații de cooperare strânse care au trasgresat cu mult cadrul obişnuit de colaborare, specific secolului trecut. În timp ce schimburile informaționale la nivel bilateral îşi consolidează poziția de principal mijloc de cooperare externă, cooperarea multilaterală în paliere precum instruirea, pregătirea de cadre,

dar şi derularea de operaţiuni de teren se înscrie de asemenea într-un trend ascendent, câştigând din ce în ce mai mult teren. Suntem aşadar martori ai unei creşteri remarcabile în ceea priveşte interconectările dintre structurile de intelligence, ceea ce face ca distincţia dintre ceea ce constituie intern şi extern să intre într-un proces de erodare.

O analiză succintă a principalelor elemente constitutive ale proiectului de reformă al SRI relevă numeroase similitudini cu modelul american de reorganizare a comunităţii de intelligence, ceea ce constituie o dovadă în plus care atestă transformarea componentei de cooperare la nivel extern şi adaptare la standardele occidentale dintr-o preocupare comună, într-una prioritară.

Prezentul studiu reflectă aşadar, latura mai puţin cunoscută a serviciilor de securitate, cea diplomatică, cooperativă, contribuind în acest fel la demontarea mitului privind opacitatea şi închistarea „tradiţională" a acestor structuri.

I. Noile ameninţări de securitate şi necesitatea „răspunsului" comun

În prezent, există un consens unanim în ceea ce priveşte caracterul emergent şi natura dinamică a noilor tipuri de ameninţări de securitate. În încercarea de a defini situaţia actuală, s-a vorbit chiar şi despre „un al patrulea război mondial".[1]

Ultimul deceniu al secolului XX a însemnat pentru întreaga lume o perioadă zbuciumată, caracterizată de transformări profunde la nivel global, transformări ce ţin atât de redesenări ale frontierelor, cât şi de schimbări de regim şi ideologie. Redesenarea graniţelor a însemnat sporirea numărului de actori statali la nivel global, iar schimbările de regim şi ideologie au generat noi tipuri de actori şi forme surprinzătoare de manifestare a acestora.[2]

Au căpătat o importanţă tot mai mare, datorită rolului manifestat pe scena globală, actorii nonstatali (corporaţii multinaţionale şi transnaţionale, ONG-uri etc.), ale căror acţiuni sunt uneori dificil de prevăzut. De asemenea, unele dintre acestea au preluat practici şi obiective pe care statele nu şi le mai puteau permite. Alte fenomene disturbante tind să sufere mutaţii

---

[1] Dr. Michael C. Desch, profesor în cadrul „Bush School of Foreign Policy", Texas A&M University citat în *Intelligence Strategy: New Challenges and opportunities– Conference Proceedings*, 26-27 septembrie 2007, National Defence Intelligence College, Washington D.C., octombrie 2008, p. 73.

[2] Nicolae Dolghin, Alexandra Sarcinschi, Mihai-Ştefan Dinu, *Riscuri şi ameninţări la adresa securităţii României. Actualitate şi perspective,* Editura Universităţii Naţionale de Apărare, Bucureşti, 2004, p. 16.

majore, căpătând statut deplin de actor al scenei internaționale, un actor al cărui chip este din ce în ce mai greu de identificat, aşa cum se întâmplă în cazul terorismului. Riscurile şi amenințările au căpătat un aspect internaționalizat „reuşind" să ignore, în manifestările lor, granițelor statale, ceea ce a avut ca urmare o estompare rapidă a diferențelor dintre securitatea internă şi cea externă. Această estompare a condus, la rândul său, spre manifestarea tendinței majorității actorilor statali de a acționa, în ceea ce priveşte domeniul securității şi apărării, în cadrul unor inițiative sau organizații regionale sau globale. S-au dezvoltat, astfel, sau sunt în plin proces de dezvoltare, politici de securitate şi apărare comune pe plan regional sau / şi global.[3]

Lărgirea ariei de acces la informații reprezintă una dintre principalele provocări cu care se confruntă actualmente serviciile de intelligence. Sursele şi resursele deținute de structurile de informații ale unui stat, indiferent de capabilitățile acestuia, nu vor putea asigura niciodată o acoperire informativă de fond, totală a mediilor de interes, fiind astfel necesară gestionarea unei palete mult mai variate de mijloace de informare, între care un loc deosebit de important este ocupat de cooperarea cu instituții similare din exterior. Serviciul de intelligence modern începe să se asemene cu o mare companie modernă, care pune accent pe eficiență, coordonare, parteneriat şi management de calitate. În multe servicii de intelligence din Occident, acest proces se află în plină desfăşurare şi reprezintă răspunsul corespunzător la amenințările în schimbare ale începutului de secol, dar este în mod cert o noutate din punctul de vedere al unor servicii care în mod tradițional preferau inițiativa în locul doctrinei şi apelul la resursele proprii în detrimentul perspectivei cooperării externe.[4] Mutațiile majore ale mediului de securitate, la care s-a făcut deja referire, au determinat transformări multiple chiar şi la nivelul acestor instituții greoaie, care, în calitatea lor de membre ale unor structuri internaționale sau de pretendente la acest statut, s-au văzut nevoite să se adapteze „din mers" noilor tendințe şi să renunțe la mai vechile practici rudimentare.

Însemnătatea deosebită a inițiativei de cooperare la nivel internațional a fost afirmată şi reconfirmată în repetate rânduri de către analişti şi lideri de marcă din domeniului activității de intelligence sau din sfera politicului. Eliza Manningham – Buller, spre exemplu, în urma atacurilor cu bombă

---

[3] *Ibidem,* p. 17.

[4] Steve Tsang, *Serviciile de informații şi drepturile omului în era terorismului global. Geopolitica lumilor secolului XXI,* trad. Irina Bondar, Cristina Dogaru, Laura Drăghici, Adelina Negoiță, Bucureşti, Ed. Univers Enciclopedic, 2008, p. 234.

de la Londra din iulie 2005 declara: „Unul dintre atuurile pe care le deţinem în confruntarea cu această ameninţare globală (terorismul internaţional) îl reprezintă îndelungata relaţie de încredere şi cooperare între serviciile de informaţii din Europa şi nu numai."[5] Sir David pe de altă parte, vorbea chiar despre oportunitatea reîntoarcerii la un sistem centralizat, considerând că doar în acest fel se poate redobândi caracterul unitar al comunităţii de intelligence şi se poate spori eficienţa acestor structuri prin asigurarea interschimbului reciproc de informaţii.

Această tendinţă a fost receptată şi asimilată şi de structurile de informaţii din România, actualul director al Serviciului Român de Informaţii, George Cristian Maior declarând în acest sens: „Chestiunea sensibilă a cooperării între serviciile de informaţii din ţări diferite nu poate fi omisă în contextul necesităţii de a face schimburi de informaţii şi mai ales de produse analitice finite; dacă ameninţările sunt transnaţionale, este evident că şi răspunsul la acestea trebuie să depăşească graniţele naţionale".[6]

Aşadar, comunitatea internaţională nu mai poate aborda noile provocări reprezentate de actorii nonstatali în lipsa unei apropieri unitare şi cooperative. Unul dintre principalii piloni pe care se fundamentează lupta împotriva terorismului şi asigurarea securităţii UE în general, este cooperarea în intelligence în vederea asigurării unui suport informaţional veritabil, acesta reprezentând de fapt un prim pas în vederea „coagulării" şi apropierii interstatale.[7]

II. Restructurări instituţionale post 9/11. Tranziţia de la *„need to know"* la *„need to share"*

Comunitatea americană de intelligence, ca de altfel majoritatea structurilor similare din alte ţări, s-a transformat profund odată cu sfârşitul Războiului Rece şi pe parcursul anilor '90 pe fondul mutaţiilor multiple survenite la nivelul mediului de securitate. A urmat apoi momentul 9/11, care a consfinţit redirecţionarea completă a priorităţilor de acţiune ale serviciilor de intelligence, marcând intrarea într-o nouă etapă, definită de noi riscuri şi ameninţări, care nu pot fi abordate decât la nivel multilateral.

---

[5] Steve Tsang, *Op.cit.,* p. 291.

[6] George Cristian Maior, autor al studiului introductiv al lucrării lui Steve Tsang, *Serviciile de informaţii şi drepturile omului în era terorismului global. Geopolitica lumilor secolului XXI*, trad. Irina Bondar, Cristina Dogaru, Laura Drăghici, Adelina Negoiţă, Bucureşti, Ed. Univers Enciclopedic, 2008, p. 12.

[7] Eveline R. Hertzberger, *Counter Terrorism Intelligence Cooperation in the European Union,* European Foreign and Security Studies Policy Program, p. 2.

Dacă până la 11 septembrie 2001 terorismul avea o semnificaţie regională, odată cu aceste evenimente, acesta devenea o problemă de securitate de interes global. Creşterea exponenţială a impactului şi importanţei atribuite acestui fenomen se află în strânsă legătură cu procesele conexe globalizării şi cu accesul tot mai uşor la tehnologie, care au avut un rol facilitator.[8] Nu întâmplător atacurile de la 11 septembrie sunt considerate o emblemă a globalizării, dar şi o nouă paradigmă de desfăşurare a atentatelor teroriste.

În aceste condiţii, prevenirea şi combaterea terorismului internaţional impun adoptarea unor noi modalităţi de evaluare, precum şi capacităţi şi metode de acţiune adecvate. Extinderea fenomenului terorist şi pericolul deosebit al acestuia au determinat acţiuni conjugate pentru contracararea lui şi realizarea unei coaliţii la nivel global. În acelaşi timp, a apărut necesitatea reconsiderării profunde a sistemului de intelligence per ansamblu şi îndeosebi a rolului şi locului componentei de cooperare externă în cadrul acestuia.

Imediat după momentul 9/11, aprecieri precum „totul s-a schimbat" sau „America şi lumea întreagă nu va mai fi aceeaşi" au fost uzitate cu o frecvenţă fără precedent. Analiza amănunţită care a urmat a scos în evidenţă erorile evidente ale percepţiei americane, care avea la bază distincţii precum „intern-extern", „mediere sau intervenţie militară", distincţii care nu se pliau aproape deloc pe realităţile curente. Raţionamentele şi concluziile Comisiei 9/11, poate mai mult ca oricare alte amendamente oficiale ale unei instituţii statale, continuă să persiste în memoria colectivă ca „un eşec de proporţii al imaginaţiei naţionale"[9].

Intelligence-ul american a fost bazat, timp de mai multe decenii, pe trei principii, două explicite şi unul implicit. Principiile explicite sunt „compartimentarea muncii" – o reflecţie directă a conceptelor organizaţionale corporative ale secolului al XIX-lea şi „need to know". Principiul implicit făcea referire la corelaţia care există între sensibilitatea procesului prin intermediul căruia informaţiile sunt obţinute şi valoarea efectivă a informaţiilor. Aceste principii au îngreunat mult orice iniţiativă de cooperare deschisă şi solidă cu entităţi similare, din interiorul ţării şi mai ales din exterior, alimentând tradiţionalul caracter opac şi închis al structurilor de intelligence.

---

[8] J. Baylis, S. Smith, *The Globalization of World Politics*, Londra, Oxford University Press, 2005, p. 480 *apud* Dr. Maricel Antipa, *Triumviratul dezastrului global*, Bucureşti, Editura Monitorul Oficial, 2010, p. 7

[9] William M. Nolte, American Intelligence after the 2008 Election, articol în International Journal of Intelligence and CounterIntelligence, Ed. Routledge – Taylor&Francis Group, 2008, p. 433.

„Schimb informațional, mai multă flexibilitate şi răspundere civilă sunt noile direcții de acțiune în comunitatea americană de intelligence”.[10] Aceste trei principii aveau să stea la baza noii imagini a serviciilor de intelligence americane, al căror proces de restructurare a fost inițiat imediat după 11 septembrie 2001. Cadrul legal adoptat în scopul susținerii demersurilor de adaptare a comunității americane de intelligence la specificul noilor amenințări de securitate a inclus: „USA Patriot Act” (octombrie 2001), „Terrorism Prevention Act” (2004), „Intelligence Reform Act” (2004) etc.

Dintre toate schimbările care au marcat sistemul de securitate național al SUA după septembrie 2001, una dintre cele mai complexe, importante, dar şi frustrante transformări se referă la procesul de reconsiderare a relației dintre guvernul federal şi instrumentele sale de securitate (militare, de intelligence şi de aplicare a legii) şi instrumentele locale sau de stat, devenite acum „aliate”, aşa cum nu s-a mai întâmplat niciodată în istoria SUA. Astfel, pe măsură ce publicul american a început sădea semne de recuperare după şocul reprezentat de evenimentele de la 11 septembrie, a apărut o reacție firească, aproape unanim împărtăşită, care făcea trimitere la eşecul autorităților federale şi statale în a stabili conexiuni şi a dezvolta relații de cooperare eficiente. Recenta apariție a Departamentului de Securitate Internă nu schimbă cu nimic faptul că, spre deosebire de cazul altor state-națiuni, securitatea internă americană reprezintă un adevărat efort federal, incluzând un guvern federal, 50 de guverne statale şi mii de primării şi municipalități. Cu toate acestea, au fost înregistrate progrese notabile în angajarea instituțiilor locale şi statale în relații directe şi strânse cu guvernul federal, într-o asemenea manieră catalogată drept „de neimaginat” cu un deceniu înainte.[11] Aceste demersuri au inclus, spre exemplu, crearea a peste 40 de „centre de fuzionare”, în cadrul cărora, oficiali guvernamentali şi locali încearcă se reunească laolaltă informații din toate sursele disponibile şi să acționeze în baza acestora.

În octombrie 2005, primul director general al comunității de intelligence, John Negroponte, a emis Strategia Națională de Intelligence a SUA. El a reamintit cerința lui G. W. Bush, formulată în cadrul Actului de Reformă al Activității de Intelligence şi a Actului de Prevenire a Terorismului din 2004, în cadrul cărora îşi exprima aşteptările în legătură

---

[10] Dr. R. Carter Morris, Director al Sectorului “Information Sharing and Knowledge Management” din cadrul Oficiului de Intelligence şi Analizăaparținând Departamentului de Securitate Internă al SUA *apud Intelligence Strategy: New Challenges and opportunities – Conference Proceedings*, 26-27 septembrie 2007, National Defence Intelligence College, Washington D.C., octombrie 2008, p. 50.

[11] *Ibidem,* p. 433.

cu „transformarea comunității de intelligence într-o structură mult mai unitară, mai bine coordonată şi eficientă”. Negroponte a adăugat: „Această strategie implică o reformă pe termen lung a mai vechilor practici şi aranjamente din domeniul intelligence-ului. Serviciile de intelligence naționale se subordonează unor obiective comune... A venit timpul ca structurile noastre de intelligence, interne şi externe, precum şi culturile pe care le promovează să evolueze şi să devină mai puternice, evoluând împreună.”[12]

„O lume în care avem de-a face cu astfel de amenințări este, cu siguranță, una plină de provocări. În cazul Războiului Rece, amenințarea unui potențial conflict deschis între SUA şi URSS putea fi una catastrofală, dar, poate URSS nu a luat niciodată în considerare, în mod real, perspectiva unui război cu America, în timp ce azi, este destul de clar că Al-Qaeda vrea să intre în război cu noi.”[13]

Cele menționate mai sus sunt de natură să sublinieze existența unor necesități de cooperare şi dialog stringente în contextul actual, necesități care devin din ce în mai vizibile şi în sfera tradițional opacă şi închisă a serviciilor de intelligence. Se cunoaşte faptul că, extinderea din ce în ce mai accentuată a cooperării între serviciile diferitelor țări reprezintă cea mai importantă schimbare recentă din domeniul activității de intelligence. Conectivitatea crescândă dintre structurile de securitate interne pe de o parte, dar şi dintre serviciile externe pe de altă parte, oferă argumente în favoarea ideii potrivit căreia, în prezent se poate vorbi nu doar de o cooperare internațională în creştere, ci poate chiar de o cooperare globală.[14]

Există totuşi, cel puțin aparent, o relativă neconcordanță între o activitate de cooperare la nivel global şi tradiționalele mecanisme de supraveghere şi spionaj, care au avut dintotdeauna un caracter național. Pe de o parte nevoia de cooperare, de coacțiune şi sprijin reciproc s-a impus ca un „trend” major şi ca o necesitate vitală pentru asigurarea capacității de răspuns a serviciilor de informații la amenințările prezentului, iar pe de altă parte, aceleaşi amenințări şi riscuri de securitate impun şi reconsiderarea

---

[12] John Negroponte, Director General al Comunității de Intelligence, apud Peter Gill, Stephen Marrin, Mark Phythian, *Op. cit.,* p. 112.

[13] Dr. Michael C. Desch, profesor în cadrul „Bush School of Foreign Policy”, Texas A&M University citat în *Intelligence Strategy: New Challenges and opportunities– Conference Proceedings*, 26-27 septembrie 2007, National Defence Intelligence College, Washington D.C., octombrie 2008, p. 73.

[14] Richard J. Aldrich, *Global Intelligence Co-operation versus Accountability: New Facets to an Old Problem*, articol în Revista *Intelligence and National Security,* Editura Routledge – Taylor&Francis Group, Vol. 24, nr.1, ediția februarie 2009, p. 26.

importanței laturii defensive a activității de intelligence, în ciuda faptului că perspectiva unui potențial conflict „tradițional" poate părea neverosimilă.

O dovadă în plus care atestă sporirea exponențială a importanței atribuite de structurile de intelligence activității de cooperare externă simultan cu redefinirea relevanței acțiunilor de contraspionaj este dată de eforturile recente ale comisiilor de anchetă naționale, regionale și internaționale de a examina, analiza și reglementa aspecte care țin de aceste domenii. Relevante în acest sens sunt aprecierile Comisiei 9/11 care fac trimitere la necesitatea stabilirii unui schimb informațional orizontal real și eficient între structurile de intelligence ale SUA, dar și între acestea și serviciile partenere din afară și crearea unei rețele informaționale sigure, de încredere. Sintagma „*unity of effort in sharing information*"[15] redă foarte elocvent însemnătatea deosebită atribuită, de autoritățile americane, activității de cooperare și se constituie într-o dovadă a disponibilității acestor structuri de intelligence, de altfel cele mai performante din lume, de a iniția și dezvolta parteneriate cu omologi străini. Aceeași comisie aduce în prim plan, în cadrul raportului întocmit după evenimentele din septembrie 2001, necesitatea restabilirii unei balanțe între informațiile dezvăluite și nevoia secretizării, adică între spectrul de parteneriate și relații de cooperare și activitățile absolut vitale de contrainformații. Recomandarea avansată face trimitere la stabilirea unor „proceduri de natură să asigure un cadru favorabil derulării activităților de cooperare"[16], astfel încât să se restabilească echilibrul între volumul de informații „împărtășit" în calitate de partener și cumulul de acțiuni de protecție, cu caracter defensiv pe care orice stat le prioritizează fără excepție, indiferent de gradul de implicare în demersurile de cooperare.

Strategia Națională de Intelligence a SUA, cuprinde de asemenea, numeroase referiri la „necesitatea de a consolida relațiile de parteneriat deja existente cu omologi externi și de a crea altele noi, astfel încât să se poată oferi un răspuns eficient provocărilor de securitate globale"[17]. Se vizează de asemenea, stabilirea de politici care să reflecte principiul „need to share" și nu „need to know" pentru toate informațiile cu relevanță și eliminarea „proprietății" printr-un flux informațional deschis, precum și dezvoltarea de

---

[15] *The 9/11 Commission Report* (document în variantă online). Loc de regăsire: adresa www.9-11commission.gov/report/911Report.pdf -, site consultat la data de 07.05.2010, p. 418.
[16] Idem.
[17] *The National Intelligence Strategy of the United States,* august 2009 (variantă online). Loc de regăsire: adresa http://www.dni.gov/reports/2009_NIS.pdf, site consultat la data de 01.05.2010, p. 9.

rețele flexibile şi sigure, având capacitatea de a se adapta la un mediu în continuă schimbare.[18] Se remarcă aşadar, tranziția graduală de la o mai veche politică definită de principii fixe şi rigide privind secretizarea şi compartimentarea muncii, de tipul „need to know", la una flexibilă, într-un continuu proces de adaptare la realitățile curente, care prioritizează deschiderea, cooperarea şi transparența (politică de tipul „need to share").

Aşadar, abordarea dominantă, survenită post 9/11, presupune o reconfigurare a comunităților de intelligence naționale, în vederea unei mai mari deschideri către exterior şi unei apropieri mai strânse în plan intern. În unele state, aceasta a condus la constituirea de noi departamente de stat responsabile cu întreaga paletă de problematici care țin de securitatea internă. În altele, schimbarea s-a concretizat într-o mai bună coordonare între departamentele existente, dar şi între acestea şi structuri similare din exterior. Stabilirea de protocoale şi proceduri de cooperare cu parteneri străini este una dintre prioritățile serviciilor de intelligence, această opțiune pobându-şi eficacitatea în repetate rânduri, în contextul unei dinamici permanente a paletei de probleme de securitate.[19]

Pe de altă parte însă, analizele de specialitate arată că acțiunile de spionaj orientate împotriva SUA nu au scăzut numeric după evenimentele de la 11 septembrie 2001. Mai mult, potrivit raportului guvernului american, „activitățile instrumentate de servicii de spionaj adverse au sporit în densitate şi complexitate în ultimii ani".[20] Cu toate acestea, fondurile care ar fi trebuit fi alocate sectoarelor de contrainformații au fost redirecționate înspre alte segmente de activitate cu implicare în războiul împotriva terorismului global.[21]

Faptul că atât „rivalii", cât şi aliații au derulat activități de spionaj pe teritoriul SUA nu reprezintă totuşi o surpriză pentru nimeni. După cum Seth Jones, oficial al RAND Corporation, a observat „sfârşitul Războiului Rece şi emergența SUA ca unică superputere mondială au transformat această

---

[18] *The National Intelligence Strategy of the United States,* august 2009 (variantă online). Loc de regăsire: adresa http://www.dni.gov/reports/2009_NIS.pdf, site consultat la data de 01.05.2010, p. 9.

[19] L. Sondhaus, *Strategic Culture and Ways of War,* Londra, Ed. Routledge *apud* Craig A. Snyder, *Contemporary security and strategy*, ediția a doua, New York, Editura Palgrave-MacMillan, 2008, p. 112.

[20] Interagency OPSEC Support Staff, *Intelligence Threat Handbook*, Operation Security Information Series, Washington D.C., p. 2 (document în variantă online). Loc de regăsire: adresa http://www.fas.org/irp/threat/handbook/index.html, site consultat la data de 7.05.2010.

[21] Chuck McCutcheon, *In an age of Terrorism, Don't Forget Conventional Spying, Experts Advise*, Newhouse News Service, 20 octombrie 2004, p.1.

țară într-o țintă atractivă pentru spionii din toate națiunile, inclusiv din cele aliate."[22] Inovațiile continue din domeniul militar, economic şi tehnologic asigurate de-a lungul timpului de companiile americane şi de agențiile guvernamentale au reprezentat un punct de interes major pentru alte state, dornice de a avea acces la aceste progrese tehnologice prin intermediul spionajului. Amplasarea bazelor militare americane în toate colțurile lumii a reprezentat un alt factor care a antrenat guvernele străine în activități secrete de intelligence, cu scopul de a înțelege mai bine demersurile actuale ale SUA şi planurile lor de viitor.[23]

Urmând aceeaşi direcție de analiză, Patrick Lang, fost analist al Defense Intelligence Agency (DIA), afirma: „Odată cu sfârşitul Războiului Rece, autoritățile au încetat să se mai preocupe cu activitatea de contrainformații. În consecință, nu a mai fost manifestată aceeaşi atenție față de menținerea persoanelor neautorizate la distanță de sfera informațiilor secrete."[24] Acest interes crescând față de descoperirea secretelor SUA „se traduce" printr-o vulnerabilitate din ce în ce mai mare față de tentativele de penetrare, care apar ca urmare a multiplelor demersuri de recrutare inițiate de agențiile de intelligence, precum şi ca urmare a disponibilității sporite de cooperare cu parteneri străini.

Cât de eficiente se vor dovedi aceste măsuri în cadrul procesului de „revitalizare" a activității structurilor de contraspionaj al SUA nu poate fi încă anticipat, mai ales în contextul sporirii fără precedent a inițiativelor de spionaj îndreptate împotriva propriilor parteneri. Cu siguranță, o bună parte din aceste activități nu vor fi dezvăluite niciodată opiniei publice. După cum explica şi fostul ofițer CIA, Frederick Hitz, „în mod normal, atunci când un serviciu este deconspirat în acțiunile sale de către un serviciu partener, cu care derulează în mod constant activități comune, chiar dacă relațiile nu sunt întrerupte, problema este soluționată de comun acord între cele două structuri implicate în incident, de o manieră cât mai discretă"[25].

---

[22] Seth G. Jones, *When Allies Send Spooks to America*, International Herald Tribune, 25 octombrie 2004, p. 284.

[23] *Ibidem,* p. 285.

[24] Citat de Faye Bowers, *U.S. unready for rising threat of 'moles'*, Christian Science Monitor, 8 aprilie 2005 *apud* Stéphane Lefebvre, *Spying on Friends?: The Franklin Case, AIPAC and Israel*, articol în *International Journal and CounterIntelligence*, vol. 19, Ed. Routledge – Taylor&Francis Group, 2006, p. 614.

[25] Frederick Hitz, fost ofițer CIA, apud Stéphane Lefebvre, *Spying on Friends?: The Franklin Case, AIPAC and Israel, articol în International Journal and CounterIntelligence, vol. 19,* Ed. Routledge – Taylor&Francis Group, 2006, p. 615.

III. Reglementări interne privind cooperarea internațională în intelligence

România, asemenea majorității noilor membri ai UE din regiunea central şi est-europeană, este percepută ca puternic „atlantistă" şi cu o viziune pro-americană, ca urmare a încercărilor repetate de a intra în NATO şi a eforturilor depuse în vederea probării democratizării şi credibilității sale. În consecință, inițierea de parteneriate strategice în diverse domenii de activitate cu SUA şi alți parteneri occidentali a fost considerată o „extensie" firească a dezvoltării statului român.[26]

„Într-o lume complexă, dinamică şi conflictuală, aflată în plin proces de globalizare, înțelegerea profundă a tendințelor majore de evoluție a securității internaționale şi a modului în care fiecare țară are şansa să devină parte activă a acestui proces constituie o condiție esențială a progresului şi prosperității."[27] Aceasta este una dintre premisele enunțate în partea introductivă a Strategiei de securitate națională a României, primul document de acest gen, al cărui conținut este făcut public. Luând ca etalon modelul occidental şi îndeosebi pe cel american, țara noastră, în calitate de membru activ al UE şi NATO, a inițiat un amplu proces de reformare la nivelul structurilor de securitate interne şi externe, în vederea ralierii prompte la standardele impuse de partenerii externi, dar şi de noile realități ale mediului de securitate.

Strategia de Securitate Națională a României dezvoltă problematica cooperării între serviciile de intelligence din România şi cele externe în decursul unui întreg capitol – „Prioritățile participării active la construcția securității internaționale: promovarea democrației, lupta împotriva terorismului internațional şi combaterea proliferării armelor de distrugere în masă"[28]. Angajarea activă în îndeplinirea celor trei direcții de acțiune amintite este considerată drept „principalul imperativ al etapei actuale pentru politica de securitate a României". Instrumentul propus pentru realizarea acestui obiectiv îl constituie relațiile de cooperare, care trebuie

---

[26] Mireille Rădoi, *My USA: Views on American National Security and Foreign Policy,* Bucureşti, Editura Tritonic, 2007, p. 61.

[27] *Strategia de securitate națională a României – 2007* (document în variantă online). Loc de regăsire: adresa http://www.presidency.ro/static/ordine/SSNR/SSNR.pdf, site consultat la data de 10.10.2011, p. 5.

[28] *Strategia de securitate națională a României – 2007* (document în variantă online). Loc de regăsire: adresa http://www.presidency.ro/static/ordine/SSNR/SSNR.pdf, site consultat la data de 10.10.2011, p. 20.

să vizeze „adoptarea şi aplicarea unor măsuri de tip pro-activ, anticipative, iar măsurile avute în vedere vor fi, prioritar, de natură politică, diplomatică, economică şi socială, dar şi de natură civică, dublate permanent de un efort adecvat, legitim şi eficient, în plan informațional."[29]

În cadrul Viziunii Strategice 2007-2010, „cooperarea" este încadrată în categoria celor patru principii care fundamentează transformarea SRI: profesionalism, capabilitate, flexibilitate, cooperare. Prin implementarea principiului cooperării se vizează „dezvoltarea relațiilor bi/multilaterale, schimburilor de informații şi operațiunilor în comun cu partenerii naționali şi internaționali."[30] Cooperarea, pe palierul național, cu celelalte servicii de informații şi consolidarea profilului SRI în cadrul comunității de informații, precum şi diversificarea conectării externe, în format bilateral şi multilateral va reprezenta un important factor de multiplicare a eforturilor serviciului în domeniul anticipativ şi în cel operațional.[31]

O analiză succintă a principalelor elemente constitutive ale proiectului de reformă al SRI relevă numeroase similitudini cu modelul american de reorganizare a comunității de intelligence, ceea ce constituie o dovadă în plus care atestă transformarea componentei de cooperare la nivel extern şi adaptare la standardele occidentale dintr-o preocupare comună, într-una prioritară. Astfel, asemenea noii Strategii Naționale de Intelligence a SUA, elaborată în anul 2009, şi proiectul de reformă al SRI face referire la „necesitatea îmbunătățirii capacității analitice şi evaluativ-predictive" sau la „dezvoltarea unui concept modern privind managementul cunoaşterii, bazat pe o infrastructură informatică integrată, fiabilă şi eficientă."[32] Totodată, inițiativa creării de noi funcții şi structuri simultan cu desființarea altora, considerate insuficient adaptate contextului actual, se regăseşte şi în planul de reorganizare a activității structurilor de securitate din România, ceea ce reprezintă o altă asemănare cu modelul american, abordat pe larg în subcapitolul anterior. Astfel, dacă în SUA au fost înființate o nouă funcție de conducere, cea de director al comunității de intelligence, peste 40 de „centre de fuzionare", precum şi un Consiliu Comun al Comunității

[29] *Ibidem,* p. 23.
[30] *Viziunea Strategică 2007-2010*, SRI (document în variantă online). Loc de regăsire: adresa http://www.sri.ro/upload/viziunea.pdf, site consultat la data de 10.10.2011, p. 6.
[31] *Ibidem*, p. 11.
[32] *Reforma SRI*, *Transformarea Serviciului Român de Informații* (document în variantă online). Loc de regăsire: adresa http://www.sri.ro/upload/reforma.pdf, site consultat la data de 10.10.2011, p. 2.

de Intelligence, în încercarea de a spori coeziunea între structurile de informații americane, în România s-a luat decizia implementării unui nou sistem de planificare integrată şi a constituirii, în cadrul Serviciului Român de Informații, a Centrului Național CYBERINT, având misiunea de a preveni, proteja şi gestiona consecințele în situația unor atacuri cibernetice.

Aceste inițiative menite să contribuie la dezvoltarea şi modernizarea structurilor de intelligence din România, astfel încât cooperarea cu partenerii externi să sporească în eficiență şi interoperabilitate, au depăşit forma pur teoretică, materializându-se în contextul participării active la lupta împotriva terorismului.

Concluzionând, cele expuse în cadrul prezentului subcapitol evidențiază de o manieră foarte elocventă transformarea radicală a percepției structurilor de securitate naționale față de rolul şi importanța atribuită relațiilor de parteneriat cu omologi externi. Sfârşitul Războiului Rece, dar mai ales evenimentele din septembrie 2001 au fost momentele de referință care au marcat trecerea într-o nouă etapă, cea a riscurilor şi amenințărilor transfrontaliere, cărora nu li se poate oferi un răspuns adecvat decât la nivel multilateral.

Considerații finale

Aşadar, demersurile de cooperare au cunoscut un trend constant ascendent, mai întâi în palierul militar, unde s-a remarcat existența unui flux informațional amplu şi extrem de eficient între diferitele structuri, în cadrul operațiunilor comune derulate prin intermediul organizațiilor internaționale, dar şi în domeniul securității, unde treptat, s-a conturat de asemenea o tendință pronunțată în acest sens, riscurile şi amenințările de securitate putând fi prevenite şi contracarate efectiv doar la nivel multilateral, prin schimburi constante de informații între servicii.

Important de avut în vedere este însă faptul că, parteneriatele la nivel internațional pot reprezenta o soluție viabilă doar în măsura în care este depăşit planul abordării teoretice şi există voința comună a tuturor actorilor implicați pentru structurarea şi implementarea unei strategii clare şi realiste, capabilă să-şi atingă obiectivele fundamentale asumate. Mai mult, cooperarea în domeniul activității de intelligence a impus o nouă etapă în conlucrarea dintre serviciile de specialitate: deplasarea centrului de greutate dintre schimbul de informații cu caracter de generalitate spre cooperarea pe cazuri şi acțiuni punctuale, ca modalitate de valorificare optimă a potențialului oferit de partenerii implicați.

Ultima perioadă (îndeosebi intervalul post 9/11) a adus progrese notabile în acest segment al muncii de informații, imperativele discreției şi secretizării, elemente-cheie pentru reuşita acțiunilor de intelligence, armonizându-se din ce în ce mai bine cu demersurile de cooperare bi şi multilaterale, devenind mult mai flexibile şi adaptabile la specificul fiecărei acțiuni impuse de mutațiile şi provocările noului mediu de securitate.

Cu toate acestea, în prezent, după cum afirma şi Eduardo Serra, fost ministru al Apărării în Spania, mecanismele cooperării la nivel internațional destinate combaterii amenințărilor transfrontaliere prezintă caracteristici perfectibile, în condițiile în care statele-membre încă apreciază că o bună parte din datele confidențiale importante pe care le dețin sunt prea sensibile pentru a fi puse la dispoziția tuturor partenerilor.[33]

Se recomandă aşadar, direcționarea eforturilor în vederea depăşirii acestor limite care apar inerent în activitatea de cooperare, precum şi formularea de soluții viabile, aplicabile în practică şi nu doar la nivel teoretic, care să permită o armonizare cât mai eficientă între interesele individuale şi de grup, între atributul „naționalismului" pe care multe state insistă încă să-l mențină şi noile tendințe de organizare sub forma entităților multilaterale, colective. Deşi prioritizarea interesului național rămâne încă o constantă a relațiilor bi şi multilaterale dintre diferitele servicii de informații, evoluția şi progresele deosebite înregistrate în acest domeniu, cel puțin în perioada post Războiul Rece, nu pot fi puse la îndoială. Din această perspectivă, se poate aprecia anticipativ, fără teama de a greşi, continuitatea procesului de dezvoltare, consolidare şi extindere a parteneriatelor dintre structurile de intelligence ale diferitelor state, ceea ce se va materializa într-o replică din ce în ce mai solidă la provocările noului mediu internațional de securitate.

Concluzionând, se impune o conştientizare a necesității deschiderii către exterior, a angrenării în forme de cooperare la nivel bi şi multilateral, concomitent cu adoptarea tuturor măsurilor necesare armonizării intereselor individuale şi colective, deziderat care nu se poate realiza decât valorificând la maximum resursele artei diplomatice.

---

[33] Eduardo Serra (ex-ministru al Apărării din Spania), *Necesitatea informațiilor în cadrul noilor politici de securitate*, articol în Revista *Securitate şi democrație. Viitorul serviciilor de informații*, Madrid, 2000 *apud* Alina Goagă, *Mecanisme şi forme de cooperare între serviciile de informații în domeniul combaterii terorismului,* Bucureşti, 2007, p. 6.

Bibliografie

1. Aldrich, J., Richard, *Global Intelligence Co-operation versus Accountability: New Facets to an Old Problem*, articol în Revista *Intelligence and National Security,* Editura Routledge – Taylor&Francis Group, Vol. 24, nr.1, ediția februarie 2009, p. 26.

2. Baylis, J., Smith, S., *The Globalization of World Politics*, Londra, Oxford University Press, 2005, p. 480 *apud* Dr. Maricel Antipa, *Triumviratul dezastrului global*, Bucureşti, Editura Monitorul Oficial, 2010, p. 7.

3. Bowers, Faye, U.S. unready for rising threat of 'moles', Christian Science Monitor, 8 aprilie 2005 apud Stéphane Lefebvre, Spying on Friends?: The Franklin Case, AIPAC and Israel, articol în International Journal and CounterIntelligence, vol. 19, Ed. Routledge – Taylor&Francis Group, 2006, p. 614.

4. Desch, C., Michael, profesor în cadrul „Bush School of Foreign Policy", Texas A&M University citat în Intelligence Strategy: New Challenges and opportunities– Conference Proceedings, 26-27 septembrie 2007, National Defence Intelligence College, Washington D.C., octombrie 2008, p. 73.

5. Dolghin, Nicolae; Sarcinschi, Alexandra; Dinu, Mihai-Ştefan; *Riscuri şi ameninţări la adresa securităţii României. Actualitate şi perspective,* Editura Universităţii Naţionale de Apărare, Bucureşti, 2004, p. 16.

6. Hertzberger, R., Eveline, *Counter Terrorism Intelligence Cooperation in the European Union,* European Foreign and Security Studies Policy Program, p. 2.

7. Hitz, Frederick, fost ofițer CIA, apud Stéphane Lefebvre, *Spying on Friends?: The Franklin Case, AIPAC and Israel, articol în International Journal and CounterIntelligence, vol. 19,* Ed. Routledge – Taylor&Francis Group, 2006, p. 615.

8. Jones, G., Seth, *When Allies Send Spooks to America*, International Herald Tribune, 25 octombrie 2004, p. 284, 285.

9. Maior, George, Cristian, autor al studiului introductiv al lucrării lui Steve Tsang, *Serviciile de informaţii şi drepturile omului în era terorismului global. Geopolitica lumilor secolului XXI*, trad. Irina Bondar, Cristina Dogaru, Laura Drăghici, Adelina Negoiţă, Bucureşti, Ed. Univers Enciclopedic, 2008, p. 12.

10. McCutcheon, Chuck, *In an age of Terrorism, Don't Forget Conventional Spying, Experts Advise*, Newhouse News Service, 20 octombrie 2004, p.1.

11. Morris, Carter, Director al Sectorului „Information Sharing and Knowledge Management" din cadrul Oficiului de Intelligence şi Analizăaparţinând Departamentului de Securitate Internăal SUA *apud Intelligence Strategy: New Challenges and opportunities – Conference Proceedings*, 26-27 septembrie 2007, National Defence Intelligence College, Washington D.C., octombrie 2008, p. 50.

12. Negroponte, John, Director General al Comunităţii de Intelligence, apud Peter Gill, Stephen Marrin, Mark Phythian, *Op. cit.,* p. 112.

13. Nolte, M., William, American Intelligence after the 2008 Election, articol în International Journal of Intelligence and CounterIntelligence, Ed. Routledge – Taylor&Francis Group, 2008, p. 429-431, 433.

14. Rădoi, Mireille, My USA: Views on American National Security and Foreign Policy, Bucureşti, Editura Tritonic, 2007, p. 61.

15. Serra, Eduardo, (ex-ministru al Apărării din Spania), Necesitatea informațiilor în cadrul noilor politici de securitate, articol în Revista Securitate şi democrație. Viitorul serviciilor de informații, Madrid, 2000 apud Alina Goagă, Mecanisme şi forme de cooperare între serviciile de informații în domeniul combaterii terorismului, Bucureşti, 2007, p. 6.

16. Sondhaus, L., *Strategic Culture and Ways of War,* Londra, Ed. Routledge *apud* Craig A. Snyder, *Contemporary security and strategy*, ediția a doua, New York, Editura Palgrave-MacMillan, 2008, p. 112.

17. Tsang, Steve, *Serviciile de informații şi drepturile omului în era terorismului global. Geopolitica lumilor secolului XXI,* trad. Irina Bondar, Cristina Dogaru, Laura Drăghici, Adelina Negoiță, Bucureşti, Ed. Univers Enciclopedic, 2008, p. 234, 291.

Surse internet

1. www.9-11commission.gov/report/911Report.pdf
2. http://www.dni.gov/reports/2009_NIS.pdf
3. http://www.fas.org/irp/threat/handbook/index.html
4. http://www.presidency.ro/static/ordine/SSNR/SSNR.pdf
5. http://www.sri.ro/upload/reformhttp://www.sri.ro/upload/viziunea.pdf

Aport de intelligence românesc la securitatea europeană

Vlăduț BRÎNZĂ
Academia Națională de Informații „Mihai Viteazul”
e-mail: **vladutz_brinza@yahoo.com**

Abstract

Within nowadays and future conditions, the European security acquires a new value as far as the Danube-Main-Rhine strategic complex is concerned. This area is complementary to the Black Sea and the North Sea with western and eastern extension as a result of the connection between these and some hydrographic pools such as Elba, Vistula, Oder, Sena. Loire, Drava, Sava, Morava etc., through Danube security.

The paper proposes for the second decade of the present century, a new design of the European security based on three main pillars: euroatlantic, mediterranean and danubian.

Keywords: strategically complex, Danube security**,** European Union, Danube, Black Sea, riscks, threats, vulnerabilities

1. Securitatea dunăreană – o nouă valoare europeană

Prin poziția sa geografică[1], prin debitul de apă şi resursele economice ale bazinului său, *Dunărea este cel mai important fluviu european*. Deşi, ca lungime şi debit, este depăşită de Volga, Dunărea are avantajul de a străbate pe orizontală continentul european, din partea occidentală a acestuia până la Marea Neagră.

„Una din cauzele permanente ale războaielor din Europa din ultimele două secole a fost controlul egoist asupra căilor de navigație europene. Vorbesc despre Dunăre, despre strâmtorile Mării Negre, despre Rin, despre canalul de la Kiel şi despre toate căile de navigație interioară ale Europei care traversează două sau mai multe state” spunea la 9 August 1945, după Conferința de la Potsdam, preşedintele Truman.

[1] Alecsandru C. Sobaru, Gabriel I. Năstase, Chiriac Avădanei-coordonatori, *Artera navigabilă Dunăre-Main-Rhin. Strategii europene orizont 2020*, Bucureşti, Editura Economică, 1998, cap.6 – prof. univ. dr. Florina Bran, lector univ. Mihai Oprițescu, pag. 99-105.

Considerăm că istoria frământată a Europei a fost strâns legată de regimul juridic al Dunării, iar tabla de şah a jocurilor intereselor politico-diplomatice şi economice a reflectat întotdeauna problemele Dunării. Şi cum fluviul Dunărea nu este o simplă cale de apă, ci o puternică bază pentru infrastructura oricăror interese, problemele sale trebuie pe deplin înțelese.

Un fluviu desparte şi uneşte în egală măsură, iar Dunărea constituie atât frontiera naturală a mai multor state europene, cât şi o excelentă, dar prea puțin folosită cale de navigație. Viziunea privind viitorul UE implică estomparea până la dispariție a frontierelor interne şi sporirea comunicării între țări şi regiuni. Dunărea are, astfel, vocația de a constitui coloana vertebrală a unei construcții macroregionale în care să se regăsească, în căutarea bunăstării comune, landuri, regiuni şi state din UE, alături de țări care nu aparțin sau încă nu aparțin Uniunii.

După 1990, eforturile de integrare europeană revin în actualitate, însă instabilitatea din Balcani, generată de dispariția Iugoslaviei, a făcut ca Dunărea să nu poată fi folosită pe deplin ca o axă a integrării europene. În condițiile politice de astăzi, există reale premise pentru ca Dunărea să asigure o integrare a țărilor din est în Uniunea Europeană. Aceasta ar permite o armonizare a economiei continentului, punând pe noi baze complementaritatea economică dintre Europa apuseană şi cea răsăriteană[2].

Dunărea traversează zone între care există puternice decalaje economice, dublate de o stare latentă de conflict. Se pot menționa spațiul ex-iugoslav şi ex-sovietic aflat în preajma gurilor de vărsare (Transnistria). Această fragilitate a mediului de securitate în zonă favorizează acțiunea factorilor şi a pericolelor de orice natură. Perpetuarea acestor conflicte aflate în proximitatea Dunării, soluțiile temporare şi limitate aduse unora dintre acestea, precum şi progresele lente ale extinderii organismelor europene au determinat consumarea şi, uneori, epuizarea posibilităților, respectiv capacităților comunității internaționale de soluționare a acestor conflicte, cu o plajă largă de cauze şi forme de manifestare, precum şi proliferării unor noi riscuri, amenințări şi pericole la adresa securității interne şi internaționale a statelor şi popoarelor din această parte a Europei.

---

[2] Reunificarea Germaniei, precum şi sfârşitul războiului din fosta Iugoslavie reprezintă factori favorabili pentru redefinirea rolului Dunării în Europa. Prin poziția sa geografică, statul german, traversat de Dunăre şi Rhin, cele două fluvii ale reunificării europene, se află în situația de placă turnantă în centrul continentului, în măsură să reia colaborarea şi cooperarea economică atât cu țările din răsăritul Europei, cât şi cu cele din zona Caucazului şi a Mării Caspice.

Din punct de vedere geografic, Dunărea are o poziție relativ egală față de Marea Nordului, Marea Baltică, Marea Adriatică şi Mediterană, vărsându-se în Marea Neagră care permite deschiderea unor căi de comunicație spre Asia Centrală. Aceste aspecte l-au determinat pe cunoscutul om de ştiință Grigore Antipa să afirme că „*Dunărea are o importanță şi un rol mondial*".

Dezvoltând ideile lui Antipa, se poate aprecia că Dunărea reprezintă astăzi un element esențial în strategiile economice care vizează atât ideea de integrare europeană, cât şi pe aceea, mai largă, de conexare la Europa a unor importante regiuni din Asia şi Orientul Apropiat[3].

Începând cu anul 1992, după finalizarea canalului Main-Dunăre, s-a realizat o nouă cale fluvială navigabilă cu o lungime de 3540 km care traversează pe diagonală Europa, de la Marea Nordului până la Marea Neagră.

În condițiile în care Uniunea Europeană parcurge o etapă de redefinire a identității şi a coeziunii interne şi a necesității de a se afirma ca actor competitiv şi dinamic într-o lume în continuă globalizare, pe fundalul „digerării" celui de-al cincilea val al extinderii, început în 2004 cu zece state şi finalizat prin aderarea României şi a Bulgariei la 1 ianuarie 2007, acest complex poate fi un factor de dezvoltare economică şi de echilibru social. Aceasta deoarece Uniunea Europeană se află într-un proces de reconectare cu proprii cetățeni şi de recâştigare a susținerii acestora pentru proiectul politic european, pe baze care să corespundă preocupărilor lor, la începutul secolului XXI.

Contextul european de realizare a unei noi arhitecturi de securitate pleacă de la existența şi funcționarea euroregiunilor. Acestea dezvoltă o adevărată axă, care se suprapune şi generează un culoar de dezvoltare cu o lățime de 150-300 km format din: Bazinul Mării Nordului, Rin, Main, canalul Main-Dunăre, Dunărea (inclusiv Canalul Dunăre-Marea Neagră) şi Bazinul vestic al Mării Negre (care prezintă un interes european, zonal, regional şi național major de integrare, dezvoltare şi securitate).

În egală măsură, Uniunea Europeană caută răspunsuri credibile şi eficiente în vederea întăririi rolului său extern, pe fondul parteneriatului, dar şi al competiției strategice cu SUA şi statele din Asia. Uniunea Europeană trebuie să facă față provocării de a se adapta permanent schimbărilor generate de o serie de factori, atât interni (extinderea, îmbătrânirea şi scăderea populației, necesitatea adaptării instituțiilor Uniunii, eficiența,

[3] Alecsandru C.Sobaru ş.a., *op.cit.*, pp.134-141.

transparența şi legitimitatea deciziei la nivel comunitar, comunicarea cu proprii cetățeni), cât şi externi (criza economico-financiară mondială, criza resurselor naturale şi de materii prime, competiția venind din partea celorlalți poli de putere şi nu numai, amenințarea teroristă, instabilitatea politică din statele Africii de Nord, amenințări care țin de mediul înconjurător, cum ar fi schimbările climatice, dezastrele naturale, pandemii etc.).

La interferența intereselor economice, dar şi politice, Dunărea reprezintă astăzi un punct cheie pentru Alianța Nord Atlantică facilitând accesul la regiunea extinsă a Mării Negre.

În acest context, Complexul Marea Nordului – Rin – Main – Dunăre – Marea Neagră poate constitui un mijloc favorizant al dezvoltării economice şi de grăbire a integrării statelor din estul şi sud-estul Europei în structurile europene şi euroatlantice. Importanța complexului este dată de factorul economic, în principal, dar nu trebuie neglijată nici valoarea acestuia ca aliniament şi direcție strategică, incluzând rolul afluenților, al sistemelor hidrotehnice, al canalelor şi lucrărilor de artă aferente.

Racordarea zonei economice a Mării Negre la interesele Uniunii Europene determină un sistem de cooperare şi alianțe. În acest mod se pot asigura: creşterea siguranței şi stabilității în zonă, conjugarea intereselor economice ale statelor şi eliminarea decalajelor de dezvoltare existente. Drept urmare, acest complex fluvio-maritim are o importantă dimensiune strategică şi de cooperare în Europa deoarece permite atât conectarea complexă la spațiul pan-european prin trasee economice şi de asigurare a securității regionale, cât şi dezvoltarea cooperării regionale pe mai multe axe fixate pe acest culoar de transport.

Rinul şi Dunărea constituie, în prezent, factorii integratori în amplul şi complexul proces de multiplicare a relațiilor dintre țările riverane şi celelalte țări ale continentului european, proces care reprezintă un factor dinamiza-tor al extinderii Uniunii Europene.

Prin deplasarea centrului de greutate spre Europa Centrală şi de Sud-Est, determinată de procesul de construcție a Uniunii Europene, putem afirma că şi din punct de vedere al securității apare o translatare a centrului de greutate acesteia pe axa danubiano-pontică, fapt ce ne îndreptățeşte să identificăm o nouă valoare a securității europene: securitatea dunăreană.

Transformările care conduc la actualii parametri ai acestui areal de securitate trezesc un interes major pentru statele riverane şi nu numai.

Uniunea Europeană, în realizarea tradiționalei strategii germane „Ostpolitik", adică pătrunderea pe continentul asiatic prin subordonarea

Europei Centrale şi, mai ales a ţărilor dunărene (lucru care s-a realizat în mare măsură), încearcă realizarea unui control al zonei. Prin axa danubiano-pontică, Uniunea Europeană doreşte să menţină controlul şi supremaţia „drumului mătăsii" şi a axei energetice euroasiatice. NATO va urmări şi se va implica în promovarea păcii şi securităţii[4] în regiune, interesele de securitate ale NATO putând fi afectate de alte riscuri de natură mai largă, incluzând actele de terorism, sabotajul şi crima organizată, precum şi întreruperea de fluxuri energetice vitale.

Arealul statelor fluvio-maritime Dunăre – Marea Neagră generează şi va genera strategii geopolitice, geostrategice şi geoeconomice cu implicaţii în sfera securităţii zonale şi a dezvoltării proiectelor energetice şi comerciale vitale Uniunii Europene. Pentru statele care nu se află în acest areal, accesul la axa ponto-danubiană se poate realiza prin reţele de canale navigabile conectate la sistem sau prin dezvoltarea reţelelor multimodale de drumuri şi căi ferate.

În viitor, partenerii euroatlantici au obligativitatea recunoaşterii statelor importante regăsite pe axa ponto-danubiană, ca actori geopolitici importanţi, în acest sens având rolul bine stabilit de a genera o reprezentare geostrategică bine conturată şi o mai mare fermitate în implicarea acestor state în proiectele generate.

2. Complexul strategic Dunăre-Main-Rhin – axă şi centru de greutate al securităţii europene:

Complexul Marea Nordului-Rin-Main-Dunăre-Marea Neagră este un ansamblu de construcţii hidrotehnice, cu funcţii deosebite, amplasate de-a lungul a două mari fluvii ce traversează Europa, alcătuind o cale navigabilă care străbate continentul de la nord la sud pe teritoriul a unsprezece state şi leagă Marea Neagră de Marea Nordului. Acest complex are ca elemente de bază fluviile Dunărea şi Rin, conexate prin intermediul canalului Dunăre-Main, fluvii care se varsă unul în Marea Neagră (prin gurile naturale ce alcătuiesc Delta Dunării şi prin canalul Dunăre-Marea Neagră), altul în Marea Nordului (prin gurile ce alcătuiesc Delta Rinului).

Complexul Marea Nordului-Rin-Main-Dunăre-Marea Neagră este de o importanţă majoră în sistemul european al căilor navigabile interioare şi această situaţie nu se va schimba nici în viitor. În prezent, cu excepţia a trei

[4] The Alliance Strategic Concept, NATO Office of Information and Press, 1999, p. 8.

state riverane, Serbia, Republica Moldova şi Ucraina, toate statele străbătute de componentele complexului sunt membre ale Uniunii Europene, ceea ce asigură condiţii bune pentru a se investi în această cale navigabilă pentru a o transforma într-o coloană vertebrală a Europei pe deplin funcţională.

Integrarea se constituie în principala modalitate de realizare a Uniunii Europene. Ea reprezintă un proces foarte complex prin care statele edifică o nouă comunitate ce se doreşte a fi de tip unitar, monolitic. Integrarea europeană nu este, deci, o simplă alăturare a părţilor, ci o nouă construcţie ce se realizează prin fuzionarea părţilor. Problema cea mai acută care se pune – cel puţin în această etapă – este dacă părţile rămân entităţi sau doar componente ale unei entităţi. Cu alte cuvinte, Europa Unită va fi o entitate de entităţi sau pur şi simplu o entitate. Răspunsurile la această întrebare împart europenii în două. Unii văd o Europă fără frontiere, fără state politice, adică o Europă a regiunilor, o Europă federală, alţii consideră că bătrânul nostru continent trebuie să devină o Europă a statelor, adică o entitate de entităţi.

Mediul de securitate la începutul mileniului III este caracterizat, în principal, de următoarele tendinţe majore[5]: accelerarea proceselor de globalizare şi de integrare regională, concomitent cu persistenţa unor acţiuni având ca finalitate fragmentarea statală, convergenţa rezonabilă a eforturilor consacrate structurării unei noi arhitecturi de securitate, stabile şi predictibile, însoţită de accentuarea tendinţelor anarhice în unele regiuni, revigorarea eforturilor statelor vizând prezervarea influenţei lor în dinamica relaţiilor internaţionale, în paralel cu multiplicarea formelor şi creşterea ponderii intervenţiei actorilor nestatali în evoluţia acestor relaţii.

La nivel european, mediul de securitate a fost puternic influenţat de încetarea *războiului rece* şi de modificările ce i-au urmat în planul reconfigurării frontierelor unor state. Pe această linie se înscrie căderea Zidului Berlinului în 1989, iar apoi reunificarea paşnică a Germaniei în 1990. Procesul a continuat cu destrămarea URSS în 1991 şi a RSF Iugoslavia. Ca urmare a acestor procese, Europa s-a îmbogăţit cu noi concepte de securitate mai diferite prin eficienţa lor şi mai exigente, au apărut noi actori, state în căutarea unor identităţi. S-a modificat astfel orientarea politică a unor state ce au ales economia de piaţă, s-au reconfigurat sferele de influenţă, apărând noi vulnerabilităţi şi conflicte, active sau înghetate, cu noi riscuri şi ameninţări la adresa naţiunilor şi a popoarelor europene.

---

[5] Cf. Manolache, Mihai, Riscuri şi vulnerabilităţi la adresa securităţii energetice în regiunea Mării Negre, Gândirea Militară Românească, nr. 3, iunie 2009, Bucureşti, p. 51.

În Zona Centrală şi Sud-Est Europeană mediul de securitate a cunoscut în cei din urmă ani cele mai ample schimbări din ultimii cincizeci de ani. Dezvoltarea acestuia este strâns legată atât de evoluţiile din Europa şi Asia, cât şi de cele din spaţiul transatlantic.

În această perioadă, caracteristicile principale ale mediului de securitate în zona Centrală şi Sud-Est Europeană se pot descrie astfel:

o menţinerea şi extinderea unor zone cu grad ridicat de risc; existenţa unor crize negestionate suficient, fapt ce amplifică pericolul reizbucnirii acestora sau al apariţiei altora noi;

o persistenţa sau escaladarea unor dispute interne care pot degenera în conflicte cu tendinţe clare de internaţionalizare;

o perpetuarea şi încurajarea unor revendicări teritoriale şi a curentelor de autonomie a unor comunităţi etnice, religioase sau culturale;

o extinderea ariei de influenţă şi de existenţă a fundamentalismului islamic, cu componenta sa radicală, ceea ce amplifică instabilitatea ariei balcanice;

o tendinţe de refacere a vechilor sfere de influenţă sau de a deveni lider zonal manifestate de unele state din zona ori din aria adiacentă;

o existenţa în apropiere a unor zone de instabilitate ca: Orientul Mijlociu, statele desprinse din fosta Iugoslavie, Caucazul ori Transnistria;

o apariţia riscurilor şi ameninţărilor nonmilitare, cu efecte negative asupra securităţii naţionale, cum sunt crima organizată, traficul de droguri, armament ori materiale strategice, migraţia ilegală de persoane;

o lărgirea, amplificarea şi diversificarea eforturilor unor state din zonă de integrare în structurile europene şi euroatlantice de securitate şi economice.

Spaţiul Complexului Marea Nordului-Rin-Main-Dunăre-Marea Neagră reprezintă punct de interes pentru Marile Puteri, indiferent de modul în care acestea consideră că trebuie să acţioneze pentru realizarea propriilor interese.

Relaţiile europene au cunoscut o evoluţie diferită în zonele străbătute de Complex. Asfel, dacă în zona Europei de Vest străbătute de Rin şi Main, mărginită de Marea Nordului, după convulsiile produse de cel de-al II-lea Război Mondial acestea s-au stabilizat prin infiinţarea unor organisme şi organizaţii de cooperare economică, politică şi militară, spaţiul dunărean şi cel al Mării Negre a cunoscut o lungă perioadă în care, atât în relaţiile dintre statele din blocul comunist din zonă, cât şi în relaţiile lor cu alte state de pe acest culoar european, au evoluat în funcţie de interesele URSS. În ultima

perioadă, după destrămarea blocului comunist s-a constatat o evoluție pozitivă a relațiilor internaționale constituite în acest spațiu, de la forme rudimentare la forme complexe de cooperare, fără de care acesta nu ar avea identitate proprie.

La interferența intereselor economice, dar şi politice, Dunărea reprezintă astăzi un punct cheie pentru Alianța Nord-Atlantică constituind facilitarea accesului la Regiunea Extinsă a Mării Negre din interiorul zonei, precum şi pentru reprezentarea geopolitică a Uniunii Europene. În acest sens, s-au exercitat într-o primă fază eforturi comune de natură economică, politică, militară, socială şi a mediului ambient, pentru ca, mai apoi, să se caute soluții pentru dezvoltarea regională în contextul globalizării.

Inițial ideea construirii canalului Rin – Main – Dunăre a încercat să traseze o linie de demarcare chiar în inima Europei, pentru ca ulterior această linie să atragă atenția asupra unei idei simple şi evidente: acest Complex este în Europa, iar cooperarea şi colaborarea regională trebuie extinse la nivelul întregii Europe din şi pentru realizarea conceptului de globalizare.

Dunărea şi Rinul nu sunt doar fluvii europene. Legate prin canalul Rin-Main-Dunăre, ele constituie o adevărată coloană vertebrală, de-a lungul căreia s-a dezvoltat un model de convieţuire bazat pe respectul diversității, civism şi multiculturalism, care poate contribui decisiv la construirea Europei unite. El poate constitui un mijloc favorizant al dezvoltării economice şi de grăbire a integrării statelor din sudul şi sud-estul Europei în structurile europene şi euroatlantice. Importanța axului este dată de factorul economic, în principal dar nu trebuie neglijată nici valoarea acestuia ca aliniament şi direcție strategică, incluzând rolul afluenților, al sistemelor hidrotehnice, al canalelor şi lucrărilor de artă aferente. Racordarea Uniunii Europene cu zona economică a Marii Negre determină un puternic sistem de cooperare şi alianțe. În acest mod se pot asigura creşterea siguranței şi a stabilității în zonă, conjugarea intereselor economice ale statelor şi eliminarea decalajelor de dezvoltare existente. Controlul Dunării şi a conexiunii sale cu Marea Neagră a însemnat şi înseamnă acces la piețe şi surse de materii prime, dar şi ținerea sub observație a unor zone cunoscute a fi gazdă şi, totodată, centre de expansiune a instabilității şi crizelor. Prin cooperare dunăreană se poate diminua efectul factorilor de risc.

Prin perspectivele politice şi economice pe care le deschide, cooperarea danubiană, în cadrul unei regiuni dunărene, mai mult sau mai

puțin formale, mai mult sau mai puțin insituționalizate, se poate constitui într-o structură esențială a Europei unite şi a lumii globalizate de mâine.

În prezent prin dezvoltare, țările care beneficiază de „curs al Dunării" sunt tot mai integrate putând afirma rolul de factor integrator al complexului strategic, ce se constituie în vector pentru resurse şi dezvoltare.

Un alt argument în susținerea importanței complexului ca axă şi centru de greutate al securității europene îl constituie şi elementele teoriei zonei pivot, dezvoltată la începutul secolului trecut de Halford Mackinder, fost decan al Facultății de Ştiințe Economice şi Politice din Londra şi vicepreşedinte al Societății Regale de Geografie. În 1919 el publică lucrarea „Democratic Ideals and Reality" în care abordează într-un mod cu totul nou lumea. El operează cu noțiuni ca: Oceanul Planetar, Insula Mare a Lumii (formată din Eurasia şi Africa), renunțând practic la împărțirea planetei în oceane şi continente. Oceanul Planetar reprezintă 3/4 din suprafața globului şi era dominat la vremea respectivă de Marea Britanie (care deținea supremația oceanică). Din această cauză, teoriile sale vor viza în special zona de uscat, adică Insula Mare a Lumii, pentru ca vastele resurse ale acesteia să fie controlate tot de către această mare putere. Autorul consideră că Africa face parte din Insula Mare a Lumii datorită faptului că ea este perfect unită cu Asia (Canalul de Suez fiind făcut de om) şi aproape unită la strâmtorile Gibraltar şi Bab-el-Mandeb cu Europa. Având în vedere faptul că Insula Mare a Lumii deținea 2/3 din suprafața uscatului, că aici trăia majoritatea populației globului şi că în plus cele mai mari bogății naturale se găseau tot aici, este de la sine înțeles de ce autorul elaborează un program de stăpânire a acestei zone. Din nefericire, din cauza condițiilor istorice (sfârşitul Primului Război Mondial, din care Anglia ieşise învingătoare) Mackinder nu a trezit interesul compatrioților săi, dar scrierile sale au avut un impact deosebit în Germania (care a văzut în ele o modalitate de a-şi câştiga supremația pierdută în război).

Mackinder vorbeşte despre heartland (inima lumii) care, după el, ar fi zona cuprinsă între Europa de Est (din Munții Urali sau de la Caspică şi Volga) şi Oceanul Pacific. Această zonă pivot este bogată în resurse naturale şi deține o poziție-cheie în ceea ce priveşte comunicarea între diferitele regiuni ale globului. Inner (marginal) crescent reprezintă frontonul maritim alcătuit de statele care sunt situate în interiorul continentului, dar care au acces la Oceanul Planetar (Germania, Turcia, India, China). Outer (insular) crescent sunt statele care sunt exterioare zonei pivot (Marea Britanie, Africa de Sud, Japonia). Având în vedere toate acestea, autorul stabileşte trei

condiții pentru dominarea lumii: „Cine stăpânește Europa de Est, stăpânește heartland; Cine stăpânește heartland, stăpânește Insula Mare a Lumii; Cine stăpânește Insula Mare a Lumii, stăpânește lumea". Teoria s-a născut din temerile autorului față de pericolul provenit dintr-o eventuală aliere a statelor din Europa de Est și din zona pivot: Germania, Rusia și China. Tot el este cel care a sesizat că între Germania și Rusia nu există bariere naturale importante, fapt pentru care o eventuală expansiune a Germaniei în Est este foarte posibilă.

Din perspectiva multipolarității, putem să privim edificarea Uniunii Europene, proiect inițial bazat pe motorul franco-german, ca alianță între o putere maritimă (Franța[6]) și una continentală (Germania) ca pe o încercare a puterilor europene de a realiza o uniune politică de durată între ele, cu scopul de a forma un centru de putere politică și economică identificabile pe scena internațională a secolului XXI și nu numai atât, unul capabil să influențeze această scenă politică în interesul său.

Pentru Uniune și implicit, pentru interesul vestic (Franța, Germania), esențial este să-și asigure o Insulă-Lume (identificabilă de noi drept regiunea bogată energetic a Asiei Centrale[7]) monolitică, gestionabilă în modalitatea condominium (împreună cu Rusia) sau prin aderarea Rusiei la Uniune și crearea EuroRusiei, proiect asumat de altfel de candidatul la Președinția Rusiei, Vladimir Putin.

Ca perspectivă a creșterii importanței complexului ca axă și centru de greutate al securității europene, subliniem potențialul de creștere adus de viitoarea integrare în Uniunea Europeană a statelor din Balcanii de Vest.

Deși în ultimii 10 ani în Balcanii de Vest au fost înregistrați pași importanți în direcția reconcilieriii, urmările războiului – probleme teritoriale, crime de război, refugiați etc.-sunt încă resimțite și, în anumite condiții, potrivit multor analiști, prezintă încă riscuri. De aceea, statele din zonă, în special cele mai fragile, și-au pus speranțele în aderarea la Uniunea Europeană și la NATO pentru asigurarea stabilității și păcii în regiune, pentru consolidarea independenței, suveranității și identității naționale.

---

[6] Țară cu ieșiri largi la Marea Mediterană (în Sud-Est) și la Oceanul Atlantic (în Nord-Vest), în timp ce Germania are două mici ieșiri, în Nord, una spre Marea Baltică și una spre Marea Nordului, ceea ce ne face să o considerăm în principal o putere continentală (de altfel, ea este percepută astfel de majoritatea specialiștilor în geopolitică).

[7] Paul Claval – *Geopolitică și geostrategie, spațiul și teritoriul în sec. al XX-lea*, trad. Elisabeta Maria Popescu, Ed. Corint, București, 2001, p. 47-48; 52-53.

După cum se cunoaşte, integrarea în Uniunea Europeană presupune nu numai reformarea sistemului politic, militar, economic, juridic, adaptarea la normele Uniunii, ci şi rezolvarea prealabilă de către fiecare stat candidat a tuturor problemelor pendinte, de risc, în raporturile cu alte state din zonă, în special cu vecinii.

Fără îndoială, dacă pe plan mondial nu intervin evenimente politice grave care să modifice echilibrul actual de forţe şi construcţiile politice ce-l susţin, integrarea, cel puţin în Uniunea Europeană, a statelor din Balcanii de Vest va fi realizată.

Ţara noastră poate participa mai activ la consolidarea unui mediu favorabil stabilizării regiunii, poate reprezenta un exemplu şi un îndemn pentru continuarea reformelor în Balcanii de Vest, sporirea prosperităţii şi stabilităţii, intensificarea dialogului regional.

Prin poziţionarea sa geografică complexul a fost şi rămâne o rută importantă de transport. Din perspectiva viitorului apropiat şi ţinând cont de importanţa crescândă a Dunării ca arteră de transport, ar fi oportună realizarea unor reţele de canale, care să ducă la apariţia unor noi căi europene de comunicaţie navală, cum ar fi Dunăre-Sava-Marea Adriatică, Dunăre-Morava-Vardar, care să îi sporească rolul de coloană vertebrală a cooperării pe multiple planuri între ţările riverane şi între statele Europei în general.

Ca urmare, perspectiva racordării bazinelor hidrografice ale Savei, Dravei şi Moravei la complex, creează pentru acesta noi axe de legătură.

3. Introducerea securităţii dunărene în opţiunea de securitate şi apărare europeană zonală, regională şi naţională

Opţiunea de securitate a acestui complex trebuie să fie însoţită şi de o opţiune pentru apărare: responsabilitate UE pentru securitatea complexului şi NATO pentru apărare.

Actuala arhitectură de securitate europeană reflectă trăsăturile esenţiale ale mediului geopolitic în care se derulează: tranziţia către sistemul internaţional multipolar, competiţia între puteri în spaţiul euroatlantic pentru redistribuirea rolurilor; adâncimea integrării în UE; tentativele Federaţiei Ruse de a menţine statutul de mare putere pe arena mondială şi de a ocupa poziţii-cheie în structurile europene de securitate.

Securitatea se bazează atât pe stabilitatea politică, cât şi pe cea militară, acestea fiind condiţionări complementare. Un sistem mobil de securitate europeană va putea fi edificat numai dacă vor fi consolidate cele două

componente. O politică de securitate bazată pe cooperare (specifică OSCE) şi renunţarea la orice idee de a impune stabilitatea prin mijloace de confruntare. Scopul este promovarea cooperării în vederea prevenirii conflictelor în sfera politică şi a reducerii pericolului confruntării armate. De asemenea, mai are scopul de a evita escaladarea potenţialelor conflicte, punând un accent deosebit pe promovarea deschiderii şi a transparenţei.

Protecţia strategică a ansamblului în cadrul UE şi NATO se realizează prin următoarele modalităţi:

o prin grija factorului politico-militar naţional – care elaborează strategii pentru funcţionarea, dezvoltarea şi apărarea complexului;

o prin beneficiile protecţiei oferite de bazele şi obiective militare existente în apropiere – categoriile de forţe amplasate în proximitate complexului, atât cele NATO, cât şi cele naţionale, sunt în măsură să asigure o apărare eficientă a elementelor vitale ale acestuia;

o prin măsuri de protecţie antiteroristă ale poliţiei complexului, derulate pe fiecare segment naţional al acestuia;

o prin protecţia proprie a obiectivelor fluviale ce îşi desfăşoară activitatea în complex – protecţie asigurată cu forţe proprii, ori angajate;

o prin protecţia satelitară oferită de NATO şi prin servicii prestate de către SUA şi Rusia. În acest scop sunt folosiţi sateliţi geostaţionari, de rotaţie şi de însoţire.

La nivel naţional, pentru fiecare segment, forţele de securitate ale complexului sunt conceptualizate, ori în bună parte, realizate. În prezent se poartă negocieri pentru realizarea unei forţe europene de securitate a complexului. La nivel naţional au fost elaborate:

- strategia de securitate a navigaţiei de-a lungul arterei;
- strategia de securitate a infrastructurii complexului;
- strategia de intervenţie antiteroristă;
- strategia de control a traficului.

Pentru securitatea de ansamblu a complexului rezolvarea trebuie să revină UE prin constituirea unor grupe acţionale terestro-aeriano-fluvialo-maritime, care să îndeplinească misiunile principale preluate de la factorul de securitate naţional.

În contextul impunerii valorii de securitate dunăreană ca parte a securităţii europene, considerăm că noua strategie de securitate a UE trebuie să aibă un capitol separat dedicat acesteia.

Odată cu aderarea la NATO, strategia de securitate a României reflectă modificările care au loc în mediul de securitate intern şi internaţional, realităţile şi tendinţele globale. Ea este parte integrantă a securităţii europene şi euroatlantice şi constituie un tot unitar fundamentat pe efort naţional, pe acţiune comună, cooperare şi parteneriat.

Securitatea naţională se asigură pri eforturi proprii şi prin cooperare cu aliaţii şi partenerii, în conformitate cu prevederile programelor naţionale, ale Strategiei de securitate a Uniunii Europene şi ale conceptelor strategice ale Alianţei. Ea vizează armonizarea eforturilor naţionale cu angajamentele internaţionale şi identificarea modalităţilor de lucru apte să prevină şi să contracareze oportun ameninţările. Eforturile vizează, totodată, promovarea democraţiei, păcii şi stabilităţii în vecinătate şi în alte zone de interes strategic, reducerea vulnerabilităţilor, dezvoltarea capabilităţilor naţionale şi transformarea profundă a instituţiilor de securitate.

Strategiile zonale de securitate generate în cadrul proceselor politice de cooperare în regiunea Dunării în Europa Centrală şi de Sud-Est precum Procesul de Cooperare Dunăreană, Pactul de Stabilitate din cadrul Procesului de Cooperare Dunăreană, Iniţiativa NATO pentru Sud-Estul Europei (SEEI), Pactul de Stabilitate pentru Europa de Sud-Est (PSSE), Acordul pentru prevenirea şi combaterea infracţionalităţii (Acordul SECI), Forţa Multinaţională de Pace din Sud-Estul Europei (MPFSEE), Acordul Central European al Comerţului Liber (CEFTA), Grupul Vişegrad (V4), Iniţiativa Central-Europeană (ICE) şi Iniţiativa de Cooperare Central-Europeană (CENCOOP) trebuie să-şi axeze conţinutul pe regiunea corespunzătoare din complex sau complementară complexului într-o armonizare cu noua componentă a securităţii europene, securitatea dunăreană.

România a susţinut şi va susţine întărirea capacităţii de acţiune comună a UE, NATO, OSCE şi Consiliului Europei în domeniul stabilizării regionale şi sporirea gradului de coordonare a implicării în soluţionarea problemelor din Balcani.

Complexul Marea Nordului-Rin-Main-Dunăre-Marea Neagră, deşi în condiţiile actuale geostrategice valoarea sa de obstacol s-a pierdut într-o mare măsură, are o valoare strategică deosebită pentru unele ţări europene nemaritime (Serbia, Ungaria, Austria, Slovacia) deoarece le permite accesul la Bosfor, Gibraltar sau Marea Nordului şi, de aici, la Oceanul Planetar. După scindarea Imperiului sovietic şi după schimbările intervenite în

Germania, de-a lungul său nu mai există zone de luptă, ci zone de legătură, în care cooperarea se amplifică pe multiple planuri.

Procesul de integrare în Uniunea Europeană a Balcanilor de Vest şi a Europei de Est va fi de o complexitate deosebită. Pentru realizarea cu succes considerăm că se impun iniţiative de securitate regională la Adriatică şi la Marea Neagră, racordate securităţii dunărene.

Securitatea, stabilitatea şi cooperarea regională se vor îmbunătăţi substanţial prin aplicarea cu fermitate de către întreaga comunitate de state din zonă a prevederilor Cartei relaţiilor de bună vecinătate, stabilitate, securitate şi cooperare în Europa de Sud-Est, adoptată de reuniunea şefilor de stat şi de guvern de la Bucureşti.

Pilon solid de stabilitate regională, ţara noastră acordă o foarte mare importanţă funcţionării eficiente a structurilor de cooperare politico-economică instituite, dialogului statelor membre ale Iniţiativei Central Europene (ICE), ale OCEMN, conferinţelor economice regionale, afirmării vocaţiei de integrare europeană a statelor regiunii, ca şi modului în care lucrează structurile militare regionale.

O Europă Centrală şi de Sud-Est puternic implicată în problemele securităţii şi stabilităţii continentului nu poate fi decât opera comună a tuturor statelor regiunii, inclusiv a României, ce realizează o coerenţă deplină între politici, strategii şi acţiuni.

Complexul Marea Nordului-Rin-Main-Dunăre-Marea Neagră poate constitui un mijloc favorizant al dezvoltării economice şi de grăbire a integrării statelor din estul şi sud-estul Europei în structurile europene şi euroatlantice, precum şi de antrenare a unor noi state în angrenajul cooperării internaţionale, pe măsura încadrării regiunii limitrofe axului în circuitul economic, cât şi geostrategice. Importanţa axului este dată de valoarea sa economică, dar nu trebuie neglijată nici valoarea sa ca aliniament şi direcţie strategică, care include rolul afluenţilor, sistemelor hidrotehnice şi al canalelor. Racordarea Uniunii Europene cu zona economică a Mării Negre determină un puternic sistem de cooperări şi alianţe. În acest mod se poate asigura creşterea siguranţei şi stabilităţii în zonă, conjugarea intereselor economice ale statelor, eliminarea decalajelor de dezvoltare existente.

Prin asigurarea securităţii şi prin promovarea unui climat de pace, prosperitate şi stabilitate şi prin realizarea securizării „Drumului Mătăsii”

se diminuează ameninţarea reprezentată de riscurile convenţionale şi neconvenţionale la adresa securităţii europene. Pentru a răspunde noilor riscuri şi ameninţări se impune un efort comun atât din partea statelor membre ale Alianţei Nord-Atlantice, cât şi din partea statelor aflate pe axa Europa-Asia. În general, statele din aceste regiuni împărtăşesc unele valori şi principii democratice şi au o istorie regională comună.

Rolul României ca beneficiar al unei mari părţi din complex şi mai ales din Dunăre, presupune iniţiativă de securitate dunăreană prin convocarea şi acordul ţărilor dunărene şi o strategie complexă în arealul Marea Neagră – Dunăre cu participarea actorilor interesaţi NATO, UE, Rusia, Turcia.

4. Concluzii

Complexul strategic Marea Nordului – Rin – Main – Dunăre- Marea Neagră creează o axă ce reprezintă „coloana" unui sistem geopolitic continental, care deschide drumul Uniunii Europene către Asia.

Complexul strategic Marea Nordului-Rin-Main-Dunăre-Marea Neagră poate lega polul înalt tehnologic occidental de polul resurselor rusesc generând un areal de integrare, dezvoltare şi securitate atractiv în cadrul procesului de globalizare.

În actualul context de securitate se impune conştientizarea importanţei securităţii dunărene în preocupările de securitate comună şi colectivă. Pentru atingerea acestui deziderat propunem activităţi susţinute prin media, dezbaterea subiectului în activităţi academice, în forumuri ştiinţifice desfăşurate la nivel naţional, regional şi continental, precum şi dezvoltarea unor proiecte cu finanţare din fonduri europene care să susţină studii pe această temă.

Iniţiativele de securitate dunăreană pe segmente zonale: occidentală, central-europeană şi sud-est europeană trebuie să realizeze conexiuni cu securitatea la Marea Negră şi Marea Nordului. Fiecare strategie va trebui să arate riscurile, ameninţările, interesele comune şi colective de securitate, scopul, resursele alocate, managementul şi să stabilească responsabilităţi.

Pentru deceniul al doilea al secolului XXI, considerăm necesară reconfigurarea securităţii europene pe trei piloni: euroatlantic, mediteranian şi dunărean.

Bibliografie:

1. Constantin Onişor, *Europa 27*, Editura A'99, Iaşi, 2008.
2. Teodoru Ştefan, Gheorghe Toma, Constantin Degeratu, Traian Liteanu, *Spațiul european sub impactul provocărilor globalizării*, vol. I şi II, Repere evolutive, dimensiuni, realizări, Editura ANI, Bucureşti, 2008.
3. Iulian Lăzărescu, Constantin Onişor, *Complex strategic de securitate europeană,* Editura ANI, Bucureşti, 2011.
4. Alecsandru C. Sobaru, Gabriel I. Năstase, Chiriac Avădanei-coordonatori, *Artera navigabilă Dunăre-Main-Rhin. Strategii europene orizont 2020*, Editura Economică, Bucureşti, 1998.
5. Gabriel Vlase, Constantin Onişor, „*Securitate în Europa de Sud-Est – Actualitate şi perspective strategice"*, Editura RAO, Bucureşti, 2010.
6. Paul Claval, *Geopolitică şi geostrategie, spațiul şi teritoriul în sec. Al XX-lea*, trad. Elisabeta Maria Popescu, Ed. Corint, Bucureşti, 2001.
7. Revista GeoPolitica nr. 39, *Axa Ponto-Danubiană – axă strategică,* Editura Top Form*,* Bucureşti, 2011.
8. Revista Gândirea românească nr. 3, Bucureşti , 2009.
9. Paul Dobrescu, Revista Geopolitica, Editura comunicare.ro, Bucureşti, 2003.

Uniunea Europeană – către un serviciu de informații european?

Gabriela TRANCIUC
Serviciul Român de Informații
e-mail: **gtranciuc@dcti.ro**

Abstract

Intelligence and security services, as main institutions that ensure strategic knowledge for decision makers, can capitalise on the cooperation with, the experience and expertise of the international partners in order to improve and enhance their analytical capacity, early warning and foresight. European and Euro-Atlantic organisations provide a multilateral framework for dialogue, consultations and cooperation on security issues, and their potential can be developed by extended information sharing, based on the comprarative advantages of each organisation.

The European Union is such an organisation, that developed in time intelligence dedicated structures to back up EU decision making, especially in crisis situations. If there is consensus on the necessity to cooperate on intelligence issues, shaping a common intelligence policy, with its subsequent tools, is still contentious, and the perspective of implementing such an initiative remains remote.

Keywords: intelligence, security, cooperation, policy, decision making, European Union

1. Introducere

Mediul de securitate actual se află în continuă schimbare şi prezintă surse de ameninţare şi insecuritate complexe, interdependente, difuze şi volatile. Niciun stat, în asigurarea securităţii naţionale, nu poate miza pe secluziune teritorială şi izolare. În protejarea intereselor şi valorilor naţionale, statele nu pot exclude certitudinea interconectării dimensiunilor externă şi internă a securităţii şi necesitatea cooperării şi a dezvoltării unor soluţii eficiente, prin solidaritate.

Serviciile de informaţii şi de securitate, în calitate de principale instituţii care asigură cunoaşterea strategică pentru factorii de decizie ai unui stat, pot valorifica, prin cooperare, experienţa, expertiza, capabilităţile

partenerilor internaționali, ceea ce poate contribui la consolidarea capacității proprii de analiză şi avertizare strategică. Organizațiile europene şi euroatlantice oferă un cadru multilateral de consultări, dialog şi cooperare pe probleme de securitate, iar potențialul acesteia poate fi consolidat, prin îmbunătățirea schimbului analitic şi asigurarea sinergiei civil-militare, luând în considerare avantajele comparative ale fiecărei organizații.

Uniunea Europeană este o astfel de organizație, care a dezvoltat în timp structuri dedicate de intelligence pentru sprijinirea procesului decizional european, în special în situații în care se impune un răspuns al UE la crize. Odată cu intrarea în vigoare a Tratatului de la Lisabona (Tratatul privind Funcționarea Uniunii Europene - TFEU), care aduce la nivelul Uniunii atât transformări structurale (noi instituții), cât şi funcționale (noi concepte, atribuții, procese), se constată la nivelul UE sporirea presiunii pentru furnizarea de produse de intelligence de calitate şi în timp real. Ca urmare, creşte presiunea spre o mai bună ancorare a serviciilor de informații ale statelor membre în cadrul european.

În acest context, în diverse medii (academice, politice etc.) este dezbătută problematica dezvoltării unui serviciu de informații al UE, această idee nefiind complet respinsă de oficialii europeni. Dacă există un consens al statelor europene asupra necesității cooperării în domeniul intelligence, controversele privind dezvoltarea unei „politici comune de intelligence”[1], cu instrumentele sale subsecvente, nu au fost încă depăşite, iar perspectiva acceptării acestei inițiative de către majoritatea statelor membre rămâne îndepărtată.

Pornind de la schimbările instituționale comunitare pe care Tratatul de la Lisabona le aduce, cu implicații asupra cooperării cu serviciile europene de informații şi securitate, această lucrare îşi propune să analizeze argumentele care susțin sau pun sub semnul întrebării necesitatea creării unui serviciu de informații european în sens clasic, concluzionând că Uniunea Europeană nu ar trebui să vizeze implementarea unei astfel de inițiative, ci să urmărească dezvoltarea unei capacități solide de analiză strategică şi avertizare timpurie care să ofere fundamentul informativ pentru procesul decizional la nivel comunitar.

---

[1] Baker, Charles, *The Search for a European Intelligence Policy,* http://www.fas.org/irp/eprint/baker.html

2. Evoluții instituționale comunitare post-Lisabona

Odată cu crearea Politicii Europene de Securitate şi Apărare – PESA (1999), UE a dezvoltat structuri şi procese de intelligence care gestionează informațiile oferite de statele membre prin intermediul serviciilor civile (către Centrul de Situații – SITCEN[2]) şi militare (către Statul Major al UE, Direcția Intelligence – Dir Intell EUMS). Momente cheie în dezvoltarea acestor structuri au fost: integrarea în SITCEN a experților detaşați din serviciile de securitate care au adus o expertiză valoroasă în domeniul terorismului (2005); consolidarea cooperării dintre SITCEN şi Dir Intell EUMS, prin crearea unor grupuri mixte de analiză (Single Intelligence Analysis Capacity, 2007); întărirea capacității de sprijin în procesul de planificare pentru misiunile şi operațiile PESA (2008)[3].

Accentul în cadrul UE este plasat pe schimbul de informații şi analize strategice, pe termen lung, cu funcție de alertă timpurie. Nu a fost prevăzut ca UE să dispună de o capacitate independentă de colectare a informațiilor în sensul clasic (HUMINT sau SIGINT). Singura capacitate de colectare de care dispune UE este Centrul Satelitar (EUSC)[4], precum şi utilizarea informațiilor din surse deschise.

Procesele şi structurile de intelligence UE au suferit modificări importante în special în contextul implementării Tratatului de la Lisabona. Intrarea în vigoare a acestui tratat (1 decembrie 2009[5]) a schimbat perspectiva instituțională comunitară, generând implicații pentru organizarea şi funcționarea organismelor europene, atribuțiile acestora şi, implicit, a mecanismelor decizionale, cu relevanță asupra intereselor statelor membre.

Prevederile Tratatului nu afectează în mod direct activitatea serviciilor de informații, securitatea rămânând responsabilitatea exclusivă a

---

[2] Centrul a funcționat până în 2011 în cadrul Secretariatului Consiliului UE, ca departament de analiză şi evaluare a posibilelor surse de amenințare la adresa Uniunii Europene.

[3] Eisl, Gunter, „Analiza strategică a informațiilor ca instrument al politicii externe. Spre un serviciu de informații al UE?", conferință la Academia Diplomatică Europeană, 2 mai 2011, Bruxelles.

[4] Centrul nu dispune de capabilități tehnice proprii (sateliți), informațiile fiind obținute prin contractare sau prin cooperare cu statele membre, avantajele centrului constând în expertiza şi analizele pe care le poate pune la dispoziția structurilor UE şi a statelor membre.

[5] Uniunea Europeană, *The Treaty at a Glance,* http://europa.eu/lisbon_treaty/glance/index_en.htm

statelor membre (conform art. 4.2 TFEU[6]), dar anumite modificări pot influența procesul de schimb de informații atât în cadrul UE, cât şi în relația cu serviciile secrete europene.

2.1. Modificări structurale

Noul tratat al UE prevede unificarea pilonului I (Comunitatea Europeană) cu pilonul al III-lea (Cooperarea polițienească şi judiciară în materie penală, cunoscut ca JAI)[7] şi crearea unor noi instituții de execuție (structuri permanente) şi de decizie (comitete)[8].

Noul Tratat prevede renunțarea la sistemul preşedinției semestriale rotative la nivelul Consiliului European (CE) şi înlocuirea acestui sistem, prin crearea unor poziții de rang înalt: preşedintele (permanent) Consiliului European[9] şi **Înaltul Reprezentant al UE pentru afaceri externe şi politica de securitate** (asimilabil unui „ministru de externe al UE")[10].

În sprijinul activității Înaltului Reprezentant a fost creat **Serviciul European pentru Acțiune Externă (SEAE)**, operațional din ianuarie 2011. Un serviciu autonom în termeni de buget şi personal (care provine de la Secretariatul General al Consiliului UE/SecGen, Comisia Europeană/COM şi prin contribuții naționale temporare ale statelor membre), acesta include pe lângă directoratele generale, împărțite pe spații geografice (*geographical desks*), birouri tematice şi pe problematici multilaterale (*multilateral and thematic desks*), Statul Major al UE, alături de structuri care asigură capacitatea de planificare, conducere a operațiilor civile şi de gestionare a crizelor, precum şi **Centrul de Situații (SITCEN)** – considerat în prezent singurul punct de intrare al produselor de intelligence în instituțiile UE[11].

---

[6] Uniunea Europeană, *The treaty of Lisbon,* http://europa.eu/lisbon_treaty/full_text/index_en.htm

[7] asupra cărora deciziile sunt adoptate prin majoritate calificată, procedura unanimității fiind menținută doar la nivelul pilonului II – Politica Externă şi de Securitate Comună/PESC.

[8] Deşi Tratatul cuprinde mai multe modificări, prezenta lucrare nu va face referire decât la aspectele relevante pentru tema aleasă.

[9] cu un mandat de doi ani şi jumătate, ales prin procedura majorității calificate de către CE, având posibilitatea de a fi reales o singură dată. Pentru această poziție a fost ales fostul premier belgian, Herman van Rompuy.

[10] care deține şi funcția de vicepreşedinte al Comisiei Europene (COM), numit de CE, cu acordul Preşedintelui COM şi aprobarea Parlamentului European. Pentru această funcție a fost desemnată baroneasa Catherin Ashton (Marea Britanie).

[11] O'Sullivan, David, *Setting Up the EEAS,* IIEA, Dublin, 14 ianuarie 2011, http://www.eeas.europa.eu/speeches/2011_1201_dos_iiea_en.pdf

Rolul SITCEN, care nu dispune de capacitate proprie de culegere de informații, este de a monitoriza permanent situația internațională, de a transmite alerte timpurii şi de a oferi informații utile pentru gestionarea crizelor, precum şi de a elabora analize strategice şi evaluări ale situațiilor de criză pe baza tuturor tipurilor de informații (civile şi militare – materiale analitice, imagini satelitare – EUSC, OSINT, rapoarte diplomatice, rapoarte ale reprezentanților sau misiunilor UE, operații PESA, agenții europene – Europol, Frontex, institute de cercetare)[12].

Constituirea SEAE, din perspectiva sprijinirii Înaltului Reprezentant în activitatea de politică externă a UE, implică sporirea cerințelor de intelligence, inclusiv prin integrarea resurselor statelor membre.

SITCEN poate fi considerat un „UE intelligence analysis hub", iar în vederea întăririi acestui rol va trebui să-şi orienteze responsabilitățile pe câştigarea şi menținerea încrederii serviciilor de informații ale statelor membre, creşterea credibilității prin reacții rapide la situații de interes pentru UE, precum şi constituirea unei rețele cât mai largi de analişti. De asemenea, o componentă esențială a activității SITCEN o reprezintă crearea unei punți de legătură între serviciile interne şi externe.

Transformarea **Europol** în agenție europeană cu buget comunitar (începând din ianuarie 2010) a determinat creşterea rolului acesteia la nivel comunitar, mai ales în ceea ce priveşte schimbul de informații.

Europol deține un rol esențial în sprijinirea eforturilor statelor membre de combatere a terorismului şi a criminalității organizate. Agenția deține atât o componentă operațională importantă, cu baze de date extinse, precum şi o componentă analitică semnificativă pe domeniul contraterorismului şi al criminalității organizate[13].

Prin intrarea în vigoare a Tratatului de la Lisabona, Europol devine principala agenție de aplicare a legii UE şi deținătorul principal de informații referitoare la infracțiuni (*criminal information*). Europol a dobândit treptat competențe sporite în domeniul intelligence, inițial resursele informaționale provenind din surse deschise (OSINT). Este de aşteptat ca Europol să continue „presiunile" în direcția colectării de informații şi intelligence (cu precădere *criminal intelligence*), dar, în mod predictibil, acestea vor viza şi dimensiunea prevenirii şi combaterii

[12] Cross, Maia K. Davis, *EU Intelligence Sharing and the Joint Situation Center: A Glass Half-Full,* 2011 Meeting of the European Union Studies Association, 3-5 martie 2011, http://www.euce.org/eusa/2011/papers/3a_cross.pdf

[13] Uniunea Europeană, Europol – http://europol.europa.eu

terorismului, cel puţin a infracţiunilor conexe terorismului, ceea ce va pune în dificultate cooperarea cu serviciile de informaţii care nu au atribuţii de aplicare a legii.

În ceea ce priveşte structurile de decizie ale UE a fost înfiinţat un nou comitet pentru securitate internă – **COSI**. Deşi încă insuficient conturate, responsabilităţile COSI includ exercitarea controlului, respectiv a coordonării activităţilor relevante pentru realizarea securităţii interne a spaţiului comunitar. Articolul referitor la constituirea acestui comitet este formulat de o manieră evazivă ("*Un comitet permanent va fi înfiinţat în cadrul Consiliului pentru a asigura că cooperarea operativă în domeniul securităţii interne este promovată şi întărită în cadrul Uniunii. ...va facilita coordonarea activităţilor autorităţilor competente din cadrul statelor membre"*- Art. 71 TFEU), iar ambiguitea conceptului de „securitate internă" ridică probleme pentru activitatea de informaţii pentru securitate, în condiţiile în care acest concept se poate referi şi la „securitatea naţională" (în dezacord cu art. 4.2 al TFEU).

2.2. Modificări conceptuale

Dezvoltarea noilor ameninţări care nu mai cunosc graniţe au determinat în cadrul UE nu numai transformări ale arhitecturii instituţionale, dar şi promovarea unui cadru strategic şi conceptual nou. Se resimte tot mai accentuat nevoia consolidării cooperării în vederea combaterii ameninţărilor transfrontaliere (în special terorismul) la nivel comunitar. Alături de documentele strategice deja existente (Strategia de Securitate Europeană, Programul Stockholm), a fost finalizată **Strategia de Securitate Internă**.

Noul concept de „**securitate internă**" a generat controverse, având în vedere ambiguitatea termenului. Nu este clar dacă acesta se referă la „securitatea internă a UE" şi/sau la „securitatea internă, respectiv naţională a statelor membre" şi dacă există – în viziunea comunitară – o diferenţă între cele două concepte. Deşi Tratatul de la Lisabona oferă asigurări asupra gestionării exclusive a securităţii naţionale de către statele membre, nu există o definiţie clară a termenului de „securitate internă" în documentele oficiale ale UE. De exemplu, securitatea internă s-ar putea referi la situaţiile în care un atac terorist sau alte tipuri de ameninţări afectează simultan mai multe state europene şi induce provocări cu impact transfrontalier (transporturi aeriene, comunicaţii etc.), impunând reacţii unitare (decizii, politici, legislaţie europeană) la nivelul UE. Definirea acestui concept este importantă din perspectiva activităţii serviciilor de informaţii, în special a celei operaţionale, care trebuie să rămână în afara ariei de interes comunitare.

Prevederile Tratatului de la Lisabona nu au adus însă suplețe arhitecturii instituționale a UE şi nici nu a facilitat eficiența procesului de luare a deciziei, ceea ce poate afecta încrederea serviciilor de informații în relevanța UE. Pentru a răspunde acestor deficiențe, în prezent se încearcă în cadrul UE o abordare coordonată şi coerentă între **dimensiunea internă şi externă a securității** (practic coordonarea eforturilor structurilor europene cu responsabilități în acest domeniu), precum şi asigurarea unei cooperări consolidate civil-militare (**sinergia civil-militară**) pe schimbul de informații şi intelligence în cadrul UE (în termeni de expertiză, proceduri pentru stabilirea priorităților informative, resurse financiare, instrumente IT, baze de date integrate).

3. Cooperarea structurilor europene cu serviciile de informații şi de securitate

Noua realitate a mediului internațional, precum şi evoluțiile din cadrul Uniunii Europene confirmă ideea potrivit căreia este nevoie de o mai bună sinergie între diversele instituții comunitare cu atribuții în domeniul securității, alături de întărirea legăturii dintre acestea şi serviciile naționale ale statelor membre. Dacă necesitatea cooperării cu serviciile este agreată la nivelul UE, prioritățile agențiilor de securitate nu coincid în totalitate cu cele comunitare, ceea ce generează dezbateri privind utilitatea dezvoltării unui serviciu european de informații sau consolidarea cooperării cu serviciile de informații, prin creşterea încrederii şi dialog.

Deşi există dificultăți în asigurarea unui proces coerent în schimbul de informații la nivelul UE, avantajele nu pot fi excluse, iar pe baza unei analize comparative a acestora trebuie găsite soluții de optimizare a cooperării în domeniul intelligence, prin stabilirea coerentă a priorităților la nivelul UE în consultare cu statele membre, prin flexibilizarea fluxului infomațional şi a procesului de decizie la nivel comunitar, precum şi consolidarea capacității de analiză strategică şi de avertizare timpurie.

3.1. Dificultățile cooperării

Restructurarea instituțiilor europene existente sau crearea altora noi în urma adoptării Tratatului de la Lisabona determină asumarea unor obiective ambițioase a acestora pentru a-şi confirma statutul şi utilitatea, precum şi restabilirea priorităților informative, ceea ce generează anumite presiuni asupra serviciilor de informații. Nu trebuie ignorat faptul că adesea serviciile sunt suprasolicitate în plan intern şi nu dispun mereu de resursele necesare pentru a răspunde şi cerințelor UE.

În plus, serviciile secrete au propriile priorități naționale şi răspund în primul rând în fața autorităților naționale. În acest sens, la nivelul serviciilor europene este susținută o independență de raportare la instituțiile UE, serviciile trebuind să se detaşeze de birocrația transnațională de la Bruxelles, care solicită adesea prea mult resursele serviciilor de informații.

O altă explicație constă în faptul că societatea civilă pretinde o eficiență totală a serviciilor de informații şi nu va accepta în niciun caz drept scuză faptul că acestea din urmă s-au supus unor exigențe birocratice la nivel european.

De asemenea, birocrația complicată a UE, cu structuri multiple, proceduri greoaie şi mecanisme de decizie şi de reacție puțin eficiente în situații de criză poate impieta asupra motivării serviciilor de a transmite informații utile.

În acelaşi timp, organizațiile tind să nu aibă încredere decât în propriile analize, astfel, pe baza informațiilor transmise de statele membre, sunt elaborate alte documente care reflectă viziunea proprie a structurii respective, ceea ce ia mult timp şi poate întârzia răspunsul la situații de criză[14], cu implicații şi asupra pierderii interesului serviciilor de intelligence de a mai asigura contribuții.

Este recunoscută reticența serviciilor statelor membre de a oferi UE informații din surse secrete, datorită relevanței acestora asupra securității naționale, care este interpretată ca un atribut exclusiv al statelor membre. De asemenea, nu se doreşte o „subordonare" a serviciilor de către structurile europene, ci menținerea suveranității acestora, în special în contextul noilor dezvoltări conform cărora Parlamentul European este tot mai interesat de activitatea de informații[15]. Toate serviciile de informații din statele membre

[14] Nomikos, John M., *European Intelligence Cooperation Beyond the Nation State: A Prerequisite for Common Foreign and Security Policy (CFSP),* 26.03.2006, http://www.worldsecuritynetwork.com/showArticle3.cfm?article_id=12992

[15] În 30 martie 2011, a avut loc în Parlamentul European o audiere privind "Viitorul procesului de intelligence UE şi securitatea internă", la care au participat oficiali UE (şeful SITCEN, reprezentanți ai Comisiei Europene), reprezentanți ai serviciilor de informații ai statelor membre (Austria) sau ai instituțiilor de aplicare a legii (Germania, Spania), precum şi reprezentanți ai mediului academic (http://www.eppgroup.eu/Press/peve11/eve015_en.asp). De asemenea, în octombrie 2010, Parlamentul European a comandat centrului DCAF din Elveția un studiu privind modalitățile în care se asigură controlul parlamentar al serviciilor de informații europene (http://www.dcaf.ch/dcaf/projects/about?id=128453).

răspund în fața parlamentelor naționale şi ca urmare nu este necesar un control suplimentar din partea Parlamentului European.

În acelaşi timp, serviciile sunt interesate în primul rând de cooperarea operațională, care este realizată în cadrul altor formate multilaterale (precum Clubul de la Berna, Grupul privind Contraterorismul - CTG[16]), care asigură un schimb de informații mult mai rapid şi eficient.

Deşi regula terței părți (o informație nu este divulgată unei terțe părți fără acordul originatorului) guvernează cooperarea în domeniul intelligence şi la nivel comunitar, unele servicii pot pune sub semnul întrebării capacitatea UE de a proteja informațiile şi implementarea eficientă a măsurilor de securitate (în special în cazul noilor structuri).

3.2. Avantajele cooperării

Tratatul de la Lisabona prevede că responsabilitatea asigurării securității naționale rămâne atribut suveran al statelor membre, însă UE este chemată să adauge valoare, acolo unde este posibil, acestor demersuri. Este recunoscut că serviciile de informații se subordonează exclusiv decidenților naționali, dar amenințările teroriste au implicații transnaționale (libertatea de deplasare şi a transporturilor, inexistența controalelor la frontiere), iar contracararea trebuie să se facă într-o manieră coordonată la nivel european. Nu poate fi contestată nevoia structurilor UE (exemplu: COM, SITCEN) de a beneficia de sprijinul statelor membre prin furnizarea de evaluări de risc, care să fundamenteze politicile şi deciziile în domeniul contraterorismului. A crescut preocuparea structurilor UE (inclusiv a COM) pentru îmbunătățirea coordonării eforturilor comune în domeniul securității, prin valorificarea resurselor structurilor europene (SITCEN, Europol, COM – DG Home) în elaborarea evaluărilor de risc, alături de analize din partea statelor membre. Structurile UE nu au nevoie de informații tactice, ci de elemente strategice (spre exemplu, nu sunt necesare informații despre cine foloseşte Internetul în scopul radicalizării, ci despre modalitățile în care acesta este folosit). În elaborarea documentelor strategice care să susțină procesele decizionale la nivel comunitar, cu implicații în plan național, este

[16] Walsh, James Igoe, *Intelligence Sharing in the European Union: Institutions Are Not Enough,* în „The International Politics of Intelligence Sharing", Columbia University Press, 2010, pp.88-110

necesară consolidarea cooperării între structurile europene şi serviciile de informaţii, pe bază de încredere şi dialog.

Pe de altă parte, luând în considerare rolul UE în gestionarea crizelor, informaţiile secrete (*hard core intelligence*) sunt esenţiale pe timp de criză, mai ales când informaţiile din surse deschise sunt cvasi-inexistente. Acest schimb de informaţii este util şi din perspectiva statelor membre care au interesul ca situaţiile de criză cu efecte transfrontaliere să fie rezolvate prin solidaritate. În acest sens, necesitatea gestionării dezvoltărilor securitare cu impact asupra securităţii naţionale încurajează cooperarea şi schimbul de informaţii între UE şi serviciile de informaţii, alături de interesul de a dezvolta sisteme de prevenire, alertă timpurie şi gestionare a crizelor, pe baza produselor de intelligence.

În acelaşi timp, nu poate fi ignorată relevanţa surselor deschise[17], care elimină dificultăţile cooperării legate de sensibilitatea informaţiilor şi protecţia informaţiilor clasificate. Avantajele incontestabile oferite de mediile publice, prin rapiditate de accesare şi partajare, costuri reduse, neexpunere la risc, atrag interesul pentru dezvoltarea unor sisteme de avertizare timpurie, având la bază analiza acestor surse deschise. Multiplicarea ameninţărilor, a surselor şi volumul semnificativ de informaţii necesită consolidarea cooperării în domeniul intelligence, inclusiv în cadru multilateral, respectiv UE. Pe fondul intensificării demersurilor UE de dezvoltare a capacităţii de avertizare timpurie, prin intermediul schimbului de informaţii din surse deschise, serviciile pot beneficia la rândul lor de instrumentele şi produsele UE (baze de date, programe de finanţare pentru proiecte).

În perspectivă, reticenţele agenţiilor de informaţii de a coopera cu structurile europene din cauza birocraţiei excesive ar putea fi îndepărtate prin implementarea unor sisteme mai eficiente de coordonare şi luare a deciziilor.

În acelaşi timp, serviciile nu pot ignora faptul că deciziile la nivel comunitar au implicaţii asupra securităţii naţionale şi din această perspectivă, trebuie să fie la curent cu dezvoltările în cadrul UE (politici, legislaţie, schimbări de proceduri, restructurări). Acest deziderat poate fi atins prin cooperare, dialog sau prin reprezentarea efectivă a serviciilor în cadrul structurilor europene.

---

[17] Podolski, Antoni, *European Intelligence Cooperation: A Failing Part of the CFSP and ESDP?,* EuroFuture Journal, pp.44-47, martie 2005, Paris, Franţa.

4. Către un serviciu de informații european?

În mediul academic şi în cadrul comunității europene, pe fondul creşterii presiunii în direcția furnizării de produse de intelligence de calitate şi în timp real pentru sprijinirea procesului decizional european, s-au intensificat dezbaterile privind oportunitatea creării unui serviciu de informații al UE. În pofida argumentelor în favoarea unui astfel de demers, explicat adesea dintr-o perspectivă neorealistă, conform căreia UE poate deveni un actor important pe plan global numai prin dezvoltarea capabilităților de intelligence[18], perspectiva acceptării acestei propuneri de majoritatea statelor membre UE rămâne îndepărtată.

În primul rând, statele membre au viziuni diferite asupra modului de organizare a unei comunități de intelligence, ceea ce ar îngreuna consensul asupra constituirii unei astfel de instituții la nivel european. În acelaşi timp, interesele de securitate diferite ale statelor membre ar împieta asupra procesului de stabilire a priorităților informative.

Totodată, serviciile exprimă preferința pentru cooperarea bilaterală, datorită cerințelor operaționale, riscul scurgerii informațiilor fiind redus în această formulă. Deşi amenințările asimetrice şi necesitatea combaterii lor au condus şi la dezvoltarea dimensiunii multilaterale a cooperării între servicii, se remarcă interesul serviciilor de informații de a menține sau consolida formatele existente, care dispun de reguli de securitate clare, sisteme de comunicații sigure şi asigură un schimb de informații eficient (precum Clubul de la Berna).

Crearea unui serviciu de informații al UE nu ar reprezenta o adevărată valoare adăugată, deoarece eforturile nu ar fi justificate – informația secretă are o „viață" limitată şi prezintă aceleaşi probleme de corectitudine (*reliability*).

De asemenea, deşi unii experți[19] susțin oportunitatea creării unui serviciu autonom de informații al UE, explicând că existența unei singure structuri europene ar fi mai eficientă decât sistemul actual care presupune apelul la servicii multiple din cele 27 de state membre, valoarea adăugată

[18] Villadsen, Ole R., *Prospects for a European Common Intelligence Policy,* Center for the Study of Intelligence, CIA Library, 2000, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/summer00/art07.html şi Politi, Alessandro, *Why Is a European Intelligence Policy Necessary?,* în "Towards a European Intelligence Policy", Chaillot Papers, 34, decembrie 1998, Institute for Security Studies.
[19] Eisl, Gunther, *loc. cit.*

a sistemului actual este dată de calitatea produselor, eficiența fluxului informațional şi capacitatea de fuzionare a informațiilor din surse diferite.

UE ar trebui să-şi consolideze structurile / expertiza / mecanismele existente şi să se orienteze mai degrabă pe prognoză pe termen lung şi pe analiză informațiilor din surse deschise (mult mai uşor de accesat)[20]. De asemenea, UE nu ar trebui să vizeze dezvoltarea de capacități de intelligence, ci mecanisme europene de reacție la amenințări transfrontaliere şi crize europene. UE are nevoie de evaluări de risc şi nu de informații tactice pentru a-şi orienta procesele de decizie. În acelaşi timp, ar fi utilă dezvoltarea capacității de avertizare timpurie, pe baza unor priorități şi obiective bine definite. Informațiile din surse deschise reprezintă doar o componentă a resurselor de care dispune UE (pe lângă rapoartele misiunilor PSAC[21], din partea delegațiilor UE, ale agențiilor etc.). În acelaşi timp, la nivelul UE nu există un mecanism pentru colectarea tuturor informațiilor relevante şi analizarea acestora. În perspectivă, eforturile UE ar putea fi concentrate pe constituirea unui astfel de mecanism în cadrul unui centru de fuziune a informațiilor (*fusion center*)[22].

În condițiile în care mentalitatea diferitelor instituții europene în domeniul securității este insulară, fiecare dezvoltându-şi propria filosofie şi rațiune de a exista, eforturile la nivel comunitar ar trebui concentrate nu pe crearea unui organism de securitate al UE, ci pe consolidarea instituțiilor existente, prin creşterea cooperării şi a încrederii[23]. Acest obiectiv trebuie dublat de încurajarea cooperării cu serviciile de informații şi securitate din statele membre.

Cooperarea cu comunitățile de intelligence europene poate urma, de asemenea, două modele de partajare a informațiilor care nu se exclud reciproc: (1) stabilirea unor centre naționale (*hubs*) conectate prin intermediul UE; (2) utilizarea mai eficientă a organismelor UE care desfăşoară activități de intelligence. [24]

---

[20] Schumann, Frederik, "Rolul intelligence-ului pe bază de surse deschise în alerta timpurie", conferință la Institul European de Relații Internaționale, 3 mai 2011, Bruxelles.

[21] În urma adoptării Tratatului de la Lisabona, Politica Europeană de Securitate şi Apărare (PESA) a devenit Politica de Securitate şi Apărare Comună (PSAC).

[22] Montanaro, Lucia, „Analiza strategică a informațiilor ca instrument al politicii externe. Spre un serviciu de informații al UE?", conferință la Academia Diplomatică Europeană, 2 mai 2011, Bruxelles.

[23] Van Germert, Wil, *Could Europe Do Better on Pooling Intelligence,* SDA Roundtable Report, Security and Defence Agenda, 26 octombrie 2009, Bruxelles.

[24] Muller Wille, Bjorn, *Could Europe Do Better on Pooling Intelligence,* SDA Roundtable Report, Security and Defence Agenda, 26 octombrie 2009, Bruxelles.

Înființarea unei agenții europene de intelligence, deşi dotată cu resursele necesare, nu reprezintă garanția funcționării eficiente a acesteia, existând pericolul ca aceasta să nu livreze rezultatele aşteptate, creând aşteptări care nu pot fi atinse.

5. Concluzii

UE este o organizație care oferă cadrul pentru dezvoltarea cooperării în domeniul intelligence, deținând structurile executive şi de decizie, procedurile şi instrumentele care pot asigura eficiența acestui proces. În condițiile în care securitatea rămâne un atribut exclusiv al statelor membre (concepție care nu va fi depăşită prea curând), iar cooperarea în domeniul intelligence este limitată în funcție de interesul şi prioritățile statelor membre, eforturile comunitare trebuie să se concentreze pe evaluări strategice, analiză de risc şi prognoză, coordonarea demersurilor de gestionare a amenințărilor şi crizelor transfrontaliere, cu impact asupra mai multor state membre, prin elaborarea de strategii pe termen scurt şi lung. De asemenea, accentul poate fi plasat pe crearea unui nou sistem de gestionare / fuzionare a informațiilor, având ca obiectiv optimizarea proceselor şi sporirea calității produselor de intelligence la nivel european.

Actualele dezvoltări şi retorica UE privind necesitatea consolidării cooperării cu serviciile de informații şi securitate naționale nu ar trebui interpretate neapărat ca o intenție a UE de a crea un serviciu de informații european, în sens clasic, ci mai degrabă ca un obiectiv de construire a unei capacități solide de analiză strategică care să ofere fundamentul informativ pentru procesul decizional la nivel comunitar.

Bibliografie

1. Baker, Charles, *The Search for a European Intelligence Policy,* http://www.fas.org/irp/eprint/baker.html.

2. Cross, Maia K. Davis, *EU Intelligence Sharing and the Joint Situation Center: A Glass Half-Full,* 2011 Meeting of the European Union Studies Association, 3-5 martie 2011, http://www.euce.org/eusa/2011/papers/3a_cross.pdf.

3. Muller Wille, Bjorn, Could Europe Do Better on Pooling Intelligence, SDA Roundtable Report, Security and Defence Agenda, 26 octombrie 2009, Bruxelles.

4. Nomikos, John M., European Intelligence Cooperation Beyond the Nation State: A Prerequisite for Common Foreign and Security Policy (CFSP), 26.03.2006, http://www.worldsecuritynetwork.com/showArticle3.cfm?article_id=12992.

5. O'Sullivan, David, *Setting Up the EEAS,* IIEA, Dublin, 14 ianuarie 2011, http://www.eeas.europa.eu/speeches/2011_1201_dos_iiea_en.pdf.

6. Podolski, Antoni, *European Intelligence Cooperation: A Failing Part of the CFSP and ESDP?,* EuroFuture Journal, pp.44-47, martie 2005, Paris, Franța.

7. Politi, Alessandro, *Why Is a European Intelligence Policy Necessary?,* în "Towards a European Intelligence Policy", Chaillot Papers, 34, decembrie 1998, Institute for Security Studies.

8. Van Germert, Wil, *Could Europe Do Better on Pooling Intelligence,* SDA Roundtable Report, Security and Defence Agenda, 26 octombrie 2009, Bruxelles.

9. Villadsen, Ole R., *Prospects for a European Common Intelligence Policy,* Center for the Study of Intelligence, CIA Library, 2000, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-ublications/csi-studies/studies/summer00/art07.html.

10. Walsh, James Igoe, *Intelligence Sharing in the European Union: Institutions Are Not Enough,* în „The International Politics of Intelligence Sharing", Columbia University Press, 2010, pp. 88-110.

Securitate națională, surse de putere şi intelligence

Viorel BUȚA
Gl. bg. (r.) prof. univ. dr., Universitatea Națională de Apărare „Carol I”
e-mail: **vbuta49@yahoo.com**

Abstract

In this paper the author analyses the relationship between the national security, sources of State power and intelligence. The study is focused on the analysis of national security, State power and intelligence and how the various branches of government institutions collaborate in order to protect and promote national interests at home and abroad.

The purpose of this paper is to provide a comprehensive overview of the elements involved in the national security policy analysis and intelligence community.

Keywords: national security, sources of State power, intelligence.

Statul reprezintă un sistem social supus unei serii vaste de influențe – pozitive sau negative – prin urmare este sensibil la o varietate de factori interni şi externi. Pentru a reduce până la absență această sensibilitate este necesar să fie eliminate vulnerabilitățile şi, prin urmare, crescută puterea statului odată cu realizarea unui nivel optim de stabilitate şi securitate. Astfel, obiectele de referință ale securității depind de domeniul abordat, acestea putând fi: teritoriul, populația, forțele armate, suveranitatea, proiectul politic, ideologia care îl susține, calitatea şi cantitatea forței de muncă, identitatea colectivă a unei națiuni sau a altor grupuri etnice sau religioase (minorități semnificative), accesul la resurse, în principal energetice, aprovizionarea cu materii prime, reglementarea funcționării sistemului financiar etc., sursele de apă potabilă, biodiversitatea. Acestea reprezintă totodată şi sursele de putere ale unui stat.

Plecând de la premisa că fiecare dintre aceste surse pot furniza informații care să conducă la evaluarea nivelului de putere a unui stat, vom aduce împreună în această lucrare intelligence-ul şi puterea statului, în încercarea de a formula noi provocări, cel puțin pentru mediul ştiințific, cu atât mai mult cu cât spațiul de manifestare al acestora este un spațiu în care diferite structuri guvernamentale îşi coroborează eforturile pentru a proteja şi promova interesele statului pe plan intern şi extern.

Securitatea națională şi sursele de putere ale statelor

Dezbaterea asupra componentelor securității şi a modurilor cum se poate realiza securitatea a devenit din ce în ce mai complexă şi mai specializată. Totuşi, din larga paletă a literaturii de specialitate din ultimele şase decenii, nu s-a desprins, încă, o definiție care să fie acceptată unanim, astfel că, în special astăzi, conceptul pare mai controversat ca niciodată. Prin urmare, conceptul de securitate rămâne destul de ambiguu în conținut, prin referirea sa la diferite aspecte şi/sau valori, acest fapt fiind posibil, în mare măsură, şi din cauza implicării unei arii vaste de contexte şi scopuri multiple ale indivizilor, guvernelor sau mediilor academice. Este un concept supus în egală măsură contradicțiilor, ca şi subtilităților.

În general, delimitarea câmpului de cercetare în studiul securității a fost realizată prin analiza amenințărilor, fiind urmărite, în principal, două caracteristici principale, şi anume: să se folosească mijloace excepționale, cum ar fi de exemplu: uzul forței, uzul forței disproporționate, restricții şi/sau interdicții în exercitarea drepturilor şi libertăților individuale şi să poată fi considerate drept *existențiale*, cu alte cuvinte, să vizeze evoluția obiectului de referință (statul, națiunea, valorile).

Domeniile care intră în vederea studiilor de securitate sunt identificate pornind de la tipurile acțiunilor umane ce le generează. Astfel discutăm despre *domeniul politic* (cel care vizează relațiile de autoritate, recunoaşterea statelor şi a guvernelor), *domeniul militar* (care presupune, în esență, mijloace coercitive), *domeniul social* (considerat frecvent prin prisma socio-economică), *domeniul cultural* (care include aspectele identitare, etnice şi/sau religioase), *domeniul economic* (axat pe aspectele financiare, de producție şi cele relaționate resurselor energetice), *domeniul informațional-tehnologic* (concentrat asupra aspectelor privind informațiile şi tehnologia informației) şi *domeniul de mediu* (care se referă la activitățile umane şi impactul acestora asupra biosferei).

Astfel, obiectele de referință ale securității depind de domeniul abordat, acestea putând fi: teritoriul, populația, forțele armate, suveranitatea, proiectul politic, ideologia care îl susține, calitatea şi cantitatea forței de muncă, identitatea colectivă a unei națiuni sau a altor grupuri etnice sau religioase (minorități semnificative), accesul la resurse, în principal energetice, aprovizionarea cu materii prime, reglementarea funcționării sistemului financiar etc., sursele de apă potabilă, biodiversitatea.

Referitor la nivelul analizei, aceasta poate fi aplicată astfel: la nivelul sistemului internațional, la nivel regional; la nivelul entităților statale sau a națiunilor, la nivelul organizațiilor multinaționale, la nivelul comunităților, grupurilor, şi la acela al individului.

Trebuie să menționăm că diversele transformări ale conceptului de securitate s-au petrecut în mod evident ca urmare a transformărilor de pe scena internațională. Considerând încheierea Războiului Rece un punct major de referință pentru schimbările generate de dezechilibrarea balanței de putere, a bipolarității, putem afirma că vechiul sistem de securitate constituit sub umbrelele nucleare ale celor două superputeri – Statele Unite şi Uniunea Sovietică –, prin menținerea parității strategice relative între blocurile militare, nu a putut rezista presiunii exercitate de factorii economici, politici sau sociali. Prin urmare, procesul de abordare a priorităților agendei de securitate a suferit o serie de transformări, acestea nemaifiind instrumentate prin mijloace exclusiv militare, ci prin acțiuni de natură politică, economică, culturală etc., corelate noilor perspective deschise de însăşi desfăşurarea concretă a evenimentelor pe scena relațiilor internaționale. În acest context, scena internațională devine, după părerea lui Zbigniew Brzezinski *marea tablă de şah* în care actorii acționează frecvent prin relațiile de putere. Puterea nu se manifestă, însă, în mod exclusiv, ca atribut al unui stat sau unei entități, ci numai în relație cu ceilalți actori internaționali. De o importanță majoră în proiectarea unor politici de securitate eficiente, puterea este rezultatul unei combinații de capacități care derivă din surse interne sau externe, ca rezultat al relațiilor internaționale. În general, sunt acceptate ca surse esențiale de putere sursele naturale, sursele sociopsihologice şi sursele sintetice[1].

Sursele naturale derivă din considerentele geografice (dispunerea statului pe glob, suprafața, ieşirea la mare, lungimea şi natura granițelor etc.), resursele naturale şi populația. Aceste surse sunt considerate a fi cele mai durabile, iar acțiunile de compensare a dezavantajelor provenite din insuficiența resurselor naturale sunt cele mai costisitoare, ceea ce provoacă frecvent transformarea lor în obiect al unor politici de lungă durată care, în timp, pot deveni tradiție politică. Totodată, importanța surselor naturale de putere[2] este provenită din rolul decisiv pe care acestea îl dețin în stabilirea şi stabilitatea strategiilor politico-militare de apărare a unui stat.

Sursele sociopsihologice ale puterii sunt cele mai delicate, în opinia noastră, deoarece se regăsesc în aspecte mai greu cuantificabile: imaginea

[1] Walter S. Jones, *The logic of International Relations*, Longman, New York 1997, p. 202.
[2] *Ibidem*, p. 188.

de sine a unui popor[3], nivelul de socializare a politicii, care reflectă procesul prin care individul îşi formează atitudinea politică, sprijinul public, forma de conducere etc. Sprijinul public, de exemplu, reflectă, în ultimă instanță, coeziunea unei națiuni în sprijinul promovării unor valori fundamentale. Lipsa sprijinului public sau prezența unui nivel redus al acestuia uzează resursele politice şi militare ale unui stat care poate suferi astfel o criză de credibilitate şi eficiență în momente dificile.

O altă categorie de surse ale puterii este constituită de *sursele sintetice*, acestea derivând din celelalte două categorii menționate anterior şi reflectând abilitatea statului de a-şi întrebuința sursele naturale şi sociopsihologice pentru afirmarea puterii. Practic, sursele sintetice de putere sunt constituite de resursele industriale, financiare, tehnico-ştiințifice şi militare.

Sursele de putere ale statului şi intelligence-ul în contextul mediului de securitate contemporan

Prin urmare, din punct de vedere al aspectelor abordate în lucrarea noastră, *intelligence-ul*, ca sursă aflată la întrepătrunderea surselor naturale cu cele socio-psihologice şi sintetice, poate avea influențe semnificative asupra puterii respectivului stat, în funcție de dinamica evoluției relațiilor între diverşii actori ce evoluează în plan intern, regional sau internațional. În funcție de evoluția acestor relații pot exista implicații asupra securității statului respectiv, în sensul menținerii sau degradării stării acesteia.

Aşa cum remarcam anterior, puterea actorilor nu mai este exprimată exclusiv în termeni clasici, militari, dimensiunii militare a puterii adăugându-i-se şi alte dimensiuni, printre care cea economică şi cea informațional-tehnologică. Putem vorbi deci, despre o abordare inter-dimensională, datorită interdependenței crescute a dimensiunilor, abordare care, în scopul realizării unei stări optime de securitate şi stabilitate, va trebui să dispună de capacități similare, multidimensionale, destinate obținerii superiorității informaționale.

Superioritatea informațională este definită, în general, drept capabilitatea de a colecta, procesa şi disemina un flux continuu de informații. Relaționând conceptul securității naționale celui de intelligence, putem afirma, aşadar că securitatea națională impune realizarea *„stării de protecție a necesităților de natură informațională ale individului, societății şi statului, care să permită asigurarea satisfacerii acestora şi evoluția lor progresivă”*[4].

---

[3] *Ibidem*, p. 190.
[4] Cristian Troncotă, *Studii de securitate,* Universitatea „Lucian Blaga” Sibiu, 2008, p.9.

Potrivit specialiştilor autohtoni[5], pentru realizarea acestei stări care să asigure evoluția acestor necesități, trebuie ca activitatea de intelligence să rezolve situații (adică să fie eficientă) şi să stabilească valori (să fie ataşată). În acest scop este necesar să fie operațională capacitatea de a colecta, prelucra şi utiliza informația. Operaționalizarea acestei capacități este realizată de către stat, prin structurile sale de securitate şi apărare, în cadrul serviciilor de informații abilitate în acest sens prin cadrul legislativ ce reglementează activitatea acestora, şi aflate, în cadrul societăților democratice, sub controlul civil al acestora.

Caracteristici ale agențiilor de intelligence – adaptabilitatea la complexitatea scenei internaționale actuale

Aşadar, serviciile de informații sunt instituții ale statului de drept, misiunile acestora fiind desfăşurate în concordanță cu obiectivele politicii interne şi externe ale statului în scopul cunoaşterii, prevenirii şi contracarării amenințărilor ce pot aduce afecta negativ valorile şi interesele naționale. Prin informațiile relevante pentru securitatea națională, care sunt puse la dispoziția factorilor decizionali, serviciile de informații contribuie la aplicarea strategiilor necesare existenței statului, ca stat democratic de drept.

Astfel, rolul *intelligence-ului* în adoptarea celor mai bune decizii devine crucial, informația, ca produs al activității desfăşurate de structurile specializate, ocupând un loc important în luarea deciziilor politico-militare.

Perioada ultimelor decenii a consemnat transformări fundamentale în activitatea agențiilor de *intelligence:* dacă la sfârşitul secolului al XX-lea, arhitectura de securitate şi *intelligence* se prezenta ca un set instituțional inflexibil, refractar la transformări, având la bază ideologia monolitică a confruntării care a funcționat în toată perioada Războiului Rece, după anul 1989 concepția privind activitatea şi organizarea intelligence-ului este reconsiderată prin prisma câtorva schimbări semnificative din mediul internațional de securitate, şi anume:

- dispariția aproape completă a distincției între amenințările interne şi cele externe – a modului de confruntare dintre acestea;

[5] Ionel Nicu Sava, *Studii de Securitate*, Centrul Român de Studii Regionale, Bucureşti, 2005, pp. 207-208.

- integrarea şi implicarea aproape completă a instituţiilor de ordine publică, la toate nivelurile administrative ale statului, în activităţile de securitate naţională.

Mai târziu, odată cu atacurile teroriste de la 11 septembrie 2001, eforturile au fost concentrate asupra eficacităţii şi coordonării funcţionale a organizaţiilor de *intelligence*, pe angrenarea tuturor factorilor instituţionali statali. A fost evidenţiată, astfel, necesitatea creşterii nivelului comunicării şi colaborării între organizaţiile de *intelligence* la nivel naţional şi internaţional. Implicaţiile acestei decizii au presupus înfiinţarea unor baze de date comune, crearea unor organism de intelligence comune, inventarea unor noi forme instituţionale de colaborare şi chiar contopirea unor instituţii[6]. Acest fapt a făcut posibilă apariţia unor noi oportunităţi, dar în egală măsură şi apariţia unui număr mai mare de provocări de înfruntat. Rolul şi natura colaborării *intelligence* în contextul globalizării (însuşi domeniul *intelligenc*e globalizându-se) reprezintă în perioada actuală una dintre consecinţele momentului 11 septembrie 2001. Avem de-a face, aşadar, cu unul dintre cele mai bine definite aspecte ale transformării intelligence-ului, şi anume cu relaţia *cooperare – conlucrare – colaborare*[7], concretizată de modalităţile prin care serviciile de informaţii şi securitate acţionează, pe baza acordurilor bilaterale şi multilaterale, în vederea realizării unor obiective comune, la elaborarea unor instrumente regionale şi internaţionale care să prevadă măsuri eficiente, imediate şi de perspectivă pentru combaterea ameninţărilor globale. Ca urmare a concretizării relaţiei amintite, remarcăm deplasarea centrului de greutate dinspre schimbul de informaţii cu caracter de generalitate spre cooperarea pe cazuri şi acţiuni punctuale, ca modalitate de valorificare optimă a potenţialului oferit de partenerii implicaţi.

Analizând critic procesul de transformare al intelligence-ului, observăm, însă, că există şi unele aspecte a căror apariţie poate conduce la o scădere a nivelului eficienţei în acest domeniu. Dintre aceste aspecte remarcăm aici:

- tendinţa către autosuficienţă, cauzată de existenţa în cadrul organizaţiilor care activează în domeniul informaţiilor, a convingerii potrivit căreia cele mai bune produse de *intelligence*

---

[6] Larry L., Watts, *Intelligence Reform in Europe's, Emerging Democracies Studies in Intelligence*, Vol. 48, No. 1, 2004, pp. 2-4.

[7] *Doctrina Naţională a Informaţiilor pentru Securitate*, adoptată în Şedinţa Consiliului Suprem de Apărare din 23 iunie 2004, p. 19.

sunt cele proprii. Această abordare determină o încredere sporită în produsele interne şi o anumită reticenţă faţă de unii parteneri şi uneori erori în fundamentarea deciziei;

- tendinţa structurilor menţionate anterior de a considera relaţiile internaţionale drept un *„joc de sumă zero”*, ca urmare demonstrând o atitudine reticentă faţă de abordarea cooperativă a procesului de integrare în domeniile apărării şi securităţii.
- limitările financiare, nu toate serviciile de informaţii militare având acces la resurse adecvate pentru a realiza un schimb echilibrat de informaţii.

Având în vedere aceste aspecte, opinia noastră este că natura conservatoare şi în acelaşi timp conservativă a structurilor de informaţii, corelată cu birocraţia sistemului euroatlantic ar putea acţiona în sensul încetinirii procesului de cooperare, mai ales în domeniul informaţiilor pentru securitate şi apărare. În acest sens, apare mai mult decât necesară identificarea celor mai bune modalităţi de utilizare şi direcţionare a resurselor umane, logistice şi financiare de care dispune comunitatea de informaţii, în vederea preîntâmpinării unui nivel scăzut de eficienţă.

Operaţionalizarea *Intelligence-ului* ca instrument de putere naţională în cazul României

Instrumentul *intelligence-ului* este operaţionalizat de către serviciile specializate dezvoltate la nivelul principalelor instituţii ale României. Activitatea de informaţii necesară realizării siguranţei naţionale este executată de către Serviciul Român de Informaţii (SRI), organ specializat pe informaţiile din interiorul ţării, Serviciul de Protecţie şi Pază (SPP), care asigură protecţia demnitarilor români şi străini pe timpul prezenţei lor în România, a sediilor de lucru şi a reşedinţelor acestora, de către Serviciul de Informaţii Externe (SIE), organismul specializat pe obţinerea de informaţii din străinătate, dar şi de către structuri cu atribuţii similare organizate la nivelul Ministerului Apărării Naţionale, al Ministerului Administraţiei şi Internelor şi Ministerului Justiţiei[8]. De asemenea, în acest sens, trebuie menţionat şi Serviciul de Telecomunicaţii Speciale (STS).

[8] Cf. Legii nr. 51/1991 privind siguranţa naţională a României, Monitorul Oficial nr. 163 din 8 iulie 1991, articolele 8 şi 9, http://www.sri.ro/upload/Lege a51.pdf.

În cadrul Ministerului Apărării Naționale, funcționează Direcția Generală de Informații ale Apărării (DGIA), structura specializată a acestui minister care este responsabilă pentru colectarea, procesarea şi verificarea informațiilor privind factorii de risc interni şi externi de natură militară şi nonmilitară, coordonează aplicarea măsurilor contrainformative şi cooperarea cu serviciile / structurile departamentale naționale de informații, cât şi cu cele ale statelor membre ale alianțelor, coaliţiilor şi organizaţiilor internaționale la care România este parte şi asigură securitatea informațiilor clasificate naționale, NATO şi UE la nivelul Ministerului Apărării Naționale (MApN)[9]. Similar, la nivelul Ministerului Administrației şi Internelor (MAI), funcționează Direcția Generală pentru Informații şi Protecție Internă (DGIPI), care este însărcinată cu colectarea şi utilizarea informațiilor cu privire la crima organizată, violențe sociale şi protecția personalului MAI.

Organizarea, conducerea şi planificarea strategică a acestor autorități sunt exercitate de către Preşedintele României, Parlament, Consiliul Suprem de Apărare a Țării (CSAT) şi Guvern. De asemenea, activitatea acestor autorități informative este planificată la nivel strategic de către Comunitatea Națională de Informații, care funcționează sub coordonarea CSAT şi care reprezintă „rețeaua funcțională a autorităților informative din sistemul securității naționale”[10].

După 1989, România şi-a creat un instrument informațional în acord cu principiile democratice, supus controlului democratic, care funcționează conform unor legi stabilite şi cu mandate bine definite, proces ce nu a fost deloc unul lipsit de dificultăți din cauza neîncrederii populației în instituțiile publice. Astfel, astăzi putem vorbi despre faptul că România beneficiază de un instrument informațional, pe care îl poate valorifica cu succes în promovarea şi apărarea intereselor naționale[11].

Funcțiile principale ale serviciilor de informații constau în evitarea surprizei strategice, în furnizarea expertizei pe termen lung în domeniul securității şi în susținerea procesului decizional. Utilitatea intelligence-ului ca instrument de promovare a intereselor naționale poate fi ilustrată şi prin

---

[9] Legea nr. 346/2006 privind organizarea şi funcționarea Ministerului Apărării, http://www.defense.ro/smg/legea_3 46.pdf.

[10] Cf. Legii privind activitatea de informații, contrainformații şi securitate, Propunere de proiect, http://www.presidency.ro/static/ordine/CSAT/Proiect_ Lege_activitate_informatii-contrainformatii.pdf.

[11] Denis DELETANT, *Ghosts from the past: succesors to the Securitate in the post-Communist Romania*, pp. 35-58, apud. Duncan LIGHT, David PHINEMORE, Post-Communist Romania. Coming to terms with transition, Palgrave, US, 2001.

definițiile pe care acesta le-a primit. Astfel, prin intelligence, se înțelege „o nevoie permanentă a tuturor statelor, indiferent de forma lor de guvernare, deoarece permite națiunilor să anticipeze riscurile la adresa securității ei fundamentale şi să se apere împotriva acestora”[12]. De asemenea, serviciile de informații „contribuie la capacitatea democrațiilor de a păstra securitatea şi bunăstarea națiunii şi populației, pentru buna guvernare şi funcționarea eficientă şi efectivă a statului”[13].

Identificarea modului concret de operaționalizare a instrumentului informațional, prin ilustrarea de evenimente aferente, este dificil de realizat în cazul acestui tip de instrument din cauza caracterului clasificat pe care îl au majoritatea activităților serviciilor de informații. Totuşi, documentele referitoare la modul de funcționare a acestor servicii relevă arii în care acestea îşi derulează activitatea. Per ansamblu, ele gestionează informațiile referitoare la întreaga gamă de riscuri şi amenințări la adresa securității naționale: terorismul internațional, crima organizată, acțiuni extremiste, proliferarea armelor de distrugere în masă sau a armamentului convențional, acțiuni de spionaj, punerea în pericol a informațiilor clasificate naționale, ale NATO sau UE, nerespectarea tratatelor internaționale referitoare la frontieră, periclitarea autorităților publice şi a instituțiilor statului prin acte de corupție, influențarea, deturnarea deciziilor politice în scopuri contrare interesului național, acțiuni care periclitează ordinea constituțională, securitatea economică, capacitatea de apărare a statului, a infrastructurilor critice sau a securității informaționale a cetățenilor[14].

De asemenea, o altă caracteristică a operaționalizării instrumentului informațional este necesitatea cooperării cu organizațiile internaționale din care România face parte şi cu statele membre ale acestora pentru contracararea unor riscuri şi amenințări transfrontaliere, comune lor. În acest sens, au existat multe dispute în mediul academic referitoare la modul în care acestea vor împărtăşi informații ce sunt considerate a fi de o importanță vitală pentru stat.

---

[12] Elizabeth RINDSKOPF PARKER, *The American Experience: One Model for Intelligence Oversight in a Democracy*, apud. Valentin Fernand FILIP, *The Intelligence phenomenon in a new democratic milieu. Romania – a case study, Thesis*, Naval Postgraduate School, Monterey, California, march 2006, http://www.fas.org/irp/world/romania/ filip.pdf, p. 2.

[13] DCAF Intelligence Working Group, *Intelligence Practice and Democratic Oversight–A Practitioner's View,* August 2003, p. 2, http://www.dcaf.ch/publ ications/Occasional_Papers/3.pdf.

[14] Cf. Legii privind activitatea de informații, contrainformații şi securitate, Propunere de proiect, http://www.presidency.ro/static/ordine/CSAT/Proiect_ Lege_activitate_infor matii-contrainformatii.pdf, pp. 7-8.

Pe de altă parte, aderarea la NATO şi UE a constituit şi un alt impuls dat reformării acestor servicii în direcția democratizării. Aceasta cu atât mai mult cu cât România este stat de graniță pentru ambele organizații, iar ieşirea la Marea Neagră, în ciuda oportunităților pe care le presupune, implică şi apropierea de posibile surse de riscuri şi amenințări de securitate precum existența unui mediu politic instabil care poate favoriza manifestarea altor riscuri (criminalitatea organizată, de exemplu), persistența unor stări conflictuale latente, criminalitatea organizată, terorismul internațional, proliferarea armamentului convențional sau a armelor de distrugere în masă, imigrația ilegală.

Cooperarea la nivel internațional în domeniul informațiilor s-a intensificat imediat după atacurile de la 11 septembrie 2001. Totodată, cooperarea în acest domeniu a devenit mai activă şi la nivelul relațiilor dintre NATO şi UE. Astfel, la nivelul ambelor organizații există organisme care au atribuții în gestionarea informațiilor cu relevanță pentru securitate, atât de natură civilă, cât şi de natură militară. În cazul UE, principalele organisme sunt: Centrul de Situații (SITCEN), Centrul Satelitar (EUSC), Divizia de Intelligence a Statului Major al UE (INTDIV) şi Europol. Toate aceste organisme, cu excepția Europol, care face parte din pilonul al treilea al construcției europene, sunt incluse în pilonul al doilea, Politică Externă şi de Securitate Comună (PESC).

Acestea funcționează în ambele sensuri – susțin activitatea informațională a statelor membre, prin furnizarea de informații, analize şi avertizare timpurie care provin din partea statelor membre sau a instituțiilor UE, dar reprezintă şi puncte de colectare a acestor informații. De asemenea, alături de acestea, funcționează şi o serie de alte organisme, cum sunt cele menite să gestioneze lupta împotriva terorismului – Coordonatorul UE pentru combaterea terorismului sau Grupul pentru combaterea terorismului, care se bazează pe acelaşi principiu al împărtăşirii informațiilor relevante sau cele referitoare la gestionarea frontierelor – FRONTEX, SIS (Sistemul de Informații Schengen, presupune schimbul de informații între autoritățile naționale responsabile pentru controlul la graniță asupra persoanelor şi bunurilor).

INTDIV reprezintă principalul punct de schimb de informații militare la nivelul UE, fiind, cel mai probabil, creat după modelul Centrului de Situații al NATO (NATO SITCEN), care este responsabil pentru primirea, schimbul şi diseminarea de informații cu caracter politic, militar în interiorul cartierelor generale. Ca şi INTDIV, NATO SITCEN este

subordonat Comitetului Militar. În plus, misiunile derulate sub mandat NATO sau UE se desfăşoară şi cu participarea ofițerilor de informații. Astfel, zece procente din forțele românești care participă la operațiuni multinaționale sunt ofițeri de informații[15]. Totodată, ambele organizații au dezvoltat şi mecanisme de schimb de informații pentru protejarea populației civile împotriva dezastrelor naturale şi antropice[16].

În acest context, suntem de părere că statutul de stat membru al NATO şi UE a determinat, pe de o parte, alinierea standardelor serviciilor de informație românești la cele ale statelor din comunitatea euroatlantică, iar, pe de altă parte, necesitatea de a utiliza *intelligence-ul* ca instrument pentru apărarea împotriva unor riscuri şi amenințări cu caracter transfrontalier, ceea ce a impus necesitatea cooperării în acest domeniu atât cu organizațiile internaționale din care țara noastră face parte, precum şi cu celelalte state membre ale acestora.

Rolul intelligence-ului militar românesc în arhitectura actuală de securitate.

O componentă de importanță majoră a efortului comun pentru securitate şi stabilitate a relațiilor în plan regional şi global o reprezintă activitatea serviciilor de informații militare care, în contextul unui mediu de securitate extrem de complex, au dezvoltat noi linii de dialog bilateral şi multilateral.

Activitatea de *intelligence* este, fără echivoc, în strânsă legătură cu conceptual de apărare. După cum remarcam anterior, superioritatea militară trebuie sprijinită de capabilități eficiente de *intelligence* pentru a putea interveni în prevenirea conflictelor şi câştigarea confruntărilor, puterea militară fiind în mare măsură dependentă de sectorul informativ. De aceea, activitatea de *intelligence* a devenit parte integrantă a apărării, indiferent dacă aceasta a luat forma asigurării securității naționale, echipării şi înzestrării efectivelor militare sau identificarea posibilelor amenințări.

În cazul României activitatea serviciului de informații militare nu poate fi definit decât pornind de la angajamentele şi obligațiile asumate de România

[15] Florina Cristiana MATEI, *Romania's Intelligence Comunity: From an Instrument of Dictatorship to Serving Democracy*, în International Journal of Intelligence and Counterintelligence, nr. 4 [20]/2007, p. 630.

[16] Vezi Constantin MOŞTOFLEI, Grigore ALEXANDRESCU, Cristina BOGZEANU, Managementul Consecințelor, Editura UNAp, Bucureşti, 2009, pp. 36-76.

în contextul securității naționale subscrise securității comune euro-atlantice şi ținând cont de faptul că informațiile militare se regăsesc în toate domeniile acțiunii sociale iar acestea sunt, subiectul şi totodată instrumentul de lucru al tuturor serviciilor de informații militare. Totodată, trebuie să conştientizăm că serviciul de informații militare constituie un vector de forță şi stabilitate tocmai prin faptul că gestionează un tip de informație care are un rol dublu:

- de formare a unei imagini sintetice, dar integrale, asupra aspectelor de interes;
- de sprijinire a adoptării deciziei strategice viabile şi eficiente din punct de vedere militar şi chiar politic.

Similar altor servicii de informații militare, cel autohton are un rol determinant în asigurarea securității atât la nivel național cât şi la nivelul structurilor de alianță şi coaliție la care România este parte. Din acest punct de vedere, se poate îndeplini o serie vastă de misiuni dintre care menționez aici:

- culegerea de date şi informații în scopul cunoaşterii fenomenului militar şi politico-militar internațional şi al prognozării evoluției acestuia;
- identificarea factorilor de risc şi a amenințărilor externe, de natură militară şi nonmilitară, care ar putea afecta interesele naționale fundamentale, securitatea şi apărarea națională;
- colectarea de informații necesare desfăşurării de acțiuni pe teritorii străine, în cadrul unor operații multinaționale, sub egida organismelor internaționale;
- colectarea de informații privind concretizarea dezvoltărilor din domeniul tehnologiilor militare;
- cooperarea cu serviciile de informații autohtone şi ale altor state, pe probleme de interes comun, în baza unor înțelegeri, acorduri, protocoale sau planuri de cooperare;
- elaborarea concepției de folosire a forțelor şi mijloacelor aflate la dispoziția sa pentru îndeplinirea eficientă a obiectivelor de interes informativ, în spațiul de interes strategic național şi / sau aliat;

*

* *

În încheiere, considerăm că armata şi agențiile de informații sunt brațul operațional al securității naționale, aici fiind implicate elemente ale gândirii strategice, de formulare a strategiilor, procese de analiză şi evaluare

a provocărilor şi riscurilor la adresa securităţii naţionale şi, prin extensie – datorită angajamentelor internaţionale asumate în cadrul unor organizaţii, alianţe sau coaliţii –, al celei internaţionale.

Totodată, concluzionăm, pe baza analizei prezentate, că relaţia securitate naţională-surse de putere ale statului-intelligence este una de tip interdependent, echilibrul acesteia depinzând în egală măsură de fiecare dintre cele trei elemente ale relaţiei.

Bibliografie

1. Florina Cristiana, Matei, *Romania's Intelligence Comunity: From an Instrument of Dictatorship to Serving Democracy*, în International Journal of Intelligence and Counterintelligence, nr. 4 [20]/2007.

2. Gustaaf, Geeraerts, *Analysing Non-State Actors in World Politics*, Pole Paper Series, Vrije Universiteit Brussel, 1995.

3. Giovani, Grevi, *The Interpolar world: a new scenario*, Occasional Paper, no. 79, June 2009, European Union Institute for Security Studies, Paris.

4. Hans J., Morgenthau, *Politica între naţiuni. Lupta pentru putere şi lupta pentru pace*, Editura Polirom, Bucureşti, 2007.

5. Loch K. Johnson, James J. Wirtz, *Intelligence and national security:the secret world of spies : an anthology*, Oxford University Press, 2007.

6. Loch K. Johnson, *The Oxford handbook of national security intelligence,* Oxford University Press, 2010.

7. Roger Z. George, Robert D. Kline, *Intelligence and the national security strategist: enduring issues and challenges*, Rowman & Littlefield, 2005.

8. Roger Z. George, James B. Bruce, *Analyzing intelligence: origins, obstacles, and innovations*, Center for Peace and Security Studies, Georgetown University Press, 2008.

9. Robert, Kogan, *End of Dream, Return of History*, in Totead the World. American Strategy after the Bush Doctrine, Eds. Melvyn P. Leffler, Jeffrey W. Legro, Oxford University Press, 2008.

10. Roy Ladner, Fred Petry*, Net-centric approaches to intelligence and national security*, Birkhäuser, 2005.

11. Stefano, Guzzini, *Realismul în relaţiile internaţionale şi în economia politică internaţională,* Institutul european, Bucureşti, 2000.

Surse internet

1. http://cssas.unap.ro/ro/carti.htm
2. http://cssas.unap.ro/ro/is.htm

Internetul şi radicalizarea migranţilor musulmani din vestul Europei. Riscuri ale societăţii cunoaşterii.

Daniela SPÎNU
e-mail: **daniella.spinu@yahoo.com**

Abstract

Radical Islam has gained more and more adherents among Muslim migrants of the second and third generation, individuals who no longer identify with any nation state, are prisoners between two cultures and, while living in western european society, studing in european universities, geting married and having children, resort to radical action. In the knowledge society, intelligence communities must connect to complex situations, difficult to prevent, full citizens of european countries turning into executives of terrorist attacks on european soil. Given this general context, the paper focuses on two axes: the role of internet in radicalizing muslim immigrants(having like central coordinates Inspire Magazine and the dialectics of radical leaders) and the intelligence community reaction.

Keywords: knowledge society, immigration, radicalization, internet, Inspire.

Introducere

Atacurile teroriste din Londra şi Madrid, în care au fost implicaţi migranţi musulmani, cu cetăţenie europeană, au dus la teoretizarea unor concepte ca „radicalizare" sau „home-grown terrorism".

Deşi implicarea diasporei în activităţile teroriste nu este un fenomen nou, guvernele din vest tolerând adesea această politică care în ultimă instanţă nu a fost percepută ca ameninţare la adresa siguranţei naţionale[1], particularitatea acestei „noi forme de manifestare a terorismului internaţional" rezidă *de facto* în emergenţa unui nou tip de modus operandi: membri ai comunităţii imigrante participă la acţiuni teroriste îndreptate chiar împotriva guvernelor care i-au adoptat.

Islamul radical a câştigat în ultima perioadă tot mai mulţi adepţi din rândul migranţilor musulmani de a doua şi a treia generaţie, indivizi care nu se mai identifică cu niciun stat naţiune, sunt prizonieri între două culturi

[1] Bruce, HOFFMAN, *The Radicalization of Diasporas and terrorism*, RAND National Security Research Division, Elveţia, 2007.

şi care, deşi trăiesc în societăţi europene occidentale, studiază în şcolile şi universităţile europene, se căsătoresc şi au copii, recurg la acţiuni radicale.

În societatea cunoaşterii, comunităţile de intelligence trebuie să se racordeze unor situaţii complexe, dificil de prevenit, cetăţeni cu drepturi depline ai statelor europene transformându-se în executanţi ai atentatelor teroriste pe teritoriul european.

Plecând de la acest context general, lucrarea vizează două axe: radiografierea (având ca şi coordonate centrale revista „Inspire" şi dialectica liderilor radicali) rolului internetului în radicalizarea imigranţilor musulmani şi reacţia comunităţilor de intelligence.

Radicalizare şi rolul internetului. Concept şi evoluţie

În ceea ce priveşte definirea conceptului de „radicalizare" nu există o poziţie comună, astfel că la nivelul literaturii de specialitate ne confruntăm cu o serie de definiţii care fac trimitere la termeni atât ca „radicalizare violentă" cât şi ca radicalizare în calitate de proces general.

Una dintre cea mai cuprinzătoare definiţii rămâne însă cea a lui Tinka Veldhuis şi Jørgen Staun care susţin că radicalizarea include „orice comportament şi expresie ideologică, inclusiv incitarea, distribuţia materialelor radicale, recrutarea, şi convingerea altora de a împărtăşi viziuni radicale, ce determină o ameninţare la adresa siguranţei societăţilor vestice, fie prin conducerea la terorism fie prin ameninţarea integrării şi facilitarea propagandei radicale ce împărtăşeşte ideologii violente"[2].

Tratând conexiunea dintre *radicalizare* şi *internet,* Magnus Ranstorp[3] susţine că evenimentele de la 9/11, invazia Irakului şi a Afganistanului au produs mutaţii considerabile în cadrul infrastructurii fizice, în sensul în care diseminarea mesajelor propagandistice , a ideologiei, a sfaturilor tactice şi strategice urmează *a posteriori* liniile impuse de reţelele virtuale. Internetul în calitate de superstructură devine „cimentul"[4] reţelelor teroriste. Paradigma este argumentată şi de Smith[5] în viziunea

[2] Tinka VELDHUIS, Jørgen STAUN, *Islamist Radicalisation. A root cause model*, Institutul de Relaţii Internaţionale, Olanda, 2009,p. 11.
[3] Magnus, RANSTORP, *Understanding violent radicalization: terrorist and jihadist movements in Europe*, Ed. Routledge, 2010, p. 111.
[4] Magnus, RANSTORP, *Op. Cit*. p. 185.
[5] Paul, SMITH, *The terrorism ahead. Confronting transnational violence in the twenty first century*, M.E Sharpe, England, 2008, p. 7.

căruia internetul, definit ca „ultimă expresie a puterii revoluției informației", *„have been turned to the advantage of groups committed to terrorizing societies to achieve their goals"*. Autorul[6] grupează valoarea internetului în două categorii: ideațională şi funcțională. Prima situație comportă capacitatea internetului de a se prevala ca o „poartă de ieşire" atât pentru mesajele teroriştilor, cât şi pentru narațiunile capabile să legitimeze acțiunile radicale şi să atragă susținere. Corolară acestei prime dimensiuni, valoarea funcțională atribuie internetului rolul de a se contura ca o interfață între radicali şi susținătorii acestora, un forum de dezbatere ce pune la dispoziția militanților informații tactice şi strategice importante.

Reunind toate aceste versiuni, Bruce Hoffman rezumă importanța internetului în acțiunile extremiste astfel : *"the weapons of terrorism are no longer simply the guns and bombs that they always have been, but now include the mini-cam and videotape(...) CD burners and e-mail accounts, and Internet and worldwide web access that have defined the information revolution today"*[7].

Logica acestui demers este cu atât mai importantă cu cât unul dintre scopurile sale devine cel de a recruta noi adepți, propaganda prin internet fiind *per se* un „vehicul-cheie inspirând, motivând şi animând atât radicalizarea cât şi violența"[8].

Radicalizarea on-line. De la revista *Inspire* la dialectica liderilor radicali

Între 1990 şi 2000 moscheele din Europa au jucat un rol crucial în împărtăşirea viziunilor radicale, transformându-se în „cluburi sociale" ce intermediază legăturile dintre indivizii radicalizați şi grupările teroriste, participând *per se* la radicalizarea şi recrutarea imigranților musulmani, dar şi a cetățenilor europeni convertiți.

Evenimentele din 11 septembrie, precum şi cele de la Londra şi Madrid au dus însă la regândirea politicii permisive. O parte dintre aceste moschei au fost închise, în timp ce imami radicali fie au fost arestați, fie expulzați[9].

---

[6] Paul, SMITH, *Op. Cit,* p. 73.
[7] Bruce, HOFFMAN, *The Use of the Internet by Islamic Extremists*, RAND Corporation, 2006, p. 3.
[8] Bruce, HOFFMAN, *Op. Cit*., p. 18.
[9] Lorenzo, VIDINO, *Radicalization, Linkage and diversity. Currents Trends in Terrorism in Europe*, RAND, 2011, p. 21.

Totuşi, departe de a soluționa problematica radicalizării, autoritățile europene sunt puse în situația de a combate radicalizarea prin internet, un obiectiv de altfel destul de dificil de pus în practică.

Mai mult, atentatele din Londra, Madrid, dar şi cazuri de autoradicalizare din Germania, Olanda sau Suedia, subliniază rolul internetului în calitate de „factor facilitator" al procesului de radicalizare. Spre exemplu, în urma anchetei derulate cu ocazia atentatelor din Madrid, s-au găsit peste 50 de manuale „descărcate" de pe internet. Similar, ancheta grupului de la Hofstaad[10] a făcut trimitere la manuale militare procurate de pe internet de membrii grupării, în timp ce în Germania doi indivizi care intenționau să comită un atentat asupra trenurilor, în iunie 2006, s-au radicalizat ca urmare a vizionării repetate a unor materiale postate pe internet.

În 2007, AIVD (Algemene Inlichtingen enVeiligheidsdienst – n. b. – Serviciul de Informații Olandez) atrăgea atenția asupra rolului internetului în procesul de radicalizare, susținând: *„propaganda nu este un proces unidirecțional: jihadistii caută să interacționeze cu persoane similare. Acest lucru, combinat cu faptul că tot mai mulți tineri îşi petrec timpul liber pe internet, sugerează capacitatea mediului virtual de a acționa ca un teren fertil pentru radicalizare"*[11].

În alte situații, postările islamiştilor radicali pe internet concură la radicalizarea tinerilor musulmani imigranți de a doua generație, aflați în căutarea unui model. Forumurile de socializare devin liniile de legătură între cei care împărtăşesc viziuni radicale cu privire la jihad, membrilor forumului[12] revenindu-le sarcini importante ca apărarea mujahedinilor, distribuirea link-urilor propagandistice sau perceperea mujahedinilor într-o manieră constructivă.

Revista Inspire, publicată în limba engleză în mediul on-line, reprezintă un alt instrument ce facilitează recrutarea şi radicalizarea, postând îndemnuri pentru declanşarea „jihadului individual". Articolul "What to expect from Jihad" trasează indicații clare pentru potențialii mujahedini: *„dacă vii din Vest, ai putea fi întrebat de mujahedini, de ce nu ai inițiat jihadul în interoriul țării tale. Dacă le răspunzi pentru a-i ajuta pe mujahedini, mulți vor răspunde că atacarea inamicului în propria gradină este unul dintre cele mai bune căi de a ajuta jihadul. (..) Efectul*

[10] Thomas, PRECHT, *"Home grown terrorism and islamist radicalization in Europe. From conversation to terrorism"*, Danish Ministery of Justice, 2007, p. 56.
[11] Johnny, RYAN, *"Countering militant islamist radicalization on the Internet"*, IEA, 2007, P. 37.
[12] *Switzerland as a a target for radical islamist propaganda*, ICT, December 2008, p. 4.

este mult mai mare, întotdeauna ruşinează inamicul, aceste tipuri de atacuri individuale fiind imposibil de premeditat"[13].

Aceeaşi revistă vorbeşte despre atacul la adresa americanilor, şi implicit a susținătorilor acestora, încercându-se fundamentarea unei legitimări axate pe dezumanizarea adversarului *„noi, musulmanii nu avem o animozitate îndreptată împotriva unui grup rasial sau etnic. Nu suntem împotriva americanilor doar pentru că sunt americani, suntem împotriva răului şi America în calitate de întreg s-a transformat într-o națiune a răului"*[14]. Divizarea lumii în funcție de dualitatea bine-rău, permite şi o multiplicare a motivațiilor, în condițiile în care acțiunile adversarilor sunt calificate ca motivații superioare idealurilor AQ în procesul de radicalizare. Astfel, făcând trimitere la Nidal Hassan, se specifică: „nu a fost recrutat de idealurile Al-Qaida ci a fost recrutat de crimele americanilor şi asta este ceea ce America refuză să admită"[15].

Reflectând orientarea globală a jihadului, cazurile prezentate ca exemplu se multiplică, accentul fiind mutat pe importanța femeilor în logica atentatelor teroriste produse pe teritoriul european. În acest sens, Roshonara Choudhry, studentă în Marea Britanie, radicalizată prin intermediul internetului, este un caz elocvent, cu atât mai mult cu cât apare în paginile revistei Inspire alături de suedezul musulman Taimour Abdulwahab al-Abdaly cu titulatura de „camarazi ai loialității fără granițe"[16]. Cazul britanicei este utilizat de Inspire ca exemplu pentru musulmanii din Europa, a căror obligație individuală este de a sprijini religia lui Allah prin moarte: *„o femeie le-a arătat bărbaților din Ummah calea jihadului. O femeie, fraților! Ruşine să le fie bărbaților care stăteau indiferenți în timp ce o femeie se implica în jihadul individual"*[17]. În ediția din martie 2011, uciderea a doi americani într-un aeroport din Germania, de către un tânăr din Kosovo de 21 de ani, este privită cu admirație, acesta fiind inspirat de „activitățile pe internet ale mujahedinilor"[18].

Catalogată ca *"the Vanity Fair of Al-Qaida"*[19], revista Inspire reuşeşte să transgreseze dialectica liderilor radicali, care s-a bazat în cele

---

[13] Revista Inspire, Fall 1431/2010, What to expect in jihad.
[14] Revista Inspire, Fall 1431/2010.
[15] Inspire 1431/2010, p. 57.
[16] Revista Inspire, 1431/2010.
[17] Ibidem.
[18] Revista Inspire, Spring 1431/ 2011, p. 6.
[19] Bob, DROGIN, *The 'Vanity Fair' of Al Qaeda*, Los Angeles Times, 26 nov 2010, (http://articles.latimes.com/2010/nov/26/nation/la-na-terror-magazine-20101126).

mai multe cazuri pe limba arabă, oferindu-le musulmanilor imigranți din Europa, capacitatea de a le înțelege mesajele.

Mai mult, mesajul Al-Qaida, de cele mai multe ori inaccesibil, este transformat în ceva care nu numai că poate fi analizat şi interiorizat de cel care vizualizează articolele online cât şi comentat, secțiunile de tip Q&A din cadrul publicației putând fi o cheie importantă de înțelegere a modului în care musulmanii europeni se identifică cu ideologia susținută în cadrul articolelor. Spre exemplu, regăsim întrebări de tipul „locuiesc în Vest şi vreau să merg în locuri ca Afganistan sau Yemen. Am banii pregătiți şi cam ştiu unde vreau să merg. Problema este că nu am niciun contact pentru a mă întâlni cu un mujahedin. Ce mă sfătuiți să fac?”[20]

Cum să pregăteşti o bombă în bucătăria bunicii, cum să utilizezi AK47 sau la ce să te aştepți în jihad sunt câteva secțiuni utilizate pentru a atrage atenția şi suportul, fiind vorba mai mult de o „recurtare ideologică” decât de una operațională[21]. Procesul este însă unul fundamental, dat fiind faptul că desenarea unei „comunități virtuale islamice”[22] constituie prima etapă în identificarea şi selecția potențialilor candidați.

La acest nivel intervine importanța dialecticii unor lideri radicali în susținerea cauzei „jihadului violent”. Cu peste 1910 înregistrări video postate pe youtube (care mai târziu au fost retrase) şi 3,5 milioane de vizualizări, Awlaki a fost unul dintre principalii factori radicalizanți ai imigranților din Vest. Reuşind să combine, în engleză şi arabă, abilitatea de a traduce concepte religioase complexe cu simplitate şi claritate, şi-a obținut o popularitate şi mai mare.

Adepții săi sunt cei care susțin legitimitatea acestuia de a oferi sfaturi utile musulmanilor din statele vestice, cu privire la credință, cu atât mai mult cu cât „trăind în Vest a fost destul de brav încât să le practice religia fără niciun compromis.”[23] Audiența sa, alcătuită în proporții uriaşe din musulmani vorbitori de limbă engleză, poate astfel mult mai uşor să înțeleagă mesajul său fără să dețină *de facto* cunoştințe solide despre cultura şi religia islamică.

---

[20] Revista Inspire, Spring 1431/ 2011, p. 11.

[21] Jonathan FIGHEL, *Radical Islamic Internet Propaganda: Concepts, Idioms and Visual Motifs* in Boaz, GANOR et all, *Hypermedia Secduction for terrorist recruiting*, IOS Press, 2007, p. 36.

[22] Jonathan FIGHEL, *Op. Cit*., pp.36-37.

[23] Jack, BARCLAY,*”Challenging the Influence of Anwar al Awlaki”*, ICSR,The International Center for the study of Radicalisation and Political Violence, King’s College London, 2010, p. 11.

Apariția lui Awlaki în vara lui 2010 într-un clip video aparținând Al-Malahim Media, casa de producție media a AQ în Peninsula Arabică, a fost interpretată de unii analiști[24] ca promovarea unui lider care se vrea mai mult decât unul spiritual. Mai mult, în timpul interviului Awlaki făcea trimitere la jihadul violent afirmând „mesajul meu către musulmani în general şi pentru cei din Peninsula Arabică în mod particular, este că trebuie să participăm la jihadul împotriva Americii"[25]. Conceptul, definit ca „principală datorie în islam şi mijloc de salvare a ummah, ce trebuie practicată de către copil chiar dacă părinții refuză, de femeie chiar dacă soțul obiectează"[26] este una dintre dezbaterile cele mai prolifice.

Aceeaşi temă este tratată şi în revista Inspire, al cărui membru fondator şi mentor a fost Awlaki, articolele sale dezbătând legitimitatea uciderii civililor, justificarea atacului îndreptat asupra statelor din vest sau chiar modalități prin care susținătorii jihadului pot contribui la lupta împotriva infidelilor.

Explicația renumelui său în rândul migranților musulmani este redată de stilul său popular, mesajele accesibile şi referințele la viața din societățile vestice. Accesabilitatea lui este atribuită capacității de a reproduce anumite comportamente, de la cele privind subiectele tratate în timpul lecturilor până la stil, adoptate de nucleul dur al clericilor radicali: Al Maqdisi sau chiar Abdulah Azzam. Linia de demarcație este tocmai lipsa unor cunoştințe solide şi a expertizei în materie de religie. Ori, în mod ironic, susțin unii autori[27], tocmai această replică i-a adus faima. Dat fiind faptul că exista un lider, în persoana lui Osama bin Laden, fiecare figură a Al-Qaida a încercat să se adapteze unui context specific. Astfel, Ayman Al Zawahiri era cunoscut ca serios şi citit sau Abu Laith Al Libi ca şeicul luptător.

Audiența lui Awlaki, spre deosebire de cea a lui bin Laden sau Maqdisi, ale căror discursuri îi atrăgeau în mod special pe extremiştii radicali, include şi indivizi care l-au urmat încă din perioada sa moderată. Câteva comentarii de pe site-ul său reproduc, pe de o parte, măsura acestei personalități, iar pe de alta, irelevanța consistenței religioase în predicile

---

[24] Jack, BARCLAY,Op. Cit., p. 2.
[25] Ibidem.
[26] Anwar, AL AWLAKI, *"44 Ways to support Jihad"*, (http://www.nefafoundation.org/miscellaneous/FeaturedDocs/nefaawlaki44wayssupportjihad.pdf). Site consultat la data de 29 aprilie 2011.
[27] Jarret, BRACHMAN, Alix LEVINE, *"You too can be Awlaki,"* în The Fletcher Forum of world Affairs, Vol35:1, winter 2011, p. 27.

sale: „nu este nevoie să aflăm dacă se numără printre ideologii adevărați sau este doar un imam. Este liderul al cărui mesaj este foarte, foarte relevant pentru musulmanii de astăzi. Aşa că ascultați-l. Nu te poți înşela. Insha'Allah."[28]

Alexander Meleagrou Hitchens argumenta că principala amenințare ce venea din partea lui Awlaki nu era de natură operațională ci se datora "încrederii radicalizante a lecturilor sale şi ideologiei absolutiste"[29].

Spre deosebire de Osama bin Laden şi Ayman al Zawahiri, reuşea să trateze subiecte legate de politica internațională cu o mai mare abilitate, subliniind complotul guvernelor infidele împotriva islamului „diplomația din lumea întreagă se concentrează în jurul unei idei centrale – lupta împotriva islamului". UE se întâlneşte pentru a discuta despre teroriştii islamişti, NATO tratează provocările terorismului islamist, iar SUA îşi mobilizează forța politică pentru a lupta împotriva amenințării islamiste. La nivel politic lumea este unită să lupte împotriva islamului. Nu există nicio excepție."[30]

Reacția comunităților de intelligence. În loc de concluzii…

„Cred că sunt cei mai buni din lume cu serviciile lor: CIA, MI5, MI6 sau cum se mai numesc în America şi în alte părți ale lumii. Ei trebuie să înțeleagă că au de-a face cu o ideologie şi ideologia pe care în acest moment 1,6 miliarde de oameni o au este mai rapidă în difuzare."[31]

Răspunsul pe care comunitățile de intelligence au încercat să îl formuleze de-a lungul timpului cu privire la rolul internetului în procesul de radicalizare nu a dat rezultatele aşteptate. Statele europene au implementat o serie de politici prin care se încearcă limitarea procesului de radicalizare, exemplele cele mai elocvente fiind al Olandei, Belgiei şi Marii Britanii. În Olanda, webmasterii site-urilor care atrag un număr mare de tineri

---

[28] Jarret, BRACHMAN, Alix LEVINE, *Op. Cit*., p. 28.

[29] Alexander, MELEAGROU HITCHENS, *"Voice of terror. Anwar al Awlaki has emerged as the most persuasive supporter of jihad for muslims in the west"*, Foreign Policy, 2011, (http://www.foreignpolicy.com/articles/2011/01/18/voice_of_terror). Site consultat la data de 29 aprilie 2011.

[30] Cristopher, HEFFELFINGER, *"Anwar Al Awlaki: Profile of a jihadi Radicalizer"*, în Combating Terrorism Center at West Point, Vol.3, Issue 3, march 2010 , p. 4.

[31] British islamist abu Abdallah al-Britani, *"The assassination of Anwar al Awlaki and Osama Bin Laden will not stop the spread of Islam"* http://www.memrijttm.org/

musulmani, simpatizanți ai jihadului violent, au implementat un sistem pe baza căruia expresiile radicale sunt înlocuite cu mesaje moderate[32].

Cazul Belgiei şi al Marii Britanii fac trimitere la rolul responsabilizării sociale în lupta împotriva radicalizării în mediul virtual. Deşi au fost create o serie de mecanisme al căror principal obiectiv este cel de a investiga siteurile de internet care promovează extremismul şi violența, cetățenii sunt încurajați să raporteze astfel de situații.

Desigur, în literatura de specialitate[33] una dintre strategiile cele mai frecvent menționate, este cea care face trimitere la utilizarea argumentelor împotriva jihadului violent (care conferă o explicație suplimentară jihadului de tip cut and paste) prin promovarea şi diseminarea viziunilor moderate ale unor imami credibili, dând prioritate educației religioase.

Dacă revista Inspire participă *de facto* mai mult la o „recurtare ideologică" decât la una operațională, eliminarea treptată a principalilor mentori ai ideologiei jihadiste, ca Osama bin Laden sau Anwar al Awlaki, nu afectează capacitatea discursului lor de a radicaliza. Mai mult, acțiunea este calificată drept o „greşeală", în sensul în care *"Obama şi apropiații nu ştiu cu ce au de-a face. Nu ştiu împotriva cui luptă. Ce trebuie să înțeleagă este că luându-ne pe fiecare în parte ca indivizi nu vor opri chemarea către Islam. Ei trebuie să înțeleagă că au de-a face cu o ideologie."*[34]

Declarația imigrantului musulman cunoscut sub pseudonimul de abu Abdallah al-Britani vine în susținerea unui mai vechi comentariu postat pe internet în accepțiunea căruia lideri ca Osama sau Awlaki devin doar purtători ai mesajului al-Islam, apărând viețile inocenților şi răspândind cuvântul adevărului: "chiar dacă ar fi să fie ucis (Awlaki) mâine într-un atac aerian, se va alătura clasicilor dar şi fraților săi recenți, Abdulah Azzam, Yusuf Al-Ayyiry care depun mărturie că nu este necesar să trăieşti printre infideli pentru a fi un propavăduitor al islamului. În acel moment va fi privit ca fiind cel mai popular propovăduitor al islamului vorbitor de limba engleză şi toată lumea îl va asculta şi mai mult"[35].

---

[32] *Radicalisation: the role of the internet*. Insitute for Strategic Dialogue, Stockholm, 2011 p. 8. (http://www.strategicdialogue.org/allnewmats/idandsc2011/StockholmPPN2011_BackgroundPaper_FINAL.pdf).

[33] Johnny RYAN, *Countering militant Islamist radicalisation on the internet: a user driven*, IEA, 2007, pp.133-136.

[34] British islamist abu Abdallah al-Britani, *The assassination of Anwar al Awlaki and Osama Bin Laden will not stop the spread of Islam* (http://www.memrijttm.org/).

[35] Jack, BARCLAY, *Op. Cit*. p. 13.

Ori la acest nivel, intervine dificultatea de a acționa. Chestiunea ideologiei devine problematică în momentul în care chiar printre moderații islamici, care dezaprobă terorismul, nu există un consens cu privire la motivele pentru care acesta ar trebui condamnat: unii fac trimitere la Sharia, la jurisprudența islamică tradițională, în timp ce alții recurg la etimologia cuvântului care nu implică sensul de „război sfânt" şi nici pe cel de conotație militară[36].

În lipsa unei viziuni moderate coerente şi a unei educații religioase, numeroasele fatwa care fac trimitere la jihad în calitate de datorie personală încurajează radicalizarea imigranților musulmani, care, trăind în societățile vestice trebuie să îşi regândească poziția față de guvernele care i-au adoptat.

Bibliografie

Surse Directe

1. BARCLAY, Jack,*"Challenging the Influence of Anwar al Awlaki"*, ICSR,The International Center for the study of Radicalisation and Political Violence, King's College London, 2010.

2. BRACHMAN, Jarret, LEVINE, Alix *"You too can be Awlaki"* , în The Fletcher Forum of world Affairs, Vol35:1, winter 2011.

3. FIGHEL, Jonathan *Radical Islamic Internet Propaganda: Concepts, Idioms and Visual Motifs* în Boaz, GANOR et all, *Hypermedia Secduction for terrorist recruiting*, IOS Press, 2007, p. 36.

4. HEFFELFINGER, Cristopher, *"Anwar Al Awlaki: Profile of a jihadi Radicalizer"*, în Combating Terrorism Center at West Point, Vol. 3, Issue 3, march 2010.

5. HOFFMAN, Bruce, *The Radicalization of Diasporas and terrorism*, RAND National Security Research Division, Elvetia, 2007.

6. HOFFMAN, Bruce, *The Use of the Internet by Islamic Extremists*, RAND Corporation, 2006.

7. PRECHT, Thomas, *"Home grown terrorism and islamist radicalization in Europe. From conversation to terrorism"*, Danish Ministery of Justice, 2007.

8. RANSTORP, Magnus, *Understanding violent radicalization : terrorist and jihadist movements in Europe*, Ed. Routledge, 2010.

9. RYAN, Johnny *"Countering militant islamist radicalization on the Internet"*, IEA, Dublin, 2007.

10. SMITH, Paul, *The terrorism ahead. Confronting transnational violence in the twenty first century*, M.E Sharpe, England, 2008.

[36] Ideea a fost dezvoltată în Daniela, SPÎNU, *„Imigrația musulmană şi identitatea națională în Europa. Împreună sau separați?"* în Sfera Politicii, Vol.XIX, Nr.4 (158), pp. 83-93.

11. VELDHUIS, Tinka, STAUN, Jørgen, *Islamist Radicalisation. A root cause model*, Institutul de Relații Internaționale, Olanda, 2009.

12. VIDINO, Lorenzo, *Radicalization, Linkage and diversity. Currents Trends in Terrorism in Europe*, RAND, 2011.

Surse Internet

1. Anwar, AL AWLAKI, *"44 Ways to support Jihad"*, (http://www.nefafoundation.org/miscellaneous/FeaturedDocs/nefaawlaki44wayssupportjihad.pdf). Site consultat la data de 29 aprilie 2011.

2. DROGIN, Bob, *The 'Vanity Fair' of Al Qaeda*, Los Angeles Times, 26 nov 2010, (http://articles.latimes.com/2010/nov/26/nation/la-na-terror-magazine-20101126).

3. British islamist abu Abdallah al-Britani, *The assassination of Anwar al Awlaki and Osama Bin Laden will not stop the spread of Islam*" http://www.memrijttm.org/

4. MELEAGROU HITCHENS, Alexander, *"Voice of terror. Anwar al Awlaki has emerged as the most persuasive supporter of jihad for muslims in the west"*, Foreign Policy, 2011, (http://www.foreignpolicy.com/articles/2011/01/18/voice_of_terror). Site consultat la data de 29 aprilie 2011.

5. Radicalisation: the role of the internet. Insitute for Strategic Dialogue, Stockholm, 2011.

(http://www.strategicdialogue.org/allnewmats/idandsc2011/StockholmPPN2011_BackgroundPaper_FINAL.pdf).

6. *Switzerland as a a target for radical islamist propaganda*, ICT, December 2008, (http://www.ict.org.il/Portals/0/Internet%20Monitoring%20Group/JWMG_Switzerland_

Radical_Islam.pdf) Site consultat la data de 20 octombrie 2011.

7. Revista Inspire, Fall 1431/2010.

8. Revista Inspire, Spring 1431/ 2011, Issue 5.

Agresiunile în spațiul cibernetic

Dumitru DUMBRAVĂ
Serviciul Român de Informații
e-mail: **dumbrava_dumitru@dcti.ro**

Abstract

Since the advent of Internet in the 1990s, not all users have acted in cyberspace for peaceful purposes. In fact the threat and impact of attacks in and through cyberspace have continously grown to the extent that cyberspace has emerged as a setting for war, with increasing potential to damage the national security of states. Because of this reason, the international community has to come up with a body of norms, or regulations that must be established in order to deter agression in cyberspace.

As cyberspace matures, the international system faces a new challenge in confronting the use of force. Non-state actors continue to grow in importance, acquiring the skill and expertise necessary to wage asymmetric warfare using non-traditional weaponry that can create devastating real world consequences. These actors involved with various types of crimes also vary in their skill sets, interests and motivations. Some are identified as internal threats, while others are external – encompassing national as well as international players. All actors vary in age, education, gender, ethnicity, as well as their skills, professional status and social relationships. Since it is nearly impossible to identify the plethora of actors according to physical discriminating factors, elements of skills, motivation and social relationships within the community of hackers can successfully be used to differentiate and categorize their threat potential. The international legal system must adapt to this battleground and provide workable mechanisms to hold aggressive actors accountable for their actions. The very nature of cyberspace: its lack of territorial definability; its organisational capacities; and its decentralised structure plays an important role in cyberspace governance.

Keywords: cyberspace, cyber agressions, cyber security, cyber intelligence.

Aprecieri preliminare

Apariția şi dezvoltarea calculatoarelor electronice a reprezentat o adevărată revoluție în societatea umană, având ca principală consecință tranziția de la societatea industrială la societatea informațională.

Calculatorul a devenit o componentă normală a activității noastre zilnice, iar tehnologia comunicațiilor şi posibilitățile oferite de Internet au produs transformări în întreaga societate, pătrunzând în toate aspectele vieții economice, sociale şi culturale.

Istoria Internetului este o lectură fascinantă, plină de paradoxuri, originile sale putând explica pe deplin configurația sa actuală. Ca în orice domeniu în care inovația joacă un rol deosebit, în Internet există etape precursoare, acumulări anterioare mai importante sau mai puțin importante. Dezvoltarea Internetului a depins, în mod evident, de tehnologie, dar în egală măsură şi de factori sociali care s-au îmbinat pentru ca acesta să ajungă ceea ce este astăzi. Iar o dată instaurat în fibrele societății, Internetul a produs şi produce consecințe noi pentru societate, cel mai important dintre acestea fiind procesul de globalizare.

În anul 1990, Internetul cuprindea aproximativ 3000 de rețele şi 200.000 de calculatoare, în 1992, existau peste 1 milion de gazde, iar în anul 1995 existau mai multe coloane vertebrale (rețele principale), sute de rețele de nivel mediu (regionale), zeci de mii de LAN-uri, milioane de gazde şi zeci de milioane de utilizatori. Mărimea Internet-ului se dublează aproximativ la fiecare an, iar creşterea lui este datorată şi conectării unor rețele existente, precum rețeaua de fizică spațială NASA.

Caracterul academic, guvernamental şi industrial pe care l-a avut Internetul până în anul 1990 s-a transformat, însă, odată cu apariția noii aplicații WWW (World Wide Web), care a adus în rețea milioane de utilizatori neprofesionişti. În zilele noastre, mediul Internet poate fi privit ca o rețea de rețele, un mediu informațional şi de calcul cu resurse şi servicii extrem de bogate, biblioteci şi baze de date, el reunind, prin facilitățile de informare şi comunicare oferite, o comunitate de persoane din toate domeniile vieții economico-sociale şi răspunzând la solicitări diverse.

Astfel, dacă în anii 1970 sintagma predominantă era aceea de Societate informatică, treptat conceptul de Societate informațională a câştigat tot mai mult teren şi a devenit o realitate din momentul exploziei Internetului, cu accente deosebite în ultimul deceniu al secolului XX, pentru prima parte a secolul XXI urmând a se pune problema Societății Cunoaşterii.

În acest context, Societatea Cunoaşterii depinde, cu siguranță, de performanțele şi securitatea infrastructurilor critice, precum: sistemele de producere, transport şi distribuție ale energiei, sistemele de telecomunicație, bănci, sistemele de transport aerian, naval, rutier şi feroviar.

„Cunoaşterea”, ca atare, a devenit o „armă” de apărare împotriva

ameninţărilor cu care se confruntă un mediu popular, uşor de utilizat şi care, în acelaşi timp, oferă o cantitate imensă de informaţie despre orice subiect posibil.

Spaţiul cibernetic

Noţiunea a fost lansată pentru prima dată de către William Gibson – scriitor canadian de science fiction – în anul 1982, prin nuvela „*Burning Crome*", apărută în revista *Omni*, care a fost ulterior popularizată în romanul său – „*Neuromancer*". Aceasta a devenit o sursă de inspiraţie artistică care a generat cybercultura şi, datorită importanţei şi relevanţei ei psiho-sociologice, un obiect de studiu pentru ştiinţele sociale, determinând apariţia unor areale teoretice şi de cercetare, precum psihologia şi sociologia cyberspaţiului, informatica socială etc.

Spaţiul cibernetic este corelat cu o serie de termeni înrudiţi, precum cei de realitate virtuală, mediu *online*, spaţiu digital, care alcătuiesc împreună un aparat conceptual, încă destul de tânăr şi, prin urmare, disputat, ce s-a conglomerat în jurul noului domeniu. Asupra noţiunii de spaţiu cibernetic s-au adunat, în timp, mai multe perspective, pe măsură ce acest fenomen s-a dezvoltat în extensie, profunzime şi nuanţe prin răspândirea şi popularizarea reţelei mondiale de computere şi telecomunicaţii (ce include Internetul, Usenetul şi alte reţele mai mici ca importanţă) şi, prin varierea instrumentelor şi aplicaţiilor (domeniul de *software*), varietate la fel de exponenţială ca şi globalizarea infrastructurii sale (*hardware şi netware*).

În principiu, spaţiul cibernetic nu trebuie confundat cu Internetul real (ca reţea), ci trebuie privit ca însumând aspectele psihologice şi sociale pe care i le conferă, prin utilizare, psihicul uman individual şi societatea în ansamblu. Acesta cuprinde, prin urmare, identităţile şi obiectele care există în reţele de computere folosite de indivizii umani în diverse scopuri.

Multitudinea perspectivelor de analiză a generat numeroase teorii şi definiţii acordate spaţiului cibernetic.

În prezent, spaţiul cibernetic a devenit coloana vertebrală a ceea ce numim Societatea Cunoaşterii, concepută ca un mediu foarte diferit, fără precedent, în care implementarea ultimelor realizări tehnice trebuie să meargă în paralel cu adoptarea de noi soluţii juridice menite să monitorizeze efectele negative ale impactului utilizării tehnologiei informaţiei şi comunicaţiilor şi ameninţările în mediul informaţional.

Ameninţări

Contrar convingerii larg răspândite, preocupările legate de securitatea cibernetică nu sunt un fenomen al anilor 1990. Viruşii şi viermii informatici au fost o parte din zgomotul de fundal al spațiului cibernetic, chiar dintr-o perioadă timpurie. Astfel, în filmul „War Games", produs în anul 1986, un tânăr adolescent hacker reuşeşte ca, prin intermediul computerului personal, să dețină comanda şi controlul asupra arsenalului nuclear american. De asemenea, celebrul incident „Cuckoo's Egg", de la mijlocul anilor '80, a atras atenția că organizațiile de spionaj au descoperit noi modalități de a obține informații clasificate, prin intermediul rețelelor de calculatoare.

În acest context, dezbaterile pe teme cibernetice, îşi au originea în Statele Unite la mijlocul anilor '90, de unde s-au răspândit ulterior în alte țări dezvoltate şi sunt trecute într-o varietate de forme pe ordinea de zi a politicilor de securitate.

Comparativ cu analiza amenințărilor tradiționale, care constă în analize ale actorilor, intențiilor şi capacităților lor, amenințările în mediul informațional au caracteristici diferite care fac atacurile dificil de monitorizat, analizat şi contracarat. Aceste caracteristici se încadrează în tipologii care pot fi regăsite în toate țările, deşi accentul pus pe una sau mai multe dintre ele conduce la diferențe considerabile.

În prezent, amenințările la adresele utilizatorilor variază de la accidente, căderi de sistem, programări greşite şi eşecuri umane, la atacuri ale hackerilor. Totodată, securitatea cibernetică este o şi problemă economică, iar acest concept este definitoriu pentru continuitatea afacerilor, în special a afacerilor on-line, care, pentru performanță, necesită acces permanent la infrastructurile de comunicații.

Şi, deşi multe organizații au investit în mod semnificativ în obținerea de informații în acest domeniu, majoritatea experților în securitatea rețelelor de calculatoare cred că un adversar bine echipat din punct de vedere tehnologic va avea mai mult succes în derularea unor agresiuni cibernetice cu impact semnificativ atât din punct de vedere distructiv cât şi al complexității tehnice, mai ales dacă dezvoltarea mecanismelor de protecție a sistemelor de calcul este singurul răspuns la un atac.

Deci, ne aflăm în fața unei mari probleme, foarte greu de rezolvat, deoarece în interiorul arhitecturii Internet actuale este aproape imposibil să se identifice sursa atacurilor cibernetice, iar capacitățile de investigație din lumea fizică sunt mult mai avansate decât sunt cele din domeniul cibernetic.

Datorită structurii globale a rețelelor de informații, atacurile pot fi

lansate de oriunde din lume, iar descoperirea originii atacurilor rămâne o dificultate majoră, în cazul în care acestea sunt într-adevăr detectate.

De asemenea, nu există statistici exacte referitor la agresiunile cibernetice care au loc anual, însă majoritatea experților consideră că numărul celor derulate în zilele noastre este atât de mare încât cifrele par irelevante. Cu titlu de exemplu, menționez că numărul lor este atât de mare încât, în anul 2004, guvernul american a oprit raportarea agresiunilor cibernetice în acel an, în condițiile în care în anul 2003 acestea depăşiseră 100.000.

Taxonomia amenințărilor

Într-un interviu cu Information Security Media Group, Dmitri Alperovitch (McAfee Labs) vorbeşte despre provocările amenințărilor prezente din mediul informațional şi face referiri la modul în care le pot contracara persoanele fizice şi juridice.

Astfel, acestea sunt principalele riscuri şi vulnerabilități identificate de McAfee Labs pentru anul 2011[1]:

Exploatarea rețelelor de socializare

Rețelele de socializare ocupă locul principal în furtul de identitate, precum şi ca distribuitor de malware pe e-mail. În mod similar, se constată, de asemenea, creşterea abuzurilor prin scurtarea URL-ului şi prin dezvoltarea serviciilor locative.

Telefoane mobile inteligente (smartphones)

Accesarea internetului de pe telefoanele mobile inteligente pentru îndeplinirea unor atribuții de serviciu are drept urmare creşterea amenințărilor cibernetice nu numai pentru indivizi, dar şi pentru angajatorii lor.

Apple

Din punct de vedere istoric, sistemele de operare Apple nu au fost direcționate pentru abuz, dar popularitatea iPad-urilor şi iPhone-urilor în afaceri şi portabilitatea uşoară de cod malițios ar putea schimba acest lucru, în anii următori.

Aplicații

[1] http://www.bankinfosecurity.asia/podcasts.php?podcastID=908

Fie la domiciliu, fie la locul de muncă, aplicațiile pe dispozitive, cum ar fi iPhone şi Androids devin din ce în ce mai populare şi vor deveni din ce în ce mai mult obiective-țintă, întrucât au un istoric slab de codare şi practici de securitate primitive, astfel încât infractorii din spațiul cibernetic vor încerca să manipuleze o varietate de dispozitive fizice prin aplicații compromise sau controlate, precum şi prin creşterea eficienței botnets la un nou nivel.

Rafinamentul imită legitimitatea

În anul 2010, s-a observat o creştere a gradului de sofisticare al unor amenințări, cum ar fi malware disimulat în fişiere normale. Deoarece această tendință s-a intensificat în anul 2011, s-a putut observa o creştere a tehnicilor şi echipamentelor destinate să creeze chei false.

Supraviețuirea Botnet

În anul următor, McAfee Labs se aşteaptă mai degrabă la o creştere a botnet-urilor care elimina datele din sistemele orientate, decât trimiterea de spam. Botnet-urile se vor angaja în colectarea de date rezultate din exploatarea rețelelor sociale.

Activismul cibernetic (Hacktivism)

În ceea ce demonstrează episodul WikiLeaks, hacktiviştii vor creşte utilizarea de crowdsourcing pentru a recruta o armată de hackeri motivați să urmeze o agendă politică. Aceste atacuri nu sunt sofisticate şi organizațiile ar trebui să poată să se apere cu succes împotriva lor în cazul în care iau măsurile corespunzătoare.

Avansarea de amenințări persistente

Aceste atacuri, efectuate fie de către statele națiune sau garantate în mod direct sau indirect, de către guverne străine, nu au fost extrem de sofisticate, dar după cum spune si numele, ele sunt persistente. Se aşteaptă intensificarea acestora în anul următor, fiind vizate arhivele e-mail, documentele şi bazele de date ale arhivelor de proprietate intelectuală.

De asemenea, în ultimele luni, o atenție deosebită a fost acordată unor evenimente de un nivel mai modest, deşi supărătoare, cum ar fi

agresiunile suportate de către RSA, Sony şi Epsilon.

În acelaşi registru, Joe Gottlieb, directorul executiv al riscului şi securităţii, furnizor de software de management SenSage, compară publicitatea agresivă promovată de hactivişti cu operaţiunile efectuate pe furiş de către actorii din operaţiunea RAT Shady[2]: „Aceste hackeri s-au implicat în colectarea de informaţii fără a trebui să trâmbiţeze atacurile lor cu succes, aceştia au rămas tăcuţi pentru a acumula în linişte IP valoroase şi alte produse digitale de contrabandă". Aceasta este cheia, respectiv actele ascunse ale agresiunilor cibernetice, pe care le vom vedea tot mai mult începând de astăzi.

Abilitatea de a automatiza colectarea datelor, eforturile tenace de folosire a Cyber-crawlerelor, crearea de spaţii tot mai largi în acelaşi timp cu transmiterea datelor recoltate înapoi la o imensă bază de date de informaţii, în vederea acumulării sunt principalele atuuri dar şi principalii factori de vulnerabilitate

Din acest punct de vedere, ameninţările cibernetice, adevărate ameninţări la adresa securităţii naţionale, ca şi atacurile împotriva infrastructurii informatice a altui stat sau oponent, sunt percepute în general ca instrumente de coerciţie strategică.

În timp ce atacurile care încalcă confidenţialitatea, integritatea sau disponibilitatea sistemelor de informaţii ar putea, cel puţin teoretic, să fie tratate ca acte de război şi să fie introduse în domeniul de aplicare al controlului armamentului, ori să fie supuse dispoziţiilor care reglementează dreptul războiului.

Aşadar, într-un mediu în care actorii şi motivele sunt necunoscuţi, iar consecinţele potenţiale pot fi de amploare, este uşor de înţeles de ce există o mare îngrijorare.

Iar în cazul în care există atât de mulţi actori, cu atât de multe motive, iar activităţile desfăşurate de aceştia ar putea fi inofensive şi chiar protejate prin Constituţie, este uşor de înţeles de ce persoanelor responsabile pentru implementarea măsurilor strategice şi tactice le vine atât de greu.

Într-o lume plină de diverse ameninţări, precum şi de acuzaţii referitoare la creşterea criminalităţii cibernetice, spionajul economic, spionajul militar şi războiul informatic, este extrem de important ca guvernele şi profesioniştii din domeniul securităţii sistemelor informatice să gândească diferenţiat despre evenimentele cibernetice de tip malware şi despre

[2] http://blogs.mcafee.com/mcafee-labs/revealed-operation-shady-rat

modalitatea de a răspunde la ele.

Punctul de pornire este acela de fracturare a agresiunilor prin sistematizare şi clasare. Cu privire la „cine" (şi în mod implicit „de ce"), poate exista o puternică atribuire, o oarecare probabilitate de atribuire (mai ridicată sau mai scăzută) sau nici o atribuire.

În aceşti parametrii, mai pragmatici, principalele ameninţări cibernetice pot fi definite pe următoarele coordonate:

Spionajul cibernetic, în care cel mai mare pericol îl reprezintă serviciile de informaţii, civile şi militare. Anumite ţări utilizează grupările de hackeri şi criminalitate organizată informatică drept forţe cu rol de proxy – în spatele cărora se ascund pentru a putea nega implicarea lor, ca actor statal.

Spionajul cibernetic are 3 dimensiuni:

a) Spionajul economic – produce prejudiciul cel mai grav, deoarece instituţii guvernamentale, companii şi cetăţeni străini sunt angrenate în operaţiuni de furt al proprietăţii intelectuale şi al informaţiilor de afaceri confidenţiale. Fiecare euro investit de statul ţintit şi fiecare an de cercetare-dezvoltare a tehnologiilor de vârf se transformă în cenţi cheltuiţi şi zile consumate de statul agresor pentru a obţine prin spionaj economic acelaşi avantaj tehnologic şi economic.

b) Spionajul politic.

c) Spionajul militar.

Datorită unui nivel scăzut al securităţii cibernetice, spionajul cibernetic oferă posibilităţi de neimaginat în culegerea de informaţii, atât în volum cât şi în sensibilitate, greu de atins prin spionajul clasic.

În acelaşi timp, constituie un nou instrument pentru acţiunea politică statală: în loc să controleze crima organizată sau să creeze diversiuni prin relatări false în ziare, un serviciu de informaţii poate influenţa decizii prin atacuri DDoS, efectuează demascări prin Internet a documentelor obţinute prin hacking sau poate utiliza viruşi sofisticaţi în încercarea de a manipula politica statului agresat.

Criminalitatea organizată cibernetică, al cărui scop este mai degrabă patrimonial, să obţină bani de la instituţii financiar-bancare, decât să sustragă proprietatea intelectuală a unor ţinte. Criminalitatea organizată cibernetică nu va urmări să atace Infrastructura Critică Informaţională a unui stat, atât timp cât infractorii sunt ocupaţi să producă prejudicii financiare, însă în anumite condiţii, aceste prejudicii pot atinge o dimensiune care să afecteze stabilitatea a unor pieţe financiare sau a unor economii, context în care devine de interes pentru securitatea naţională a unui stat.

Se consideră că, în anumite țări, criminalitatea organizată cibernetică poate juca un rol important de forță proxy, atât timp cât oferă unor state capacitatea de a nega implicarea în operațiuni de spionaj sau acțiuni politice.

Activismul cibernetic (hactivismul) – în prezent nu reprezintă un risc acut pentru securitatea națională, însă va continua să-şi mențină tendința atât de intensificare, motivat de un spectru din ce în ce mai larg de motivații pentru sancționarea unor atitudini politice, sociale, ecologice, religioase şi militare, cât şi de radicalizare a impactului acestor atacuri.

Terorismul cibernetic – acesta nu este un risc în acest moment. Teroriştii nu au lansat, până în prezent, nici un atac cibernetic şi ca atare, se consideră că nu sunt întrunite condițiile ca aceste grupări să asimileze cunoştințele tehnologice necesare astfel încât, pe termen scurt şi mediu (3-5 ani) să realizeze un atac de complexitate mare la adresa ICI ale unui stat.

Pe termen lung, nu este, totuşi, exclusă o astfel de evoluție, având în vedere tocmai asimetria amenințărilor cibernetice.

Riscul unui război cibernetic a apărut pe harta de riscuri ale unui stat modern, odată cu apariția virusului Stuxnet, şi deşi este în prezent într-o fază incipientă, evoluția va fi extrem de dinamică. Pe termen scurt, atacurile militare cibernetice vor fi utilizate doar într-un context mai larg al unui conflict militar convențional.

De asemenea, o amploare deosebită a luat în ultimii ani şi **agresarea comunicațiilor electronice.** Astfel, în primul trimestru al anului 2011, a fost semnalată intruziunea în comunicațiile electronice provenite din 199 de țări de pe mapamond. Myanmar a fost în topul surselor de atac al comunicațiilor, reprezentând 13% din totalul agresiunilor observate.

În acest domeniu, Statele Unite ale Americii şi Taiwan ocupă cea de a doua şi, respectiv, cea de a treia poziție, acumulând împreună aproape 20% din totalul atacurilor[3]. Concentrația agresiunilor a fost mai mică cu 10 porturi decât în al patrulea trimestru din anul 2010, reprezentând 65% din totalul agresiunilor observate, fiind remarcat inclusiv un set de atacuri care au urmărit au căutat să utilizeze instrumentele de confidențialitate TOR de pe Internet ca modalități de a-şi ascunde urmele.

Securitatea cibernetică

Protejarea spațiul cibernetic este o responsabilitate comună, nicio entitate individuală sau grup de persoane interesate neputând rezolva singuri

[3] http://www.akamai.com/stateoftheinternet/

problemele în acest domeniu.

Cei implicați în industrie, consumatorii, marile companii şi guvernele trebuie să ia toate măsurile pentru a-şi asigura propriile sisteme informatice, fiind nevoie să colaboreze unii cu alții pentru a defini şi a pune în aplicare politici din domeniul securității cibernetice şi al tehnologiei.

Securitatea cibernetică nu presupune doar protejarea împotriva amenințărilor actuale. Ea permite, de asemenea, creşterea randamentului şi beneficiul de a permite utilizări extinse şi mai sofisticate în mediul digital.

Totodată, securitatea cibernetică oferă persoanelor fizice, companiilor şi guvernelor mai multă încredere că pot opera în acest mediu, şi îi pot încredința bunuri de valoare şi informații.

În lumina celor de mai sus, putem concluziona că elementele de referință pentru asigurarea securității spațiului cibernetic trebuie orientate pe următoarele coordonate:

- Securitatea din spațiul cibernetic nu este o problemă opțională, ci o necesitate imperioasă, având în vedere impactul acesteia asupra securității naționale, siguranței publice şi bunăstării economice.
- Problema securității cibernetice trebuie să treacă dincolo de măsurile tradiționale, tehnologice, cum ar fi programele anti-virus si firewall-uri.
- Securitatea cibernetică trebuie să fie dinamică în structura sa, şi să aibă profunzimea necesară pentru a identifica, opri şi preveni atacurile.
- Securitatea informațiilor trebuie să constituie o componentă integrantă a securității în spațiul cibernetic, pentru a fi în măsură să anticipeze atacuri, să adopte măsuri adecvate de combatere şi să-şi însuşească atributele de acțiune împotriva posibilelor atacuri.

Cu alte cuvinte, trebuie urmărită corelarea eficientă a informațiilor recepționate din surse multiple şi monitorizarea în timp real a bunurilor care au nevoie de protecție, prin asigurarea expertizei corespunzătoare pentru a face față situațiilor de criză.

Apărarea cibernetică

În timp ce securitatea cibernetică este activitatea de protecție a informațiilor şi a sistemelor informatice (rețele, calculatoare, baze de date, centre de date şi aplicații), cu măsuri de securitate adecvate din punctul de vedere procedural şi tehnologic şi are un caracter generic, incluzând toate activitățile de protecție, apărarea cibernetică se referă la o activitate mult mai specializată, legată de aspecte particulare şi de organizare.

În general, apărarea cibernetică este determinată de informațiile obținute cu privire la amenințările îndreptate contra sistemului de apărare, care conduce, colectează, analizează şi difuzează informații relevante şi secrete utilizabile pentru părțile interesate de inițierea unor demersuri proactive necesare, în vederea întreprinderii măsurilor de prevenire şi protecție, termenul specific acesteia fiind acela de „cyber intelligence". Acesta este un termen despre care nu auzi prea multe, dar care ar putea reține o atenție mult mai mare în perioada următoare.

Cu privire la acesta, Chuck Alsup, vice-preşedintele desemnat cu politica Alianței Nord-Atlantice a declarat că „Noi nu sunt încă pregătiți să propunem o definiție definitivă". „În acest moment, vorbim despre amenințările neidentificate din domeniul cibernetic, cu potențiale consecințe enorme, de la distrugerea fizică la haosul economic. Oamenii care monitorizează şi răspund de aceste amenințări formează o singură organizație constituită cu ajutorul guvernului, zonei de afaceri şi mediului academic, precum şi al partenerilor străini"[4].

Principiile directoare ale securității cibernetice

Standardele internaționale stabilite de către industrie şi acceptate pe plan internațional, stau la baza tehnologiei informației de la nivel mondial (IT), fiind menite să impulsioneze dezvoltarea şi utilizarea unor tehnologii inovatoare şi sigure. Politica securității cibernetice ar trebui să mențină rolul standardelor internaționale.

Politicile de securitate cibernetică trebuie să recunoască natura fără margini a Internetului, a economiei globale şi a amenințărilor cibernetice şi, drept urmare, este indicat ca guvernele să coopereze pentru a asigura cadrul legislativ național de politică cibernetică integrată în abordările şi practicile globale.

Regimurile sunt de obicei definite drept „seturi de principii implicite sau explicite, norme, reguli, şi procese de luare a deciziilor în jurul unor valori determinate", elemente care converg spre domeniul relațiilor internaționale.

În ultimele două decenii, o serie de inițiative au fost întreprinse pe plan internațional în vederea îmbunătățirii securității şi fiabilității sistemelor, a practicilor de management, precum şi a cooperării polițieneşti internaționale.

Astfel, pentru a ajuta guvernele să construiască şi să implementeze planuri cuprinzătoare şi viabile, care să funcționeze la nivel național şi mondial,

[4] http://blogs.govinfosecurity.com/posts.php?postID=1061

Business Software Alliance BSA a stabilit următorul set de principii directoare[5]:

1. Politica marilor trusturi cibernetice ar trebui să sporească încrederea consumatorilor, întreprinderilor şi guvernelor cu privire la confidenţialitatea, integritatea şi disponibilitatea mediului on-line.
2. Inovaţia în mediul cibernetic este o cursă extrem de rapidă, în care ne lovim de acţiunea infractorilor cibernetici, care se adaptează în mod constant.
3. Politica în domeniul securităţii cibernetice ar trebui să maximizeze capacitatea organizaţiilor de a dezvolta şi adopta cea mai recentă gamă posibilă de soluţii cibernetice.
4. În cadrul unei abordări bazate pe riscuri, consumatorii, întreprinderile şi agenţiile guvernamentale încearcă să protejeze un spectru extins de obiective împotriva unei game largi de ameninţări cibernetice.
5. Mecanismele securităţii cibernetice permit punerea în aplicare a măsurilor de prevenire care sunt cele mai potrivite pentru a atenua riscurile specifice cu care se confruntă.

Posibile soluţii

Peisajul ameninţărilor cibernetice a evoluat semnificativ în ultimii ani, în primul rând de la contestarea serviciilor şi vandalism pe site-urile web în ultimii ani, la adversarii din prezent bine echipaţi din punctul de vedere tehnologic, care utilizează tehnologii complexe pentru a obţine beneficii financiare şi politice.

Privind în urmă, anii 2010-2011 par să fi fost dominaţi de rapoarte pe o singură problemă de securitate analizată într-un mod special: ameninţările cibernetice. Prejudiciul provocat de atacurile cibernetice este din ce în ce mai frecvent, mai organizat şi mai costisitor, iar percepţia asupra acestui fenomen s-a schimbat.

Rezultatul este clar: atacurile cibernetice sunt considerate unele dintre ameninţările de securitate de top şi au fost reglementate în documentele naţionale de strategie peste tot în lume.

Astfel, descoperirea Stuxnet, super-viermele sabotor al industriei, care a speriat politicienii din toată lumea, poveştile despre spionajul chinez în mai multe variante, creşterea nivelului de specializare al infractorilor cibernetici aşa cum reiese din escrocheriile lor impresionante, precum si documentele Wikileaks despre canalele diplomatice şi acţiunile ulterioare ale grupului de hackeri Anonim, toate acestea au catapultat subiectele

[5] http://www.bsa.org/~/media/Files/Policy/Security/CyberSecure/Cybersecurity_Framework.ashx

cibernetice din domeniul excentricilor experţi IT şi al strategilor militari într-o fobie publică.

Devine clar pentru toată lumea că securitatea cibernetică este tot mai pregnant o problemă de securitate naţională, societatea aşa cum o ştim, precum şi valorile sale de bază fiind pe cale de dispariţie, din cauza dependenţei lor de domeniul informaţiei şi tehnologiei comunicaţiilor.

Acţiunea împotriva acestei ameninţări se desfăşoară, atât la nivel naţional cât şi în plan internaţional, pe mai multe niveluri tehnice, legislative sau organizatorice, iar actorii sunt specialiştii în securitatea informatică.

Având în vedere această stare de spirit generală, menţiunile NATO se referă în documentul „Noul Concept Strategic”[6] din noiembrie 2010 la atacurile cibernetice ca fiind unele dintre problemele esenţiale pentru viitorul său de securitate.

Dar pentru NATO acest fapt nu a reprezentat doar o potenţială strategie, el este totodată un element de referinţă prin care marchează un punct culminant în politica de securitate a Alianţei care se ocupă cu analiza ameninţării.

Pornind de la aceeaşi concluzie evidentă că nici o naţiune din zilele noastre nu poate face faţă ameninţărilor cibernetice pentru a gestiona pe cont propriu arhitectura globală de reţele, deoarece natura acesteia, împreună cu numărul semnificativ de agenţi implicaţi în administrarea sistemelor, face imposibilă identificarea unei limite de aplicare în cadrul jurisdicţiilor stabilite sau definite teritorial, Consiliul Europei a elaborat în anul 2001, Convenţiei privind Criminalitatea Cibernetică.

Păstrând aceleaşi coordonate, în ultimii ani, instituţiile UE au făcut un pas important pentru a contracara ameninţările atacurilor cibernetice îndreptate împotriva lor, a organismelor şi agenţiilor, prin înfiinţarea unui Computer Emergency Response pre-configuration TEAM (CERT)[7]. Echipa astfel formată reuneşte experţi în securitate IT de la toate instituţiile UE. La terminarea stagiului de un an pregătitor în echipă, va fi făcută o evaluare menită să conducă la o decizie cu privire la condiţiile de stabilire a unui CERT pe scară largă pentru instituţiile UE.

În ultimii ani, CERT au fost dezvoltate în sectoarele privat şi public, atât în echipe mici de cyber-experţi conectaţi la Internet, care pot în mod eficient să răspundă la incidentele de securitate a informaţiilor şi la ameninţările cibernetice, de multe ori pe o durată de 24 de ore pe zi, timp de şapte zile

[6] http://www.nato.int/strategic-concept/index.html
[7] http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/694

pe săptămână.

În Agenda digitală pentru Europa[8], adoptată în luna mai 2010 (a se vedea IP/10/581, MEMO/10/199 şi MEMO/10/200), Comisia s-a angajat să stabilească un CERT pentru instituţiile UE, ca parte a angajamentului asumat, într-o reţea consolidată la nivelul UE si a politicii de informaţii pentru securitate în Europa.

În luna august 2010, Comisia a solicitat unui număr de patru experţi în securitatea cibernetică, cunoscuţi sub numele de „Rat der IT Weisen"[9], să facă recomandări cu privire la modul de a înfiinţa un astfel de CERT.

Raportul lor a fost finalizat în luna noiembrie 2010. Agenda digitală, de asemenea, invită toate statele membre să stabilească propriile lor CERT-uri, deschizând calea către o reţea de echipe naţionale şi guvernamentale Computer Emergency Response, la nivelul UE, până în anul 2012 (a se vedea IP/11/395).

Concluziile adoptate pe data de 27 mai de către Consiliul UE al miniştrilor telecomunicaţiilor au confirmat acest obiectiv.

Neelie Kroes, vicepreşedinte al Comisiei Europene pentru Agenda digitală, a declarat că „cyber-atacurile sunt o ameninţare foarte reală şi în continuă creştere, fie împotriva unor entităţi statale, a companiilor sau cel mai recent împotriva Comisiei Europene, acestea putând paraliza cheile de infrastructură şi cauza daune imense pe termen lung".

Implementarea acestui CERT pre-configurare în echipă este o demonstraţie a modului în care instituţiile UE iau în serios ameninţările la adresa securităţii informatice.

În loc de concluzii

Din cele prezentate un fapt devine evident, acela că securitatea informaţiilor se referă atât la oameni cât şi la tehnologii şi, ca atare, există o nevoie clară de concentrare atât asupra activităţii oamenilor şi a proceselor tehnologice. Este nevoie de timp pentru a identifica cele mai bune soluţii, dar acestea trebuie să aibă în vedere că cele mai bune soluţii tehnologice disponibile s-ar putea dovedi ineficiente fără o utilizare a forţei de muncă într-un mod adecvat, instruit şi calificat, pentru obţinerea unor rezultate eficiente într-un domeniu extrem de specializat, reprezentat de securitatea cibernetică.

Astfel, apărarea are nevoie să fie construită încă din faza de proiectare conceptuală, atunci când vine vorba despre dezvoltarea şi implementarea infrastructurilor critice de informaţie, spre deosebire de mecanismele de protecţie care au ca obiectiv implementarea după un proiect ulterior.

Planificarea strategică a securităţii cibernetice este, în prezent,

[8] http://ec.europa.eu/information_society/digital-agenda/index_en.htm

[9] http://www.enisa.europa.eu/media/news-items/speech-on-european-and-international-cooperation-on-incident-response

în plină dezvoltare şi trebuie concentrată pe dezvoltarea la scară largă a serviciilor, pentru realizarea acestui deziderat fiind necesar ca toţi actorii implicaţi să acţioneze în mod concertat.

Din punctul de vedere istoric, majoritatea naţiunilor au elaborat versiuni originale ale Strategiilor societăţii informaţionale, cu o elementară atenţie acordată criminalităţii cibernetice în cadrul politicii naţionale de securitate cibernetică reflectată la dimensiunea securităţii naţionale.

Astfel, Guvernele din întreaga lume îşi recunosc atribuţii multiple în asigurarea securităţii cibernetice, incluzând:

1. Protecţia sistemelor informatice.
2. Colaborarea cu sectorul privat pentru a proteja infrastructura digitală.
3. Investigarea, cercetarea şi urmărirea penală a infractorilor cibernetici.

Însă, într-un mediu în care există atât de mulţi actori, cu atât de multe motive, în care consecinţele potenţiale pot fi de amploare, iar activităţile desfăşurate de actori sunt uneori la limita legalităţii şi chiar protejate prin Constituţie, este uşor de înţeles de ce există o mare îngrijorare şi de ce, mai mult ca oricând, este extrem de important ca guvernele şi profesioniştii din domeniul securităţii sistemelor informatice să-şi conjuge eforturile pentru a putea asigura protecţia unui spaţiu precum cel cibernetic.

Bibliografie selectivă

Resurse Internet

1. http://www.bankinfosecurity.asia
2. http://blogs.mcafee.com
3. http://www.akamai.com
4. http://blogs.govinfosecurity.com
5. http://www.bsa.org
6. http://www.nato.int
7. http://europa.eu
8. http://ec.europa.eu
9. http://www.enisa.europa.eu

Războiul din Georgia pe fluxurile de ştiri

dr. Alexandru IOAN
Radio România Actualităţi, Societatea Română de Radiodifuziune
e-mail: **alexandru_ioan@yahoo.com**

Abstract

Mass-media has a crucial contribution to securing the international environment. The presentation is about press reports in a frozen conflict zone, where the conflict was reloaded. This analisys shows how „the 5 Days War" - as the invasion of Georgia by Russian troops in the summer of 2008 was named-was covered. This case was chosen because unlike other operations which were widely publicized long before their triggering, the increasing tension in Southern-Caucasus had a sporadic and anemic coverage in international media. The study has focused on the greatest news agencies of the world: Reuters and AFP, the russian news agency Itar-Tass, Interfax, Ria Novosti and Regnum and the romanian news agencies: Agerpres, Mediafax and Rador.

Keywords: Georgia, Russia, invasion, mass-media, security

Scurtă prezentare a cazului

Georgia serveşte drept coridor strategic pentru magistralele de petrol şi gaze dinspre Marea Caspică spre pieţele europeană şi mondială de energie. Poziţia ei pe hartă compensează insuficienţa resurselor energetice. În plus, fosta republică sovietică s-a dovedit a fi unul dintre statele cu o foarte rapidă evoluţie spre democratizare, ceea ce este cu totul remarcabil dacă avem în vedere situarea ei între Federaţia Rusă, Turcia şi Iran.

Acţiunile militare s-au declanşat la 4 luni de la summitul NATO desfăşurat la Bucureşti. Încă preşedinte în exerciţiu al Federaţiei Ruse la acea vreme, Vladimir Putin declarase la Palatul Parlamentului (care găzduia reuniunea şefilor de stat şi de guvern ai statelor Aliate şi partenere) că, în opinia sa, „Războiul Rece era încheiat". Afirmaţia făcută la conferinţa de presă era nu atât un răspuns la întrebarea directorului NewsIn, Cosmin Popa, cât mai degrabă un mesaj public adresat preşedintelui George W. Bush, formulat în aceiaşi termeni în care liderul american îi reproşase gândirea inerţială, în logica Războiului Rece (Bush, 2008). Confruntarea armată ruso-georgiană din vara anului 2008 avea să demonstreze că practicile războaielor locale din timpul Războiul Rece sunt remanente în mentalitatea unora.

Premize istorice

La data de 8 august 2008, în prima zi a conflictului armat, una dintre cele mai importante agenții de presă de pe glob – Reuters – a dat publicității o cronologie preluată apoi de mass-media din întreaga lume (Baldwin & Cutler, 2008). Ea a constituit baza de raportare a multora dintre analiştii care au studiat conflictul ruso-georgian. Documentul plasează originea acestei confruntări în noiembrie 1989, când regiunea separatistă Osetia de Sud şi-a proclamat autonomia față de Republica Sovietică Socialistă Georgiană. Războiul a durat trei luni. În decembrie 1990, între Georgia şi Osetia de Sud s-au declanşat noi confruntări care au durat până în 1992. Armistițiul semnat la Soci de liderii ruşi, georgieni şi sud-oseți prevedea înființarea unei forțe tripartite de menținere a păcii în componența căreia intrau câte 500 de militari din fiecare tabără. Pe fondul protecției oferite de această forță şi a încurajărilor indirecte, dar constante ale liderilor de la Moscova (Gavrilă, 2008), Osetia de Sud îşi redactează, în noiembrie 1993, propria Constituție, iar 3 ani mai târziu îşi alege primul preşedinte. Abia după 7 ani, în decembrie 2000, Rusia şi Georgia semnează un acord inter-guvernamental pentru refacerea economiei în zona de conflict. Un an mai târziu, Eduard Kokoitî este ales preşedinte al Osetiei de Sud. El cere Moscovei (în 2002) să recunoască independența republicii şi să accepte integrarea ei în Federația Rusă. Demersul este contracarat parțial de planul Georgiei care acordă regiunii sale separatiste o autonomie extinsă în schimbul renunțării la ambițiile de independență, proiect aprobat de Rusia în ianuarie 2005. În noiembrie 2006, chemată la referendum, populația Osetiei de Sud se pronunță pentru separarea teritoriului de Georgia. Premierul georgian a catalogat acest eveniment ca fiind o nouă manevră a Rusiei pentru întreținerea stării de tensiune (Baldwin&Cutler, 2008). Cinci luni mai târziu, în aprilie 2007, parlamentul de la Tbilisi aprobă o lege privind înființarea unei administrații temporare în Osetia de Sud, decizie care a condus la intensificarea tensiunilor cu Rusia. Pe fondul acestei acțiuni şi în urma unor acuzații ale separatiştilor sud-oseți privind atacarea de către trupele georgiene a capitalei sud-osete Ținvali, negocierile mediate de OSCE între Georgia şi Osetia de Sud, eşuează în octombrie 2007. Câteva luni mai târziu, realegerea, în Georgia, a preşedintelui Mihail Saakaşvili a eliminat presupunerea că înlocuirea şefului pro-occidental al statului ar face Tbilisi mai obedient față de Moscova şi a determinat Rusia să îi impună vecinului său de la sud, noi sancțiuni economice. Scânteia care a aprins butoiul

cu pulbere a fost declarația de independență adoptată de provincia Kosovo cu sprijinul puterilor occidentale. Cu toate că membrii comunității internaționale s-au grăbit să respingă avertismentul Rusiei şi să precizeze că secesiunea provinciei sârbe nu putea constitui un precedent pentru nici o altă zonă de pe glob, deci nici pentru regiunea Caucazului, în martie 2008, Osetia de Sud cere Națiunilor Unite recunoaşterea independenței sale, după modelul provinciei Kosovo. Unii autori consideră că acțiunea în forță a Rusiei (Gavrilă, 2008) a constituit-o chiar simpla enunțare publică, la Summit-ul de la Bucureşti, a imposibilității invitării Georgiei în NATO. Am putea fi de acord cu acest punct de vedere doar dacă am considera că Moscova a văzut decizia Alianței atât de lipsită de consistență politică încât nu numai că şi-a permis să o ignore ci, mai mult decât atât, i-a putut atribui semnificația unui asentiment al aliaților pentru menținerea Ucrainei şi Georgie în sfera sa de influență prin amânarea acordării acestora a Membership Action Plan (MAP). Până la urmă, indiferent de interpretarea care i se dă deciziei de la Bucureşti, finalitatea rămâne aceeaşi. Rusia a putut acționa nestingherită, întărindu-şi relațiile politice şi militare cu cele două regiuni separatiste ale Georgiei, Abhazia şi Osetia de Sud. Acestă evoluție i-a determinat pe unii analişti să conchidă că decizia Kremlinului de a declanşa invazia Georgiei a fost premeditată (Filipescu, 2008). Printre argumentele invocate în sprijinul acestei afirmații se numără decretul semnat la 16 aprilie 2008, prin care Rusia a stabilit relații de tip stat-la-stat cu Osetia de Sud şi Abhazia. Ca o consecință imediată, Moscova a adus în cele două provincii georgiene separatiste un număr important de militari şi echipament militar greu dar şi specialişti care au reabilitat şoselele şi căile ferate spre Georgia. În paralel, sub pretextul antrenării trupelor pentru respingerea unor atacuri teroriste, manevrele militare ruse din primăvara anului 2008 – „Kavkaz-2008" (circa 8000 de militari) – au simulat invazia Georgiei (Bedwell&Nicholson, 2008). „*În prima săptămână din august 2008, provocările armate ale militarilor oseți contra satelor georgiene din Osetia de Sud au creat o situație intolerabilă. «Pacificatorii» ruşi nu au intervenit*." (Filipescu, 2008). În replică, în Caucazul de Sud, aproximativ 1.000 de militari americani s-au alăturat celor 600 din armata Georgiei la exercițiile comune de la baza militară Vaziani în apropierea capitalei Tbilisi. Purtătorul de cuvânt al Ministerului georgian al Apărării, Nana Intskirveli, a refuzat să spună dacă manevrele de trei săptămâni la care au mai participat şi 100 de ostaşi provenind din Ucraina, Azerbaidjan şi Armenia aveau

legătură cu încălcarea spațiului aerian de către Rusia sau cu violențele înregistrate în Abhazia şi Osetia de Sud (Bedwell&Nicholson, 2008).

Pe acest fond pregătit asiduu şi de presa rusă, la 3 august 2008, Ministerul de Externe de la Moscova avertiza comunitatea internațională despre riscul izbucnirii unui grav conflict militar şi atrăgea atenția comunității internaționale că situația din regiune s-a degradat subit la 1 şi 2 august. „*Amenințarea unor acțiuni militare de mare anvergură între Georgia şi Osetia de Sud devine din ce in mai reală*", se arăta în comunicatul de presă, care denunța Georgia că „*în seara de vineri şi în noaptea de 2 spre 3 august, Georgia a desfăşurat manevre militare la periferia Thinvali*", capitala Osetiei de Sud (www.zf.ro). Existența unor premize mai vechi de transformare în confruntare militară a conflictului de interese dintre Georgia şi Osetia de Sud – de care Moscova nu era deloc străină – este confirmată şi de preşedintele Comisiei pentru Afaceri Politice a APCE, suedezul Göran Lindblad. „*Au fost provocări, schimburi de focuri şi ciocniri dar situația s-a agravat odată cu atacul Georgiei asupra oraşului Ținvali. În opinia sa, georgienii au fost atraşi în această capcană deoarece Armata 58 şi ruşii erau deja pregătiți. «În justiția penală, calificăm această acțiune drept premeditare iar evenimentele au fost premeditate de partea rusă* [subl.n.]. *Problema este că Georgia a folosit excesiv forța, dar a făcut-o pe teritoriul său», a arătat Lindbald*" (Cliveti, Glăvan, 2008). Prin urmare, la ordinul preşedintelui Saakaşvili, trupele georgiene au atacat capitala sud-osetă, Ținvali. Informația că militarii georgieni ar fi comis masacre de purificare etnică în Ținvali soldate cu peste 2.000 de morți, cu care Moscova – prin intermediul presei ruse – a încercat să manipuleze opinia publică mondială, fost infirmată de observatori independenți, care au găsit mai puțin de 150 de victime (Filipescu, 2008). Concomitent cu invazia militarilor ruşi din Osetia de Sud, trupele ruse din Abhazia au deschis un al doilea front împotriva Georgiei, fără nicio provocare. În mod coordonat, forțele aeriene şi navale ale Rusiei au declanşat bombardamente intense împotriva infrastructurii militare şi economice din Georgia. Partea de nord a țării şi oraşul-port la Marea Neagră Poti au fost ocupate de trupele ruse. Preşedintele Rusiei, Dmitri Medvedev – recent instalat la Kremlin – şi premierul Vladimir Putin au pretins că militarii rusi au intervenit în Georgia în 2008 ca să prevină acțiunile de „genocid" şi „purificare etnică" ale georgienilor împotriva sud-oseților.

Invazia Georgiei de către forțele terestre, aeriene şi navale ale Rusiei, din 8 august 2008, şi proclamarea independenței provinciilor georgiene separatiste Osetia de Sud şi Abhazia au avut consecințe politice, economice şi de securitate drastice pentru țările din vecinătatea Federației Ruse, au deteriorat relațiile Moscovei cu democrațiile occidentale şi au determinat condamnări severe în străinătate. Decizia liderilor ruşi de a utiliza forța militară împotriva unei țări vecine cu capacitate militară mult inferioară a surprins comunitatea internațională, a alarmat celelalte state desprinse din fosta Uniune Sovietică şi a provocat discuții intense în comunitatea euro-atlantică în legatură cu reevaluarea atitudinii față de Rusia.

Scurtă analiză de conținut a mediatizării războiului din Georgia de către unele agenții de presă

Pentru a observa modul în care este mediatizat un conflict deschis între două state ne-am concentrat atenția asupra conținutului „materiei prime" oferite de trei categorii de furnizori de informație: de talie globală, din vecinătate şi locali. Este vorba de agențiile internaționale de presă Reuters şi AFP, de agențiile româneşti Agerpres, Mediafax şi Rador, precum şi de cele „locale" – Interfax, Ria Novosti, Itar-Tass şi Regnum. Deoarece analiza de conținut este o cercetare extrem de vastă, aici ne vom rezuma la prezentarea succintă a instrumentelor folosite şi a concluziilor desprinse din studiul pe care l-am făcut separat asupra rolului mediei în războaiele locale, în intervalul 19 iulie-19 august 2008.

Ipoteze de lucru

Patru ipoteze am avut în vedere atunci când am pornit la cercetarea conținutului prezentărilor făcute de presă războiului din Georgia:

a) Principiul neutralității precum şi cel al independenței presei sunt alterate în situații de criză şi, de regulă, mijloacele de informare în masă devin componente ale sistemelor naționale de apărare ale statelor (părților) direct implicate.

b) Presa prezintă o realitate prefabricată şi contribuie la inducerea în mentalul colectiv a unor stereotipuri şi reprezentări conforme poziției pe care o are față de actorii din teatrul de operații: țări, națiuni, minorități, lideri politici etc.

c) Cantitatea şi conţinutul informaţiilor din presa occidentală diferă în funcţie de interesele pe care statele de care aparţin le au în regiune şi, toate acestea, la un loc, se diferenţiază de cele transmise de media locale. În lupta pentru o imagine favorabilă părţii pe care o reprezintă (şi pentru compromiterea adversarului) presa distorsionează faptele şi este capabilă să exacerbeze sau chiar să construiască un conflict şi, mai ales, este capabilă să construiască anumite stereotipuri referitoare la părţile implicate.

d) Ca şi în alte cazuri (Ştefănescu, 2004), din raţiuni care ţin de factorii de amplificare a impactului, presa identifică naţiunea, poporul sau etnia cu conducătorul politic.

Pentru a verifica afirmaţiile formulate în ipoteze, am surprins următoarele dimensiuni (categorii de analiză): „concepte", „agenţi state / provincii[1] / organizaţii internaţionale)" şi „agenţi individuali (lideri / personaje politice sau militate)". Pentru înregistrarea lor am folosit ca unitate de înregistrare cuvântul. Am consemnat numărul de apariţii al unităţilor de înregistrare în raport cu totalul articolelor analizate şi am determinat frecvenţa apariţiei lor pe articol. Cu cât valoarea acestui indice este mai mare, cu atât unitatea de înregistrare respectivă a fost mai des mediatizată.

Grila de analiză

Grila completă a analizei de conţinut a cuprins 19 dimensiuni (categorii de analiză). Pentru 16 dintre acestea[2], unitatea de înregistrare a fost tema iar pentru trei dimensiuni a fost cuvântul. În primul caz am consemnat dacă tema apare sau nu în articol iar în al doilea caz am numărat cuvintele avute în vedere. Pentru această parte a cercetării ne-am concentrat pe analiza dimensiunilor materializate în cuvinte-cheie, abordare care ne

[1] Prin cuvântul cheie **provincie** am desemnat entităţile administrativ-teritoriale care şi-au declarat unilateral independenţa dar nu sunt recunoscute ca state suverane, de sine stătătoate, decât de un număr limitat de ţări şi nu sunt acceptate în organizaţiile internaţionale .

[2] Analiza de „conţinut" a mediatizării războiului din Georgia mai cuprinde o parte calitativă, de „atitudine" a mediatizării şi o parte care ţine de practica jurnalistică, analiză făcută pe baza a 16 dimensiuni (categorii de analiză) pentru care unitatea de înregistrare a fost tema (am consemnat prezenţa sau absenţa temei în articol): IV. „*Actori-georgienii*", V. „*Actori-separatiştii (oseţi şi/sau abhazi)*", VI. „*Actori-ruşii*", VII. *„Cauze"*, VIII. *„Definirea zonei de conflict"*, IX. *„Încadrare, contextualizare"*, X. *„Evaluare georgieni"*, XI. *„Evaluare separatişti"*, XII. *„Evaluare ruşi"*, XIII. *„Atitudine faţă de poziţia propriei ţări din care provine agenţia de presă"*, XIV. *„Stil"*, XV. *„Tipuri de surse de informare utilizate"*, XVI. *„Tipul sursei preluate"*, XVII. *„Tipul sursei media"*, XVIII. *„Utilizarea sursei (cât şi cum a preluat de la sursă)"*, XIX. *„Gen jurnalistic"*.

permite surprinderea „cantitativă" a temelor analizate, măsura în care ele sunt sau nu mediatizate, dacă sunt folosite excesiv, rareori sau ignorate.

Cele trei dimensiuni pentru care unitatea de înregistrare a fost cuvântul (acele cuvinte au fost numărate de fiecare dată când au fost folosite în text) sunt:

I. ***„Concepte"***, cu următoarele unități de înregistrare (cuvinte căutate şi numărate în text: 1. Război / conflict / confruntare / atac / agresiune / 2. agresor / ocupant / rebeli / separatişti / separatişti susținuți de Moscova (Rusia) 3. Genocid; 4. Masacru / măcel; 5. Crime / asasinate / atrocități / execuții (inclusiv „crime de război" sau „crime în masă"); 6. Exod etnic; 7. Conflict interetnic; 8. Purificare / epurare etnică; 9. Catastrofă / tragedie umanitară; 10. Înscenare / capcană; 11. Terorism; 12. Deportați / refugiați / alungați; 13. Prizonieri; 14. Negocieri / negociatori; 15. Morți; 16. Răniți; 17. Dispăruți; 18. Distrugeri.

II. ***„Agenți" state, provincii[3] sau organizații internaționale***, cu următoarele unități de înregistrare: 1. ONU; 2. UE; 3. NATO; 4. Consiliul de Securitate; 5. Înaltul Comisariat ONU pentru Refugiați; 6. OSCE; 7. UNOMIG; 8. Comunitatea internațională; 9. Comitetul Internațional de Cruce Roşie; 10. SUA; 11. Germania; 12. Franța; 13. Marea Britanie; 14. Italia; 15. Georgia; 16. Federația Rusă; 17. Osetia; 18. Abhazia; 19. Kosovo.

III. ***„Agenți" individuali, lideri / personaje politice sau militare*** cu următoarele unități de înregistrare: 1. Mihail Saakaşvili; 2. Dmitri Medvedev; 3. Vladimir Putin; 4. Eduard Kokoitî; 5. Serghei Bagapş; 6. George W. Bush; 7. Condoleeza Rice; 8. Angela Merkel; 9. Nicolas Sarkozy; 10. Gordon Brown; 11. Ban Ki-moon; 12. Antonio Guterres; 13. Alexander Stubb; 14. Serghei Lavrov; 15. Bernard Kouchner; 16. Şota Utiaşvili; 17 Alexander Gruşko; 18. Viaceslav Borisov; 19. Dmitri Rogozin; 20. Frank-Walter Steinmeier.

Rezultatele analizei

A) Concepte

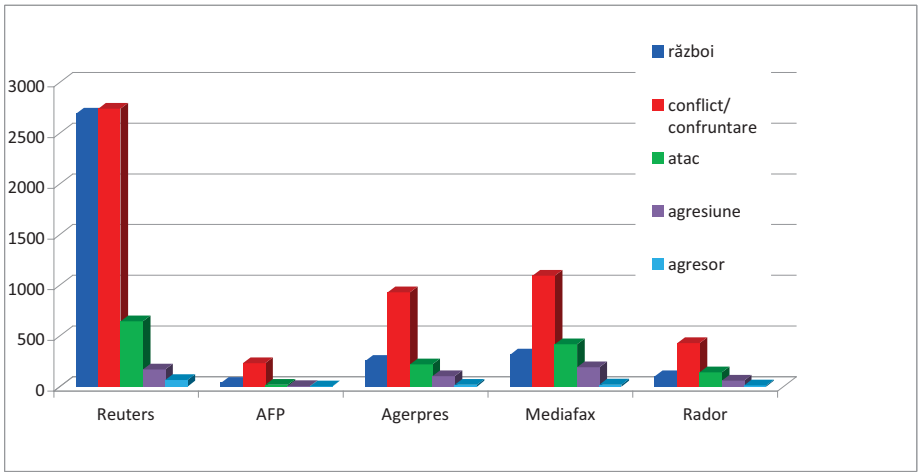
Analiza conceptelor care au zugrăvit tabloul confruntării armate din Georgia scoate la iveală o repartizare inegală a expresiilor „tari", care urmăresc să sensibilizeze publicul consumator de informație, în raport cu cele mai puțin dure.

Reuters a publicat, între 19 iulie şi 19 august 2008, 1337 de articole în care a utilizat conceptul dur „război" de 2694 de ori, în echilibru cu termenii considerați mai „soft" precum „conflict" sau confruntare care apar

[3] Cu acest cuvânt cheie am definit provinciile separatiste Osetia de Sud şi Abhazia.

de 2740 de ori, adică un indice apariții / articol[4] de 2,01, respectiv, 2,05, pentru fiecare termen în parte. Cum cele trei cuvinte se referă la confruntare armată extremă, numărul mediu de apariții urcă la 4,06 pe articol. Termenele atac, agresiune, agresor apar în medie de 0,66 de ori într-un articol, iar catastrofă, genocid, masacru, crime, atrocități, tragedii de circa 0,37 ori pe articol. Atunci când vorbesc despre sud-oseți şi abhazi, articolele folosesc, expresiile „rebeli" – 326 de cazuri, „separatişti" – 916 cazuri şi, uneori, „separatişti susținuți de Moscova (Rusia) – 30 de utilizări. Frecvența medie a acestor termeni este de 0, 95, adică de aproape un cuvânt pe articol. Pentru a ilustra efectele războiului, materialele Reuters folosesc cuvintele morți, răniți, dispăruți, refugiați, prizonieri, distrugeri. Acestea apar de 493 de ori, adică o medie de 0,16 pe articol.

Rezultatele obținute sunt prezentate sintetic în graficul de mai jos.



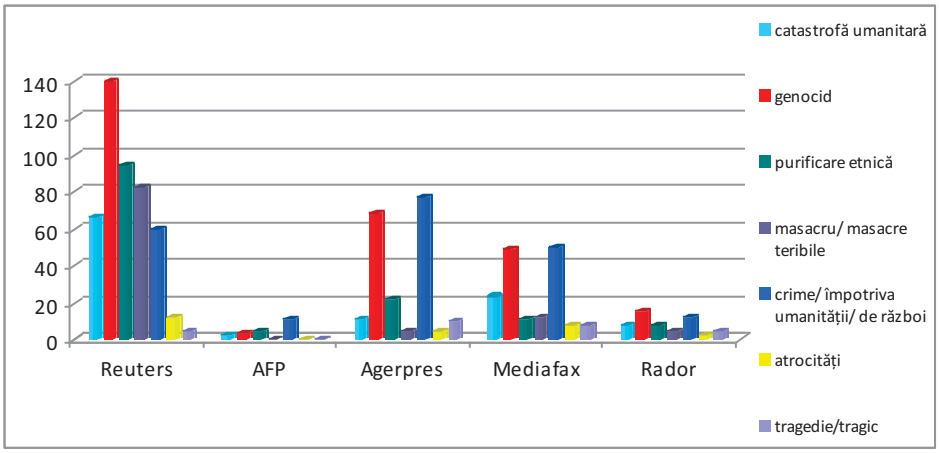
Grafic 1. Concepte mai „dure" şi mai „soft" utilizate de agențiile de presă pentru a caracteriza acțiunile de luptă din Georgia

AFP se remarcă, înainte de toate, printr-o mediatizare relativ redusă a conflictului dintre Federația Rusă şi Georgia, agenția franceză publicând în intervalul de referință, numai 56 de articole referitoare la confruntările din spațiul caucazian. Se constată însă tendința de a da confruntării militare o tentă mai „acceptabilă" prin utilizarea disproporționată a termenului

[4] Indicele apariții / articol a fost calculat prin împărțirea numărului de apariții ale unui termen la numărul de articole referitoare la confruntarea armată din Georgia publicat de agenție.

„război" (de numai 35 de ori) față de „confruntare" sau „conflict" (222 de utilizări). Luate împreună cele trei expresii se întâlnesc de 257 de ori şi înregistrează o frecvență medie de 4,59 utilizări într-un articol, valoare mai mare decât cea consemnată la Reuters. Cuvintele „atac", „agresiune", „agresor" apar de 23 de ori, adică de 0,41 de ori într-un articol. Expresiile care definesc cele două provincii segregaționiste şi pe cetățenii lor drept „rebeli" apar în 5 cazuri şi drept „separatişti" – în 52 de cazuri, pe ansamblul articolelor referitoare la temă rezultând o frecvență medie de 1,02. Şi aici se observă prezența termenilor foarte duri precum: „catastrofă", „genocid", „masacru", „crime", „atrocități" şi „tragedii" care apar de 16 ori, media apariției acestor cuvinte fiind de 0,28 pe articol, indice mai mare decât la Reuters. Primele articole despre situația din Georgia surprinse în intervalul de cercetare datează din 25 iulie şi 3 august şi se referă la conferința de presă susținută de Subsecretarul de stat american, Matthew Bryza, respectiv, la avertismentul Moscovei cu privire la premizele unui conflict major ca urmare a exploziilor de la 1 august care uciseseră şase persoane în Osetia de Sud.

Rezultatele cercetării sunt prezentate sintetic în tabelul şi graficul de mai jos.

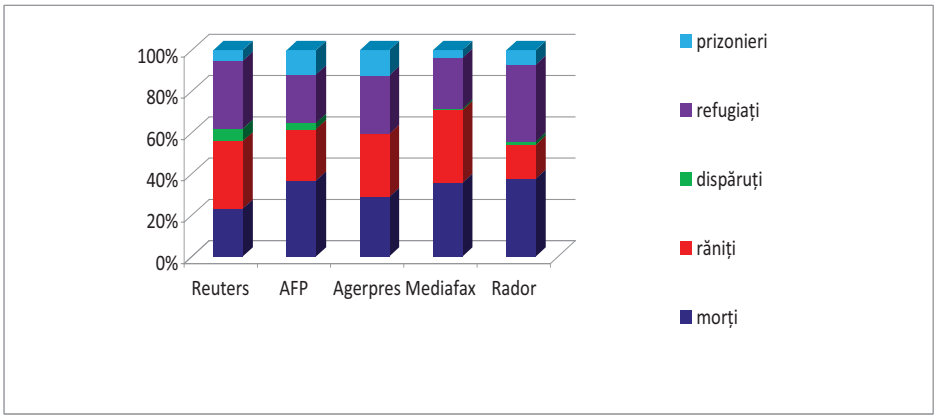


Grafic 2. Concepte dure care descriu efectele acțiunilor din teatrul de operații

Agențiile de presă din România supuse observației au fost: Agerpres, Mediafax şi Rador.

Agenția Națională de Presă Agerpres, a publicat în intervalul 19 iulie – 19 august 1072 de articole referitoare la confruntarea armată din Georgia. În cuprinsul acestora, cuvintele „război" şi „conflict/confruntare" apar de 1183 de ori; media apariției acestor termeni într-un articol fiind de 1,1 ori. Şi aici există însă o asimetrie a utilizării termenilor. În timp ce expresia „război" este întâlnită de 254 de ori, „conflict" şi „confruntare" apar de 929 de ori, de aproape 4 ori mai des. Cuvintele „atac", „agresiune", „agresor" apar de 439 de ori, adică de 0,41 ori/articol. Termenii foarte duri precum: „catastrofă", „genocid", „masacru", „crime", „atrocități" şi „tragedii" sunt prezenți de 172 de ori, înregistrând o medie de 0,16 într-un articol. Atunci când vorbesc despre sud-oseți şi abhazi, articolele folosesc, expresiile „rebeli" – 17 de ori şi „separatişti" – în 616 cazuri. Frecvența medie a apariției termenilor într-un articol este de 0,6 –semnificativ mai mică decât la cele două agenții de presă occidentale. Cuvintele „morți", „răniți", „dispăruți", „refugiați", „prizonieri", „distrugeri" cu care Agerpres descrie efectele războiului, apar de 365 de ori. Raportat la numărul total de articole dedicate acestui subiect, rezultă o frecvență medie de 0,34 ori într-un articol.

Rezultatele cercetării sunt prezentate sintetic în graficul de mai jos.



Grafic 3. Ponderea conceptelor care ilustrează pierderile umane în ştirile fiecărei agenții

Mediafax, a doua agenție de presă din România a publicat în perioada de referință cu aproape 26 la sută mai multe articole decât Agerpres, adică 1449. Materialele publicate de Mediafax au folosit cuvintele „război" şi „conflict / confruntare" de 1825 de ori realizând o medie de 1,26 de apariții pe articol. Şi aici, însă, ca şi la AFP şi Agerpres, cuvintele „conflict /

confruntare" sunt de trei ori şi jumătate mai utilizate decât „război" (1093/315). Aparţinând aceleiaşi categorii de expresii „dure", cuvintele „atac", „agresiune", „agresor" apar de 794 de ori. Media apariţiei acestor termeni se apropie de 0,55/ articol. Termenii „rebel" şi „separatist" apar de 35, respectiv, de 1002 ori. De aici rezultă o medie de aproape un cuvânt pe articol (0,99). Agenţia Mediafax foloseşte şi ea expresiile „morţi", „răniţi", „dispăruţi", „refugiaţi", „prizonieri", „distrugeri" pentru a descrie efectele confruntărilor militare din Georgia. În conţinutul articolelor, acestea apar de 711 ori, ceea ce corespunde unei medii de 0,5 termeni într-un articol.

Rador, agenţia de monitorizare a presei interne şi internaţionale din cadrul Societăţii Române de Radiodifuziune, a publicat, în intervalul 19 iulie – 19 august 2008, 386 de ştiri referitoare la războiul din Georgia. Numărul semnificativ mai mic decât al celorlalte agenţii de presă este explicat prin obiectivul agenţiei de a furniza beneficiarilor cele mai noi informaţii, comentariile proprii şi materialele de sinteză fiind realizate numai la cerere, fără o distribuţie în reţea. Şi la agenţia Rador constatăm aceeaşi tendinţă de a diminua gravitatea confruntării militare prin utilizarea de 4 ori mai rară a termenului de „război" (101 ori) faţă de cel de „conflict / confruntare" (429 de utilizări), împreună întâlnite de 530 de ori. Frecvenţa de utilizare pe articol este de 1,37 de prezenţe pe articol. Expresiile „dure" precum „atac", „agresiune", „agresor" apar în articole de 272 de ori, cu o frecvenţă de apariţie pe articol de 0,7. În perioada de referinţă, agenţia Rador foloseşte termenul „rebel" de 5 ori şi pe cel de „separatist" de 169 de ori, rezultând o frecvenţă medie de 0,45 de cuvinte pe articol. Expresiile „morţi", „răniţi", „dispăruţi", „refugiaţi", „prizonieri", „distrugeri" pentru a descrie efectele confruntărilor militare apar de 378 de ori., cu o medie de 0,98 de prezenţe pe articol.

B) „Agenţi state, provincii sau organizaţii internaţionale"

Cei mai mediatizaţi „Agenţi state, provincii sau organizaţii internaţionale" în legătură cu războiul din Georgia au fost, după cum era de aşteptat, în primul rând, statele direct implicate în conflict: Georgia şi Rusia, urmate de Osetia de Sud, Statele Unite şi Abhazia şi abia apoi de organizaţiile internaţionale NATO, UE, ONU şi OSCE. De remarcat este şi numele Kosovo la care fac trimitere toate agenţiile de presă.

a) Georgia apare în articolele Reuters cu o frecvenţă de 9,98 cuvinte pe articol; AFP – frecvenţă 10,54 ori / articol, Agerpres – frecvenţă 3,1 ori / articol; Mediafax – frecvenţă 3,8 ori / articol şi Rador – frecvenţă 3,78 ori /

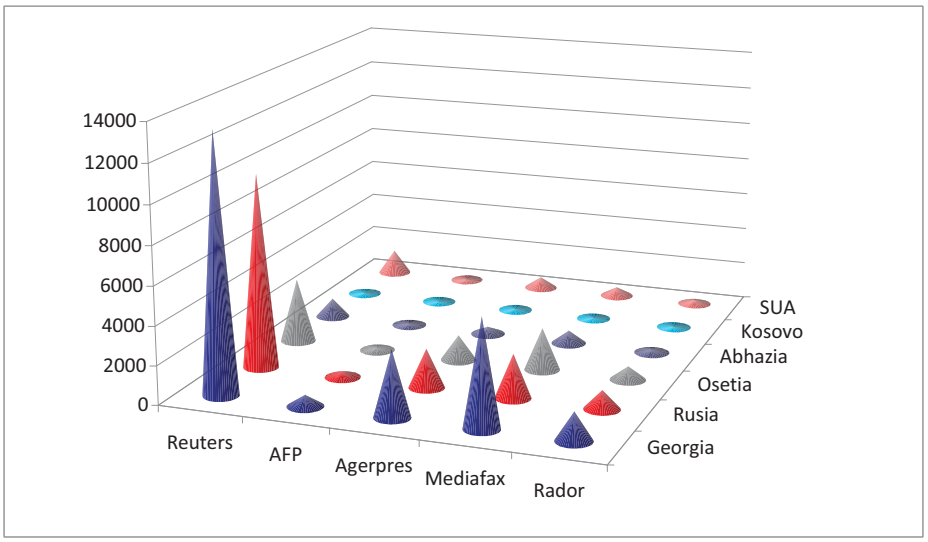
articol, ceea ce relevă o diferență substanțială de mediatizare între agențiile de presă internaționale şi cele naționale.

b) Rusia, pe Reuters – frecvență 7,55 ori / articol; AFP – frecvență 5,7 ori / articol, valori semnificativ mai mari față de cele înregistrate la agențiile naționale de presă: Agerpres – frecvență 1,9 ori / articol, Mediafax – frecvență 1,6 ori / articol şi Rador – frecvență 2,55 ori / articol.

c) Osetia de Sud, pe Reuters – frecvență 0,2 ori / articol; AFP – frecvență 2,8 ori / articol; Agerpres – frecvență 1,2 ori / articol; Mediafax – frecvență 1,5 ori / articol şi Rador – frecvență 1,8 ori / articol.

d) SUA, pe Reuters – frecvență o apariție pe articol; AFP – frecvență 0,5 ori / articol; Agerpres – frecvență 0,6 ori / articol; Mediafax – frecvență 0,3 ori / articol şi Rador – frecvență 0,6 ori / articol.

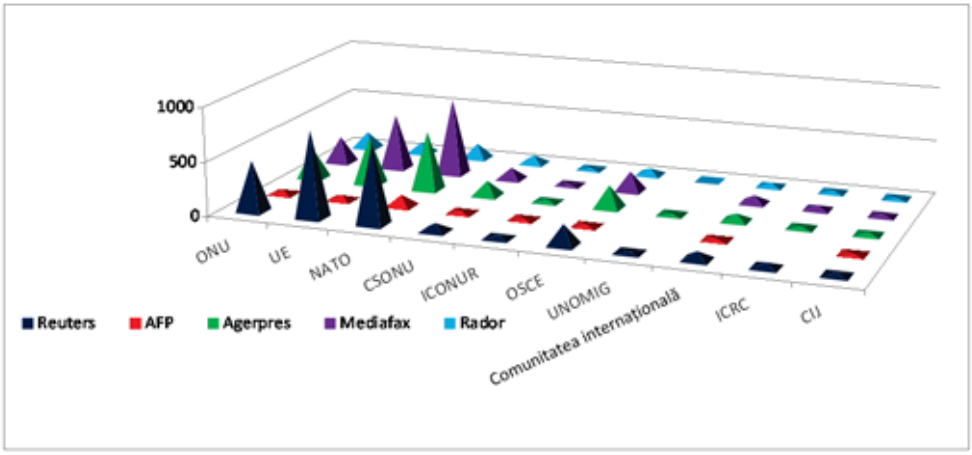
e) Kosovo apare în articolele agenției Reuters de 39 de ori, în ştirile AFP de numai 3 ori, dar mult mai des la agențiile de presă românești: de 63 de ori la Agerpres, de 51 de ori la Mediafax şi de 27 de ori la Rador.



Grafic 4. Prezența agenților state şi provincii în articolele agențiilor de presă în timpul războiului din Georgia

f) NATO, pe Reuters – frecvență 0,5 ori / articol; AFP – frecvență 1,9 ori / articol; Agerpres – frecvență 0,5 ori / articol; Mediafax – frecvență 0,5 ori / articol şi Rador – frecvență 0,4 ori / articol.

Tot în această categorie se mai observă o foarte redusă mediatizare a Curții Internaționale de Justiție, a Comitetului Internațional de Cruce Roşie, precum şi a Misiunii de Observare a ONU[5] în Georgia – UNOMIG – care apare de doar cinci ori pe Reuters şi numai o dată pe Agerpres.



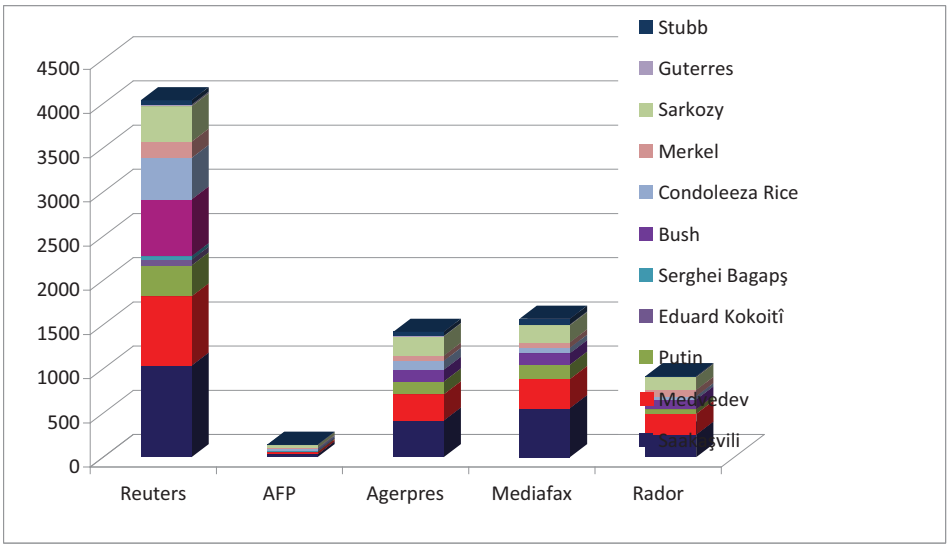
Grafic 5. Prezența actorilor organizații internaționale în informațiile agențiilor de presă.

C) „Agenții individuali – personaje / lideri politici sau militari"

Cei mai mediatizați agenți individuali sunt preşedinții Georgiei – Mihail Saakaşvili, Federației Ruse – Dmitri Medvedev şi SUA – George W. Bush. În comparație cu aceştia, un număr înjumătățit de apariții înregistrează premierul Vladimir Putin, Secretarul de Stat Condoleeza Rice, preşedintele Nicolas Sarkozy (care deținea la acel moment şi funcția de preşedinte în exercițiu al UE). Interesant de remarcat este faptul că, exceptând UE, liderii organizațiilor internaționale precum Secretarul General ONU, Ban Ki-moon, Înaltul Reprezentant ONU pentru Refugiați, Antonio Guterres, sau preşedintele în exercițiu al OSCE, Alexander Stubb, înregistrează un număr foarte mic de mediatizări inducând impresia unei slabe implicări a lor şi a unei forțe foarte reduse a organizațiilor pe care aceşti actori le reprezintă. Unele excepții de la această regulă sunt semnalate la AFP care acordă o atenție la fel de mare preşedintelui georgian şi celui francez, liderului de la Kremlin şi şefului diplomației americane.

[5] Misiunea UE în Georgia a fost activată la 1 octombrie 2008, după expirarea intervalului de studiu.

Ca o caracteristică generală, constatăm că „agenții individuali" sunt mult mai puțin mediatizați în comparație cu „agenții state sau organizații internaționale". Nici un nume nu ajunge la o apariție pe articol. Saakaşvili apare de 0,8 ori / articol în Reuters, de 0,6 ori / articol în AFP, de 0,4 ori / articol în Agerpres şi Mediafax şi de 0,7 ori / articol în Rador. La polul opus, Guterres apare de 0,01 ori / articol Reuters, de 4 ori la o sută de articole în AFP, dar o singură dată în mai mult de 1000 de articole Agerpres!



Grafic 6. Gradul de implicare şi importanța dată de presă agenților individuali (selecțiuni).

Sursele ruseşti, ne-au interesat în măsura în care au fost preluate de marile agenții de presă dar şi de agențiile locale (româneşti).

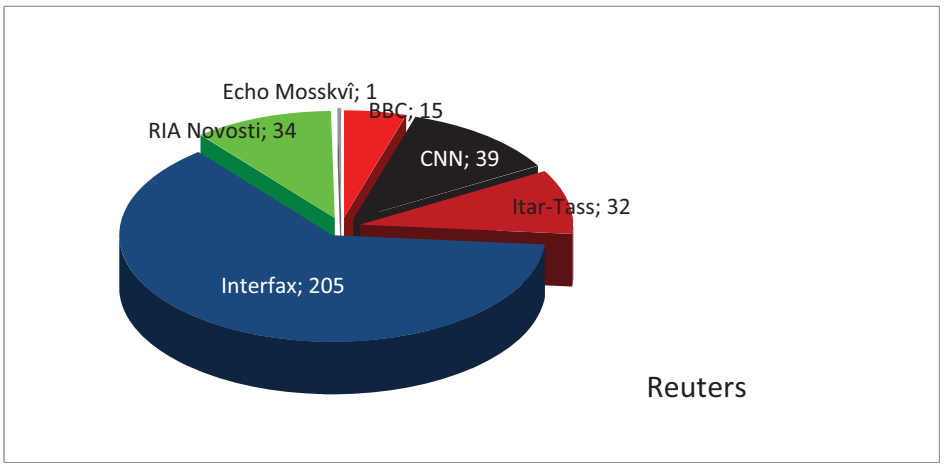
Interfax, a publicat informații şi articole citate de 205 ori de Reuters, dar de numai 3 ori de AFP. De altfel, Interfax este singura agenție rusă de presă citată de Agenția Franceză de Presă. Agențiile româneşti, o preiau de 261 de ori – Mediafax, de 131 de ori – Agerpres, şi de 18 ori – agenția Rador. Prelucrate sau citate integral, informațiile publicate de Interfax în intervalul 19 iulie-19 august au fost dezvoltate în 622 de articole ale agențiilor internaționale.

Ria Novosti, în intervalul de referință, este citată de 34 de ori de Reuters, de 122 de ori de Mediafax, de 57 de ori de Agerpres şi de 18 ori de Rador. Cele 231 de articole rezultate au constituit „materia primă" pentru

majoritatea covârşitoare a mijloacelor de informare în masă internaționale şi locale care au dorit să prezinte şi perspectiva rusească a evenimentelor. Interesant de semnalat că AFP nu face nici o referință la agenția Ria Novosti.

Itar-Tass, este preluată de Reuters de 32 de ori, iar de agențiile româneşti: de 47 de ori de Rador, de 45 de ori de Mediafax şi de 14 ori de Agerpres. Interesant de semnalat ni se pare ştirea publicată de această agenție de presă potrivit căreaia sâmbătă (19 iulie 2008) dimineață, în zona conflictului georgiano-abhaz, a fost atacat armat un post georgian de poliție situat în apropierea localității Şamgon din raionul Zugdidsk, controlat de partea georgiană, în imediata apropiere a raionului Galsk din Abhazia. Îl cităm parțial pentru că este una dintre puținele surse de informare care fac credibilă afirmația că reacția deosebit de dură a Georgiei a fost „provocată" (Filipescu, 2008) de Moscova. *„După cum au anunțat surse din cadrul organelor de ordine ale raionului Zugdidsk, "membri unei formațiuni armate abhaze din raionul Galsk au deschis focul asupra postului de poliție georgian, situat în apropierea localității Şamgon."*[6]

Regnum a fost citată de 12 ori de agenția de monitorizare a presei Rador şi de două ori de Agenția Mediafax.



Grafic 7. Repartiția celor 326 de informații preluate de Reuters de la surse străine în ansamblul celor 1337 de articole publicate în intervalul de referință.

[6]*În zona conflictului georgiano-abhaz a fost atacat armat un post georgian de poliție*, publicat de ITAR-TASS la 20 iulie 2008.

Alte surse sporadice din spațiul rusesc: preluate de agențiile de presă studiate sunt posturile Radio Rossia, Echo Moskvî, publicațiile Kommersant, Vremea Novosti şi Forum. Din aceste surse, demn de semnalat ni se pare ştirea transmisă de postul de radio Echo Moskvî, la 22 iulie 2008: „*Reprezentantul permanent al Georgiei la ONU, Irakli Alasania, a declarat că participanții la ședință* [CS al ONU, n.n.] *au condamnat agresiunea militară desfăşurată în ultima perioadă împotriva Georgiei. De asemenea, potrivit afirmațiilor lui, majoritatea membrilor CS al ONU au condamnat violarea spațiului aerian georgian. Este vorba de zborurile efectuate, la începutul lunii iulie, de avioane militare ruse deasupra zonei conflictului georgiano-oset. Reprezentantul permanent al SUA pe lângă ONU, Zalmay Khalilzad, a declarat că Washingtonul a calificat aceste zboruri ca o încălcare a dreptului internațional. La rândul său, reprezentantul permanent al Rusiei la ONU, Vitali Ciurkin, a chemat încă înaintea începerii şedinței CS al ONU la soluționarea problemelor pe cale paşnică. Amintim că, potrivit unor funcționari ruşi, zborurile deasupra zonei de conflict au fost efectuate cu scopul de a nu permite dezvoltarea situației după un scenariu violent.*" (www.echo.msk.ru).

Din analiza efectuată rezultă că, spre deosebire de celelalte confruntări militare din ultimii douăzeci de ani, războiul din Georgia s-a bucurat de o foarte slabă pregătire de presă. Numai 238 de materiale au fost difuzate în aproape trei săptămâni: 57 de articole publicate de Reuters, 3 – de AFP, 66 – de Agerpres, 79 – de Mediafax şi 33 – de Rador. Dintre trăsăturile articolelor publicate de Reuters mai observăm, pe lângă raritatea acestora până la declanşarea operațiunilor în noaptea de 7 spre 8 august, ştirea publicată la 18 iulie, care vorbea despre eşecul planului propus de Germania pentru dezamorsarea tensiunii dintre Georgia şi regiunile sale separatiste, prin respingerea lui de către Abhazia. Abia o săptămână mai târziu, într-un interviu pentru Reuters vorbind despre vizita sa la Tbilisi, Subsecretarul de stat american, Matthew Bryza, anunța că în loc să se atenueze, starea de tensiune în regiune se agravează.

Numărul mai mare de articole difuzate de agențiile de presă locale (româneşti) poate fi explicat prin interesul special pentru o zonă de conflict înghețat aflată în apropierea României şi prin similitudinile pe care acest

conflict le are cu cel din Transnistria. Aici mai trebuie relevat că majoritatea informațiilor din perioada premergătoare declanșării confruntărilor armate au ca sursă primară de informații agențiile de presă și media ruse. De exemplu, 28 dintre articolele puse la dispoziție de Rador provin de la agențiile de presă ruse, Reuters citează aceleași surse de 24 de ori, Agerpres de 18 ori și Mediafax face 90 de referiri la sursele de informație din Federația Rusă.

Deși selectate cu mare atenție și cu toate măsurile de verificare a informațiilor preluate din presa rusă, prima imagine a „Războiului de 5 zile" creată de media internațională a fost aceea a unui lider nesăbuit, care târăște micul său stat în război cu propria națiune și cu colosul rus. Având lecția învățată din conflictul din Kosovo, și demonizându-l pe Saakașvili, mijloacele de informare în masă ruse au reușit, în primă fază, să credibilizeze scenariul unui război interetnic pus la cale de un „Miloșevici local" între georgieni, pe de-o parte, și sud-oseți și abhazi, pe de altă parte. Manevra a reușit pentru că, până la 1 august 2008, atenția comunității internaționale rămăsese inerțial îndreptată spre Kosovo (a cărei independență de Serbia declarată unilateral nu este nici acum recunoscută de toți membrii ONU). În condițiile în care, în majoritatea lor, reporterii de „război" erau concentrați încă în spațiul balcanic, nevoia de informații din Georgia a fost acoperită de sursele rusești. Abia după această dată, marile trusturi de presă și-au trimis corespondenții în noua zonă de conflict deschis. Deja situația se agravase irevocabil, evenimentele se succedau cu repeziciune și analiza lucidă era greu de făcut. Absența presei internaționale și a unor observatori neutri în perioada premergătoare și-a pus amprenta asupra înțelegerii corecte a evenimentelor și, în ultimă instanță, asupra desluşirii cauzelor reale ale declanșării războiului. Oricât de mari ar fi fost sacrificiile jurnaliștilor georgieni, fără sprijinul mass-media internaționale eclipsarea fie și parțială a acelei prime imagini ar fi fost greu de realizat și comunitatea internațională ar fi rămas convinsă de lipsa de discernământ a președintelui Saakașvili fără a lua o clipă în calcul abilitatea strategilor de la Moscova în utilizarea mijloacelor de informare în masă și dezechilibrul evident de forțe din teren.

Bibliografie

1. Baldwin, C. & Cutler, D., 8 august, 2008, *GEORGIA-OSSETIA/CHRONOLOGY – Conflict between Georgia and South Ossetia*, Reuters. Disponibil la http://uk.reuters.com/article/idUKL857385920080808 (cu titlul *TIMELINE - Conflict between Georgia and South Ossetia;* http://www.mediafax.ro/externe/cronologie-conflictul-dintre-georgia-si-osetia-de-sud-2873042 (cu titlul *Cronologie: Conflictul dintre Georgia şi Osetia de Sud,* Mediafax)

2. Bedwell, H. & Nicholson, A., 15 iulie 2008, *Russia, Georgia Begin War Games as Tensions Escalate*, Bloomberg. Disponibil la http://www.bloomberg.com/apps/news?pid=20601095&sid=a.mv7C.Q97s4&refer=east_europe.

3. Cliveti, M. (dep.), Glăvan, Ş. (dep.), 15 octombrie 2008, *Informare privind participarea la partea a patra a sesiunii Ordinare a APCE – Dezbatere de urgență privind „Consecințele războiului dintre Georgia şi Rusia*, Strasbourg, 29 septembrie – 3 octombrie 2008, prezentată în Camera deputaților.

4. Filipescu, N., 2 decembrie 2008, *Consecințele războiului din Georgia*, revista 22. Disponibil la: http://www.revista22.ro/consecintele-razboiului-din-georgia-5142.html.

5. Gândul, 4 aprilie 2008, *Bush către Putin: Războiul Rece s-a încheiat*.

6. Gavrilă, G. (2008). *Implicațiile conflictului din Georgia asupra securității în regiunea Mării Negre*, publicat în *Politici şi strategii în gestionarea conflictualității*, Sesiunea Anuală de Comunicări Ştiințifice cu Participare Internațională a Centrului de Studii Strategice de Apărare şi Securitate, 20-21 Noiembrie 2008, Bucureşti, Editura UNAp, *VOL. 5*, *Despre orizontala şi verticala securității,* 2008, pp. 9-16.

7. Ştefănescu, S., 2004, *Media şi conflictele*. Bucureşti: Editura Tritonic.

8. www.echo.msk.ru, 22 iulie 2008, *La inițiativa părții georgiene a avut loc o nouă şedință a CS al ONU*, difuzat de Echo Moskvî, ora 19:00.

9. www.zf.ro/politica/politica-externa/rusia-crede-ca-un-razboi-intre-georgia-si-osetia-este-iminent-3177430/.

O viziune strategică a securității mediului în era globalizării

Ana Ligia LEAUA
Asistent universitar, Academia Națională de Informații „Mihai Viteazul”
e-mail: **leaualigia@gmail.com**

Abstract

Environmental change is global; no part of the world is spared and we have to face change now; ignoring the challenge is not an option if our children are to thrive. In an increasingly connected world, security is more than just the absence of war; it depends on diverse, but linked – indeed, often competing - factors such as political, social, economic, and environmental interests. Environmental degradation may destabilize societies by reducing economic opportunity. Environment is thus central to modern security and the question for policymakers is how, in practical terms, to align these diverse interests. Environmental security is therefore the ability of individuals to avoid or adapt to environmental change so that things that are important to their well-being are not substantially negatively affected.

Keywords: environment, degradation, security, risks, threat, intelligence, challenge, policymakers, needs, violent conflicts.

1. Mediul de securitate actual - teoria complexității, teoria haosului

Domeniul principal de interes pentru oamenii politici şi oamenii de ştiință l-a reprezentat capacitățile militare pe care statele ar trebui să le dezvolte pentru a face față amenințărilor la care sunt supuse. În ultimul rând, această concepție despre securitate a fost criticată din cauza naturii sale etnocentrice[1] (influențată cultural) şi a caracterului prea restrâns. În schimb, un număr important de autori contemporani au promovat

[1] Conform lui Walker Conner, în „Ethnonationalism: the Quest for understanding”, apărută la Princeton University Press, NJ, 1994, etnocentrismul este o consecință a etnonaționalismului, adică credința că faptul de a aparține unei anumite naționalități conferă o stare de superioritate față de membrii altor naționalități, considerate inferioare. Etnocentrismul „hrăneşte”, în mod incontestabil, conflictele interetnice

o concepție asupra securității, extinsă peste limitele tradiționale ale securității naționale, în sensul strict al termenului, concepție ce include un set de alte considerații. *Barry Buzan*[2] ridică probleme importante şi interesante despre măsura în care considerațiile de securitate internațională şi națională pot fi compatibile şi dacă statele, dată fiind natura sistemului internațional, sunt capabile să gândească în termeni globali, favorabili unei cooperări internaționale mult mai largi. Secolul al XXI-lea deschide o nouă perspectivă în politica internațională în care securitatea şi, implicit, competiția pentru dobândirea unui loc în ierarhia puterilor mondiale devine tot mai stringentă atât pentru ocuparea unei poziții centrale în determinarea evoluției lumii cât şi pentru stabilirea noii ordini internaționale. Nici o instituție statală ori multistatală de astăzi nu este pregătită şi structurată pentru a fi eficientă în gestionarea unor fenomene atât de actuale precum progresiva ciocnire între valorile civilizațiilor, diferențele mari, la nivel global privind calitatea vieții, insuficiența resurselor vitale precum cele energetice, (iar, la un orizont nu prea îndepărtat, cele legate de apa şi alimente), manifestarea unor grave probleme de mediu, şi accentuarea fenomenelor migrationiste etc. Toate acestea generează riscuri noi, complexe şi multidimensionale, pentru a căror gestionare statele, chiar şi cele mai puternice, sunt depăşite, iar organizațiile internaționale nu dispun de mecanisme eficiente. Astăzi, în percepția publică, deplasările de trupe care, altădată, alertau toate instituțiile politice şi militare sunt percepute a fi mai puțin îngrijorătoare decât prețul petrolului şi evoluția cursului dolarului, accesul la resursele de hidrocarburi are o rezonanță politică mai mare decât armele performante, problemele de mediu şi schimbările climatice au depăşit faza soluțiilor locale, iar descurajarea nucleară pare a nu mai avea atâta relevanță față de manifestările unui adversar numit terorism.

De aceea, mediul de securitate este dependent, mai mult decât oricând, de ineficiența acelor acțiuni şi măsuri inițiate de state şi organizații internaționale, mai curând pentru a reda măreția de altădată a statului

[2] Şcoală academică de gândire privind relațiile internaționale, reprezentată de teoreticienii Barry Buran, Ole Waever şi Jaap de Wilde, şi care pune accentul pe aspectele sociale ale securității. Majoritatea teoreticienilor securității ai acestei şcoli sunt membri ai Institutului de Cercetare a Păcii din Copenhaga, iar cartea cea mai reprezentativă este „Popoarele, statele şi teama: problema securității naționale în relațiile internaționale", semnată de către teoreticienii Barry Buran, Ole Waever şi Jaap de Wilde.

în competiția sa cu actorii nonstatali a căror influență politică este în creştere, decât să se constituie în soluții. Această perspectivă se observă cel mai evident în relațiile de putere la nivel global sau chiar în manifestarea puterii, în general, ca realitate politică continuă a lumii, ca „şansă a unui actor politic de a-şi impune voința sa altui actor politic”[3], cum a denumit-o *Max Weber*[4].

În încercarea de a creiona caracteristicile mediului de securitate actual, am pornit în această analiză de la corelația existentă între teoria complexității[5], a haosului şi conceptul de securitate. Astfel, am abordat lucrările lui **Ilya Prigogine**[6], “*The End of Certainty, Time, Chaos, and the New Laws of Nature”,1997* şi *Order Out of Chaos: Man's new Dialogue with nature, 1984*. În opinia lui Ilya Prigogine complexitatea este nondeterministă şi nu oferă nici o cale de predicție exactă a stării viitoare a sistemului. Teoria complexității ar studia un domeniu între determinism şi întâmplare, care mai este numit şi „marginea haosului”. Prin urmare, principala diferență dintre sistemele haotice şi cele complexe constă în istoria acestora, întrucât sistemele haotice nu se bazează pe istoria lor în măsura în care o fac sistemele complexe. Comportamentul haotic împinge un sistem echilibrat într-o ordine haotică, iar, pe de altă parte, sistemele complexe evoluează departe de starea de echilibru, la marginea haosului. Acestea evoluează într-o stare critică, construită dintr-o istorie de evenimente imprevizibile şi neaşteptate. Într-un anumit sens, sistemele haotice pot fi percepute asemeni unui subset al sistemelor complexe ce se disting, în principal, prin absența dependenței istorice.

---

[3] Max Weber, *Wirtschaft und Geselschaft. Grunddriss der Verstehen den Soziologie,* Verlog Mohr, Tulingen, 1972, p. 35.

[4] Sociolog şi economist german, Max Weber (21.04.1864 – 14.06.1920) este, împreună cu Vifredo Pareto, Emile Durkheim, Georg Simmel şi Karl Marx, unul din fondatorii sociologiei moderne, ocupându-se, cu precădere, de studiul sociologiei religiilor şi a guvernului. În lucrarea sa „Politica drept vocație”, Weber defineşte statul drept o entitate ce posedă monopolul asupra folosirii legitime a forței.

[5] Începând cu secolul trecut au fost testate mai multe modele matematice pentru fundamentarea teoretică a câtorva discipline umane: cibernetica, teoria catastrofelor, teoria haosului, teoria sistemelor complexe, însă, în prezent, sistemele complexe constituie subiect de cercetare pentru o mare varietate de ştiințe şi metode de practici profesionale, utilizate inclusiv în analiza securității.

[6] Laureat al Premiului Nobel pentru Chimie în anul 1997 şi membru al Academiei Române, Ilya Prigogine (25.01.1917-28.05.2003) este chimist şi fizician belgian, care a dezvoltat teoria potrivit căreia ştiința clasică considera fenomenele drept determinate şi reversibile, ceea ce este în contradicție cu experiența cotidiană.

Studiile lui Ilya Prigogine îşi au originea în lucrările matematicianului francez ***Jules Henri Poincaré***[7], în opinia căruia haosul este perceput de acesta nu ca o absenţă a ordinii, ci asemeni unui sistem de informaţii extrem de complicat. Totuşi, o distincţie importantă între haos şi complexitate este aceea că haosul rămâne determinist. Altfel spus, având o cunoaştere perfectă a condiţiilor iniţiale şi a contextului unei acţiuni, cursul acestei acţiuni poate fi prezis.

Printre promotorii acestor teorii putem aminti pe ***James N. Rosenau***[8], care a studiat evoluţia mediului internaţional de securitate, înainte şi după Războiul Rece, prin prisma aceleiaşi teorii a complexităţii, concluzia acestuia fiind că, după Războiul Rece, se naşte o nouă epocă, a multiplelor contradicţii:

- sistemul internaţional este nu mai puţin dominant, dar mai puternic;
- statele se transformă, dar nu dispar;
- suveranitatea statului este erodată, dar puternic valorizată;
- graniţele nu permit trecerea intruşilor, dar sunt caracterizate de un grad crescut de porozitate.

Alvin M. Saperstein[9] susţine, în studiul „*Complexitate, haos şi politica de securitate naţională: metafore sau instrumente?*”, că interacţiunile dintre statele-naţiune, inclusiv războiul, sunt similare interacţiunilor dintre particule, ce sunt studiate în cadrul fizicii.

Potrivit lui ***D. Colander***[10], studiul complexităţii este opusul studiului haosului. Complexitatea se referă la felul în care un număr mare de seturi

---

[7] Matematician, fizician şi filozof francez al secolului al XIX-lea, Jules Henri Poincaré este fondatorul teoriei haosului şi precursorul major al teoriei relativităţii restrânse, fiind unul din ultimii mari savanţi universali din domeniul matematicilor

[8] Profesor la catedra de relaţii internaţionale din cadrul Universităţii George Washington şi fost preşedinte al Asociaţiei de Studii Internaţionale, James N. Rosenau şi-a concentrat activitatea didactică asupra dinamicii politicii mondiale, fiind printre primii care au aplicat, în ştiinţele politice şi relaţiile internaţionale, teoria complexităţii, sistem interdisciplinar de analiză originar din ştiinţele exacte. Potrivit revistei „Foreign Policy”, James Rosenau a fost desemnat drept unul din cei mai influenţi savanţi în domeniul afacerilor internaţionale

[9] Profesor de fizică şi membru al Centrului pentru Studii privind Pacea şi Conflictul din cadrul Waine State University, al Societăţii Americane de Fizică şi al Asociaţiei Americane pentru Progresul Ştiinţei, Alvin M. Saperstein a publicat o serie de cărţi şi articole legate de fizică, mediul înconjurător, strategii şi tactici militare, controlul armelor şi modelarea dinamică a relaţiilor internaţionale

[10] David Colander (născut în 1947) este profesor de economie la Middlebury College, fiind cunoscut pentru studiile sale de economie şi sociologie. Autor al cărţii ”The Making of an Economist”, D. Colander şi-a concentrat eforturile asupra teoriei complexităţii şi a aplicării acesteia în politicile economice

de relaţii foarte complicate şi dinamice pot genera modele comportamentale simple, pe când comportamentul haotic, în sensul haosului determinist, este rezultatul unui număr relativ mic de interacţiuni neliniare.

În centrul acestei viziuni se află convingerea că ordinea care caracterizează familiile, comunităţile, ţările şi sistemul global se bazează pe contradicţii, ambiguităţi şi incertitudini. Cu toate că această abordare a studiului securităţii este deosebit de interesantă, până în prezent nu a fost făcută publică o metodologie clară de analiză.

Într-adevăr, lumea este caracterizată de contradicţii şi incertitudini, însă scopul paradigmelor lineare existente nu este unul radical reducţionist, ci doar pentru a simplifica complexitatea în vederea înţelegerii sale. Astfel, teoria complexităţii reprezintă o modalitate de investigare a dinamicii sistemelor nonlineare, ce nu este complementară metodelor lineare destinate măsurării unei lumi neregulate (de exemplu statistica).

Sistemele nonlineare au următoarele caracteristici:

- intrările (inputs) şi ieşirile (outputs) nu sunt proporţionale;
- întregul nu este egal din punct de vedere cantitativ cu suma părţilor sale şi, din punct de vedere calitativ, nu este identificabil prin caracteristicile elementelor componente;
- înlănţuirea cauză-efect nu este evidentă;
- fenomenele din acest mediu nu sunt previzibile, dar, în interiorul graniţelor proprii, se autoorganizează.

Întrucât în contexte de cercetare diferite, sistemele complexe sunt definite pe baza atributelor diferite, cele mai importante probleme legate de sistemele complexe sunt cele vizând dificultăţile cu formalizarea modelelor şi simularea acestora. Având în vedere că toate sistemele complexe au multe componente interconectate, ştiinţa reţelelor şi teoria reţelelor sunt aspecte importante în studiul sistemelor complexe. Aceste studii caută să descopere în primul rând felul în care relaţiile dintre părţi dau naştere comportamentului colectiv al sistemului şi felul în care sistemul interacţionează şi formează relaţii cu mediul său înconjurător. Însă un consens în privinţa unei singure definiţii universale a sistemelor complexe încă nu există.

2. Globalizarea/glocalitatea - factori catalizatori în configurarea agendei de securitate

Tendinţele mediului de securitate se manifestă în condiţiile accentuării globalizării, „un proces deosebit de dinamic al creşterii interdependenţelor dintre statele naţionale, ca urmare a extinderii şi adâncirii legăturilor

transnaționale în tot mai largi şi mai variate sfere ale vieții economice, politice, militare, sociale şi culturale"[11].

Thomas L. Friedman susținea, în anul 2007, că „în sistemul globalizării, veți găsi, deopotrivă, conflictul civilizațiilor şi omogenizarea civilizațiilor, catastrofe ale mediului înconjurător şi acțiuni uluitoare de salvare a acestuia, triumful capitalismului liber, al pieței libere şi o împotrivire acerbă la adresa lor, perpetuarea statelor naționale şi apariția unor actori nestatali cu o putere enormă"[12]. Interdependența dintre țări a crescut şi, prin urmare, conjunctura internațională determină tot mai mult conjunctura națională. Provocarea acestei ere a globalizării atât pentru țări, cât şi pentru indivizi constă în a găsi un echilibru echitabil între conservarea spiritului de identitate şi de comunitate, a sentimentului de „acasă" şi respectarea regulilor pentru a putea supraviețui în sistemul globalizării.

Complexitatea mediului de securitate, rezultată ca efect al proceselor de globalizare, precum şi al altor procese, cu accentuarea decalajelor economice şi tehnologice, a generat şi continuă să genereze noi riscuri şi amenințări. În momentul de față asistăm la o amplificare şi particularizare a unor vulnerabilități, riscuri şi amenințări cu extindere globală care, pe termen mediu şi lung, vor aduce atingere integrității, securității şi bunăstării statelor sau grupurilor de state, alianțelor economice şi politice regionale şi vor supune la grele încercări şi provocări însăşi pacea mondială. Se prefigurează tot mai clar unele amenințări globale, cu efecte dintre cele mai neaşteptate pe planul securității internaționale.

„Agenda strategică globală este marcată de tranziția spre o percepție mai largă a ceea ce înseamnă securitatea ca paradigmă a acțiunii statului: vorbim de securitate de mediu, alimentară, de securitatea pieților financiare, de securizarea accesului la energie, domenii în care – aparent paradoxal – asistăm nu doar la o diversificare a riscurilor, ci şi la recurența unor amenințări clasice care se manifestă ca element de potențare a acestor fenomene. Avem un melanj de riscuri clasice de securitate, care, însă, îmbracă, uneori, forme noi de manifestare şi de riscuri noi, derivate din accentuarea unor crize şi vulnerabilități atât regionale, cât şi globale."[13]

„Trăim într-un mediu interdependent în care toate evoluțiile globale au efecte în cascadă tot mai greu de anticipat, de înțeles. Ceea ce astăzi este perceput ca vulnerabilitate, mâine devine amenințare, ceea ce azi definim ca

---

[11] Ioan Bari, *Probleme globale contemporane,* Editura Economică, Bucureşti, 2003
[12] Thomas L. Friedman, *Lexus şi măslinul*, ediția a II-a revăzută, Editura Polirom, Iaşi, 2008
[13] Interviu acordat de ambasadorul George Cristian Maior, directorul SRI, Agenției de ştiri „Agerpres" (Bucureşti), 10.12.2008, realizator Dănuț Puşcaşu

risc, mâine poate fi pe prima pagină a ziarelor ca fapt împlinit."[14]

Vulnerabilitățile se asociază cu procesele economico-sociale în derulare, resursele materiale existente, condițiile de mediu, precum şi cu multiplele ipostaze ale comportamentului actorilor statali şi nonstatali. Globalizarea, fenomen plurivalent, controversat şi contestat, aduce, pe lângă progresele din toate domeniile vieții socioeconomice, şi posibilitatea de răspândire şi resimțire a efectelor vulnerabilităților concentrate în diferite părți ale lumii. Prin procesele pe care le incumbă, generează tensiuni multiple care influențează nu întotdeauna pozitiv mediul internațional de securitate, integrarea şi fragmentarea, internaționalizarea şi localizarea, precum descentralizarea fiind doar câteva din situațiile care pot genera insecuritate.

Realitatea demonstrează că globalizarea este cea mai importantă şi puternică forță în crearea unei noi matrice a securității internaționale, fiind asociată cu creşterea insecurității, în principal din cauza uneia dintre caracteristicile sale, anume creşterea interdependențelor. Evoluția acestui proces nu numai că a transformat caracteristicile riscurilor, pericolelor şi amenințărilor deja existente, ci a creat unele noi, specifice unei lumi în care timpul şi spațiul par a se contracta. Războiul, de exemplu, a evoluat de la definiția clasică (conflict armat deschis, adesea prelungit, ce implică violență organizată între națiuni, state sau facțiuni motivate politic), la interpretări care ilustrează noile caracteristici ale mediului de securitate influențat de globalizare, de terorism şi de inovațiile tehnologice surprinzătoare. Este evident că s-a petrecut o modificare de substanță şi în sursele războiului, de la expansiunea geopolitică şi aspecte ideologice, la conflictele asupra resurselor şi identităților.

Globalizarea insecurității este accentuată şi de existența statelor eşuate (failed states). Sărăcia, lipsa stabilității economice şi incapacitatea de a furniza bunăstare socială şi securitate în acest tip de state pot crea condiții favorabile revoltelor şi mişcărilor transnaționale de insurgență. Mai mult, statele eşuate pot găzdui grupări şi activități teroriste şi reprezintă, adesea, sursa crizelor de refugiați generate de extremismul religios şi politic, degradarea mediului şi acțiunile organizațiilor criminale.

Amenințările politice, în majoritatea lor, sunt îndreptate împotriva ordinii de drept dintr-un stat sau a statutului unui organism internațional şi se pot realiza prin presiuni asupra organelor de decizie în favoarea

[14] Interviu acordat de către ambasadorul George Cristian Maior, directorul SRI, Agenției de ştiri „Agerpres" (Bucureşti), 10.12.2008, realizator Dănuț Puşcaşu

unor anumite politici; răsturnarea guvernului dintr-un stat sau a organelor de conducere colectivă a unui organism internaţional, distrugerea puterii politice, etc.

Ameninţările economice rezidă într-o economie globală generată de interdependenţele apărute între economiile statelor, în care pieţele depind unele de altele, devin emergente şi nu mai pot fi protejate în totalitate prin intervenţia statelor naţionale. Accentuarea procesului de globalizare a declanşat o explozie a producţiei internaţionale şi a tranzacţiilor financiare în cadrul pieţei internaţionale. Trebuie amintit că discriminările apărute în răspândirea prosperităţii au determinat fenomenul migraţionist, sensul fiind inversat în situaţiile în care sunt periclitate, ameninţate resursele naturale, vitale, interne sau externe, ceea ce determină ca ţările industrializate să intervină asupra economiilor ţărilor din Lumea a doua sau a treia.

Problema resurselor şi a competiţiei pentru resurse reprezintă un alt aspect important al globalizării insecurităţii. Interdependenţele dintre resurse, pe de o parte, şi dezvoltare, prosperitate şi putere, pe de altă parte, au modelat decisiv evoluţia politică a lumii. Cea mai puternică motivaţie pentru război este achiziţia, accesul ori controlul resurselor critice. Pe măsură ce populaţia planetei continuă să sporească, va creşte şi consumul de resurse vitale, generând sărăcie, inegalitate şi violenţe intra- şi interstatale. Raritatea resurselor precum apa şi hrana pot produce disfuncţionalităţi la nivelul întregii comunităţi internaţionale. Lipsa resurselor energetice, în special a petrolului şi gazelor naturale, reprezintă o preocupare majoră a multor state, întrucât consumul în creştere, corelat cu rezervele în scădere, va conduce la o reformulare dramatică a intereselor strategice în lume.

Problemele ecologice sunt şi acestea strâns legate de globalizarea insecurităţii. Problema deteriorării mediului înconjurător este mai recentă şi reflectă faptul că densitatea crescândă a ocupării planetei de către oameni a început să disturbe grav activitatea naturală a ecosferei, deoarece piaţa este forţa principală care dirijează activitatea umană, acţiunile desfăşurate în cadrul acesteia continuând a fi o parte a problemei mediului înconjurător. Ameninţarea constă în poluarea externă (prin noxe eliberate în atmosferă, utilizarea îngrăşămintelor, prezenţa unor reziduuri de metale grele şi deversări de hidrocarburi) sau prin asalturile directe asupra unor părţi ale ecosferei (tăierea copacilor, mineritul, funcţionarea fermelor, pescuitul), care rezultă din activitatea economică şi care va determina, până la urmă, şi, probabil,

destul de curând un dezastru ecologic major, care va degrada semnificativ condițiile de existență a oamenilor pe planetă.

Diminuarea diversității speciilor de plante poate conduce la mărirea simțitoare a nivelului radiațiilor solare ce ajung pe suprafața planetei, în timp ce efectul de seră al emisiilor de dioxid de carbon şi al altor gaze de către societățile industriale poate avea drept consecințe schimbarea temperaturii globale.

Tendința actuală de deteriorare a mediului, cel puțin în țările industrializate, constituie o agresiune împotriva sistemelor ecologice, ce distruge capacitatea ecosistemului de a menține existența umană. Schimbările semnificative ale climei afectează toate aspectele activității umane, cu consecințe asupra bunăstării economice şi sociale a statelor. Chiar dacă dezastrele ecologice şi schimbarea climei au impact asupra mediului de securitate, acest efect nu este distribuit în mod egal între state, gravitatea unui astfel de eveniment şi capacitatea de a-i face față diferă de la o țară la alta, ceea ce va provoca pagube economice şi sociale diferite, de la un caz la altul. O astfel de situație poate conduce şi la exacerbarea tensiunilor existente între state, de exemplu, resursele insuficiente de apă reprezintă o vulnerabilitate a statelor din Africa Sahariană, Orientul Apropiat şi Mijlociu şi Asia Centrală.

Riscurile şi amenințările de natură ecologică pot avea consecințe majore asupra situației politice, economice şi sociale, printre care cele mai importante sunt: migrația masivă a populației, stagnarea sau reducerea creşterii economice, eventuale proteste, scăderea nivelului de trai, discreditarea guvernării etc.

Problemele populației – expansiunea demografică (cu urmări economice, şocuri politice şi militare) ce se intersectează cu îmbătrânirea şi reducerea populației, coroborate cu accentuarea sărăciei, alimentează valuri de emigranți ce amenință zonele mai stabile din punct de vedere economic şi politic. Pe de altă parte, există legături directe între expansiunea demografică, exploatarea excesivă a terenurilor şi degradarea solurilor, defrişarea pădurilor, conflictele economice şi etnoculturale, etc. Tendința de creştere ritmică a populației se manifestă cu pregnanță în China şi India.

Bolile, sărăcia extremă, degradarea educației, coroborate cu depopularea unor teritorii întinse şi foarte bogate în resurse, plasate în vecinătatea unor state în expansiune demografică, vor continua să stimuleze instabilitățile locale şi regionale, politico-militare.

Lumea provocărilor actuale este, cu certitudine, un mediu al interconectărilor şi al interdependențelor în care reconstrucția trebuie făcută

şi după criterii morale şi unde trebuie implicate toate statele, fapt ce impune mai multă solidaritate socială, toleranță etnico-religioasă, dialog politic, căutarea consensului în luarea marilor decizii şi abordarea neconflictuală a diferențelor existente sau care apar[15].

Având în vedere că mediul de securitate global evoluează neuniform, contextul actual fiind caracterizat de factorul neprevăzut, se poate spune că resursele naturale, mediul înconjurător şi economia globală reprezintă elementele care vor modela omenirea în următorii ani.

În noul secol, provocările globalizării se referă la conservarea avantajelor, iar, în cazul dezavantajelor, țările trebuie să învețe să dezvolte multiple filtre pentru a preveni ştergerea propriei identități prin efectul omogenizator al capitalismului global. Datorită forței şi vitezei globalizării, acele țări care nu sunt suficient de puternice pentru a proceda astfel vor fi asimilate, chiar şi cu riscul pierderii identității naționale, într-un mod subtil şi lent.

În opinia lui *Friedman*, „glocalizarea" reprezintă abilitatea de a asimila influențele aducând un plus de valoare, dar, în acelaşi timp, de a ține piept celor care îi sunt realmente străine, de a separa aspectele care sunt, într-adevăr, diferite. Glocalismul singur nu este considerat suficient pentru a proteja culturile indigene de globalizare, prin urmare, este nevoie de crearea unor filtre şi mai puternice.

Un glocalism sănătos este întotdeauna un proces de încercare şi eroare, dar este din ce în ce mai necesar. Astfel, într-o lume din care au fost înlăturate şi vor mai fi înlăturate multe ziduri de protecție, garduri şi tranşee, „culturile care se pricep la glocalizare au un real avantaj, iar cele care nu se pricep vor trebui să învețe acest lucru"[16]. Globalizarea reprezintă un real pericol pentru culturile care nu sunt, în mod evident, bune glocalizatoare.

În consecință, conceptul de „glocalitate" are menirea de a depăşi opoziția binară dintre „global" şi „local" şi de a oferi o reprezentare lingvistică exactă a îmbinării acestor doi termeni în viața reală.

Astfel, la nivel conceptual, noțiunea de „glocalitate" prezintă un context, unde, într-un mod permanent, „mari şi mici jocuri" sunt jucate constant, în calitatea lor de componente ale unui concurs sau ale unei competiții, la toate nivelele în spațiul mondial. Această glocalitate reflectă

---

[15] Gabriel Oprea, Constantin Onişor, Radu Timofte, *România – integritate şi securitate*, Editura Balcanii şi Europa, Bucureşti, 2005

[16] Thomas L. Friedman, *Lexus şi măslinul*, ediția a II-a revăzută, Editura Polirom, Iaşi, 2008

un anumit grad de omogenitate între macro şi microafacerile actorilor din interiorul statelor şi dintre state, implicând deseori şi actori nonstatali, fie virtuali, fie din imediata sau îndepărtata vecinătate. Procesele din ce în ce mai interconectate dintre societăţi fac ca evenimentele dintr-o parte a lumii să aibă un impact şi mai mare asupra popoarelor şi societăţilor din alt colţ al lumii. Din această perspectivă, lumea pare a fi văzută ca un singur loc (un exemplu metaforic fiind: „dacă cineva strănută la New York, altcineva din Beijing sau Canberra face gripă).

A fi „glocal" înseamnă combinarea elementelor locale şi mondiale în cadrul activităţilor umane. Globalul şi localul se interpenetrează mai degrabă decât să-şi menţină un caracter distinct autonom. Acest concept poate fi aplicat tuturor certitudinilor sau incertitudinilor prezente şi viitoare, la toate nivelurile ordinii mondiale, în termenii securităţii tradiţionale şi nontradiţionale. Recentele evenimente legate de activităţile teroriste, consecinţele schimbărilor climatice, diminuarea resurselor în general şi a celor energetice în special, ameninţările pandemice şi chiar efectele crizei economice mondială au demonstrat că societăţile sunt vulnerabile în faţa vicisitudinilor forţelor glocale, care operează, de cele mai multe ori, dincolo de controlul lor, favorizând apariţia a numeroase provocări.

3. Răspunsuri ale politicii de securitate la adresa provocărilor de mediu la nivel global

Pentru ca o comunitate sau o multitudine de comunităţi să fie într-adevăr viabile şi durabile, trebuie să adopte o abordare care să ia în considerare resursele economice, ale mediului înconjurător precum şi cele culturale nu numai pe termen scurt, ci şi pe termen lung. Resursele mediului înconjurător şi securitatea acestuia reprezintă o problemă majoră şi, în acelaşi timp, o componentă de bază a schimbărilor produse de globalizare.

Astăzi, succesele, dar şi problemele noastre izvorăsc din evoluţia impresionantă a economiei mondiale în ultimul secol. Cererile globale ale umanităţii au depăşit puterea de regenerare a resurselor pământului.

Astăzi, cererile mondiale privind sistemele naturale depăşesc cu peste 25% capacitatea de sustenabilitate a acestora. Mediul înconjurător descrie cel mai bine gradul de civilizaţie a societăţii în care trăim, în civilizaţia noastră modernă, supertehnologizată este mult mai uşor de uitat că economia, motorul însuşi al existenţei noastre, depinde, în integralitatea sa, de sistemele şi resursele naturale ale Pământului. Fiecare dintre noi depinde de produsele

şi serviciile pe care le oferă ecosistemele planetei, de la păduri până la bazine hidrografice, de la recifuri de corali până la păşuni.

Şi, pe măsură ce resursele naturale ale pământului, la nivel local, sunt epuizate, declinul posibilităţilor economice duce la o migraţie accentuată a refugiaţilor pe considerente de mediu.

Intrăm într-o eră nou, o perioadă climatică rapidă şi, de multe ori, imposibil de prevăzut. Schimbarea este noua regulă climatică. Astăzi nu numai că ştim că pământul se încălzeşte, dar putem începe să vedem unele dintre efectele temperaturilor mai ridicate.

Oamenii de ştiinţă au concluzionat că „ridicarea temperaturii datorate încălzirii globale va face din ce în ce mai dificilă hrănirea populaţiei, din exploatarea pământului".

Deficitul global de apă este rezultatul triplării cererii în ultima jumătate a secolului trecut. Conexiunea dintre apă şi alimente este una puternică, 70% din volumul total de apă utilizat se foloseşte pentru irigaţii, 20% - în industrie, iar 10% - în scopuri casnice. Din cauza cererii de apă în creştere pentru toate cele trei categorii, competiţia dintre sectoare este din ce în ce mai intensă, iar agricultura pierde aproape de fiecare dată. Alocarea apei între interese concurente în şi între societăţi este o parte a unei nou apărute politici determinate de penuria resurselor.

Creşterea anuală a nivelului atmosferic de CO^2, una din cele mai previzibile tendinţe ale mediului de pe glob este rezultatul eliberării anuale în atmosferă a 1,5 miliarde tone de carbon, rezultate din arderea combustibililor fosili şi a 1,5 miliarde tone ca efect al despăduririlor. ÎPe măsură ce se acumulează CO^2 în atmosferă, cresc şi temperaturile.

Pe o scală mai mare, topirea celor două mari calote glaciare – Antarctica şi Groenlanda – ar putea ridica nivelul mării enorm de mult (topirea calotei Groelandei ar putea creşte nivelul mării cu 7 metri), dar şi o topire parţială a acestor calote ar avea efecte dramatice privind creşterea nivelului mării.

Presiunile asupra pădurilor continuă să crească. Dintre cele 3,5 miliarde metri cubi de lemn colectat, la nivel mondial, în 2005, jumătate a fost folosit drept combustibil (în ţările în curs de dezvoltare aproape trei sferturi din totalul lemnulului exploatat este utilizat pe post de combustibil).

Creşterea populaţiei în decursul secolului al XX-lea a forţat agricultura să se extindă în multe ţări pe terenuri extrem de vulnerabile, situaţie care a condus la degradarea solului (apariţia aşa numitelor „văi de praf") şi care la rândul lor determină formarea furtunilor de praf.

Degradarea terenurilor din cauza păşunatului excesiv are un impact

major sub forma diminuării producției de produse animale.

Toate tipurile de specii sunt amenințate de distrugerea habitatelor. Alterarea habitatelor prin creşterea temperaturilor, poluarea chimică sau introducerea speciilor exotice poate decima atât speciile de animale, cât şi cele de plante.

Deoarece piața este forța principală care dirijează activitatea umană, acțiunea ei continuă devine o parte a problemei referitoare le protecția mediului înconjurător. Poluarea rezultată din activitatea economică prin asalturile directe asupra unor părți ale ecosferei creează condițiile unui potențial dezastru ecologic major, cu consecințe grave asupra existenței umane: diminuarea diversității speciilor (care poate determina ecosistemele să fie mai vulnerabile sau chiar să intre în colaps), subțierea stratului de ozon poate face să crească simțitor nivelul radiațiilor solare, efectul de seră datorită creşterii concentrațiilor de CO^2 precum şi a emisiilor şi altor gaze cu acelaşi efect de către societățile industriale poate duce la schimbarea temperaturii globale.

Este necesar, în aceste condiții, să includem consecințele asupra mediului în calculele de cost ale pieței, operațiune dificilă în condițiile unei piețe descentralizate şi competitive. Marile incertitudini legate de vulnerabilitatea mediului îngreunează şi acțiunea politică. La fel şi acțiunea egoistă a statelor care încearcă să-şi îmbunătățească poziția pe piață.

Amplificarea problemelor de mediu poate conduce la apariția unor conflicte determinate de cantitatea de resurse vitale şi distribuția acestora. În legătură cu aceasta se pot intui următoarele forțe şi tendințe dimpreună luate ca amenințări şi riscuri:

✓ deteriorarea mediului înconjurător ca urmare a emisiilor continue de la obiectivele industriale cu un înalt grad de poluare precum şi prin deversarea sau depozitarea necorespunzătoare a deşeurilor industriale şi menajere;

✓ degradarea echilibrelor ecologice ca urmare a poluării apei, aerului şi solului, exploatării necorespunzătoare a resurselor biologice, precum şi producerii de accidente tehnologice sau sabotaje la obiectivele economice;

✓ poluarea transfrontieră ca urmare a unor accidente industriale;

✓ poluarea unor cursuri de apă;

✓ producerea de incendii catastrofale care se propagă şi dincolo de frontierele naționale;

✓ provocarea unor sabotaje sau acte teroriste care urmăresc degradarea mediului (distrugerea de baraje, infestarea unor cursuri de apă);

✓ importul de deşeuri toxice.

La nivel global solul, apa, aerul sunt alterate, datorită urbanizării

galopante, despăduririlor, poluării mărilor şi fluviilor, încălzirii climei, subţierii stratului de ozon, şi ploilor acide, toate punând în pericol viitorul umanităţii. Acţiunile ostile ecologice ca o formă de destabilizare a unui stat au fost sesizate recent, cu toate că, de-a lungul istoriei, acestea s-au materializat din perioada apariţiei industriei poluante şi a goanei după profit.

Odată cu efectele pozitive ale globalizării, se manifestă însă şi puternice forţe care acţionează în sensul fragmentării sociale, accentuării nivelului critic al vulnerabilităţilor entităţilor statale, creând premisele necesare manifestării violenţei şi conflictelor. Atunci când se manifestă, crizele economice au un efect de destabilizare globală, toate aceste implicaţii ale globalizării având puternice conotaţii în domeniul securităţii naţionale şi internaţionale.

Globalizarea facilitează dezvoltarea şi răspândirea, la nivel planetar, a unor efecte negative, chiar perfide, din cauza caracterului lor insidios. Aceste consecinţe se întrepătrund şi se corelează reciproc, efectul lor cumulat asupra stabilităţii şi securităţii internaţionale fiind mult mai pregnant decât simpla sumă a componentelor lor.

O mare varietate de ameninţări la adresa securităţii se regăsesc, în prezent, la nivel global şi au devenit mult mai periculoase ca urmare a răspândirii cunoştinţelor tehnologice, a accesului mai rapid la ultimele cuceriri ştiinţifice şi tehnice, cât şi a deplasării mai rapide şi mai puţin controlabile a populaţiei.

Aceste evoluţii, combinate cu extinderea interacţiunilor economice, contribuie la acutizarea problemelor şi resentimentelor care stau la baza ameninţărilor la adresa securităţii. În mod paradoxal, astfel de aspecte ale globalizării oferă noi oportunităţi de stimulare a creşterii economice, de promovare şi răspândire a democraţiei în întreaga lume, reducând violenţa unora dintre ameninţările actuale.

Importanţa globalizării pentru securitate constă în faptul că, în timp ce securitatea devine internaţională, legătura dintre economie şi securitate a devenit tot mai naţională, forţele globalizării şi agenda tot mai lărgită a securităţii conducând la creşterea interconectării regiunilor, la o amplificare a competiţiei şi a agregării, la o schimbare de stil în intervenţiile militare, la alianţe complexe şi la aranjamente de securitate. În pofida acestor factori, creşterea şi percepţia insecurităţii continuă.

Încă persistă destule confuzii în definirea securităţii, dar un lucru este clar şi anume faptul că securitatea nu înseamnă doar protecţia fizică a actorului de referinţă, ci implică şi protecţia economică, energetică, politică sau culturală a valorilor sau intereselor acestuia.

De aceea, formularea unei politici de securitate realiste în contextul globalizării trebuie să înceapă prin stabilirea unei definiții operaționale a securității, a unui set clar de criterii pentru evaluarea acestei politici, precum şi luarea în considerare a tuturor efectelor procesului de globalizare. Modelul trebuie să cuprindă probleme ca sărăcia, migrația, traficul de armament, droguri şi persoane, riscurile de mediu, amenințările economice sau politice, epuizarea resurselor energetice, creşterea demografică şi nerespectarea drepturilor omului, crima organizată, terorismul şi, nu în ultimul rând, conflictele armate. Securitatea fiind un concept mult mai complex decât apărarea granițelor prin mijloace militare, este necesar un cadru conceptual, o metodologie sistemică de evaluare a mediului de securitate sub impactul globalizării, de identificare a amenințărilor reale şi a intereselor din acest context, strategiile de securitate propunându-şi să protejeze diferite entități: indivizi, state, regiuni sau sistemul internațional. Într-o democrație, elita politică, deținătoarea puterii prin delegare din partea poporului, este cea care propune viziunea strategică.

Formularea viziunii strategice este o etapă de bază a politicii de securitate națională. În comunitatea euroatlantică însă se vorbeşte de seturi de strategii naționale organizate la fiecare nivel strategic. În concepția lui *Arthur F. Lykke*[17], strategia de securitate națională „este o ecuație de gradul trei bazată pe tot atâția piloni: obiective, concepte şi resurse strategice". Strategia de securitate națională se va construi în jurul valorilor şi a intereselor naționale, iar, dacă acest aspect este analizat în contextul realităților globale, se constată, ca o caracteristică generală, raportarea lor la conceptul globalizării. Astfel, din ce în ce mai mult, strategia îşi lărgeşte sfera de acțiune, cuprinzând domenii dintre cele mai variate, utilizându-se deja ca termeni consacrați: strategia de securitate, strategia energetică, strategia de dezvoltare durabilă.

Edificatoare în această direcție poate fi amintită crearea unor strategii de securitate europene sau euroatlantice pornind de la interesul europenilor, şi anume acela de a construi un continent puternic şi unitar sau interesul țărilor care fac parte din NATO de a genera acel mediu de securitate favorabil creării condițiilor necesare desfăşurării unei vieți liniştite şi prospere care să țină sub control crizele şi amenințările şi să reducă la maximum vulnerabilitățile şi riscurile posibile ale societății în acest prim deceniu al secolului al XXI-lea.

Construirea unei noi arhitecturi de securitate la baza căreia se află

[17] Colonel în retragere şi profesor la Colegiul de Război al SUA

încrederea şi cooperarea internaţională, democraţia şi economia performantă, asigurarea şi respectarea drepturilor omului, concomitent cu promovarea şi afirmarea valorilor naţionale, nu este un proces utopic aflat în sfera virtualului, ci se dovedeşte a fi unul perfect realizabil, dar care solicită aranjamente şi demersuri politice specifice, într-o anumită perioadă, precum şi angajarea unor importante resurse economice şi financiare, pe o durată de timp mult mai lungă decât se preconiza iniţial.

Globalizarea securităţii este o consecinţă firească a creşterii conexiunilor sociale, alternativa fiind o dezordine socială, generalizată, în care nu se mai acceptă nimic ca fiind legal sau moral. Aceasta favorizează nu numai competiţia pentru putere, ci şi lupta pentru resurse, indiferent care sunt acestea, şi pentru pieţele de desfacere, iar apariţia actorilor nonstatali şi creşterea influenţei lor în acest mediu este o realitate tot mai evidentă.

Una din condiţiile reuşitei globalizării o reprezintă globalizarea securităţii, care presupune un „*răspuns global*" nu numai la riscuri şi ameninţări, ci şi la cerinţele de gestionare a acestora, de monitorizare şi reducere a vulnerabilităţilor. Această reacţie globală include soluţionarea situaţiilor care pun în pericol securitatea oricărui stat, cu participarea tuturor forţelor de care este nevoie şi unde este nevoie. Nimic nu mai corespunde unor şabloane de intervenţie, la aceasta pot participa structurile modulare de forţe, structurile comune, structurile integrate, forţele de reacţie rapidă, forţele speciale, forţele nucleare strategice, structurile de răspuns la crize, etc. Ele pot fi dintr-un stat, dintr-o alianţă, dintr-o coaliţie sau, pur şi simplu, dintr-o reuniune de state cu aceleaşi interese care impun folosirea aceloraşi concepte.

Date fiind caracteristicile acestui mediu de securitate, revin în actualitate strategiile preventive credibile, care necesită noi standarde de securitate, în cadrul unor sisteme de securitate capabile să furnizeze avertismente timpurii şi să dispună de capacităţi şi disponibilităţi ridicate la nivel naţional şi internaţional.

O modalitate de a răspunde prompt împotriva noilor ameninţări ce se manifestă pe fondul globalizării este concentrarea pe realizarea unor mecanisme funcţionale de securitate naţională şi internaţională. Un alt posibil răspuns îl poate constitui analiza problemelor de importanţă globală şi regională în comparaţie cu evenimentele din regiunea considerată obiect de studiu şi din arealele adiacente.

Globalizarea pericolelor şi ameninţărilor şi sporirea caracterului simetric al acestora au determinat statele să-şi reevalueze strategia de securitate naţională. Este nevoie ca o asemenea strategie de securitate, creată în contextul procesului de globalizare, să fie configurată astfel încât

să protejeze interesele statelor şi să promoveze valorile general umane pe care acestea le-au îmbrăţişat. În acelaşi timp, strategia trebuie să urmărească şi promovarea unor valori globale, concomitent cu dezvoltarea unor sisteme, instituţii şi norme globale viabile. Întrucât conceptul de securitate este structurat pe câteva dimensiuni clasice – economică, politică, militară, socială şi de mediu – este necesar ca viziunea globală a strategiilor de securitate naţională să ia în considerare riscurile la adresa securităţii naţionale determinate de globalizare pe toate cele cinci dimensiuni.

În acest context, identificarea şi implementarea unor politici în vederea contracarării, la nivel naţional, a insecurităţii globalizate devin tot mai dificile. Adaptarea ţărilor la noile condiţii ale mediului de securitate depinde, în ultimă instanţă, de puterea, voinţa de asumare a responsabilităţii şi flexibilităţii, transparenţa instituţiilor naţionale şi internaţionale din care fac parte, dar şi de cultura organizaţională şi capacitatea liderilor de a adapta atât instituţiile, cât şi cultura pentru o nouă eră.

Sarcina de a cunoaşte sursele generatoare de insecuritate şi instabilitate în scopul protejării proceselor care susţin funcţionalitatea statelor democratice revine serviciilor de informaţii. Nevoia de anticipare operativă a tipurilor de riscuri existente sau prognozabile, pentru a asigura funcţia esenţială de avertizare timpurie, impune dezvoltarea unor programe de eficientizare a activităţii serviciilor de informaţii, altfel spus responsabilitatea fundamentală a serviciilor de informaţii este de a identifica corect şi din timp ameninţările interne şi externe la adresa securităţii, astfel încât acestea să fie soluţionate fără a cauza pagube şi pierderi umane sau materiale.

Cunoaşterea riscurilor şi ameninţărilor în actualul context presupune nu doar analiza fenomenelor, ci şi anticiparea evoluţiilor cu impact asupra securităţii naţionale. În acest context se remarcă o serie de vulnerabilităţi importante care ne afectează securitatea – în zona economică, a infrastructurii, în domeniul energetic, al protecţiei mediului şi securităţii alimentare, pentru a nu enumera decât câteva – peste care se suprapune accentuarea unor fenomene cu risc important, generate de extinderea terorismului, a reţelelor de trafic şi crimă organizată, dar şi persistenţa unor rivalităţi statale.

Conjugarea interesului naţional cu necesitatea socială într-un mediu de securitate complex şi imprevizibil, cum este cel pe care-l trăim, oferă posibilitatea cunoaşterii, de către cetăţeni, a raţiunii sociale a serviciilor de informaţii, precum şi a importanţei misiunilor pe care le primesc acestea în vreme de pace, criză sau război.

Cultura de securitate constituie indicatorul capacităţii decidenţilor politici de a cunoaşte, preveni şi contracara disfuncţiile, vulnerabilităţile, riscurile, ameninţările, stările de pericol şi posibilele agresiuni la adresa

organizărilor sociale şi a entităţilor sociopolitice. Aceasta oferă societăţii civile reperele necesare implicării active în formularea unor politici şi strategii de securitate.

Lărgirea spectrului de riscuri neconvenţionale, cu caracter transnaţional, diversificarea tipologiei crizelor şi a conflictelor generează provocări multiple care necesită reacţii multidirecţionale, bazate pe mobilitate, oportunitate, diversitate, coerenţă şi complementaritate.

În acest sens, futurologul *Alvin Toffler*[18] sublinia: „dintre toate instituţiile de securitate naţională, niciuna nu cunoaşte o nevoie mai profundă de restructurare şi de reconceptualizare decât acelea de informaţii (...). Pe măsură ce prinde contur noua formă de război – cel al informaţiei – activitatea informativă fie îşi va asuma o formă proprie, reflectând noul rol al informaţiei şi cunoaşterii în societate, fie va deveni costisitoare, irelevantă sau primejdios de derutantă".

Datorită caracterului global şi interconectat al principalelor riscuri şi ameninţări, dimensiunea transnaţională şi transdisciplinară a acestora, precum şi asimetria şi potenţialul acestora de a genera schimbări abrupte şi chiar catastrofice, afectează securitatea oricărei naţiuni. Ameninţările cu caracter global generează, de cele mai multe ori, efecte de intensităţi diferite în plan local, ceea ce se repercutează negativ asupra disponibilităţii de a le trata sistemic şi, în consecinţă, asupra eficienţei soluţiilor adoptate.

Ca atare, gestionarea şi contracararea acestor riscuri şi ameninţări necesită:

⇒ o abordare sistemică şi transnaţională, având în vedere caracterul global şi interconectat al acestora;

⇒ evaluarea permanentă a modului de gândire şi acţiune, care să asigure identificarea celor mai potrivite soluţii la problemele noi, cu caracter asimetric;

⇒ eforturi susţinute pentru adaptarea instituţiilor cu atribuţii în domeniul securităţii la schimbările survenite.

[18] Alvin Toffler (născut la data de 03.10.1928) este scriitor, sociolog şi futurolog american, fiind primul, alături de soţia sa, care a avertizat asupra consecinţelor schimbării de paradigmă, asociată erei informatizării, în toate domeniile vieţii umane.

Bibliografie

1. Barry Buzan, *Popoarele, statele şi teama,* Chişinău, Editura Cartier, 2000, ediția a doua, pag. 26 – 36, 105 – 115, 120 – 148;

2. David Held, *Transformări globale. Politică, economie şi cultură,* Iaşi, Editura Polirom, 2004, pag. 34 – 53;

3. Joseph E. Stiglitz, *Mecanismele globalizării,* Iaşi, Editura Polirom, 2004, pag. 19 – 36, 61 – 62, 147 – 162;

4. Thomas L. Friedman, *Lexus şi măslinul,* Iaşi, Editura Polirom, 2004, ediția a II-a revăzută, pag. 48 – 61, 244 – 266, 267 – 295;

5. Coord. George Cristian Maior, *Un Război al Minții. Intelligence, servicii de informații şi cunoaştere strategică în secolul XXI,* Bucureşti, Editura RAO, 2010, pag. 21 – 60;

6. Jon Barnett, *The meaning of environmental security: ecological politics and policy in the new security era,* London, Zed Books, 2001, pag. 12 – 49, 108 – 121, 139 – 156;

7. Simon Dalby, *Environmental security,* USA, University of Minnesota Press, 2002, pag. XIX – XXVI, 21 – 40, 143 – 162;

8. Kurt M. Campbell, *Climate Cataclysm. The foreign policy and national security implications of climate change,* USA, Brookings Institution Press, 2008, pag. 1 – 25, 213 – 224;

9.Phillip F. Cramer, *Rethinking environmental protection,* USA, Lexington Books, 2000, pag. 1 – 20, 183 – 205, 207 – 231;

10. Narottam Gaan, *Environmental security: Concept and dimensions,* India, Kalpaz Publication, 2004, pag. 51 – 112, 171 – 226;

11. Edit. Hans Gunter Brauch, *Hexagon series on human and environmental security and peace,* volume 3, Springer, 2008, Germany; pag. 27 – 44;

12. Stephen Stec, Besnik Baraj, *Energy and environmental challenges to security,* NATO, Springer, 2007, pag. 33 – 56;

INSTRUCȚIUNI PENTRU AUTORI

Pregătirea materialelor pentru publicare şi criterii de evaluare

Editorii şi redactorii *Revistei Române de Studii de Intelligence (RRSI)* selectează materialele transmise de autori[19] şi, acolo unde este cazul, le ameliorează prin dialog constructiv, doar cu acceptul acestora din urmă, asigurând astfel corectitudinea şi valoarea ştiinţifică a materialelor ce urmează a fi publicate. *RRSI* acceptă doar editoriale, articole şi recenzii care nu au fost anterior publicate.

Evaluarea calităţii academice a materialelor se face conform procesului *double blind review*, corespondenţa dintre evaluatori şi autori realizându-se prin intermediul e-mailului cnita@dcti.ro.

RRSI garantează că lucrările nu sunt respinse / modificate pentru că ideile exprimate sunt contrarii altor studii publicate anterior sau poziţiilor evaluatorilor, ci doar în cazul în care nu fac dovada cercetării ştiinţifice.

Colectivul de redacţie asigură confidenţialitatea pentru materialele respinse de la publicare, precum şi pentru modificările aduse acestora, iar autorul îşi asumă întreaga responsabilitate pentru ideile exprimate în articol, pentru documentarea invocată şi sursele citate.

Redacţia revistei nu-şi asumă responsabilitatea pentru opiniile exprimate de autori în articolele trimise spre publicare şi-şi rezervă dreptul de a face modificări editoriale, cu condiţia ca acestea să nu afecteze nici înţelesul şi nici originalitatea textului.
Articolul nu trebuie să conţină conotaţii politice de partid.

În vederea unei cât mai facile prelucrări şi integrări a materialelor transmise, vă rugăm să respectaţi următoarele **criterii de redactare**:

- dimensiunile articolului pot varia între minim 8 şi maxim 15 pagini (inclusiv note de subsol şi bibliografie, eventual tabele şi / sau grafice), paginile nu se numerotează;
- articolul trebuie să aibă o structură logică, respectiv introducere, capitole (subcapitole), concluzii;
- textul trebuie redactat cu caractere Times New Roman de mărimea 12, diacritice, la un rând, Word Microsoft Office 2003/2007, format fişier „.rtf”;
- prima pagină trebuie să conţină titlul lucrării (Times New Roman de mărimea 14, bold, centrat) şi afilierea autorului (Times New Roman de mărimea 12, nume şi prenume, titlu ştiinţific, apartenenţa la o instituţie / asociaţie / organizaţie, statut de masterand / doctorand, precum şi adresa de e-mail);

[19] Autorii interesaţi de publicarea unor lucrări în „*Revista Română de Studi de Intelligence*” vor trimite propunerile de articole în format „word” pe adresa de e-mail cnita@dcti.ro, cu menţiunea „Propunere de publicare în RRSI”.

- articolul va fi însoțit de un rezumat / abstract (de până la 100 de cuvinte) şi de cuvinte-cheie (keywords), ambele într-o limbă de circulație internațională (Times New Roman de mărimea 11);

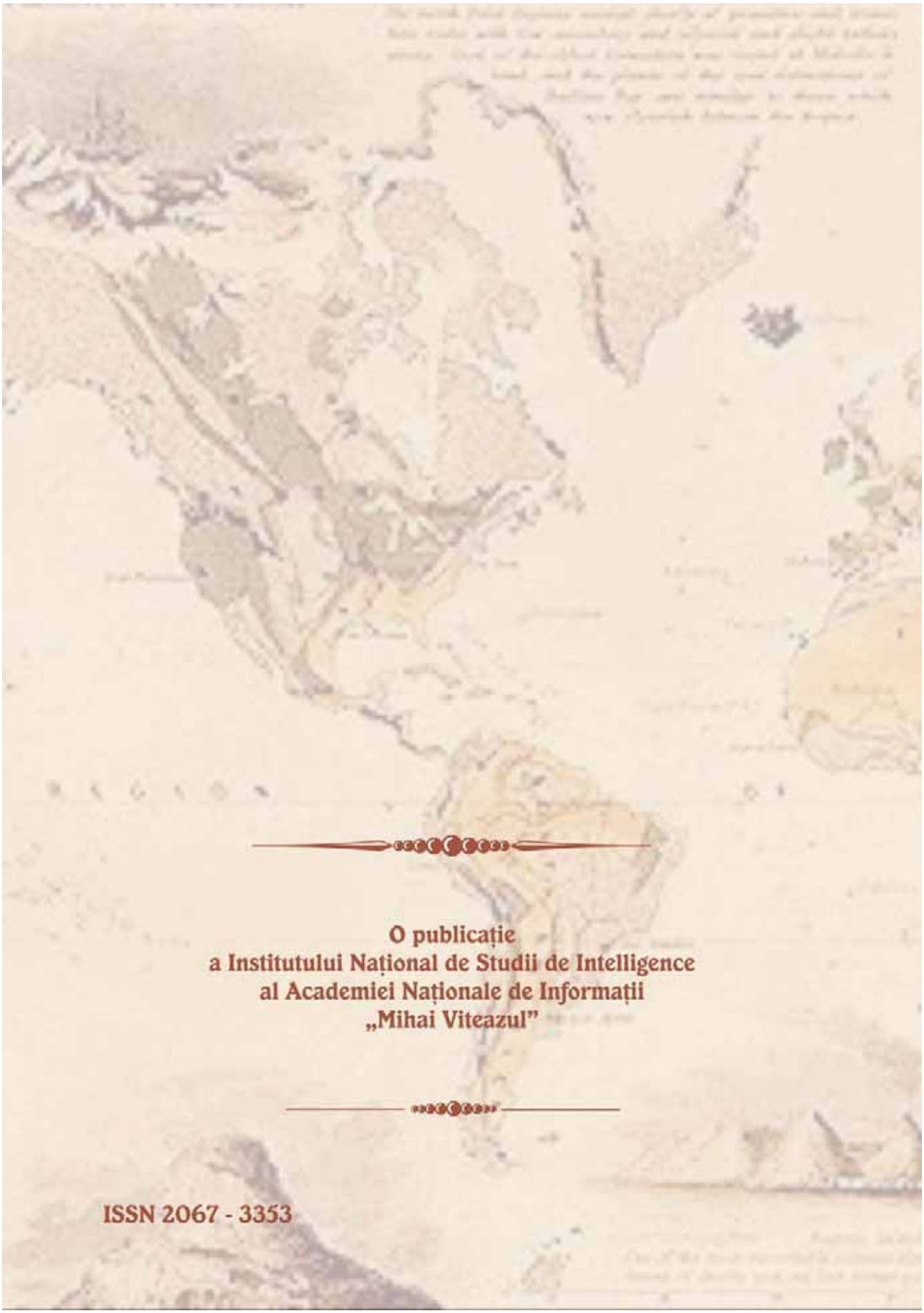
- sursele bibliografice se vor preciza sub forma notelor de subsol (Times New Roman de mărimea 10, la un rând), după cum urmează: nume (cu majuscule), prenume autor (i), *titlul lucrării*, volumul / ediția, editura, localitatea, anul, pagină / pagini, iar trimiterile Internet se citează cu linkul întreg şi data la care a fost acesta accesat. Pentru citarea unui articol se vor preciza următoarele elemente: autor (i), titlul între ghilimele, *publicația*, volumul, numărul, zi/lună/an apariție, p./pp. Dacă lucrarea nu are autor, se trec trei steluțe liniare (***) sau numele instituției sub egida căreia a apărut lucrarea;

- pentru citate se folosesc ghilimele („ – pentru deschidere şi ” – pentru închidere);

- tabelele se numerotează, iar titlul acestora se scrie se scrie cu un corp mai mic cu 2 puncte decât textul de bază, justify şi centrat deasupra tabelului. Numerotarea tabelului se face deasupra titlului. Titlul tabelului se scrie cu un corp mai mic decât textul de bază. Dacă există tabele care cuprind note, acestea se vor scrie imediat după tabel, nu la piciorul paginii şi nici în interiorul tabelului;

- figurile se numerotează. Titlul figurii se scrie cu un corp mai mic cu 2 puncte decât textul de bază, justify şi centrat, imediat sub aceasta, fără spații, după care se dă explicația figurii, respectiv a graficului şi se precizează sursa, dacă este cazul;

- bibliografia (Times New Roman de mărimea 11, la un rând) se plasează la sfârşitul articolului, după anexe. Lucrările se scriu în ordinea alfabetică a numelor autorilor, numerotându-se cu cifre arabe urmate de punct; când sunt doi sau mai mulți autori pentru o lucrare, regula privitoare la ordinea alfabetică este valabilă doar pentru primul nume. Ordinea datelor este următoarea: numele şi prenumele autorului, titlul lucrării, volumul / ediția, editura, localitatea, anul.



O publicație
a Institutului Național de Studii de Intelligence
al Academiei Naționale de Informații
„Mihai Viteazul"

ISSN 2067 - 3353