REVISTA ROMÂNĂ
DE STUDII DE INTELLIGENCE

Nr. 4
Decembrie
2010

Bucureşti
- 2010 -

CUPRINS

Waterboarding, rendition, secret flights and secret prisons: degeneration or fruition of intelligence in the fight against terrorism?

– Paper presented within a EENET workshop* –

Bob de GRAAFF – University of Utrecht
e-mail: **ani@sri.ro**

Abstract:
This article examines the new developments in the field of intelligence with an impact on the ethical framework of intelligence activity, urging the re-questioning and rethinking of the role of ethics in this profession. Easing the tension beween intelligence effectiveness and moral statndards is a challenging task, albeit one which will trace the course for intelligence recognition or intelligence degradation in a democratic society.
Keywords: intelligence ethics, intelligence methods, intelligence profession.

To bridge the tension between on the one hand effectiveness, such as intelligence and security services or their political sponsors want, and on the other hand the moral standards that from a broader social context are set for these services, the criteria of proportionality and subsidiarity have been developed.[1]

These criteria imply that a certain relationship must exist between the purpose of intelligence gathering and deployed intelligence resources (proportionality) and that no resources are to be used for intelligence gathering in cases where the information could be obtained with much less intrusive methods (subsidiarity).

I will now briefly discuss some of the intelligence methods used in the context of the so-called war on terror, in particular to try to answer the following questions:

1. Are there any new developments that are relevant to an ethical analysis?

[1] They make a comparison with the theory of just war possible and can also be found back in the Dutch Law on Intelligence and Security. Several writers on ethics and intelligence use the theory of just war as a starting point e.g. J.M. Olsen, *Fair Play. The Moral Dilemmas of Spying*, Washington D.C. 2006, pp. 20-22; D.L. Perry, *Partly Cloudy. Ethics in War, Espionage, Covert Action, and Interrogation*, Lanham, MD, etc 2009, p. 95; M. Phythian, "Intelligence theory and theories of international relations. Shared worlds or separate worlds?", P. Gill, S. Marrin and M. Phythian (eds.), *Intelligence Theory. Key questions and debates*, London/New York 2009, p. 64; P.H.J. Davies, "heory and intelligence reconsidered", *ibidem*, p. 200.

2. is the existing ethical framework sufficiently developed and does it proffer sufficiently clear criteria for intelligence staff in practical situations to make ethically justified decisions?

3. do the intelligence resources that are used live up to the criteria of proportionality and subsidiarity? and

4. are they effective?

1. What are new developments in the field of intelligence?

I would like to summarize the new developments that are relevant for this argument under the term "blurring of the lines". I will briefly mention some of these developments, each time immediately followed by the consequences they have. The blurring of distinctions occurs in many fields, primarily in the US, but to a lesser degree also in other parts of the Western world. In the first place in the socio-political context in which intelligence and security services operate:

1. The difference between international and national threats diminishes. Result: the distinction between offensive intelligence gathering abroad and the protection of national security and the democratic order at home becomes obscured; the distinction between national citizenry and citizenry of the world falls away;[2] residents and citizens of one country may be subject to the legal system of another country or even be kidnapped or slain by a foreign power; furthermore, the system of "targeted killings" threatens to expand over ever wider categories;[3]

2. the distinction between personal and public life fades. Result: interference with privacy by the government can easily be explained away; in principle, the private sphere, therefore, has been eliminated;[4]

3. the distinction between public and private activities blurs in the field of security (this applies to both police and surveillance and military and intelligence functions). Result: there is a situation likely to arise in which what the government is not permitted is carried out by private services, which

[2] Th. Darnstädt, *Der globale Poliziestaat. Terrorangst, Sicherheitswahn und das Ende unserer Freiheiten*, Hamburg 2009; A. Mattelart, *The Globalization of Surveillance*, Cambridge / Malden, MA, 2010.

[3] C. Whitlock, "Afghans Oppose U.S. Hit List of Drug Traffickers", *Washington Post*, 24 October 2009.

[4] Cf. P. Schaar, *Das Ende der Privatsphäre. Der Weg in die Überwachungsgesellschaft*, München 2007.

are subject to less stringent standards; furthermore, the public-private mix may lead to incestuous relationships and breaches of integrity;

4. partly due to the great pressure of time in which authorities believe they are due to the threat of terrorism, especially in the case of possible use by terrorists of weapons of mass destruction, rational decision-making is more and more replaced by instinctive and improvisational acting. Result: possible consequences of action are getting less thought out, there is an unbridled desire for action, without much intelligence, both in the sense of brainpower and in the sense of prior information-gathering.

Intelligence itself also changes character:

5. the succession of distinct intelligence activities as parts of a continuous intelligence cycle makes way for parallel core intelligence activities. Result: intelligence officers get less guidance and (re)direction from either outside or above; their work is increasingly based on trial and error;

6. as a result of the information revolution, intelligence and security services use open sources more and more frequently. Result: the distinction between information and intelligence fades, as reflected in the frequent use of data mining, profiling and pattern recognition by intelligence and security services, contributing to a situation where, in principle, every citizen swims into the dragnets of a secret service, a situation in which every citizen is suspect, unless…;[5] the outcry that Western states have become surveillance states, that gather more and more data about their citizens and make the standard deviation an increasingly important criterion for their citizenries, is becoming louder and louder;[6]

7. the gap between policy formulation or decision making on the one hand and intelligence on the other gets filled: the distinction between strategic and tactical operations, including strategic and tactical intelligence, is also likely to disappear.[7] Result: decision-makers become their own

[5] Cf. B. de Koning, *Alles onder controle. De overheid houdt u in de gaten*, Amsterdam 2008, p. 18.

[6] E.g. S. Harris, *The Watchers. The Rise of America's Surveillance State*, New York 2010; M. den Boer and J. van Buuren (eds.), *Door het oog van de staat. Publieke controle op de burger*, Amsterdam 2010.

[7] Vgl. UK Ministry of Defence, *Joint Doctrine Note 1/10. Intelligence and Understanding*, Shrivenham 2010, pp. 1-6.

intelligence analysts or try to micromanage intelligence operations.[8] This politicization of the intelligence process either leads to demoralisation in the intelligence community because the lack of recognition of its professionalism or to the delivery of "intelligence to please";[9] the politicization of intelligence also implies a concentration on today's problems with too little attention to the problems of tomorrow;

8. secret services have increasingly become part of the public domain and debate. The result: political pressure on intelligence and security services, partly again due to a public pressure; the increased transparency of intelligence and security services since the end of the Cold War has not been accompanied by an effective management of public expectations; on the contrary, politicians have been selectively peddling intelligence to the public that was based on dubious sources and thus ultimately became the victims of their own "information policy"; in order to prevent image damage of politicians intelligence and security services had to suffer loss of prestige;

9. the distinction between military and civilian intelligence fades. Result: in the US, according to insiders, the CIA and the Pentagon increasingly resemble each other;[10]

10. the distinction between intelligence analysis and intelligence operations is weakening. Result: this may not only cause amateurism that

[8] The former was the case with the Dutch prime minister on the eve of the Iraq war, the latter with President Bush, who during daily briefings so interfered with operational details that presidential pressure on the staff of intelligence and security services led to professionally and ethically irresponsible performance. One can also think of the actions of Vice President Dick Cheney, who in the run up to the Iraq war visited the CIA as many as eight times, and not to be informed, Th. Powers, "The CIA and WMDs: The Damning Evidence", *The New York Times Review of Books*, 19 August 2010. Or think of the Abu Ghraib affair (Cf. Perry, *Partly Cloudy*, p. 86) or of the so-called proof of a relation between Saddam Hussein and Osama bin Laden, known on the eve of the American invasion of Iraq as "the Big Lie", J. Kiriakou, *The Reluctant Spy. My Secret Life in CIA's War on Terror*, New York 2009, p. 152.

[9] E.g. Kiriakou, *Spy*, pp. 156-157 en 162. Cf. the remark by an employee of the National Intelligence Council Fulton Armstrong about the "pressure" by Cheney and other members of the Bush administration and "the power of an administration's flattery", Armstrong, "The CIA and WMDs".

[10] S. Shane, M. Mazzetti and R.F. Worth, "Secret Assault on Terrorism Widens on Two Continents", *New York Times*, 14 August 2010; Kiriakou, *Spy*, p. 104.

affects the "victims" of intelligence or the quality of intelligence analysis, it can also be dangerous for intelligence personnel, as showed in late 2009 in Afghanistan when seven employees of the CIA working at the intersection of both disciplines were blown to pieces in a suicide attack by an informant;

11. the distinction between intelligence and covert operations is reduced. Result: the American practice, in which the two have been brought together long ago, shows that historically ninety percent of all criticism and moral indignation about the CIA is not about intelligence in the strict sense, but concerns the covert operations; a mixture of both therefore threatens to affect intelligence in an ethical sense;

12. intelligence gathering and law enforcement seem to merge. Risk: police threaten to develop into secret police and to the intelligence and security services executive powers are made available that had so far been denied to them in some western countries on the basis of experiences during the Third Reich.

The combined threat of terrorists and weapons of mass destruction has also contributed to the blurring of distinctions.

13. the distinction between war, terrorism, guerrilla and insurgency is fuzzy. Consequence: it is nowadays easy to view any form of conflict as part of a global conflict, a global war on terror or a global counterinsurgency, also thereby threatening the transplantation of methods that a government considers acceptable as part of a counterinsurgency to the national territory;

14. terrorism moves at the interface between crime, warfare, a social problem and a threat to national security and the democratic order. Result: precisely because the phenomenon of terrorism crosses different domains of government, a government that pursues a comprehensive approach or a grand strategy against this phenomenon may become seduced to refurbish a political structure that is the more or less balanced result of decades or even centuries of building, or may even be seduced to partially demolish it;

15. self-defense and pre-emptive actions seem to be synonymous, i.e., defense and aggression begin to resemble each other;[11] this is also due to the fact that the boundary between (political-military) power and powerlessness is fading. Result: in their fight against terrorists governments begin to appear much the same as their opponents (by using such tactics

[11] Cf. M. Ignatieff, *The Lesser Evil. Political Ethics in an Age of Terror*, Toronto etc., 2004, p. 164.

as unexpected attacks, kidnapping, humiliation and assassination as well as showing an unwillingness to negotiate) and are consequently losing the moral high ground;

16. the difference between war and peace has become rather unclear. One result: in particular the status of prisoners in the fight against terrorism is unclear: is he a prisoner, a POW, the subject of protective custody, known as *Schutzhaft* at the time of the Nazis, or is he withheld from the public eye as a *Nacht und Nebel* detainee?;

17. more than during the Cold War the war on terror has created a dependence on non-Western intelligence and security services that use other legal and ethical standards than their Western partners use(d) to maintain.[12] Result: Western governments are at risk of becoming guilty of torture and murder by proxy; a lack of clear ethical guidelines in respect of foreign liaison already leads sometimes to qualms among employees of intelligence and security services;[13]

18. authorities, including law enforcement, act, both nationally and internationally, increasingly on the basis of assumptions rather than on the basis of evidence. Result: not only does the blurring between evidence and suspicion arise in national legal systems, partially as the result of a more general prevention optimism, but this blurring also manifests itself in the international arena; this blurring was perhaps the most clearly summarized in the so-called "one-percent" or Cheney doctrine, which states that if there is a one percent chance of a nuclear threat by a terrorist group the U.S. government will have to treat it "as a certainty in terms of our response".[14]

19. governments assess people increasingly on the basis of their ideas and intentions rather than according to their actual deeds. Result: the attention of governments, especially in the radicalization discourse, for what they deem dangerous thoughts and intentions of citizens has been an essential contribution to the beginning of the creation of a thought police and has much contributed to mutual distrust among their citizens;

---

[12] E.g. Kiriakou, *Spy*, pp. xv-xvi, 99-100, 106, 122-123, 142; K. Silverstein, "Official Pariah Sudan Valuable to America's War on Terrorism: Despite Once Harboring Bin Laden, Khartoum Regime Has Supplied Key Intelligence, Official Says", *Los Angeles Times*, 29 April 2005.

[13] For an example from the practice of the CIA see Perry, *Partly Cloudy*, p. 99.

[14] R. Susskind, *The One Percent Doctrine. Deep Inside America's Pursuit of Its Enemies Since 9/11*, London 2007, p. 62.

20. the difference between traditionally democratic states and dictatorships has become less obvious. Result: it can not be excluded that individual officials of Western countries are now at risk of prosecution for war crimes, and e.g. the United Kingdom has on inter alia the length of detention without charge been ranged by some human rights watchdogs in the category of countries such as China and Russia.

2. The ethical framework

It is already difficult enough to develop a professional ethics for intelligence officials. A basic problem for intelligence and security services in democracies is the question: for whom do they and their employees work, to put it differently: what is the good cause they serve in operations that under other circumstances would be characterized as unethical? There is a reluctance to say that intelligence personnel works for the (incumbent) government and in the run up to the Iraq war it became once again apparent that there are risks involved in serving the immediate policy objectives of the incumbent government; therefore it is said that intelligence and security services work not for the government, but for the state, for the people, in the national interest, for a just cause or in the spirit of the constitution. But in practice, these services and their employees have to decide themselves in individual cases as to what the state or the people want and what the national interest, the good cause or the spirit of the constitution implies.

Another important ethical issue for intelligence and security services is the balance between freedom and stability. In the ethical framework that dominated during the Cold War freedom was a value of paramount importance. After the wars in Afghanistan and Iraq, which by the way already lasted longer than World War II, one may wonder whether the value of stability should not be upgraded in comparison with the value of freedom.

It is difficult to see how the blurring of lines outlined before will not lead to a blurring of the professional standards and would in any case make it difficult to establish a well-defined ethical framework.

3. Proportionality and subsidiarity

In recent years terrorism has so much been depicted as the "absolute evil" that the issue of proportionality had of course to suffer from it. Indeed, the only remedy against absolute evil are absolute means. President Bush's

statement, "We have no higher responsibility than stopping terrorists", made any ethical consideration superfluous.[15]

In several respects Western intelligence and security services have in recent years exceeded the limits of subsidiarity and proportionality, albeit often encouraged by politicians. Central to this is stretching the limits of interrogation methods by U.S. intelligence and security services, known as "enhanced interrogation techniques" that are contrary to both the Convention against Torture, signed by the U.S., and U.S. law.[16]

But not only at the level of acts has proportionality been lost from sight. All over the world there has been a tremendous growth of intelligence and security services. The U.S. now has the appalling number of about 845,000 people working in the sphere of intelligence and security, i.e. 0.7 percent of the total workforce. I wonder if there is a quantitative standard to indicate the concept of 'police' or 'intelligence state' and the numerical ratio in respect of the workforce that can be considered to be the treshold for such a qualification.

4. Effectiveness

Thus we come to the question of effectiveness, because the question is whether with such cumbersome organizations and bureaucratic relationships real-time intelligence has not become an illusion to begin with. In any case, the American approach of connecting the dots seems to have suffered from it.

Furthermore, western intelligence and security services have advanced little further by stretching boundaries and standards. The use of interrogation techniques that involve torture, is, as long known,[17] not as effective as claimed, said a CIA man with experience in Pakistan in 2002, John Kiriakou: people are prepared to say anything to stop the torturing:

[15] Bush said this in March 2008, when he vetoed a bill of the Amerikaanse Congres, which would have resulted in bringing the CIA's interrogation techniques back within acceptable limits, Perry, *Partly Cloudy*, p. 225.

[16] Title 18, section 2340A of the American Penal Code See also Perry, *Partly Cloudy*, p. 207. For an overview of those techniques see e.g. Kiriakou, *Spy*, pp. 135-139. For their consequences see: Ph. Sands, *Torture Team. Deception, Cruelty and the Compromise of Law*, London etc., 2008.

[17] Vgl. Perry, *Partly Cloudy*, p. 202; H. Katchadourian, "Counter-terrorism: torture and assassination", G. Meggle (ed.), *Ethics of Terrorism & Counter-terrorism*, Frankfurt etc., 2005, p. 191.

"In practice, more empathetic psychological means, whimpy as that may sound, can yield much better results."[18] Using the practice of targeted killing may also make one shoot in his own foot. It carries the risks that it will be reciprocated, may lead to dependency upon the support of dubious regimes, to severe image damage in international opinion, the danger of misjudgements and the risk that it will increase the number of potential adversaries rather than reduce it.[19] The use of ethically dubious methods has also led to demoralization of intelligence personnel and the appearance of whistleblowers.[20]

Conclusion

In conclusion, I note that an ethical framework for intelligence personnel is of limited value if not also an ethical code applies to the heads of state and ministers responsible for the intelligence and security services.

Secondly, I note that the field of intelligence and security is very much in a state of flux and everything seems to be connected with everything, an inherent feature of the (post) modern, globalized world. Some may be inclined to consider the extent to which the intelligence business is integrated into society as an element of recognition or fruition of the intelligence business, the ultimate emancipation of a "dirty profession". However, from the perspective of an ethical operation of intelligence and security services in countries with a constitutional and democratic character I am inclined to speak of a degeneration. Consequently, I would plead that the intelligence and security services should emphasize their autonomous and specific disciplinary nature much stronger than they do now. Restoring branche specifity will improve standards and facilitate their enforcement. Thus ethics will prove to be a part of professionalism and as outlined above, the application of professional ethics will not at all thwart goal attainment by the intelligence community.

---

[18] Kiriakou, *Spy*, p. 130. See also *ibidem*, p. 132.

[19] E. Patterson and T. Casale, "Targeting Terror: The Ethical and Practical Implications of Targeted Killing", *International Journal of Intelligence and Counterintelligence*, vol. 18, isue 4 (2005), pp. 647-649. Zie ook G. Blum and Ph. Heymann, "Law and Policy of Targeted Killings", *Harvard National Security Law*, vol. 1 (27 June 2010), pp. 145-170; S. Shane, M. Mazzetti and R.F. Worth, "Secret Assault on Terrorism Widens on Two Continents", *New York Times*, 14 August 2010.

[20] E.g. Kiriakou, *Spy*, pp. xxi, 140-142, 145.

Precisely because so much is in flux, the individual information officer's personality has to be tested for his integrity prior to appointment,[21] he has to be provided with a rudimentary ethics code, [22] he will then need to be trained in independently weighing up ethical considerations and finally, within the intelligence community, a structural platform should be offered for the presentation of ethical issues. At any rate, the solving of ethical dilemmas should not be left to the individual intelligence officer as this has proved to be a recipe for "confusion, abuse, and cover-up".[23]

*** Editor's note EENeT** (European Expert Network on Terrorist Issues) is an informal network established in 2007, between the EU Member States, bringing together experts on terrorism, officials of Law Enforcement and National Security Agencies, EUROPOL officials, as well as scholars from the academic field dedicated to the study of the terrorist phenomenon and related issues.

A Romanian representative, on behalf of the Romanian Intelligence Service is taking part in the activities organized by this informal structure.

The relations between the Romanian Intelligence Service and the European experts on counter-terrorism from the academic field have been considerably strengthened in the context of the EENeT Annual Meeting (held on the 19th-21st of September 2010, in Brussels) Consequently, the Romanian Intelligence Service is continuously benefiting of their past experience materialized in studies on terrorism. These papers have been made available to us in order to be published by the Romanian Journal of Intelligence Studies.

This is also the case of Bob de Graaff' s presentation held at the aforementioned meeting. Bob de Graaff is a historian, Phd. Professor at Utrecht University (former Professor at Hague – Leiden University, Terrorism and Counter-terrorism Department), specialized in the field of Intelligence and Security.

[21] As an anonymous CIA-employee once said: "This is such a dishonest business that only honest people can be in it." Quote in Perry, *Partly Cloudy*, p. 133.
[22] Vgl. Olsen, *Fair Play*, p. 226; Perry, *Partly Cloudy*, pp. 102-104.
[23] Olsen, *Fair Play*, p. ix. See also *ibidem*, p. 225.

Aspecte etice în activitatea de intelligence din surse deschise

Cristina POSAŞTIUC
Emilia ENESCU
Serviciul Român de Informaţii
e-mail: **ani@sri.ro**

Abstract

The exponential growth of intelligence activities following the September 2001 events, as well as the disagreements on the role of intelligence in the war against terrorism have constantly led to increased interest in the ethical dilemmas confronting experts in the field.

Issues such as kidnappings and the use of interrogation techniques for national security purposes prevail in specialized literary works on the ethics of intelligence activities, published in English.

Keywords: intelligence ethics, open source intelligence, intelligence estimate errors.

Consideraţii generale

În contextul semnalelor insistente ale unor organizaţii internaţionale pentru apărarea drepturilor omului şi ale mass-media cu privire la utilizarea torturii în scopul obţinerii de informaţii de la presupuşi terorişti, Consiliul Europei şi Parlamentul European au lansat apeluri insistente serviciilor secrete de a adopta **reglementări etice**.

În 2005, Adunarea Parlamentară a Consiliului Europei (APCE) a votat o rezoluţie privind stabilirea unui **cod european de etică în domeniul informaţiilor**, care să fie aplicat în toate statele membre[1].

Etica procesului de intelligence – preocupare majoră a agenţiilor de informaţii

O parte semnificativă a procesului de intelligence nu poate fi subiect al observării publice şi există riscul încălcării legislaţiei. Informaţiile cu privire la surse, metode şi operaţii, precum şi cooperarea cu servicii din alte ţări au caracter clasificat chiar şi în cele mai transparente democraţii.

[1] Andregg Michael, *Intelligence Ethic*s, în „Strategic Intelligence", 2007, p. 52.

Secretizarea poate face ca cele mai multe cazuri de incompetență să rămână necunoscute, iar **etica** devine **unul dintre principalele mecanisme de control intern**. Din acest punct de vedere, sunt imperative studierea acesteia şi explorarea modalităților de îmbunătățire a standardelor etice[2].

În lupta împotriva terorismului, serviciile de informații au fost implicate într-o serie de controverse puternic mediatizate, ce au creat o dilemă majoră intelligence-ului în societățile deschise: cum pot să apere societățile democratice, în condițiile în care cea mai mare parte a activității lor este clasificată şi pot apărea situații de încălcare a drepturilor omului, în numele siguranței şi securității naționale[3]?

Clarificări terminologice

Sintagma etica procesului de intelligence este descrisă drept un **oximoron** de către majoritatea autorilor[4], dar este considerată valoroasă în susținerea eforturilor de îmbunătățire a profesionalismului şi controlului serviciilor de informații.

Principalele **paliere de analiză** a eticii procesului de intelligence sunt:

- relația dintre etică şi lege;
- niveluri instituționale şi individuale de responsabilitate etică;
- abordări etice ale procesului de intelligence[5].

Activitățile agențiilor de informații sunt reglementate prin **legi naționale şi internaționale**. Întrucât responsabilii din acest domeniu au de rezolvat sarcini complexe, situații neprevăzute şi de luat decizii dificile, legile nu pot fi proiectate astfel încât să reglementeze orice situație imaginabilă. Una din principalele caracteristici ale activității de intelligence este discreția, care este definită ca „alegere permisă explicit de lege sau care există prin ambiguitatea inerentă legii”[6]. În condițiile ambiguității legislative, etica devine un ghid esențial pentru acțiune. Din acest motiv, legile sunt necesare, dar nu suficiente.

---

[2] Andregg Michael, *Intelligence Ethics*, în „Strategic Intelligence”, 2007.
[3] Ibidem.
[4] Nolte William M., *Ethics and Intelligence*, în „JFQ” / iulie-septembrie 2009, accesibilă prin ndupress.ndu.edu.
[5] Andregg Michael, *Intelligence Ethics*, în „Strategic Intelligence”, 2007.
[6] Gill Peter, *Security Intelligence and Human Rights: illuminating the heart of darkness*, lucrare prezentată la seminarul ESRC cu tema „The New Economy of Security: Policy-Military Security Interfaces”, King’s College London, din 4 Mai 2007, pp. 12-13.

Etica diferă de lege: în timp ce legile sunt întotdeauna formale, etica poate fi informală, funcționând pe baza unor principii care adeseori nu sunt codificate oficial; legile sunt aplicate printr-un sistem juridic, în vreme ce respectarea normelor etice este, de obicei, lăsată la latitudinea grupurilor profesionale sau a organizației.

Din acest punct de vedere, utilitatea codurilor de etică în agențiile de informații poate fi pusă sub semnul întrebării, în special în condițiile **reticenței previzibile a specialiştilor din domeniu la coduri etice rigide**. Structurile de control al activității de informații pot fi însă angrenate în evaluarea adeziunii serviciilor de intelligence şi a personalului acestora la coduri profesionale de etică (dacă acestea există).

În ceea ce priveşte **nivelul de responsabilitate etică**, acesta poate fi individual şi instituțional. Serviciile de informații sunt responsabile de demersul etic al organizației ca întreg şi au obligația de a stabili parametri etici pe care angajații să îi respecte[7].

În intelligence, apare problema **fragmentării responsabilității**, dat fiind că este vorba despre instituții birocratizate şi puternic ierarhizate, în care fiecare are o arie de responsabilitate limitată. Astfel, un lucrător în domeniul analizei de intelligence nu este responsabil pentru felul în care sunt colectate informațiile sau modul în care sunt utilizate acestea.

A doua problemă este legată de „**negarea plauzibilului**" – teză dezvoltată în anii '50, care se referă la crearea unor structuri de putere şi canale informale suficient de slabe pentru a putea fi negate, dacă este necesar[8].

Un exemplu cunoscut este cel în care serviciul francez de informații externe a aruncat în aer un vas al organizației „Greenpeace" în portul Auckland. Ulterior, s-a aflat că preşedintele Francois Mitterand a ordonat această operațiune pentru a opri implicarea previzibilă a navei în blocarea testului nuclear francez în sudul Pacificului. Cu toate acestea, Francois Mitterand a negat ferm orice resposabilitate şi a concediat conducerea serviciului de informații externe, care susținea că a executat ordinul şefului statului[9].

---

[7] Erskine Toni, *„As Rays of Light to the Human Soul?" Moral Agents and Intelligence Gathering*, Intelligence and National Security, 2004, p. 363.

[8] Dacă responsabilii guvernamentali consideră oportun, pot da instrucțiuni controversate serviciilor de informații, pentru a putea nega, ulterior, implicarea executivă, în cazul în care o operațiune eşuează sau este expusă public.

[9] Dyson John, *Sink the Rainbow Warrior! An enquiry into the Greenpeace Affair*, Victor Gollancz, London, 1986.

Literatura de specialitate inventariază **3 abordări ale eticii** în domeniul intelligence-ului: realistă, ce ține cont de consecințe şi deontologică[10].

Conform **abordării realiste**, securitatea națională justifică toate demersurile şi, în consecință, oficialii din domeniul intelligence pot derula orice acțiuni pentru asigurarea securității naționale. Eşecul în obținerea de informații ar echivala cu negarea datoriei morale a unui guvern față de cetățenii săi, întrucât fără informație oportună cu privire la capacitatea şi intențiile potențiale ale unui inamic, nu este posibilă apărarea. Din perspectiva abordării realiste, agenții de informații care au acționat imoral au angrenat toate mijloacele avute la dispoziție pentru apărarea securității naționale[11].

Abordarea ce ține cont de consecințe presupune cântărirea rezultatelor probabile în raport cu mijloacele utilizate, pentru a decide dacă este sau nu etică o anumită acțiune, conform conceptului de ***echilibru etic*** propus de Michael Herman[12]. Activitățile de informații trebuie să fie analizate prin prisma consecințelor lor manifeste. Această abordare poate justifica „aproape orice metodă de colectare de informații", din punctul său de vedere nicio activitate (precum tortura şi uciderile extrajudiciare) nefiind în sine eronate.

O **variantă** a abordării bazate pe consecințe este **teoria „intelligence-ului just"**, pornind de la cea a „războiului just", care recomandă evaluarea etică atât în selectarea țintelor activității de intelligence, cât şi în alegerea metodelor de colectare a informațiilor. Teoreticienii „intelligence-ului just" susțin că, în realizarea acestor evaluări, trebuie să se țină obligatoriu seama de:

- justețea cauzei;
- şansele de succes;
- proporționalitatea mijloacelor angrenate cu rezultatele vizate;
- riscul afectării oamenilor nevinovați;
- nevoia de supervizare a acțiunilor[13].

---

[10] Erskine Toni, *„As Rays of Light to the Human Soul?" Moral Agents and Intelligence Gathering*, Intelligence and National Security, 2004, pp. 364-374.

[11] Pfaff Tony; Tiel Jeffrey, *The Ethics of Espionage*, în „The Journal of Military Ethics 3", 2004.

[12] Herman Michael, *Ethics and Intelligence After September 2001*, în „Intelligence and National Security", 2004.

[13] Gendron, Angela, *Just War, Just Intelligence: An Ethical Framework for Foreign Espionag*e, în „International Journal of Intelligence", 2005; Omand, David, *Ethical Guidelines in Using Secret Intelligence*, în „Cambridge Review of International Affairs", 2006.

Ţinând cont că teoria „intelligence-ului just" a apărut în contextul războiului împotriva terorismului, este probabil ca aceasta să fie puternic influenţată de rolul serviciilor de informaţii în susţinerea operaţiunilor militare şi implicarea lor directă în interogarea aşa-numiţilor combatanţi inamici din zonele de război. Extinderea logicii războiului la procesul de intelligence în timp de pace este potenţial periculoasă, întrucât poate servi la justificarea eludării aspectelor etice.

A treia **abordare** este cea **deontologică**, care susţine că unele activităţi sunt eronate prin ele însele şi nu pot fi motivate, pornind de la teoria „imperativului categoric" a lui Immanuel Kant[14]. Abordarea deontologică este reflectată parţial în Convenţia Internaţională a Drepturilor Civile şi Politice (ICCPR), conform căreia nu este posibilă nicio derogare de la drepturile de bază, inclusiv cel la viaţă. Conform ICCPR, nicio situaţie nu justifică încălcarea acestor drepturi, indiferent dacă se referă la cetăţeni nevinovaţi sau agenţi străini.

Funcţiile majore ale eticii procesului de intelligence

În literatura de specialitate, planificarea, colectarea, analiza şi diseminarea sunt examinate din perspectiva consideraţiilor etice inerente ciclului clasic al procesului de intelligence.

Planificarea

Include decizii luate atât la nivel executiv, cât şi al serviciilor de informaţii, referitoare la: planificarea strategică şi stabilirea priorităţilor; planificarea operaţională şi aprobarea acţiunilor; alegerea ţintelor; politicile de recrutare.

Deciziile luate la acest nivel definesc parametrii pentru etapele următoare ale ciclului de intelligence şi implică o gamă întreagă de probleme etice la nivel instituţional:

- *rolul Guvernului în stabilirea priorităţilor serviciilor de informaţii;*

Guvernele aprobă sau resping operaţiunile propuse pentru a ajunge la rezultatele vizate. Principalele consideraţii etice trebuie să fie protejarea securităţii naţionale şi a cetăţenilor săi, la care se adaugă: obligaţia de a nu exercita presiuni asupra serviciilor să obţină informaţii cu orice preţ, fapt ce ar

[14] Conform căreia actele indivizilor ar trebui considerate acceptabile doar dacă pot fi justificate când sunt universal aplicate.

pune aceste instituții în situația de a ignora considerațiile etice şi / sau de a încălca legile; luarea în considerare a implicațiilor etice ale stabilirii rezultatelor de intelligence dezirabile, înainte de demararea ciclului de intelligence;

o *legitimarea funcțiilor sau sarcinilor care justifică implicarea serviciilor de informații;*

Agențiile de intelligence trebuie să adopte decizii cu privire la zona în care să îşi concentreze resursele şi la grupurile sau persoanele de urmărit pentru colectarea informațiilor. Unii autori consideră că trebuie luată în considerare motivația colectării de informații: în timp ce interesele de securitate națională pot justifica acțiunile de culegere, promovarea intereselor economice naționale nu[15].

Alți autori subliniază legitimitatea țintei, susținând că etica urmăririi anumitor persoane pentru colectarea de probe depinde de poziția celui vizat. Există o tipologie bazată pe nivelul de implicare al persoanelor în „jocul" informațiilor, iar categoriile variază de la cetățeni „inocenți", care nu dețin nicio informație utilă, la cei care sunt conştienți de valoarea datelor pe care le dețin pentru serviciile secrete străine[16].

o *recrutarea şi instruirea agenților care să îndeplinească sarcinile proiectate.*

Literatura de specialitate recomandă aplicarea de teste etice în timpul procesului de recrutare, inclusiv prin angrenarea viitorilor angajați în situații dificile, precum şi o examinare din care să rezulte disponibilitatea acestora de a acționa violent[17].

Colectarea

Cea mai mare parte a lucrărilor privind etica procesului de intelligence se concentrează pe dilemele etice care apar în timpul colectării de informații, analizate în funcție de tipul surselor utilizate: umane – HUMINT, imagistice – IMINT, semnale – SIGNINT şi din surse deschise – OSINT.

---

[15] Quinlan Michael, *Just Intelligence: Prolegomena to an Ethical Theor*y, Centre for Intelligence and International Security Studies Annual Lecture, 2005.
[16] Pfaff, Tony; Tiel, Jeffrey, *The Ethics of Espionage*, în „The Journal of Military Ethics 3", 2004.
[17] Godfrey Drexel, *Ethics and Intelligence*, în „Foreign Affairs", 1978, p. 405.

În procesul de colectare din surse umane (HUMINT), implicarea directă, personală a ofițerilor de caz creează probleme etice reale. În primul rând, situația ofițerilor care nu sunt cine susțin a fi, având o identitate legendată inclusiv față de familie – nume, ocupație şi alte detalii – şi care trebuie susținuți în comportamentul lor conspirativ.

Pe de altă parte, astfel de activități sunt imposibil de realizat în afara cadrului etic, nu doar din motive operaționale, ci şi pentru sănătatea psihică şi chiar morală a ofițerilor[18].

Temele recurente în literatura de specialitate cu privire la etica procesului de colectare de informații din surse umane sunt:

- *utilizarea torturii;*
- *extrădările extraordinare;*
- *problemele etice ce provin din colectarea de informații din surse umane cu ajutorul informatorilor şi participarea agenților la activitățile țintei.*

Colectarea de informații din surse umane pune în pericol ofițerii de intelligence şi, deşi expunerea la anumite niveluri de risc este inevitabilă, agențiile de informații au obligația etică de a lua în considerare pericolul la care este supus personalul. Unii autori consideră că orice **risc** la care sunt supuşi agenții **trebuie să fie proporțional cu beneficiile** care este probabil să fie obținute în urma valorificării informațiilor respective. Este elocvent cazul lui Oleg Penkovsky, ofițer GRU care a furnizat informații Occidentului înainte şi în timpul crizei rachetelor din Cuba, dar care a fost arestat şi executat[19].

Colectarea de informații din surse umane poate conduce la dileme etice dramatice, dar şi cea prin SIGINT şi IMINT presupune unele provocări etice, îndeosebi în ceea ce priveşte **implicațiile intruziunii în viața privată**. Unii autori sugerează că, în acest caz, este necesar un control strict al interceptării comunicațiilor.

În SUA există limite în colectarea prin mijloace tehnice de date referitoare la cetățenii americani sau chiar la anumite categorii de străini (personalul ONU), iar Agenția Națională Geospațială (NGA) a fost criticată pentru sprijinul acordat la întocmirea hărții consecințelor Uraganului Katrina[20].

---

[18] Nolte William M., *Ethics and Intelligence*, în „JFQ" / iulie – septembrie 2009, accesibilă prin ndupress.ndu.edu.
[19] Ibidem.
[20] Ibidem.

Analiza

Definită ca „proces de transformare a informațiilor fragmentare colectate într-un produs utilizabil de către factorii decidenți”[21], analiza are propriile considerații etice.

Rezultatul analizei de intelligence poate avea un impact profund asupra politicilor guvernamentale, cu implicații majore asupra alocării de fonduri publice, utilizării serviciilor de securitate şi a forțelor armate şi, posibil, asupra elaborării proiectelor legislative. Ca urmare, există conotații etice semnificative asociate analizei de intelligence.

Deşi serviciile de informații şi analiştii din acest domeniu sunt supuşi unor constrângeri de timp şi presiuni politice considerabile, au câteva obligații etice atunci când îşi formulează analizele.

Politizarea, ca distorsiune a unei analize pentru a se potrivi unei politici dezirabile sau unui rezultat dorit, este considerată principala problemă etică cu care se confruntă analiştii. Adeseori, erorile analitice provin nu din „furnizarea către decidenți a ceea ce doresc să audă”, ci din **preluarea concepțiilor eronate** ale acestora sau din neinformarea lor cu privire la faptul că baza de date din care a fost realizată evaluarea este limitată[22].

Autoritățile din domeniul intelligence au „responsabilitatea morală” de a nu cere un produs exhaustiv sau o certitudine mai mare decât poate fi garantată[23].

La rândul lor, serviciile de informații au obligația etică de a formula concluziile analizelor cu precauție, avertizând asupra posibilelor **erori de estimare**. Aceasta face ca produsul de intelligence să fie utilizat cu precauție de către instituțiile guvernamentale în formularea politicilor.

Comisia Butler din Marea Britanie a evidențiat eşecul serviciilor de informații de a evidenția limitele analizelor privind armele irakiene de distrugere în masă[24].

---

[21] Shulsky Abram; Schmitt, Gary, *Silent Warfare, Understanding the World of Intelligence*, Dulles, VA, 2002, pp. 11-18.

[22] Nolte William M., *Ethics and Intelligence*, în „JFQ” / iulie – septembrie 2009, accesibilă prin ndupress.ndu.edu.

[23] Quinlan Michael, *Just Intelligence: Prolegomena to an Ethical Theor*y, în „Centre for Intelligence and International Security Studies Annual Lecture”, 2005.

[24] Lord Butler, *Review of Intelligence on Weapons of Mass Destruction*, London, Stationery Office, 2004, p. 82.

Analistul care, în anii '90, a redactat capitolul din National Intelligence Estimate (NIE) în care a anticipat prăbuşirea fostei Uniuni Sovietice, luând în calcul renunțarea Partidului Comunist la monopolul politic pe care îl exercita, trebuie să fi suportat o presiune puternică pentru a găsi dovezi care să susțină o asemenea idee[25].

Analiştii se confruntă cu probleme etice în ceea ce priveşte relaționarea cu procesul de colectare. Cei mai mulți lucrează pentru instituții care au ca principală sarcină colectarea, fie din surse umane, fie tehnice. Având ca referință un singur tip de surse, analiştii NSA şi cei ai NGA procesează rezultatele activității de colectare de semnale sau imagini. Aceştia au **responsabilitatea etică de a realiza analiza multisursă**, **conexând informațiile obținute de propria agenție sau de alta cu cele din surse deschise**[26].

Revoluția tehnologiei informației înclină balanța în favoarea surselor deschise. Cetățenii pot vedea imagini din satelit ale unor locuri la care doar elitele aveau acces cu doar o generație în urmă, iar specialiştii serviciilor de informații pot urmări comunicațiile din întreaga lume şi obține profiluri specifice ale aproape oricui – mai dificil ale teroriştilor, care evită, de obicei, mijloacele de comunicare[27].

Diseminarea

Există o serie de aspecte etice asociate diseminării informației:

- *transmiterea adevărului factorilor decidenți;*

Singura normă care ar trebui să se aplice activității de intelligence este prezentarea rezultatelor analizelor în integralitatea lor, pornind de la premisa că informarea corectă a factorilor decidenți este scopul activității de intelligence.

- *diseminarea neautorizată a produselor de intelligence;*

Deşi majoritatea acțiunilor de diseminare de produse de intelligence este autorizată, au existat întotdeauna cazuri de transmitere neautorizată de informații.

---

[25] Nolte William M., *Ethics and Intelligence*, în „JFQ" / iulie – septembrie 2009, accesibilă prin ndupress.ndu.edu.
[26] Ibidem.
[27] Andregg Michael, *Ethics and Professional Intelligence*, în „The Oxford Handbook of National Security Intelligence", Oxford University Press Inc, 2010.

Scurgerile de informații sunt ilegale şi nu fac parte în mod clar din ciclul de intelligence, reprezentând o **problemă etică majoră**. Diseminarea neautorizată poate consta în furnizarea de informații clasificate oficialilor străini, țintelor sau mass-media.

- *schimbul de informații pe plan național;*

Primul aspect etic derivă din colectarea informațiilor cu privire la indivizi sau grupuri care au fost obținute pentru un anumit scop, dar sunt utilizate de alte agenții pentru alte scopuri, în detrimentul persoanelor respective.

Cei vizați ar putea să nu fie conştienți că au fost supuşi unui proces de culegere de informații sau că acestea au fost transferate altor instituții. Aceştia este puțin probabil să aibă ocazia să conteste veridicitatea informațiilor şi există riscul ca datele transmise altei agenții să fie utilizate pentru şantajarea țintei în vederea obținerii de informații[28].

Un exemplu elocvent este transmiterea de informații către serviciile de imigrare, care ar putea să respingă cererile de vize sau drept de şedere pe teritoriul unei țări pe baza unor astfel de date, adeseori fără ca cei vizați să aibă posibilitatea de a contesta decizia.

- *schimbul de informații pe plan internațional.*

Importanța cooperării în acest domeniu a crescut concomitent cu amenințarea terorismului global. Deşi este un instrument valoros în combaterea amenințărilor transnaționale, schimbul de informații cu agențiile străine este problematic, întrucât acestea **pot să nu respecte aceleaşi standarde legislative sau etice**. Serviciile de informații care furnizează date celor din alte țări sunt parțial responsabile pentru acțiunile desfăşurate în baza acestora.

Specificități ale eticii în domeniul OSINT

Caracteristica definitorie a informațiilor obținute din surse deschise este că nu sunt necesare proceduri legale sau tehnici de colectare clandestine.

Prin intermediul Internetului pot fi obținute date referitoare la persoane, adeseori în schimbul unei taxe. Companii precum „Lexis-Nexis”,

[28] Cazul Ahmed Zauoi, semnalat de http://www.amnesty.org.nz/ (28 august 2007).

„Auto Track", „Accurint" oferă acces la o largă varietate de baze de date publice, facilitând obținerea de informații deosebit de detaliate cu privire la diferite persoane vizate. Astfel, pot fi obținute multe detalii care, odată analizate, pot contribui la realizarea profilurilor unor suspecți, utile în cadrul investigațiilor. În plus, bibliotecile universităților oferă, gratuit sau contra cost, o serie de instrumente de cercetare[29].

Culegerea de date din surse deschise referitoare la persoane suspectate de implicare în acțiuni de criminalitate organizată ori terorism nu presupune încălcarea drepturilor acestora. De exemplu, monitorizarea site-urilor propagandistice islamist-radicale ori ale organizațiilor extremiste pentru obținerea de informații referitoare la inițiatori, ținte ale mesajelor ori acțiuni planificate nu încalcă drepturile omului.

Pentru a putea fi incluse într-un dosar, literatura de specialitate recomandă ca informațiile provenite din surse deschise privind anumite persoane să se refere la o încălcare a legii, nefiind relevantă sursa acesteia[30].

Aceasta întrucât, ulterior, ar putea apărea probleme în a justifica păstrarea informațiilor despre persoana suspectată, în cazul în care legătura dintre aceasta şi o grupare teroristă sau extremistă nu poate fi probată în urma coroborării datelor provenite din surse diferite.

Provocări în studierea eticii în domeniul intelligence

Ca urmare a caracterului secret al activității, este dificilă înțelegerea detaliată a activităților specifice serviciilor de informații. Adeseori, se spune că doar eşecurile ajung să fie cunoscute şi că, prin urmare, nu putem avea o imagine completă a unei operații de succes.

Principala barieră la studierea eticii în domeniul intelligence este **lipsa de informații disponibile publicului cu privire la standardele etice în intelligence**. Codurile oficiale după care acționează specialiştii sunt rareori făcute publice, fapt ce face ca orice analiză comparativă a acestora să fie practic imposibil de realizat[31].

[29] Carter David el et al., *Law Enforcement Intelligence*, School of Criminal Justice, Michigan State University, 2004.
[30] Ibidem.
[31] Andregg Michael, *Intelligence Ethics*, în „Strategic Intelligence", 2007.

Literatura de specialitate indexează două excepții: **Codul CIA** din 1982 şi **Codul Africii de Sud** pentru angajații din domeniul informațiilor („White Paper on Intelligence", Pretoria, 1994)[32].

Conform „Washington Post", regulile de angajare în domeniul operațiuni speciale sub acoperire în **Israel** sunt foarte explicite. Colonelul Daniel Reisner, fost colonel în forțele de apărare israeliene, în perioada 1995-2004, a stabilit 6 condiții ce trebuie întrunite concomitent pentru ca o operațiune antiteroristă să fie considerată etică şi care au fost adoptate oficial:

- arestarea trebuie să fie imposibilă;
- este necesară aprobare la nivel înalt pentru fiecare acțiune;
- pot fi vizate exclusiv ținte combatante;
- civilii să fie cât mai puțin afectați;
- operațiunile sunt permise doar în zonele aflate în afara controlului israelian;
- amenințarea să fie serioasă.

În viziunea fostului oficial israelian, asemenea operațiuni nu pot fi considerate pedepse sau răzbunări, ci au exclusiv rol de auto-apărare şi intimidare[33].

De asemenea, Israelul a stabilit coduri specifice referitoare la *cât de multă presiune fizică* poate fi exercitată asupra suspecților în diferite situații. Amos Guiora, ofițer pe profil juridic în cadrul forțelor israeliene de apărare, a precizat că cea mai gravă dilemă morală pe care a întâmpinat-o a fost autorizarea *uciderilor țintite* (cum sunt denumite oficial asasinatele autorizate) şi potențialul ridicat al acestora de a provoca victime în rândul celor nevinovați[34].

David Omand[35] a recomandat **comunității britanice de intelligence** aplicarea următoarelor principii de bază care să ghideze proiectarea şi dezvoltarea capacităților de intelligence:

- motivație sustenabilă;
- integritatea motivelor;
- proporționalitatea metodelor utilizate;

[32] Disponibil pe site-ul http://ethics.iit.edu/codes/coe/us.gov.cia.conduct.html.
[33] Carew Tom, *Law, Ethics, Intelligence*, accesat pe http://www.globalpolitician.com/26255-israel (iunie 2010).
[34] Andregg Michael, *Ethics and Professional Intelligence*, în „The Oxford Handbook of National Security Intelligence", Oxford University Press Inc., 2010.
[35] ***, *Ethical Guidelines in Using Secret Intelligence for Public Security*, în „Cambridge Review of International Affairs", nr. 4, 2006.

- autorizarea operațiunilor;
- perspective rezonabile de succes;
- utilizarea surselor secrete ca ultimă opțiune.

Nu toți autorii sunt însă de acord că publicarea codurilor de etică în domeniul informațiilor este de dorit, argumentând că un astfel de demers poate compromite metodele utilizate[36].

Unii responsabili din domeniul intelligence privesc cu reticență şi chiar cu dispreț fățiș problemele de etică. Un fost oficial britanic consideră etica „un obstacol", apreciind că împovărarea cu reguli suplimentare în activitatea de intelligence ar putea inhiba funcționarea eficientă a procesului şi ar pune, astfel, în pericol securitatea națională.

Din fericire, există profesionişti care sunt de părere că etica reprezintă un ghid valoros pentru acțiune, care **ar putea consolida încrederea opiniei publice în serviciile de informații**. Fostul director al CIA, amiralul Stansfield Turner, a opinat că „există un singur test pentru etica activităților de intelligence din surse umane – dacă cei care le aprobă consideră că îşi pot argumenta acțiunile în fața opiniei publice, în cazul în care acestea devin cunoscute"[37].

Bibliografie

1. Andregg, Michael, *Intelligence Ethics*, în „Strategic Intelligence", 2007.
2. Andregg, Michael, *Ethics and Professional Intelligence*, în „The Oxford Handbook of National Security Intelligence", Oxford University Press Inc., 2010.
3. Butler, Lord, *Review of Intelligence on Weapons of Mass Destruction*, London, Stationery Office Bellamy, 2004, Alex, *No pain, no gain? Torture and ethics in the war on terror*, în „International Affairs", 2006.
4. Carter, David et al., *Law Enforcement Intelligence*, School of Criminal Justice, Michigan State University, 2004.
5. Carew, Tom, *Law, Ethics, Intelligence*, disponibil la http://www. globalpolitician.com/26255-israel (02.03.2010), 2010.
6. Dyson, John, *Sink the Rainbow Warrior! An enquiry into the Greenpeace Affair*, Victor Gollancz, London, 1986.

[36] Andregg Michael, *Intelligence Ethics*, în „Strategic Intelligence", 2007.
[37] Quinlan Michael, *Just Intelligence: Prolegomena to an Ethical Theory*, Centre for Intelligence and International Security Studies Annual Lecture, 2005.

7. Erskine, Toni, *„As Rays of Light to the Human Soul?" Moral Agents and Intelligence Gathering*, Intelligence and National Security, 2004.

8. Gendron, Angela, *Just War, Just Intelligence: An Ethical Framework for Foreign Espionage*, în „International Journal of Intelligence", 2005.

9. Godfrey, Drexel, *Ethics and Intelligence*, în „Foreign Affairs", 1978.

10. Herman, Michael, *Ethics and Intelligence After September 2001*, în „Intelligence and National Security", 2004.

11. Nolte, William M., *Ethics and Intelligence*, în „JFQ" / iulie – septembrie 2009, disponibilă la ndupress.ndu.edu, iunie 2010.

12. Pfaff, Tony; Tiel, Jeffrey, *The Ethics of Espionage*, în „The Journal of Military Ethics 3", 2004.

13. Shulsky, Abram; Schmitt, Gary, *Silent Warfare, Understanding the World of Intelligence*, Dulles, VA, 2002.

14. Quinlan, Michael, *Just Intelligence: Prolegomena to an Ethical Theory*, Centre for Intelligence and International Security Studies Annual Lecture, 2005.

15. ***, *Ethical Guidelines in Using Secret Intelligence for Public Security*, în „Cambridge Review of International Affairs", nr. 4, 2006.

16. Gill, Peter, *Security Intelligence and Human Rights: illuminating the heart of darknes*s, prezentată la seminarul cu tema „The New Economy of Security: Policy-Military Security Interfaces", King's College London, 2007.

17. http://www.amnesty.org.nz/, iunie 2010.

18. http://ethics.iit.edu/codes/coe/us.gov.cia.conduct.html, iunie 2010.

19. http://intelligence-ethics.org/, iunie 2010.

20. https://www.cia.gov/library, iunie 2010.

Rețelele sociale online din perspectiva securității

Laurențiu MIHĂILESCU
Tudor RAȚ
Serviciul Român de Informații
e-mail: **ani@sri.ro**

Abstract

Social Networking Services provide both advantages and disadvantages for individual users and the Intelligence Community alike.

While individuals can develop vast networks of friends and acquaintances, they must be aware that these new means of communication bring along a threat to their security.

Social networks' ubiquity nowadays offers an impressive number of new domains of interest for intelligence agencies, but, as with any „uncharted territory", they come with great security issues, digital espionage being just one of them.

Keywords: social network services, captive audience, web 3.0.

1. Expansiunea SNS

În ultimii ani rețelele sociale online („social networking services", SNS) au devenit omniprezente. Au existat chiar voci care au afirmat că relaționarea prin intermediul site-urilor de socializare reprezintă modul în care s-a ajuns să se comunice predominant în secolul al XXI-lea.

Posibilitatea de a publica şi a aduna informații (legate de interese, activități sau opinii ale apropiaților, cunoscuților) a reprezentat încă de la început un factor major în succesul Internetului, însă acesta a devenit abia în anul 2003 un spațiu activ de socializare pentru majoritatea utilizatorilor[1].

Rețele sociale online implică adesea organizarea în grupuri a unor indivizi sau organizații. În timp ce numeroase rețele sunt comunități legate de un interes comun principal (precum „Reno.ro", „Animale.ro"), există şi site-uri cu un orizont general de socializare, de genul „MySpace" sau

[1] Mika Peter „Flink: Semantic web technology for the extraction and analysis of social networks", Journal of Web Semantics, vol. 3, pp. 211-223, octombrie 2005.

„Facebook", care nu se concentrează pe un anumit interes, numite uneori „tradiționale" şi care sunt deschise tuturor internauților.

Cele mai multe rețele sociale online solicită ca ambii utilizatori să confirme că sunt prieteni, înainte ca între ei să fie creată o legătură. Alte rețele au o secțiune, numită în general „Favorit", „Fan" sau „Interesat" care nu necesită aprobarea celuilalt utilizator, însă unele SNS folosesc tot termenul de „Prieten", ceea ce poate duce la confuzii, deoarece legătura nu înseamnă în mod neapărat prietenie în sensul clasic, iar motivele pentru care oamenii intră în contact pot fi foarte variate.

Dincolo de profiluri, prieteni, comentarii şi mesaje private, rețelele sociale online variază foarte mult în funcție de aplicațiile pe care le utilizează şi utilizatorii cărora li se adresează[2]. Unele dintre ele permit „sharing"-ul de fotografii sau filmulețe, altele găzduiesc bloguri şi tehnologii pentru transmiterea de mesaje instant. Multe rețele sociale online vizează persoane din anumite regiuni geografice sau anumite grupuri lingvistice, deşi aceasta nu determină întotdeauna componența rețelei.

> De exemplu, „Orkut" a fost lansat în SUA cu o interfață doar în limbă engleză, însă brazilienii vorbitori de portugheză au devenit repede grupul dominant de utilizatori[3].

Avantaje

În condițiile în care relaționarea cu alte persoane avea loc în mod tradițional la locul de muncă, în instituții de învățământ sau în locuri foarte frecventate, comunicarea pe platformele de socializare este mult mai populară, milioane de oameni căutând să cunoască noi persoane, să adune şi să împărtăşească impresii, gânduri, informații pe diverse teme, să discute despre interese comune, să dezvolte alianțe personale şi profesionale, să găsească locuri de muncă sau să stabilească eventuale contacte de afaceri.

Punctul central al site-urilor de socializare este reprezentat de profilurile personale ale utilizatorilor, un loc în care aceştia îşi exprimă sentimentele şi gândurile, postează fotografii şi se laudă cu rețeaua lor de prieteni. Cele mai populare rețele sociale pun un accent deosebit pe profilul

---

[2] Boyd Danah şi Ellison Nicole „Social Network Sites: Definition, History, and Scholarship", URL: http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html, 2007.

[3] Kopytoff Verne „Google's Orkut puzzles experts. San Francisco Chronicle" *URL:* www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2004/11/29/2004/BUGU9A0BH441.DTL, 2004.

personal, făcându-l uşor de folosit, dar capabil în acelaşi timp să reflecte personalitatea acestuia.

Dezavantaje

Deşi reţelele sociale online au făcut să apară noi forme de interacţiune între utilizatori, problemele în materie de intimitate şi securitate devin tot mai mediatizate, ajungând în atenţia tuturor celor interesaţi de acest fenomen.

Implicaţiile în materie de intimitate depind în general de gradul în care pot fi identificate informaţiile postate de utilizator, de posibilii beneficiari şi de modul în care pot fi folosite. Deşi cele mai multe reţele sociale nu expun în mod deschis identitatea utilizatorilor, ele furnizează suficiente date pentru identificarea profilurilor. Acest lucru se poate realiza, de exemplu, prin recunoaşterea fizionomiilor[4] sau ca urmare a faptului că adesea utilizatorii folosesc aceeaşi fotografie sau unele similare pe site-uri diferite. De asemenea, identificarea profilurilor este posibilă cu ajutorul unor date demografice sau a unor caracteristici care se dovedesc unice sau rare. Un profil anonim sau pseudonim poate fi identificat fie pe baza unor cunoştinţe anterioare despre caracteristicile şi trăsăturile acestuia, fie prin deducerea unora necunoscute anterior.

Chiar şi în aceste condiţii, administratorii site-urilor de socializare încurajează împărtăşirea publică a informaţiilor personale şi stochează date pe care apoi le vând unor terţi interesaţi de publicitate. Nu e de mirare: aceste grupuri de oameni cu interese comune, profiluri psihologice similare şi trăsături împărtăşite constituie o resursă de marketing formidabilă.

Cele mai cunoscute pericole legate de relaţionarea online sunt „prădătorii virtuali" (indivizi care pretind că sunt altceva decât sunt în realitate), furturile de date, viruşii, în condiţiile în care foarte multe persoane sunt dispuse să facă publice date cu caracter personal, iar, uneori, simple informaţii despre locul şi data naşterii unei persoane pot fi exploatate în scopuri ilicite.

În ultimii ani, s-a remarcat un nou pericol: adicţia psihologică pe care aceste reţele de socializare o pot genera. Programele software de tip jocuri (în special „Farmville"), chestionare şi alte aplicaţii menite să facă

[4] Gross R., „Re-identifying facial images. Tehnical Report", URL: http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf, 2005.

din utilizatori un „public captiv" sunt omniprezente pe aceste site-uri. Este şi uşor de înțeles de ce: conform unor statistici oferite de „Facebook"[5], în fiecare zi, utilizatorii petrec cumulativ 3 miliarde de minute relaționând cu prietenii, comentând status-uri de activitate sau jucând diverse jocuri.

Un nivel şi mai ridicat de dependență îl pot provoca noile tipuri de rețele sociale apărute, cu un grad înalt de imersiune, precum „Second Life", „World of Warcraft" sau „eRepublik". Aceste platforme care integrează rețele sociale, jocuri de tip multiplayer, blog-uri sau activități jurnalistice şi chiar activități economice, reprezintă o nouă etapă a relaționării umane.

Țări precum Republica Maldive, Suedia, Serbia, Estonia, Columbia, Macedonia, Filipine, Israel şi Albania şi-au deschis ambasade şi centre culturale sau organizații de promovare turistică în „Second Life". Astfel, natura relațiilor diplomatice se schimbă profund, vechile şi complexele reguli şi uzanțe politice nemaigăsindu-şi aplicabilitatea.

Nu doar diplomația capătă noi nuanțe în mediile virtuale, însăşi relaționarea şi agregarea umană se schimbă. Oraşele din „Second Life" se construiesc în jurul ideilor şi intereselor, nu în funcție de existența resurselor naturale (ape curgătoare, forme de relief, calitatea pământului arabil etc.). Putem găsi oraşe ale muzicii rock gotice, oraşe ale comunismului sau metropole religioase. Forme vechi de secole de devoțiune religioasă au căpătat un corespondent virtual, un exemplu elocvent în acest sens putând fi pelerinajul virtual la Mecca, la rândul lui, oraş virtual omonim cu cel saudit.

În mediul virtual, chiar şi ordinea puterilor mondiale se realizează după alte coordonate. De exemplu, „eRepublik" le permite utilizatorilor săi să urmărească o carieră politică (se organizează alegeri de diferite forme), să devină soldați virtuali sub „drapelul" țărilor din care fac parte sau să participe la viața economică. „Statele" din „eRepublik" pot purta tratative diplomatice, pot declara război sau încheia alianțe.

Pe „eRepublik", la 03.06.2010, România era angrenată, în războiul israeliano-turc, de partea Israelului. Deşi se poate observa o paralelă a evenimentelor virtuale cu acțiuni care se întâmplă în timp real (forțele israeliene au capturat, la data de 31.05.2010, o flotilă cu scop umanitar care a plecat din Turcia cu destinația Fâşia Gaza), dinamica forțelor militare este mult schimbată din cauza sistemelor de alianțe virtuale. În „eRepublik", țara noastră are alianțe încheiate cu țări de pe diferite continente, cum ar fi Spania, Israel, Australia, Japonia sau Peru. Rapiditatea cu care aceste

[5] „Facebook" (site oficial), URL: http://www.facebook.com/press/info.php?statistics.

configurații de putere se schimbă este impresionantă: alianțele nu se încheie pe ani, ci pe săptămâni sau zile, războaie „mondiale" putând începe şi încheia într-o lună.

Un alt aspect demn de menționat este creşterea influenței şi puterii financiare a administratorilor acestor site-urilor de socializare: revista „Forbes" a estimat valoarea de piață a „Facebook" la 6,5 miliarde de dolari americani[6], mai mult decât Produsul Intern Brut al multor state africane (Togo, Sierra Leone, Rwanda etc.), iar „Google", administratorul platformei de socializare „Orkut", a avut în anul 2009 un profit similar valorii de piață a „Facebook", aproximativ 6,520 miliarde de dolari[7].

Puterea de care se bucură aceşti giganți corporatişti are capacitatea de a influența politici de securitate ale unor mari puteri mondiale. Exemplul Chinei, care a pierdut temporar controlul asupra conținutului accesibil internauților săi, este relevant în acest sens. La 23.03.2010, „Google" a anunțat că-şi va redirecționa serviciile prin filiera Hong Kong[8], după ce în urmă cu 4 ani încheiase un acord cu China prin care se angaja să cenzureze anumite referințe la evenimente sau topicuri de discuție pe care guvernul chinez le consideră sensibile (protestele din Piața Tiananmen, situația uigurilor, Tibet).

Prin această mişcare, pe care multe voci au considerat-o curajoasă, utilizatorii chinezi au putut ocoli restricția impusă de autoritățile chineze, având acces, cel puțin temporar, la întregul conținut disponibil pe *world wide web*.

Acest fenomen este cu atât mai îngrijorător cu cât autoritățile anumitor state, cum ar fi cazul Statelor Unite ale Americii, depind de serviciile „Google" pentru desfăşurarea activităților zilnice. Peste 60% din agențiile guvernamentale ale Statelor Unite folosesc aplicații „Google", în special stocarea datelor pe servere deținute de această companie[9]. Cu alte cuvinte, date deținute de drept de autoritățile americane sunt stocate în locații ce aparțin „Google", sunt depozitate pe soluții hardware asupra cărora „Google" are drept

[6] „Forbes" (site-ul revistei) URL: http://www.forbes.com/forbes/2010/0118/outfront-facebook-shares-internet-friends-like-these.html.

[7] „Google investor relations" (tabel cu venituri realizate) URL: http://investor.google.com/financial/tables.html.

[8] „The Guardian" (publicație, UK) URL: http://www.guardian.co.uk/technology/2010/mar/23/google-china-censorship-hong-kong.

[9] „Philosecurity.org" (blog IT) URL: http://philosecurity.org/2009/12/24/our-google-government.

de proprietate, iar angajaţi „Google" au acces fizic în spaţiile de depozitare a serverelor. Mai mult, „Google" are încheiate parteneriate similare cu alte state, unele cu interese divergente faţă de cele americane. Exemplul Chinei, cu care „Google" a colaborat timp de 4 ani, acceptând termenii cenzurii şi făcând excepţii semnificative de la politica de operare şi codul etic corporatist care definesc compania, face necesară nuanţarea politicii de colaborare cu această companie din ce în ce mai influentă.

Ţinând cont de aceste tendinţe, se poate afirma că mediile de socializare virtuale se îndreaptă spre disoluţia barierei public-privat, majoritatea utilizatorilor găsind acest mod de a interacţiona cu firme şi agenţii de publicitate mai eficient, deoarece se elimină mesajele nedorite sau în neconcordanţă cu interesele fiecăruia. Chiar şi aşa, grupuri de indivizi conduc campanii de conştientizare tot mai vocale cu privire la aspectele etice ale practicilor de încurajare şi uneori chiar de „păcălire" a utilizatorilor prin folosirea unui limbaj ambivalent sau a unor clauze care lasă loc de echivoc.

2. Interesul serviciilor de informaţii

Reţelele sociale online devin din ce în ce mai interesante din perspectiva serviciilor de informaţii, fapt dovedit de programul „Total Information Awareness" al Agenţiei pentru Proiecte de Cercetare Avansată în domeniul Apărării (DARPA) din SUA care efectua cercetări aprofundate în domeniul strategiilor pentru analiza reţelelor sociale pentru a stabili dacă cetăţeni americani prezintă ameninţări asimetrice pentru securitatea naţională. În cadrul acestui program, proiectul „Scalable Social Network Analysis" viza, între altele, dezvoltarea unor tehnici bazate pe analiza reţelelor sociale pentru a stabili caracteristicile unui grup terorist şi pentru a diferenţia aceste grupări de alte tipuri de grupuri sociale[10].

În urma criticilor legate de faptul că dezvoltarea şi desfăşurarea de tehnologii specifice ar putea duce la un sistem de supraveghere în masă, unele proiecte nu au mai primit fonduri, însă altele au continuat să existe sub nume diferite[11].

---

[10] Ethier Jason, „Current research in social network theory" URL*:* http://www.ccs.neu.edu/home/perrolle/archive/Ethier-SocialNetworks.html, 15.03.2009.

[11] „Electronic Frontier Foundation" (site oficial) URL: http://w2.eff.org/Privacy/TIA/20031003_comments.php; Harris, Shane „National Journal" (site oficial) URL: http://nationaljournal.com/about/njweekly/stories/2006/0223nj1.htm.

La nivel internațional, serviciile de informații desfăşoară o serie de activități în domeniul SNS, printre care cele de recrutare, de monitorizare şi de avertizare.

Promovarea imaginii serviciilor de intelligence

Caracteristicile rețelelor de socializare online, în special uşurința diseminării informației, accesul la un grup de indivizi interesați de problematica pe care respectivul serviciu doreşte să o comunice şi interacțiunea lipsită de rigori formale, fac din acestea un mijloc de comunicare extrem de valoros. Informarea publicului devine astfel un proces de dialogare în beneficiul serviciului de informație care foloseşte acest instrument, informația ajungând la receptori netrunchiată, imediat şi într-un mod controlat de emițător.

Deoarece milioane de utilizatori petrec tot mai mult timp pe rețelele sociale, ele par să fi devenit chiar şi parte componentă a strategiilor operaționale ale serviciilor de informații, prin cooptarea internauților în soluționarea unor cazuri de dispariții de persoane, cum este cazul Biroului Federal de Investigații (FBI).

Agenția Centrală de Informații (CIA), Serviciul britanic de informații externe (MI6) sau Serviciul de Informații şi Securitate Australian (ASIO) şi-au creat pagini proprii pe „Facebook", unde au publicat informații privind oportunitățile de angajare[12] sau au demarat diferite acțiuni de promovare în cadrul strategiilor de relaționare cu publicul. Astfel, membrii rețelei sunt invitați să se înregistreze, să citească informațiile privind oportunitățile de angajare, iar serviciile de informații, în calitate de angajatori, pot căuta date despre actualii sau potențialii angajați, formându-şi o imagine despre valorile şi profilul moral al acestora, după modelul unor companii private[13].

Demonstrându-şi racordarea la noile realități ale comunicării publice, Ministerul israelian al Afacerilor Externe a anunțat, la 03.06.2010, organizarea unei conferințe pe site-ul „Facebook", pentru a expune punctul de vedere israelian cu privire la evenimentele din 31.05.2010, când forțele speciale israeliene conduse de „Shayatet 13" (Forțele Speciale Navale) au

[12] „US News" (portal de ştiri, SUA) URL: http://www.usnews.com/news/national/articles/2009/02/05/the-cia-and-nsa-want-you-to-be-their-friend-on-facebook.html.

[13] „Sophos" (site-ul oficial al companiei internaționale omonime) URL: http://www.sophos.com/sophos/docs/eng/papers/sophos-security-threat-report-jan-2010-wpna.pdf.

preluat controlul flotilei care se îndrepta spre Gaza cu scopul declarat de a transporta ajutoare umanitare[14].

Yigal Palmor, purtător de cuvânt al MAE israelian, a precizat că această conferință va fi organizată prin conectarea la grupul virtual „Gaza Flotilla – the world should know the truth" (Flotila pentru Gaza – lumea ar trebui să ştie adevărul). Acest grup, înființat după data de 31.05.2010, a strâns, în mai puțin de 3 zile, 115.000 de membri din întreaga lume.

Un risc demn de luat în calcul cu privire la aceste două conturi menționate este posibilitatea inducerii în eroare a utilizatorilor conectați la acestea de către cei care le administrează. Fotografiile cu siglele instituțiilor, trimiterile la site-uri oficiale şi postarea datelor de contact (adrese, numere de telefon) conferă un aspect „oficial" acestor două conturi.

Monitorizare şi avertizare

În prezent, anumite servicii de informații supraveghează rețelele media de socializare, precum „Facebook", „YouTube", blogurile şi camerele de discuție online, în condițiile în care s-a constatat o proliferare a instrumentelor, tehnologiilor şi metodelor utilizate în desfăşurarea unor activități ilegale online, precum: fraudă, furt de identitate, trafic de ființe umane, comunicații teroriste, atacuri asupra site-urilor guvernamentale etc..

Dacă în urmă cu un deceniu agenții federali americani monitorizau camerele de discuții de pe „AOL" şi „MSN" în vederea identificării persoanelor suspectate de abuzuri sexuale sau comiterea de infracțiuni diverse, în 2009, CIA a decis să preia în observare şi cercetare toate rețelele de socializare, semnând, prin intermediul diviziei sale de investiții, „In-Q-Tel", un „parteneriat strategic" cu compania Visible Technologies, „furnizor de analize social-media şi soluții de interacțiune cu consumatorii"[15]. CIA nu este singurul serviciu de informații care supraveghează rețelele de socializare, alte exemple fiind FBI, NSA, Shin Bet şi Mukhabarat.

Potrivit unui document intern al Departamentului american de Justiție, datat martie 2010, agențiile guvernamentale americane recurg la identități şi profiluri false pe site-urile de socializare pentru a comunica

[14] Site-ul oficial al Ministerului israelian de Externe URL: http://www.mfa.gov.il/MFA/About+the+Ministry/MFA+Spokesman/2010/MFA-web-conference-with-FACEBOOK-group-3-Jun-2010.htm.

[15] „News.ro" (portal de ştiri, România) URL: http://www.news.ro/stire/94178/cia-vede-tot-ce-faceti.html.

cu diverşi suspecţi. Spre exemplificare, FBI, alături de alte servicii de informaţii, a folosit conturi false pe platforma „Facebook" pentru a culege informaţii despre persoane de interes[16].

Acest document, obţinut în urma unui proces privind dreptul la informare, indică faptul că agenţii americani folosesc logarea clandestină pentru a interacţiona cu suspecţii, pentru a le stabili cercul relaţional şi pentru a consulta informaţii private, cum ar fi postări, fotografii şi filmuleţe personale[17]. Totodată, agenţii de investigaţii pot să verifice alibiurile suspecţilor, comparând declaraţiile date Poliţiei cu mesajele trimise din perioada respectivă privind locul unde se aflau.

Totuşi, pentru a accesa date despre persoane de interes, nu este obligatorie asumarea unei identităţi false sau crearea unui cont, informaţiile postate pe reţelele de socializare putând fi consultate de persoane interesate. Fotografiile postate pe reţele sociale reprezentând persoane pozând cu arme, bijuterii sau maşini de lux, pot constitui indicii pentru agenţii de investigaţii în legătură cu desfăşurarea unor activităţi ilegale. În ultima perioadă, a crescut numărul referirilor mediatice în presa occidentală la cazuri de persoane arestate după ce au publicat, în special pe „Facebook", fotografii în care se afişau purtând arme[18].

Un alt exemplu este cel al lui Pasquale Manfredi, persoană importantă în ierarhia Mafiei italiene şi urmărit general în Peninsulă, care a fost capturat datorită faptului că a divulgat informaţii privind locaţia sa pe „Facebook"[19].

Serviciile de informaţii acordă atenţie şi campaniilor de avertizare privind pericolul reprezentat de spionajul digital. Shin Bet[20] le-a solicitat israelienilor să acorde o atenţie deosebită corespondenţei pe această reţea socială online, explicând că au existat tentative din partea unor grupări

---

[16] „USA Today" (publicaţie, SUA) URL: http://content.usatoday.com/communities/ondeadline/post/2010/03/fbi-uses-phony-profiles-on-social-networks-to-gather-information-on-suspects/1.

[17] „On Dead Line" (portal de ştiri şi informaţii, SUA) URL: http://content.usatoday.com/communities/ondeadline/post/2010/03/fbi-uses-phony-profiles-on-social-networks-to-gather-information-on-suspects/1.

[18] „The Sun" (site-ul publicaţiei omonime, UK). URL: //www.thesun.co.uk/sol/.../Facebook-gun-pics-catch-Crew.html.

[19] „USA Today" (publicaţie, SUA) URL: http://content.usatoday.com/communities/ondeadline/post/2010/03/italian-police-track-down-most-wanted-suspect-via-facebook-/1.

[20] „Taragana" (blogul companiei IT, SUA) URL: http://blog.taragana.com/index.php/archive/israel-says-arabs-are-hiring-spies-through-facebook/.

violente de a atrage cetățeni israelieni să se întâlnească față-n față cu membri ai organizațiilor teroriste, „pentru a-i răpi, ucide sau recruta ca spioni”[21].

La rândul lor, Serviciul General de Informații şi Securitate (AIVD)[22] şi Serviciul de Informații Militare şi Securitate (MIVD) din Olanda au demarat o campanie de informare destinată persoanelor care lucrează cu informații clasificate, explicând că oamenii pot fi urmăriți uşor pe Internet, prin intermediul unor rețele precum „Facebook”.

Eradicarea scurgerilor de informații

Un alt aspect care prezintă interes pentru serviciile de informații este reprezentat de datele personale postate pe profilurile de pe rețelele sociale online de indivizi care activează în domenii sensibile.

Un exemplu este cazul unui şef al serviciului MI6, John Sawers, a cărui soție a publicat pe „Facebook” fotografii şi date personale despre membrii familiei, precum şi adresa locuinței cuplului[23].

Totodată, armata SUA[24] şi cea israeliană (Țahal)[25] au impus restricții legate de accesarea acestui gen de rețele de către soldați sau de conținutul postat de militari la profilurile lor în urma unor cazuri în care informații sensibile au ajuns la inamici prin intermediul rețelelor sociale.

Mai mult, Țahal a anunțat înființarea în cadrul serviciilor proprii de securitate, a unei divizii noi cu responsabilități în eradicarea scurgerilor de informații secrete în media, acordând o atenție sporită rețelelor de socializare[26].

Oportunități de culegere de informații pe probleme de securitate

SNS oferă multiple facilități (acces instantaneu la informații şi la un grup de beneficiari extins din arii geografice diferite, schimb rapid de

[21] „Haaretz” (ediția electronică, Israel) URL: http://www.haaretz.com/hasen/spages/1086343.html.

[22] „Radio Netherlands Worldwide” (site-ul oficial al postului de radio, Olanda) URL://www.rnw.n/english/article/digital-spying-rife-dutch-agency-warns.

[23] „CBS News” (site-ul oficial, SUA) URL: http://cbsnews.com/stories/2009/07/05/tech/main5135008.shtml.

[24] „Wired” (ediția electronică, SUA) *URL*: http://www.wired.com/dangerroom/2009/06/army-orders-bases-stop-blocking-twitter-facebook-flickr/.

[25] „BBC News” (site-ul oficial, UK) URL://http://news.bbc.co.uk/2/hi/7343238.stm.

[26] „Anima News” (site-ul oficial al agenției de ştiri, Israel) URL:http://www.animanews.com/eveniment/tiri/691-armata-israelian-i-a-fcut-divizie-de-facebook.html.

informaţii şi posibilitate de coordonare, anonimizare, mobilitate, promovare cu costuri reduse) care pot fi, şi în multe cazuri sunt, exploatate de către indivizi sau structuri interesate şi implicate în activităţi ce intră în contradicţie cu interesele de securitate ale unui stat sau ale comunităţii în ansamblul său. Arhitectura reţelelor sociale şi tipul de comunicare pe care acestea îl presupun sunt compatibile cu noile forme de ameninţări asimetrice conştientizate pe scară largă după evenimentele din 11 septembrie 2001.

O platformă de socializare se poate dovedi vehiculul ideal de comunicare între membrii reţelelor teroriste, mesaje criptate sau steganografiate[27] putând fi schimbate între membri fără nicio legătură fizică. Lipsa necesităţii de a declina identitatea reală în mediul virtual poate conferi un nou nivel de anonimizare a comunicării, în spatele unor conturi cu nume fictive putându-se ascunde indivizi cu intenţii teroriste sau împotriva securităţii unor state.

Cenzură

Forumurile de discuţii, reţelele precum „Twitter" sau blogurile pot fi utilizate în coordonarea unor proteste, a unor acţiuni de stradă, pentru diseminarea unor informaţii care să influenţeze percepţia opiniei publice în legătură cu anumite evenimente sau instituţii sau pentru argumentarea ori criticarea unor decizii socio-politice.

Intitulată „prima revoluţie web 2.0"[28], mişcarea de protest a tinerilor din Chişinău din aprilie 2009 s-a bazat pe platforme precum „Twitter" şi „Facebook" pentru a oferi informaţii în timp real despre evenimentele din capitala Republicii Moldova în condiţiile în care guvernul moldovean impusese o restricţie mediatică pe canelele clasice (radio, televiziune, presă) cu privire la mişcările de protest.

În iunie 2009, Iranul a blocat accesul protestatarilor iranieni la reţelele online de socializare „Twitter", „Facebook", „Flickr" şi „YouTube", folosind un sistem performant de telecomunicaţii[29].

---

[27] Obiectivul steganografiei este de a transmite neobservat un mesaj într-un alt mesaj şi nu de a face neinteligibil conţinutul acestuia altcuiva.

[28] „9am News" (publicaţie online) URL:http://www.9am.ro/stiri-revista-presei/International/126977/Prima-revolutie-web-2-0-Protestele-de-la-Chisinau-LIVE-pe-internet.html.

[29] Idem 19.

Grație acestui sistem, serviciile de informații din Iran au putut controla, cenzura şi chiar modifica mesajele de telefonie mobilă şi mesajele online ale protestatarilor.

Cu ajutorul unei bănci de date a disidenților, serviciile de informații au preluat controlul asupra computerelor şi telefoanelor mobile ale acestora, fiind transmise mesaje false pentru a-i induce în eroare pe cei care comunicau cu disidenții.

3. Web 3.0

Următoarea schimbare de paradigmă în ceea ce priveşte rețelele sociale online este un subiect de interes pentru investitori, utilizatori şi persoane interesate de acest mod de interacțiune umană.

Viitoarele rețele de socializare, versiunea „3.0" a celor existente acum, nu au căpătat o formă, nici măcar la nivel de concept, unanim acceptată. Întrebarea „Cum va arăta SNS 3.0?" este una legitimă, cu atât mai mult cu cât platforme cum ar fi „Facebook" sau „LiveJournal" au integrate o multitudine de aplicații oferite de terți (bloguri, jocuri, materiale video).

Manoj Sharma, consultant pe probleme de strategie organizațională din India, este de părere că rețelele sociale se îndreaptă spre imersiunea totală a utilizatorului în mediul virtual, acesta fiind conectat „cradle-to-grave"[30].

Cu mult înaintea vremii lui, Isaac Asimov a descris, în cel de-al doilea roman al său, „Soarele Gol" (1957), o societate în care oamenii trăiau izolați, la mari distanțe geografice, iar singura lor formă de comunicare se realiza prin intermediul unei interfețe electronice. La nivel psihologic, acele personaje dezvoltaseră fobii cu privire la contactul uman, evitând cu orice preț expunerea în fața altui om în carne şi oase.

Se pare că intuiția autorului de origine rusă s-a apropiat de anumite aspecte ale realității contemporane într-o măsură semnificativă. Un articol scris de Robin-Marie Shepherd şi Robert J. Edelmann indică faptul că ar putea să existe o legătură între folosirea Internetului pentru socializare şi anxietatea socială, anxietatea în general şi depresia utilizatorilor[31].

---

[30] Manoj Sharma (site personal) URL:„http://www.manojsharma.com/keynotes/the-brave-new-world-of-web-3-0-the-next-big-thing-its-integrative-impact-on-the-world-governments-businesses-society-you/".

[31] „Science Direct" (site-ul oficial al revistei) URL:http://www.sciencedirect.com/science?_ob=ArticleURL&_udi=B6V9F-4G94HHC-2&_user=9292790.

4. Concluzii

Deşi există indicii conform cărora reţelele sociale pot avea efecte negative, variind de la aspectele personale până la cele de siguranţă a statului, nu trebuie pierdute din vedere numeroasele oportunităţi pe care acestea le oferă în toate aceste domenii.

Cert este că reţelele sociale online se dovedesc a fi un mediu extrem de interesant, în special din perspectiva securităţii, oferind noi oportunităţi de analiză, dar prezentând şi pericole de natură să vulnerabilizeze entităţi oficiale ale oricărui stat.

Bibliografie

1. Albrechtslund, Anders. „Online Social Networking as Participatory Surveillance", 2008.

2. Backstrom, Lars, Dwork, C. şi Kleinberg, Jon. „Wherefore art thou r3579x? Anonymized social networks, hidden patterns, and structural steganography", 2007.

3. Boyd, Danah şi Ellison, Nicole. „Social Network Sites: Definition, History, and Scholarship", 2007.

4. Ethier, Jason. „Current research in social network theory", 2009.

5. Gross R., „Re-identifying facial images. Tehnical Report", 2005.

6. Mika, Peter. „Flink: Semantic web technology for the extraction and analysis of social networks", Journal of Web Semantics, vol. 3, 2005.

7. Ploderer, Bernd, Howard, Steve şi Thomas, Peter. „Being online, living offline: The influence of social ties over the appropriation of social network sites", 2008.

OSINT – la granița dintre secret şi public

Theodor MITU
Daniela MITU
Serviciul Român de Informații
e-mail: **ani@sri.ro**

Abstract

OSINT lies at the basis of the current transformations experienced by the intelligence sector, being both a rich source of information and technological innovation, responding to agencies' various challenges.

Besides the operational advantages provided, open sources play an important role in public communication, functioning both as a PR platform, encouraging the relations with beneficiaries and academic circles, and a promoter of security culture.

OSINT manages to accomplish the transition from secret sources to open sources, enabling us to talk about a specific symbiosis between classified and public information.

Keywords: open source intelligence, secret vs. open, multiple source analysis

1. Secret *versus* deschis

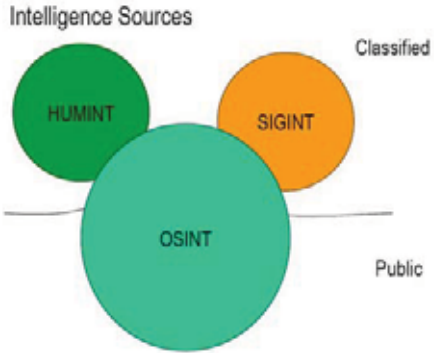


Figura nr. 1

http://langtech.jrc.it/

Natura ambivalentă – *secret* – *public* – a OSINT este reflectată încă din definiția dată în lucrarea „NATO Open Source Intelligence Handbook": „OSINT este informația neclasificată, care a fost descoperită deliberat, selectată, filtrată şi diseminată pentru o audiență specifică în vederea răspunderii la o anumită solicitare. [...] Aplicate într-un mod sistematic, produsele OSINT pot reduce cererile de colectare a informațiilor secrete,

limitând aceste solicitări doar la acele subiecte la care nu se poate oferi un răspuns din surse deschise"[1].

Modul în care se completează reciproc informațiile din surse deschise (OSINT) cu cele din surse secrete (HUMINT) s-a aflat în atenția mai multor specialişti. Subliniind punctele tari şi pe cele slabe ale surselor secrete şi ale celor deschise, autorii fie pledează pentru importanța acordată uneia sau alteia dintre categorii, fie pentru fuziunea informațiilor obținute din acestea.

S-a susținut că HUMINT sunt mai importante decât OSINT, care au doar rolul de a umple *casetele libere* lăsate de primele[2]. Sursele secrete prezintă avantajul de a *pătrunde*, prin metode specifice, acolo unde corespondenții ziarelor nu pot ajunge, exemplul extrem fiind în preajma organizațiilor teroriste.

Alte comentarii favorizează OSINT, care pot face ca serviciile de intelligence să devină mai performante[3]. Se apreciază că jurnaliştii, analiştii din cadrul think tank-urilor pot avea cunoştințe mult mai solide într-un domeniu pe care l-au studiat ani de zile ori prin cunoaşterea unei societăți, a unei culturi etc. Totodată, OSINT oferă informații în zone care, de cele mai multe ori, nu sunt foarte bine acoperite de mijloacele de culegere şi analiză tradiționale – infrastructură, economie, evenimente culturale, demografie.

Robert David Steele, unul dintre cei mai înverşunați promotori ai OSINT, afirmă faptul că intelligence-ul din surse deschise „contextualizează nevoia de informații, oferind matricea în care pot acționa celelalte tipuri de intelligence, orientează acțiunea pentru ca acestea să devină mai eficiente".

Expertul consideră că OSINT „ar trebui să fie fundamentul pentru toate disciplinele de colectare a informațiilor secrete şi (...) ar putea fi

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

[2] Rob Johnston, *Analytic Culture in the US Intelligence Community. An Ethnographic Study*, The Center for the Study of Intelligence, Washington, 2005.

[3] „Comunitatea nordică (Danemarca, Finlanda, Norvegia şi Suedia) a luat locul Canadei [...] în suportul direct al intelligence-ului care susține misiunile de pace ale ONU. Acest lucru se poate datora faptului că autoritățile de la Ottawa sunt mult prea dependente de informațiile din surse secrete furnizate de SUA şi nu au capabilități proprii la nivel global. Un alt motiv ar putea fi acela al combinării, de către nordici, a două percepții: înalta apreciere față de OSINT, respectiv îndelungata practică de participare la operațiuni multinaționale şi centre de intelligence" în Robert David Steele (2010), *Intelligence for Earth, Clarity, Diversity, Integrity, & Sustainability*, Oakton, Earth Intelligence Network, p. 52 disponibil la http://www.phibetaiota.net/?p=19357 [iunie 2010].

punctul de plecare pentru punerea în aplicare a conceptului mai larg de intelligence național sau global, ceea ce unii numesc intelligence colectiv sau creierul lumii”[4].

Şi aceasta pentru că, „în ultimele două decenii de pionierat al OSINT şi până în prezent, în era multinațională, multiinstituțională, multidisciplinară, de analiză şi partajare a informației în mai multe domenii *(Multinational, Multiagency, Multidisciplinary, Multidomain Information-Sharing and Sense-Making – M4IS2)*, factorul uman a devenit tot mai important, deoarece esența secolului al XXI-lea este nu să furi un secret de la o persoană pentru beneficiul unora, ci să te străduieşti să diseminezi informația pe întreaga planetă în beneficiul întregii comunități”[5].

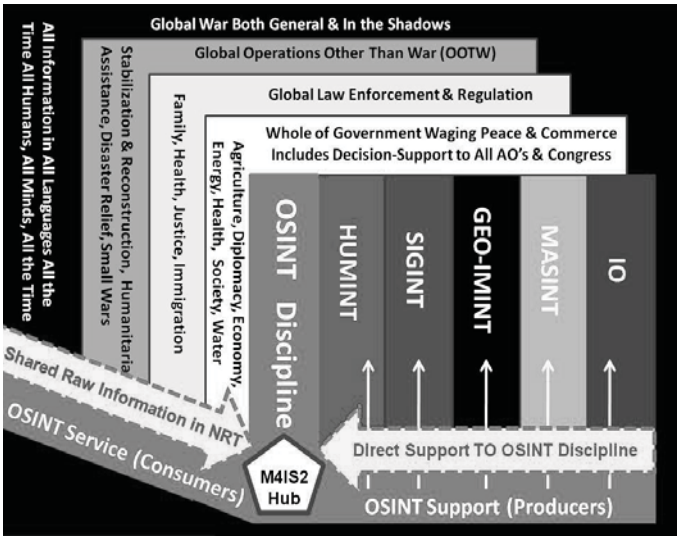


Figura nr. 2

http://www.phibetaiota.net/?p=19

Unii specialişti, precum fostul ofițer CIA Arthur Hulnick, consideră OSINT ca fiind chiar „temelia pe care se construieşte informația secretă”.

[4] Robert David Steele, „Open Source Intelligence”, în Johnson Loch (ed.), *Strategic Intelligence: The Intelligence Cycle*, Westport, Praeger, 2007, p. 97.
[5] Robert David Steele, *Intelligence for Earth, Clarity, Diversity, Integrity, & Sustainability*, Oakton, Earth Intelligence Network, 2010, p. 163, disponibil la http://www.phibetaiota.net/?p=19357 [iunie 2010].

Acesta estimează că produsele obținute din surse deschise contribuie în proporție covârşitoare la baza generală de informații[6].

Cele mai multe opinii merg însă pe ideea potrivit căreia „un amestec de OSINT, HUMINT şi celelalte tipuri de intelligence *(all-source fusion of intelligence)* este vital şi poate produce sinergii importante”[7].

Acesta pare a fi şi punctul de plecare pentru clasificarea datelor şi informațiilor realizată de William J. Lahneman, unul dintre cei mai cunoscuți specialişti în intelligence din spațiul anglo-saxon[8].

Conform acestuia, datele sunt fie secrete (clasificate), fie nesecrete (neclasificate) – *secret versus open*. Orice informație de securitate națională care rezultă din acestea este folosită pentru a fi combinată cu produse informaționale secrete sau nesecrete (care provin din surse deschise). Reies patru tipuri de *fluxuri informaționale*, ce au conținut şi beneficiari diferiți.

Fluxurile *secret-secret* (I) şi *deschis-secret* (II) sunt asociate cu activitatea tradițională de intelligence.

Astfel, în fluxul I informațiile de securitate națională provin din surse secrete sensibile, care ulterior sunt analizate prin intermediul canalelor secrete pentru a fi realizate produse informaționale clasificate.

În cazul celui de al II-lea flux, serviciile de intelligence corelează informațiile, folosind metode şi surse clasificate, astfel produsele rezultate secrete fiind folosite pentru informarea oficialilor guvernamentali.

Potrivit autorului, nevoia concretizării fluxului III – *secret-deschis* – a crescut după atentatele din data de 11 septembrie 2001, când a fost evident faptul că nivelul de clasificare a informațiilor a constituit un obstacol în partajarea acestora între diferitele entități ale statului.

Fluxul III presupune ca informațiile obținute prin metode specifice din surse secrete sensibile să fie declasificate pentru a fi informate autoritățile locale şi cele cu atribuții în aplicarea legii.

---

[6] Stephen C. Mercado, „Sailing the Sea of OSINT in the Information Age”, în *Studies in Intelligence*, vol. 48, nr. 3, 2007.

[7] Peter Gill, Stephen Marrin şi Mark Phytian, *Intelligence Theory. Key Questions and Debates*, London & New York, Routledge, 2009.

[8] William J. Lahneman, „The Need for a New Intelligence Paradigm”, în *International Journal of Intelligence and CounterIntelligence*, vol. 23, nr. 2, 25 februarie 2010, pp. 212-214.

Ultima categorie, cea de-a IV-a, *fluxul deschis-deschis*, creşte, în opinia lui Lahneman, ca importanță, „de vreme ce oficialii guvernamentali monitorizează constant raportările mass-media”[9]. Practic, relatările presei sunt folosite pentru realizarea de avertismente şi evaluări asupra diferitelor riscuri de securitate.

Lahneman deschide un nou curent în discuțiile care privesc exploatarea surselor deschise şi realizarea produselor de intelligence în baza acestora, prin transferul dezbaterilor de la paradigma *secret-deschis* la cea *clasificat-neclasificat*, arătând prin aceasta importanța OSINT.

În recentul *The Oxford Handbook of National Security Intelligence*, Arthur Hulnick apreciază faptul că „deşi produsele OSINT provin din surse publice şi alte tipuri de surse deschise, unele din aceste surse trebuie tratate drept sensibile, iar rezultatul final extras şi analizat clasificat, nu doar pentru a convinge beneficiarul că merită citit”.

Autorul o citează pe Jennifer Sims, expert pe probleme de securitate şi actual director pentru studii de intelligence la Georgetown University, potrivit căreia „intelligence trebuie şi ar trebui să fie clasificat... din cauza înțelegerilor pe care le dobândeşte beneficiarul de la acea sursă”. Unul dintre motivele pentru care OSINT ar trebui să fie clasificat ar fi cel al copyright-ului. Un altul ar fi acela de a proteja descoperirea unui fapt pe care adversarii doresc să-l ascundă[10].

2. Valorile *secrete* ale OSINT

Ca produs informațional independent, analiza OSINT constituie o importantă capabilitate pentru factorii de decizie, prin furnizarea de imagini asupra aspectelor critice ale agendei de securitate, pentru ca aceştia să poată stabili şi, mai ales, aplica politici pe termen lung, întărind capacitatea de prevenire şi de răspuns la eventualele crize.

---

[9] William J. Lahneman, „The Need for a New Intelligence Paradigm”, în *International Journal of Intelligence and CounterIntelligence*, vol. 23, nr. 2, 25 februarie 2010, pp. 212-214.

[10] Arthur S. Hulnick, *The Dilemma of Open Source Intelligence: Is OSINT Really Intelligence?*, în „The Oxford Handbook of National Security Intelligence”, Loch, K. Johnson, Oxford University Press, 2010.

Pe de altă parte, informațiile deținute din surse deschise contribuie la realizarea analizei multisursă, atât prin identificarea unor elemente necesare înțelegerii contextului general cât şi prin facilitarea accesului la anumite tipuri de expertiză din mediile academice.

Figura nr. 3
http://www.einiras.org/

Indiferent că este vorba de OSINT produs independent sau componentă a analizei multisursă, experții subliniază potențialul său de *resursă tactică*, *operațională* şi *strategică*[11].

Fie că este vorba despre oferirea de informații cu privire la activitatea unei organizații teroriste ori că ajută la realizarea de avertizări timpurii şi evaluări strategice, OSINT deține un rol covârşitor în reducerea imprevizibilului, a *incertitudinii* ce caracterizează mediul actual de securitate.

În cazul avertizărilor timpurii, dacă sunt înțelese situațiile care definesc un fenomen şi factorii care le determină, ar trebui să fie uşor de identificat oportunitățile pentru a sesiza din timp problemele şi a îndrepta lucrurile în direcția dorită[12].

---

[11] Chris Pallaris, *Open Source Intelligence (OSINT) and the Future of IR Librarianship*, pentru cea de-a 19-a conferință EINIRAS – International Relations and Security Network, Madrid, Spania, 18 septembrie 2009, disponibil la http://www.einiras.org/conf/conferences/documents/CPallaris_EINIRAS09.pdf [iunie 2010].

[12] Thomas Fingar, *Reducing Uncertainty: Intelligence and National Security. Using Intelligence to Anticipate Opportunities and Shape the Future*, lucrare susținută la Stanford University, octombrie 2009.

Cu toate acestea, avertizarea timpurie înseamnă să se *scaneze* informaţia conţinută pentru sesizarea aşa-numitelor semnale pierdute, care nu sunt foarte evidente, pentru a putea fi reperate ameninţările şi riscurile până atunci necunoscute[13].

La rândul lor, evaluările strategice au ca obiectiv identificarea celor mai importante curente şi a modului în care acestea vor interacţiona, astfel încât decidenţii politici să formuleze strategii şi politici pentru a menţine traiectoria pozitivă a evenimentelor.

Evaluările strategice reflectă „eficienţa unui serviciu în slujba naţiunii, aceasta fiind dată de modul său de raportare la actul de guvernare, la obiectivele politice şi strategice ale statului şi societăţii"[14]. Acestea îndeplinesc cel puţin două obiective: adaugă plus valoare informaţiei existente, prezentând factorilor de decizie acele elemente care ajută la realizarea, pe termen lung, a obiectivelor prevăzute în strategia naţională de securitate; contribuie la planificarea strategiei de informaţii şi ajustarea priorităţilor factorilor de decizie[15].

Date fiind numărul mare de variabile şi de jucători, caracterul dinamic al evenimentelor, elaborarea de scenarii în care se pot încadra evenimentele anticipate s-a dovedit în multe dintre situaţii eronată. Întotdeauna există o doză de imprevizibil care poate răsturna şi cele mai bine fundamentate concluzii despre cum va arăta viitorul.

Nicholas Taleb[16], profesor, eseist, statistician, fost om de afaceri, defineşte această notă de imprevizibil prin sintagma *lebăda neagră*. Taleb consideră că trebuie luate în calcul *surprizele strategice* care ar putea răsturna proiecţiile realizate, evenimentele rare ce ar putea avea un impact major şi care se află dincolo de aşteptările noastre.

---

[13] ****OSINT Report 1/2010*, International Relations and Security Network, disponibil la http://intellibriefs.blogspot.com/2010/04/osint-report-12010.html [iunie 2010].

[14] George Cristian Maior, „Intelligence eficient: de la control la cooperare", în *Revista 22*, 23-29.12.2008, disponibil la http://www.sri.ro/upload/Rev22dec2008.pdf [iunie 2010].

[15] William J. Lahneman, Jacques S. Gansler, John D. Steinbruner şi Ernest J. Wilson III, *The Future of Intelligence Analysis*, vol. I, Center for International and Security Studies at Maryland, 2006.

[16] Nicholas Taleb, *Lebăda Neagră: Impactul foarte puţin probabilului*, Bucureşti, Editura Curtea Veche, 2008.

3. Valorile *publice* ale OSINT

Datorită caracterului lor neclasificat, precum şi al produselor rezultate, sursele deschise sunt cele mai indicate pentru *implicarea experţilor din cadrul mediilor academice* în activitatea de analiză pe anumite probleme de securitate, pe de o parte, precum şi pentru dezvoltarea procesului de *outsourcing*, pe de altă parte[17].

Numeroase opinii, lansate inclusiv în spaţiul românesc, pledează pentru ca, printre analiştii de intelligence, să se regăsească experţi din domenii cum ar fi cel economic, religie, sociologie, psihologie etc.

Această idee a fost subliniată şi de William J. Lahneman. Proiectul lansat de acesta şi de echipa de la Universitatea din Maryland prin care se propune valorificarea platformelor colaborative şi a avantajelor OSINT, chiar dacă a fost iniţiat în anul 2006[18], continuă să suscite interes, fiind reluat în anul 2010, într-o prezentare în prestigioasa publicaţie „International Journal of Intelligence and CounterIntelligence”[19].

Pentru a fi eficiente, serviciile de informaţii trebuie să fie capabile să genereze *reţele colaborative* care să ofere produse informaţionale ce necesită analiza interdisciplinară. *Aceste reţele trebuie să integreze OSINT* şi *să conţină experţi atât din sectorul privat, cât şi din structurile de intelligence*. „Această schimbare presupune ca analiştii să partajeze informaţia cu alţi analişti din cadrul organizaţiilor de intelligence, dar şi cu instituţii din afară pentru a produce produse informaţionale de calitate referitoare la probleme complexe”[20].

Contactele cu mediile de experţi din afara structurilor de informaţii le permite ofiţerilor să aibă acces la cunoştinţe ştiinţifice de primă mână, necesare în special în analiza unor ameninţări nonmilitare. Expertiza mediului academic prezintă avantajul unor unghiuri diverse de analiză şi al perspectivelor culturale variate, care ar putea fi valorificate în cadrul unor proiecte comune de analiză, mese rotunde, seminare, conferinţe etc.

---

[17] Hamilton Bean, *Tradecraft versus Science: Intelligence Analysis and Outsourcing Research Institute for European and American Studies*, 2006, disponibil la se2.isn.ch/serviceengine/Files/RESSpecNet [iunie 2010].

[18] William J. Lahneman, Jacques S. Gansler, John D. Steinbruner şi Ernest J. Wilson III, *The Future of Intelligence Analysis. Final Report*, Center for International and Security Studies at Maryland, martie 2006.

[19] William J. Lahneman, „The Need for a New Intelligence Paradigm”, în *International Journal of Intelligence and CounterIntelligence*, vol. 23, nr. 2, 25 februarie 2010.

[20] Ibidem.

Un alt element al dimensiunii publice a OSINT este cel de *outsourcing*, care s-a extins atât pe componenta de colectare, cât şi pe cea de analiză.

Acesta presupune angrenarea în activitatea de intelligence a anumitor think tank-uri şi institute academice de cercetare, care să contribuie cu perspective diverse de abordare, metodologii şi, în general, cu întreaga lor expertiză.

Externalizarea serviciilor în domeniul OSINT către grupuri de cercetare consacrate oferă posibilitatea structurilor de informaţii de a-şi confrunta analizele interne şi hărţile de riscuri proprii cu cele venite din afară.[21]

Pregătirea în exploatarea surselor deschise în mediul universitar este o altă latură a caracterului public al OSINT. Mai multe centre universitare prestigioase (din SUA, Marea Britanie, Canada şi ţările nordice), organizează cursuri de master şi doctorate în domeniul intelligence, unele dintre acestea fiind destinate cu precădere studiului OSINT.

Studiile postuniversitare de acest gen contribuie la crearea unui adevărat spaţiu de recrutare pentru structurile de informaţii[22].

Promovarea culturii de securitate este o altă misiune ce revine structurilor de intelligence, în contextul actual fiind necesar să se depăşească simpla raportare privind activitatea pe care aceste organizaţii o fac publică anual.

Concept care se înscrie pe linia de comunicare publică a serviciilor de informaţii, cultura de securitate se impune tot mai mult în dezbaterile mediilor de intelligence. Este şi unul dintre cele cinci principii pe care se fundamentează transformarea Serviciului Român de Informaţii.

Cultura de securitate presupune participarea întregii societăţi la asigurarea securităţii, prin „promovarea şi consolidarea valorilor democratice, dezvoltarea unei înţelegeri comune a provocărilor şi oportunităţilor în domeniul securităţii naţionale la nivelul statului şi al societăţii”[23].

---

[21] *********OSINT Report 1/2010*, International Relations and Security Network, disponibil la http://intellibriefs.blogspot.com/2010/04/osint-report-1/2010.html [iunie 2010].

[22] Universitatea Henley-Putnam / San Jose, California, SUA, oferă *Bachelor or Master of Science Degree in Intelligence Management* cu tema „Abilităţi avansate de învăţare în Analiza OSINT”, precum şi *Master of Arts in Intelligence Management, Terrorism and Counterterrorism Studies, Management of Personal Protection*, care include un modul de OSINT avansat – http://www.henley-putnam.edu/532-233.html.
La rândul său, King’s College, Londra, Marea Britanie, deţine un centru – International Centre for Security Analysis – implicat în studierea mai multor problematici, printre care şi metodologia de exploatare a surselor deschise – http://www.kcl.ac.uk/schools/sspp/ws/grad/programmes/options/opensource.html.

[23] http://www.sri.ro/upload/viziunea.pdf [iunie 2010].

OSINT, prin caracterul său deschis, este cea mai în măsură sursă de intelligence să ajute la promovarea educației de securitate, deoarece dispune de instrumentele şi de statutul necesar pentru a rezolva această cerință, prin organizarea de evenimente publice care să reliefeze provocările majore ale securității.

O abordare matură în problematica de securitate națională bazată pe comunicare activă are capacitatea de a elimina o parte dintre „frustrările" şi percepțiile eronate din societatea românească asupra instituțiilor de securitate, fiind un bun exercițiu de imagine.

Concluzii

În actualul context geopolitic, să ignori potențialul de valorificare a OSINT reprezintă o imensă vulnerabilitate de securitate, capacitatea surselor deschise de a răspunde, pe toate palierele de informare şi cunoaştere, la nevoile beneficiarilor crescând pe măsura progreselor care se înregistrează în acest domeniu.

Includerea, în activitățile specifice OSINT, a unor reprezentanți din mediile academice este deosebit de importantă, în special datorită expertizei şi informațiilor din noi surse pe care aceştia le dețin.

Strategiile serviciilor de informații ar trebui să prevadă încurajarea mediilor universitare de a-şi extinde curricula în domeniul studiilor de securitate, intelligence şi OSINT.

Nu în ultimul rând, prin intermediul surselor deschise, serviciile de informații pot contribui la promovarea şi dezvoltarea, în rândul societății civile, a valorilor de securitate.

Bibliografie

I. Lucrări de sinteză

1. Gill, Peter; Marrin, Stephen şi Phytian, Mark, *Intelligence Theory. Key Questions and Debates*, London & New York: Routledge, 2009.

2. Lahneman, William J.; Gansler, Jacques S.; Steinbruner, John D. şi Wilson, Ernest J. III, *The Future of Intelligence Analysis. Final Report*, Center for International and Security Studies at Maryland, 2006.

3. Taleb, Nicholas, *Lebăda Neagră: Impactul foarte puțin probabilului*, Bucureşti: Editura Curtea Veche, 2008.

II. Studii, articole, comunicări ştiinţifice

1. Hulnick, S. Arthur, *The Dilemma of Open Source Intelligence: Is OSINT Really Intelligence?*, în „The Oxford Handbook of National Security Intelligence", Loch, K. Johnson, Oxford University Press, 2010.
2. Steele, Robert David, *Open Source Intelligence*, în Johnson Loch (ed.), *Strategic Intelligence: The Intelligence Cycle*, Westport: Praeger, 2007.
3. Mercado, Stephen C., *Sailing the Sea of OSINT in the Information Age*, în *Studies in Intelligence*, vol. 48, nr. 3, 2007.
4. Lahneman,William J., *The Need for a New Intelligence Paradigm*, în *International Journal of Intelligence and CounterIntelligence*, vol. 23, nr. 2, 2010.
5. Fingar, Thomas, *Reducing Uncertainty: Intelligence and National Security. Using Intelligence to Anticipate Opportunities and Shape the Future*, lucrare susţinută la Stanford University, 2009.

III. Surse Internet

1. Bean, Hamilton, *Tradecraft versus Science: Intelligence Analysis and Outsourcing Research Institute for European and American Studies*, disponibil la se2.isn.ch/serviceengine/Files/RESSpecNet [iunie 2010], 2006.
2. Maior, George Cristian, *Intelligence eficient: de la control la cooperare*, în *Revista 22*, 23-29.12.2008, disponibil la http://www.sri.ro/upload/Rev22dec2008.pdf [iunie 2010], 2008.
3. ****OSINT Report 1/2010*, International Relations and Security Network, disponibil la http://intellibriefs.blogspot.com/2010/04/osint-report-12010.html [iunie 2010].
4. Pallaris, Chris, *Open Source Intelligence (OSINT) and the Future of IR Librarianship*, pentru a 19-a conferinţă EINIRAS – International Relations and Security Network, Madrid, Spania, 18 septembrie 2009, disponibil la http://www.einiras.org/conf/conferences/documents/CPallaris_EINIRAS09.pdf [iunie 2010], 2009.
5. Steele, Robert David, *Intelligence for Earth, Clarity, Diversity, Integrity, & Sustainability*, Oakton: Earth Intelligence Network, disponibil la http://www.phibetaiota.net/?p=19357 [iunie 2010], 2010.
6. http://www.henley-putnam.edu/532-233.html.
7. http://www.kcl.ac.uk/schools/sspp/ws/grad/programmes/options/opensource.html.
8. http://www.oss.net/dynamaster/file_archive/030201/ca5fb66734f540fbb4f8f6ef759b258c/NATO%20OSINT%20Handbook%20v1.2%20-%20Jan%202002.pdf [iunie 2010].
9. http://www.sri.ro/upload/viziunea.pdf [iunie 2010].

Impactul evoluțiilor tehnologice asupra OSINT

Dragoş DINU
Maria Daniela BUNOIU
Serviciul Român de Informații
e-mail: **ani@sri.ro**

Abstract

One of the most effective ways to meet the new security challenges seems to be „taming" the information, by finding new methods to collect, process, and disseminate it. Also, as both the national and international security environment change, intelligence agencies must find ways to dynamically reinvent themselves by learning and adapting.

Keywords: new-technology, competitive, intelligence multidimensional resources, cyber operation.

„Este prima specie de pe această planetă care se autoreproduce şi al cărei părinte este un computer". Acum câteva decenii – ar fi inutil să mai vorbim de secole – o astfel de frază ar fi zguduit lumea ştiinţifică, comunităţile religioase şi culturale şi ar fi condus, probabil, la proteste în masă. În prezentul în perpetuă schimbare, era doar o chestiune de timp până când cineva o va pronunța[1].

Evoluțiile înregistrate în domeniul biologiei, biogeneticii, roboticii, nanotehnologiei au făcut ca noțiuni precum inteligență artificială, date biometrice, energii alternative, armament electromagnetic, capacități nucleare şi încălzire globală să devină subiecte la ordinea zilei.

Dacă sistemele militare ale secolului precedent s-au bazat pe progrese în domeniul fizicii, ingineriei, informaticii şi matematicii, viitorul prezintă o noua gamă de amenințări şi „arme" din ce în ce mai inventive. Tendințele în domeniul informaticii, conectivitatea şi schimbul de informații generează noi oportunități, dar şi riscuri la adresa securității naționale[2].

[1] Autorul este biologul american Craig Venter, care a anunțat, în luna mai a.c., că a creat prima celulă sintetică din lume, bacteria Mycoplasma mycoides.

[2] Unii experți susțin că această tendință contribuie la descentralizare sau la trecerea puterii de la națiuni la indivizi sau grupări, care nu pot fi definite prin granițele politice.

„Societate bazată pe informație”[3], „interdependență”, „globalizare” reprezintă concepte care au marcat profund actualul mediu de securitate, astfel încât este nevoie mereu de perfecționare şi adaptare a strategiilor, tacticilor, managementului. O comunitate de informații trebuie să se reinventeze permanent, într-un mod dinamic, prin învățare continuă şi prin adaptare[4].

Resursele multilaterale pot fi avantajate de creşterea capacității națiunilor şi entităților de a răspunde la amenințările care survin, prin îmbunătățirea schimbului de informații şi prin colaborare strânsă ca răspuns la amenințările manifestate. Totodată, securitatea colectivă poate fi îmbunătățită prin extinderea modalităților şi oportunităților structurilor marginale de a participa în acțiuni sincronizate împotriva amenințărilor comune la adresa ordinii internaționale[5].

Propagarea tehnologiilor de ultimă oră, care ar putea fi folosite în detrimentul intereselor naționale de securitate, nu mai este rezervată națiunilor „de elită”. Rezultatul este sporirea potențialelor amenințări şi creşterea incertitudinii. Deşi oferă beneficii, îmbunătățind răspunsurile globale colective fără costuri semnificative, prin schimbarea modului în care resursele şi capacitățile globale sunt gestionate, progresele tehnologice creează paradigme de securitate problematice.

Dacă în trecut identificarea adversarului era relativ uşoară, în contextul a ceea ce a primit numele de „noua normalitate cibernetică” identificarea reprezintă excepția.

Grupările paramilitare sau insurgente, precum şi alți participanți non-statali şi forțe militare din state în curs de dezvoltare achiziționează din ce în ce mai multă tehnologie şi îşi transformă metodele de acțiune.

---

[3] În revoluția informațională, pentru preocupările strategice au fost considerate relevante, inițial, trei „curente”: utilizarea la scară largă a telefoniei mobile, transparența şi războiul cibernetic.

[4] Andrus D. Calvin, „The Wiki and the Blog: Toward A Complex Adaptive Intelligence Community”, iulie 2005.

[5] Un prim pas în dezvoltarea comunităților este armonizarea legilor interne şi internaționale, precum şi ajungerea la un acord cu privire la activitățile care ar trebui contracarate, cum ar fi terorismul, atacurile cibernetice şi traficul de armament. De asemenea, este necesară o infrastructură de bază (supraveghere şi schimb de informații), care să gestioneze amenințările globale şi să înlocuiască modelele de securitate fragile şi antagonice, limitate la protejarea frontierelor.

Rețeaua „al-Qaida", de exemplu, împreună cu afiliații şi susținătorii săi, foloseşte Internetul pentru a-şi propaga doctrina. Grupul consideră atenția media şi prozelitismul („dawa") ca fiind de o importanță egală sau mai mare decât violența. Materialele sunt diseminate în scopul planificării, instructajului, propagandei şi radicalizării.

Dacă în trecut războiul asimetric era considerat „arma celui mai slab" sub aspectul aplicării metodelor neconvenționale pentru a profita de vulnerabilitățile celui puternic, în actualul mediu, reprezintă „arma celui mai inteligent". Cibernetica este omniprezentă: toată lumea atacă pe toată lumea, astfel încât, „sentințe" precum cea dată de Jim Langevin, membru al Comisiei pentru securitate internă a Camerei Reprezentanților, din Congresul SUA, conform căreia „niciodată nu vom mai asista la un război major fără o importantă componentă cibernetică", s-ar putea dovedi valabile[6].

Cum informațiile sunt elementul esențial în eforturile de asigurare a securității, iar procesul de colectare şi analizare a lor necesită, în prezent, o mobilizare de resurse tehnologice impresionantă şi un efort uman semnificativ, numeroase agenții guvernamentale analizează, în prezent, implicațiile stocării datelor pe termen nedefinit, în scop operativ, legal, administrativ sau istoric. Este necesară, însă, şi elaborarea unei serii de reglementări privind gestionarea şi schimbul de informații clasificate, care să corespundă capacităților tehnologice avansate de colectare, stocare şi analiză a datelor, consolidarea măsurilor de securitate şi protecție fiind, de asemenea, esențială.

Evoluțiile în domeniul tehnologic au condus şi la o reorientare în ceea ce priveşte politica de personal, atât la nivelul organizațiilor private, cât şi la cel al serviciilor de informații. Abilitățile comunicaționale şi utilizarea mediului online ar putea deveni esențiale în procesul de recrutare. O rețea de angajați ce comunică virtual, mult mai rapid, ar conduce la o eficientizare a lucrului în echipă, dar şi a procesului de analiză.

Suplimentarea numărului de specialişti în structurile de securitate, în vederea combaterii criminalității cibernetice, este de asemenea utilă pentru combaterea atacurilor altor state, organizațiilor sau hackerilor, astfel încât instruirea în domeniul IT, dar şi recrutarea de personal pregătit din sectorul privat s-au transformat în necesitate[7].

---

[6] Stephen W. Korns, „Cyber Operations. The New Balance".

[7] „Cyber In-Security. Strenghtening the Federal Cybersecurity Workforce", Booz Allen Hamilton, iulie 2009.

În vederea soluționării problemelor existente, agențiile de informații americane caută în afara structurilor guvernamentale / de specialitate experți IT. Un oficial din cadrul Departamentului de Securitate Internă a estimat că 83% din personalul din cadrul biroului ofițerilor superiori de informații este reprezentat de contractori din mediul privat. Administrația nu trebuie doar să recruteze şi să instruiască mai multe persoane cu calificare în domeniul IT, ci are nevoie efectiv de specialişti capabili să activeze în cadrul structurilor ce asigură securitatea cibernetică.

Comunicare neîngrădită

Blogul, email-ul, rețelele sociale, mesajele text au deschis noi perspective, noi medii în care schimbul de informații poate avea loc, teoretic, neîngrădit. Eliminarea treptată a barierelor „tehnice" nu putea rămâne fără urmări, astfel încât libertatea de exprimare a condus la transformarea acestor medii în ținte sigure pentru ceea ce unii ar numi „cenzură", iar alții – „echilibru", „coordonare" sau „mediere a conținutului"[8].

Creşterea numărului şi tipurilor de surse a condus şi la dezvoltarea conținutului ce trebuie analizat şi validat, astfel încât a apărut o preocupare deosebită pentru găsirea unor metode de a „controla" volumul de informații, fie prin extinderea prerogativelor instituțiilor de stat, fie prin crearea unor baze de date în vederea monitorizării şi stocării informațiilor comunicate prin telefon sau rețele sociale (Marea Britanie, SUA, Suedia).

Dezvoltarea şi menținerea unei rețele de angajați şi contactelor externe, în vederea asigurării de informații despre evoluțiile de piață din cadrul industriei respective au constituit o provocare şi pentru departamentele corporatiste de *competitive intelligence*. Crearea şi menținerea „rețelelor de surse umane" reprezintă o bună practică de intelligence competitiv ce asigură atât achiziționarea de informații unice, nepublicate, cât şi opinii şi comentarii profesioniste în vederea sprijinirii procesului de analiză de intelligence[9]. Introducerea de sisteme colaborative în munca de analiză a facilitat realizarea

[8] Într-un discurs ținut la 21 ianuarie 2010, secretarul american de stat, Hillary Clinton, sublinia: „Considerăm că este critic ca utilizatorilor de Internet să le fie asigurate anumite libertăți de bază. Iar libertatea de exprimare este prima dintre ele. Aceasta nu mai este definită doar de posibilitatea ca cetățenii să meargă în piața publică şi să critice autoritățile fără a se teme de consecințe".

[9] Rețelele de socializare şi aplicațiile web 2.0 oferă practicienilor o multitudine de noi „instrumente" ce pot facilita dezvoltarea de rețele de surse umane atât în interiorul, cât şi în afara „proiectului".

unor rapoarte mai complexe, chiar dacă nu pot fi eliminate toate obstacolele întâmpinate în cadrul muncii în echipă. Cei care iau decizii în funcție de informațiile de care dispun, precum şi cei care îşi duc la îndeplinire misiunile bazându-se pe resursele informaționale trebuie să beneficieze de dreptul de a face schimb de informații, pentru a se asigura că primesc cele mai relevante date.

Ideea[10] a fost extinsă, astfel încât, în mediul actual, extinderea cooperării şi a schimbului de informații între organizații sau națiuni tinde să se transforme în regulă. Un factor de influență l-a constituit, probabil, şi dezvoltarea incredibilă a riscurilor şi amenințărilor. Societatea prezentă este atât de dominată de tot ceea ce înseamnă IT, încât orice descoperire sau evoluție în domeniu conduce rapid la apariția de modalități de decriptare sau de speculare a punctelor slabe.

În consecință, cadrul pentru realizarea schimbului de informații trebuie să includă şi instrumente tehnologice pentru reducerea riscului dezvăluirii neintenționate a informațiilor personale, inclusiv instrumentele de criptare, de asigurare a anonimatului şi managementul drepturilor digitale.

Instrumente noi la riscuri noi

În prezent, se poate spune că tehnologia dictează tendința de dezvoltare pe care domeniul intelligence trebuie să o urmeze.

Îndepărtarea Internetului de computere conectate fizic într-o rețea şi apropierea acestuia de terminalele mobile a determinat o abordare nouă a metodelor de diseminare a informațiilor (achiziționarea de terminale iPhone, iPad, BlackBerry).

Noul Internet se reorientează în viitorul apropiat, adoptând o nouă sintagmă: „Everything, everywhere, always". Implementarea tehnologiilor „web-ului semantic" va elimina confuziile generate de informațiile nestructurate, trasând astfel delimitări clare între Internetul serviciilor, Internetul mobil şi Internetul lucrurilor.

Progresele tehnologiei au condus la apariția unor soluții din ce în ce mai eficiente pentru realizarea unui ciclu complet OSINT, iar această

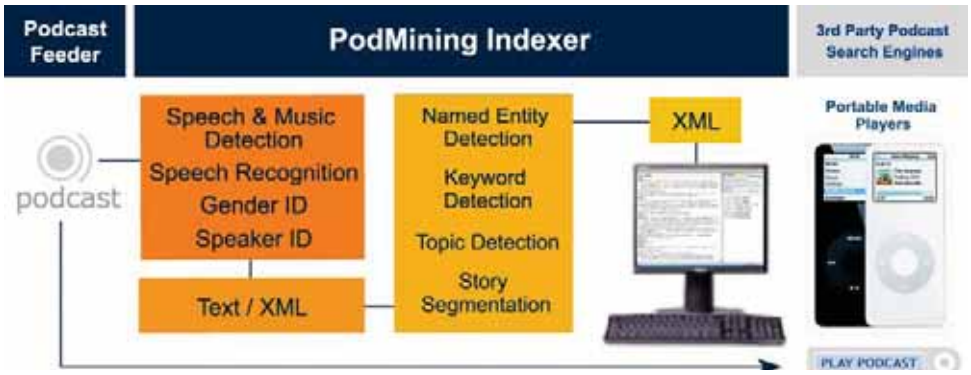
[10] „Revoluția" a început în 2005 cu introducerea mai multor servicii de colaborare: Intellipedia, serviciul mesagerie rapidă în întreaga agenție, o funcție socială similară del.icio.us., o capacitate de căutare şi blog-urile la nivelul organizației. Intellipedia se bazează pe acelaşi tip de programe ca şi Wikipedia, enciclopedia on-line, dar când Intellipedia a fost lansată, comunitatea de intelligence a hotărât că nu va putea fi folosită ca o enciclopedie, ci pentru a deveni un loc pentru colaborarea directă.

dezvoltare forțează organizațiile din domeniul intelligence să se alinieze la ultimele apariții în domeniu.

Pornind de la automatizarea culegerii datelor din diverse surse (audiovideo şi Internet) şi continuând cu procesarea acestora până la diseminarea informațiilor, ciclul OSINT se închide cu feedbackul, uneori dedus din desfăşurarea directă a evenimentelor. Diseminarea cu rapiditate a informațiilor provenite din surse deschise este şi trebuie să fie unul din punctele focale ale procesului OSINT. Varietatea formelor şi viteza de diseminare, precum şi calitatea informațiilor din surse deschise vor face diferența între organizațiile din domeniul intelligence.

Problema cea mai importantă de soluționat în momentul în care există enorme baze de date din surse deschise este descoperirea unui mod de a le „converti" în intelligence.

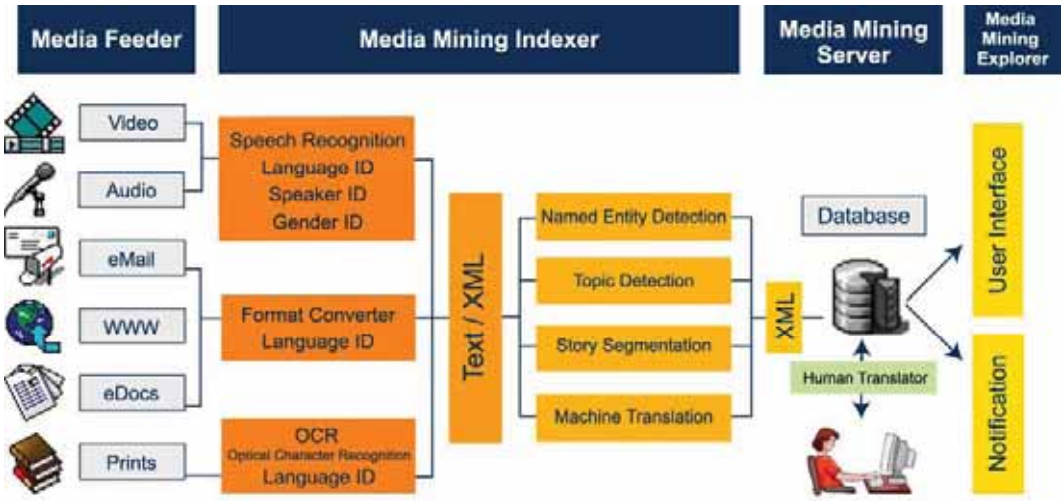
Au apărut, astfel, companii care pun la dispoziție instrumentele necesare monitorizării surselor şi facilitării, colectării şi procesării informațiilor. „Sail Labs" (cu sediul în Viena), de exemplu, este una dintre cele mai importante companii ce activează în domeniul „speech technology" şi oferă servicii destinate eficientizării procesului de colectare a informației (sisteme de *media*, *text / podcast mining*), cu ajutorul cărora date nestructurate din surse multiple (televiziune, radio, podcast-uri, streaming media) sunt procesate în informație structurată, uşor de căutat şi accesibilă. În cadrul acestui proces, conținutul unui fişier video sau audio este transcris, tradus şi indexat în mod automat, în timp real, în funcție de limbă, vorbitor, subiect, nume sau cuvinte-cheie.



Sistem media mining[11]

[11] http://www.sail-technology.com.

Sistem podcast mining[12]



Conținutul informațional poate fi „descoperit" prin eliminarea / depăşirea segmentelor irelevante, urmărirea datelor de interes printr-un sistem de alertă automată şi afişarea sintetizată a surselor în timp real[13].

În ceea ce priveşte traducerea automată aproximativ în timp real, aplicațiile pentru dispozitivele „smart" sunt pe punctul de a deveni general valabile în cel mult trei ani, dat fiind că cercetătorii sunt aproape de a definitiva tehnologia necesară şi de a o aplica sub forma *smart phones*, fiind utilizate, în cadrul procesului, un soft optic pentru recunoaşterea caracterelor şi tehnologia *Google Translate*[14].

Un dispozitiv de comunicare unidirecțional este folosit de câțiva ani în domeniul militar. Phraselator P2, produs de compania „Voxtec", asigură comunicarea a mii de fraze, cu ajutorul unor traduceri înregistrate în prealabil. În cel mult 18 luni, „Voxtec" speră să obțină un dispozitiv de comunicare bidirecțional limitat[15].

---

[12] http://www.sail-technology.com.
[13] Site-ul companiei „Sail Labs", http://www.sail-technology.com.
[14] De asemenea, tehnologii precum „Languageweaver" asigură traduceri aproximativ în timp real din mai multe limbi arabe.
[15] Felix Juhl, Chris Pallaris, Florian Schaurer, *OSINT Report 1/2010 – Technology Trends*, publicat de „International Relations and Security Network".

Progresul impune şi necesitatea găsirii unor noi modalităţi de validare, de exemplu, şi conţinutul generat de utilizator se numără, în prezent, printre „sursele" de interes. Ceea ce era până acum suficient pentru evaluarea acurateţii şi credibilităţii informaţiei-text nu se mai aplică şi altor tipuri de conţinut, mai ales că sursele „scrise" constituie, în prezent, un procentaj minor din masa enormă de informaţii utilizate de analiştii OSINT. Din această perspectivă, a devenit evident faptul că, pentru a depăşi obstacolele, trebuie conştientizat că OSINT nu se limitează la „Internet mining" sau monitorizarea presei, ci solicită de la cei implicaţi abilităţi sociale şi culturale considerabile.

Concluzii

În noul mediu de securitate, schimbul de informaţii interagenţii sau interstatal, precum şi desfăşurarea activităţii într-un sistem colaborativ au devenit extrem de importante în vederea contracarării riscurilor emergente.

Progresele în materie de sisteme media sau comunicare au transformat domeniul intelligence, desfăşurarea activităţii de analiză fiind, practic, imposibilă, în prezent, fără conştientizarea necesităţii alinierii la cele mai noi descoperiri tehnologice.

Bibliografie

1. Ackerman, Robert K., *Intelligence Community Embraces Virtual Collaboration*, publicat pe site-ul Armed Forces Communications and Electronics Association / AFCEA, mai 2009.

2. Andrus, Calvin, *The Wiki and the Blog: Towards a Complex Adaptive Intelligence Community*, iulie 2005.

3. Juhl, Felix, Pallaris, Chris, Schaurer, Florian, *OSINT Report 1/2010 – Technology Trends*, publicat de International Relations and Security Network.

4. Korns, Stephen W., *Cyber Operations. The New Balance*, publicat în revista „Joint Force Quarterly", nr. 54, 2009, elaborată de National Defense University Press.

5. *Cyber In-Security*, publicat de asociaţia „Booz Allen Hamilton", iulie 2009.

6. http://www.sail-technology.com.

Training OSINT

Dan FIFOIU
Serviciul Român de Informații
e-mail: **ani@sri.ro**

Abstract

Training represents an essential step for the development of professional Open Source Intelligence capabilities, enabling the identification of overarching methods, best practices, considerations, challenges and tools available to the OSINT analysts.

This article is meant to provide an overview of the current OSINT training practices landscape, and to reveal the place of specialized open source instruction in the fulfilment of the national security intelligence requirements.

Keywords: training, new-media, open source center, academia.

1. Rolul instruirii în Open Source Intelligence

Accesul tot mai larg şi în timp real la informație este, în prezent, un fapt, şi, în acelaşi timp, o consecință a ceea ce a devenit cunoscut drept „revoluția OSINT": transformarea surselor deschise de informare într-o capabilitate extrem de importantă pentru munca de intelligence şi pentru formularea politicilor în domeniul securității naționale.

Rolul OSINT în cadrul acestora a crescut exponențial în ultimii ani, rezultatul fiind, la nivelul organizațiilor a căror activitate şi dezvoltare depind de gestionarea eficientă a informației, în special serviciile de informații, dezvoltarea segmentelor specializate în exploatarea surselor deschise. Asemenea evoluții au contribuit la transformarea treptată a conceptelor tradiționale de intelligence şi la definirea unor noi cadre de acțiune pentru structurile de siguranță națională.

Urmarea firească a fost acutizarea unei necesități a deschiderii, atât din punctul de vedere al valorificării surselor de informații, cât şi din perspectiva inter-relaționării şi a dezvoltării modelului de lucru colaborativ în domeniul intelligence.

Toți aceşti factori au acționat convergent în configurarea **imperativului adaptării / îmbunătățirii competențelor fiecărui lucrător în intelligence** şi specializarea / perfecționarea simultană a eşantioanelor

de comandă şi planificare, cât mai ales a segmentului de execuţie din cadrul organizaţiilor cu profil OSINT.

Ca proces complex, specializat şi distinct, Open Source Intelligence integrează experienţa umană cu datele obţinute din surse deschise, în scopul producerii de informaţii şi de documente informative relevante pentru deciziile / politicile de siguranţă naţională.

Fie că este vorba de traininguri aplicate, cu durată redusă (de ordinul săptămânilor) sau de programe educative extinse, implementate de / în cooperare cu instituţii academice, pregătirea şi formarea continuă a specialiştilor în OSINT vizează tocmai îmbunătăţirea acestei experienţe, respectiv eficientizarea valorizării tuturor resurselor, în prezent tot mai „generoase" şi mai accesibile, care stau la baza întocmirii de produse de intelligence relevante şi complete.

Emergenţa de noi paradigme ale activităţii de intelligence, focalizate asupra necesităţii impunerii **modelului colaborativ** de lucru, respectiv a **principiului adaptabilităţii** şi **creşterii capacităţii de reacţie**, în timp real, în cazul unor evenimente cu potenţial impact asupra stării de securitate naţională, constituie în acelaşi timp paşi importanţi în evoluţia serviciilor de informaţii, dar şi provocări semnificative din punctul de vedere al pregătirii cadrelor.

Pe un palier distinct, obiectivul instruirii constante este dictat inclusiv de dinamica **transformărilor de ordin tehnologic** care vizează accesul, exploatarea şi gestionarea într-un mod colaborativ, mult mai facil, mai rapid şi mai puţin costisitor a unui volum imens de date.

Evoluţia tehnologiei informaţiei şi a comunicaţiilor a facilitat extinderea Internetului şi trecerea la utilizarea aplicaţiilor Web 2.0, a căror implementare presupune popularizarea, prin intermediul trainingurilor, a formatului de tip wiki şi a cunoştinţelor de management al colaborării intra şi inter-instituţionale.

Cele trei niveluri ale formării unui specialist OSINT – iniţierea, specializarea, perfecţionarea – vizează atingerea unor obiective specifice pliate pe principalele etape ale procesului OSINT, respectiv:

- **Planificarea**;

Rolul trainingurilor OSINT în acest caz este ameliorarea capacităţii unui lucrător de a-şi planifica activitatea în funcţie de criterii precum:

- reperele semnalate de solicitantul produsului informativ în asignarea unei sarcini;
- resursele de care dispune şi sursele la care are acces;
- termenul de transmitere a documentului informativ.

A şti unde să caute o informaţie, cu care analişti specializaţi în problematica respectivă să discute, cum să stabilească succesiunea fazelor întocmirii textului în funcţie de relevanţa diverselor aspecte ale subiectului supus analizei – iată câteva elemente ale activităţii unui lucrător pe care trainingul le teoretizează şi le transpune în proceduri de lucru cu grade diferite de standardizare.

- **Colectarea datelor şi convertirea lor în informaţii**;

Modificarea rapidă a tabloului de surse deschise – în special dezvoltarea aşa-numitelor „new media" – şi transferul celei mai mari părţi a conţinutului surselor clasice în spaţiul virtual, alături de tendinţele de evoluţie a caracteristicilor informaţiilor furnizate, au crescut semnificativ complexitatea competenţelor de căutare şi procesare a acestora.

Cu toate că nu a fost formulată o definiţie general acceptată a „new media", acestea fiind percepute diferit de diversele categorii de utilizatori, ele sunt apreciate ca reprezentând orice produs media digital care este interactiv şi distribuit prin reţele informatice, sau totalitatea textelor, sunetelor, imaginilor şi elementelor grafice prelucrate pe computer şi reunite în baze de date.[1]

Cantitatea enormă de informaţie – numărul imens de website-uri corporate / personale, bloguri, forumuri publice, reţelele sociale care deja contabilizează sute de milioane de conturi –, creşterea exponenţială a conţinutului generat de utilizatori şi diversitatea limbilor / pachetelor în care este livrată informaţia reprezintă provocări care se traduc, din perspectiva nevoii de a le gestiona, în obiective distincte ale instruirii, precum:

- însuşirea de cunoştinţe aprofundate şi specializate de navigare şi exploatare a Internetului;
- dezvoltarea aptitudinilor de identificare a celor mai bune surse de informare;
- dobândirea de competenţe privind validarea surselor;
- metode şi tehnici de căutare a datelor;
- dobândirea de competenţe privind validarea şi organizarea datelor;
- dezvoltarea tehnicilor de procesare.

[1] Dorina Guţu, „New Media", Editura „Tritonic", Bucureşti, 2007.

- **Elaborarea produsului informativ**.

Este etapa care presupune cea mai complexă şi aprofundată pregătire a lucrătorului în intelligence din surse deschise, fapt pentru care trainingurile OSINT axate pe analiza informațiilor sunt cele mai consistente, elaborate şi extinse.

Formarea continuă şi perfecționarea analiştilor de informații din surse deschise este esențială pentru creşterea calității produselor informative pe care le întocmesc, instruirea în acest domeniu având atât rolul de a specializa lucrătorul pe anumite tipuri de analiză (în funcție de necesitățile organizației din care face parte), cât şi de a asigura menținerea sa constantă într-o zonă de cunoaştere a elementelor specifice principalelor activități de intelligence (ştiut fiind faptul că omiterea sau necunoaşterea unor aspecte importante ale situației analizate poate altera utilitatea produsului livrat beneficiarilor).

Complexitatea activității de elaborare a unui document de informare de tip analitic dictează structurarea atentă a trainingurilor în module clar delimitate în funcție de obiectivele propuse.

În prezent, criteriile de formulare a acestor obiective sunt stabilite în principal de:

- **tipul de analiză a informațiilor pentru care sunt instruiți lucrătorii**;

Analiza tactică, strategică, analiza de trend, analiza de risc, analiza predictivă – sunt doar câteva exemple de domenii caracterizate de mijloace şi metodologii proprii de realizare a materialelor în format integrat.

- **spațiile monitorizate**;

Oscilația polilor de instabilitate pe anumite perioade de timp şi în spații diferite determină focalizarea atenției analiştilor OSINT pe respectivele regiuni / state, în vederea informării extinse şi operative a beneficiarilor, respectiv pentru susținerea cât mai eficientă a deciziilor relevante pentru siguranța națională.

- **problematicile pe care le au în competență**.

Tratate separat sau interconectate din perspectiva cauzalității anumitor evoluții, problematici precum terorismul, proliferarea armelor de distrugere în masă, criminalitatea organizată, securitatea economică, conflictele înghețate, extremismul, radicalizarea şi fundamentalismul religios etc. presupun metode specifice de abordare în cuprinsul documentelor analitice, în special din punctul de vedere al încadrării lor în anumite tipuri de analiză şi al resurselor utilizate în elaborarea produselor informative.

2. Modele şi exemple de bune practici

Statele Unite ale Americii

După ce, în iulie 2004, Comisia pentru investigarea atentatelor din 11.09.2001 a recomandat înfiinţarea unei Agenţii de Surse Deschise, Directorul Comunităţii de Intelligence a Statelor Unite ale Americii a anunţat crearea, în noiembrie 2005, a **Open Source Center**, instituţie independentă de stat care, pe lângă elaborarea de produse informative pentru Guvernul american şi alţi beneficiari, are sarcina de a pregăti analişti de intelligence în scopul ameliorării eficienţei exploatării surselor deschise.[2]

Crearea Open Source Center a ranforsat în mod considerabil cadrul instituţional de stat al SUA specializat în intelligence din surse deschise şi a contribuit, prin dezvoltarea unor formule de cooperare cu reprezentanţi ai mediilor academic şi privat, calitatea instruirii specialiştilor OSINT, devenind principalul reper al statelor Uniunii Europene în dezvoltarea unui unei structuri similare[3].

> Cursurile organizate de Open Source Center prin **Open Source Academy**, lider pe segmentul de training OSINT în SUA, se adresează efectivelor din cadrul organismelor comunităţii de intelligence americane şi sunt structurate pe principiul transmiterii cunoaşterii către un public-ţintă segmentat în funcţie de activităţi specifice (Armata, Forţele Aeriene, Marina Militară, Departamentul Apărării, Departamentul Securităţii Naţionale, Agenţia de Informaţii a Apărării, Agenţia Naţională pentru Securitate).[4]

De asemenea, prin înfiinţarea Centrelor de Excelenţă (Intelligence Community Centers of Academic Excellence – ICCAE), Biroul Directorului Comunităţii Naţionale de Intelligence (ODNI, creat la 21 aprilie 2005) a inclus oficial dezvoltarea parteneriatelor cu sectorul privat şi mediul academic în programul de transformare a Comunităţii de Informaţii a SUA.

> Centrele de Excelenţă vizează îndeplinirea obiectivului strategic de formare, la nivel naţional, a fondului de selecţie a cadrelor specializate în intelligence, iar participarea este deschisă tuturor colegiilor şi universităţilor americane acreditate, cu o durată a studiilor de patru ani.

---

[2] www.opensource.gov.

[3] Axel Dyevre (preşedintele CEIS – European Company for Strategic Intelligence), *Intelligence cooperation: the OSINT option*, 28.10.2008, http//:www.europolitics.info/dossiers/defence-security/intelligence-cooperation-the-osint-option-art151325-52.html.

[4] Douglas Peak, *The Open Source Academy helps the intelligence community make the most of open sources*, http://findarticles.com/p/articles/mi_m0IBS/is_4_31/ai_n16419802/.

În perioada 2006-2010, ODNI a inclus în proiectul ICCAE şaptesprezece universităţi americane (California State University San Bernardino; Clark Atlanta University; Florida International University; Norfolk State University; Tennessee State University; Trinity University; University of Texas El Paso; University of Texas Pan American; University of Washington; Wayne State University; Florida Agricultural and Mechanical University, Tallahassee; Miles College, Birmingham, Alabama; University of Maryland, College Park; University of Nebraska; University of New Mexico; Pennsylvania State University; Virginia Polytechnic Institute and State University), care au sarcina de a elabora şi aplica, pe întreaga perioadă de studii, programe / curricule specializate în formarea resurselor umane pe toate palierele de activitate în intelligence, inclusiv OSINT.[5]

Uniunea Europeană

În octombrie 2007, Comitetul Director al **Agenţiei Europene pentru Apărare** (structură creată în cadrul Consiliului Uniunii Europene în vederea susţinerii Politicii de Apărare şi Securitate Europeană) a aprobat propunerea de lansare, în 2008, a unor **cursuri-pilot la nivel avansat de perfecţionare în domeniul OSINT**[6], ale căror module au ca principale obiective acoperirea problemelor de ordin teoretic şi practic în cadrul procesului OSINT, a aspectelor conexe segmentului analizei de intelligence din surse deschise, popularizarea noilor instrumente OSINT şi creşterea nivelului de pregătire a specialiştilor în open source intelligence.

Cursurile se adresează tuturor statelor membre ale UE şi sunt parte a strategiei EDA de asigurare a predării noţiunilor şi cunoştinţelor de bază pentru analiştii de intelligence şi au la bază trei piloni: transferul de cunoaştere referitor la o anumită arie geografică (Africa, Asia Centrală, Orientul Mijlociu), aprofundarea abilităţilor specifice colectării datelor din surse deschise şi dezvoltarea capacităţilor de evaluare şi integrare a informaţiilor extrase alături de cunoaşterea disponibilă în acel moment.[7]

Cursurile organizate în anul 2009 au fost structurate în funcţie de nivelul de specializare al conţinuturilor, respectiv:

[5] http://www.dni.gov/cae/.
[6] http://www.eda.europa.eu/genericitem.aspx?area=organisation&id=308.
[7] http://www.eda.europa.eu/WebUtils/downloadfile.aspx?fileid=440.

- **cunoştinţe de bază** – Definirea OSINT şi locul său în ciclul de Intelligence; Terminologie; Formularea întrebărilor potrivite / inteligente – tactici de bază; Teoria informaţiilor / ştirilor; Tehnologii web, motoare de căutare şi alte instrumente; Prezentarea generală a procesului de căutare; Sursele – organizarea informaţiei; Internetul şi WorldWideWeb; Servicii Internet; Motoarele de căutare – teoria, istoricul şi selectarea acestora; Instrumente specifice de căutare; Strategii de căutare; Validarea informaţiilor; Alcătuirea unei „biblioteci" proprii – noţiuni teoretice; Căutarea în „deep web" – noţiuni teoretice; Căutare eficienţă / inteligenţă; Ameliorarea rezultatelor căutării – noţiuni teoretice; Securitatea în mediul Internet – noţiuni teoretice;

- **cunoştinţe avansate** – Organizarea unui centru OSINT; Căutarea în bazele de date comerciale – LexisNexis, Factiva – noţiuni teoretice; OSINT – aspecte legale; OSINT şi sursele de informare non-web; OSINT şi mijloacele Multimedia – noţiuni teoretice; OSINT şi riscurile de ţară – noţiuni teoretice de analiză şi raportare; Instrumente de traducere; OSINT şi contraterorism.

Similar, **The Crisis Room**, structură din cadrul Directoratului General pentru Relaţii Externe al Comisiei Europene, al cărei profil de activitate include asigurarea instrumentelor de monitorizare şi analiză OSINT, are o contribuţie importantă pe segmentul de instruire în intelligence, organizând şi desfăşurând cursuri de pregătire în domeniul exploatării surselor deschise.

Atribuţiile Crisis Room în domeniile OSINT şi „Early Warning" sunt:

- organizarea, implementarea şi întreţinerea platformei Tarîqa (inclusiv extensia accesului la statele membre UE şi organizaţiile neguvernamentale), prin intermediul căreia se asigură accesul personalului Directoratului şi reprezentanţilor regionali la cele mai recente ştiri, analize şi materiale audio / video, grupate tematic sau pe zone geografice, precum şi la baze de date prestigioase – Oxford Analytica, Jane's, LexisNexis;
- gestionarea sistemului ARGUS (achiziţia, prelucrarea şi diseminarea imaginilor satelitare);
- monitorizare şi alertă;
- furnizarea de materiale de informare, la iniţiativă sau la cerere;
- identificarea de noi surse pentru mărirea capabilităţilor OSINT şi „Early Warning";
- colaborarea / coordonarea cu celelalte centre de criză ale instituţiilor europene şi ale statelor membre;
- organizarea şi susţinerea de cursuri în domeniul OSINT.

Sesiunile de instruire coordonate de Crisis Room se axează în principal pe aplicarea, specifică problematicilor de securitate aferente

zonelor de interes ale Uniunii Europene, a tehnicilor de căutare şi analiză pentru obținerea şi utilizarea produselor analitice.

Tipul de training dezvoltat de Crisis Room este adaptat pregătirii şi perfecționării membrilor unei comunități interstatale pe problematici specifice ale activității de intelligence, vizând efectuarea în mod convergent şi unitar a transferului de cunoaştere şi a fixării / operaționalizării conținutului transmis cursanților.

Parteneriatul public-privat în spațiul euroatlantic

Cooperarea dintre instituțiile guvernamentale, serviciile de informații, mediul academic şi organizațiile private cu competențe în domeniul intelligence a generat, în cazul statelor europene şi euroatlantice, avantajul strategic al eficientizării integrării informațiilor din surse deschise şi creşterii complexității trainingurilor OSINT.

Acest lucru s-a datorat faptului că multitudinea **perspectivelor şi unghiurilor de abordare a exploatării OSINT** au condus la transpunerea acestora, în cadrul conferințelor, stagiilor şi cursurilor de instruire în Open Source Intelligence, în obiective variate, destinate acoperirii întregului cadru de cunoaştere, reflexie, evaluare critică, dezbatere şi aplicații concentrate asupra specificului activității OSINT.

Elocvente din punctul de vedere al calității rezultatelor şi resurselor implicate sunt parteneriatele stabilite între instituțiile de stat şi companii private din:

- **Statele Unite ale Americii** – alături de numeroase alte organizații de profil, compania **Open Source Solutions Network Inc.**, fondată în anul 1992 de Robert David Steele, unul dintre cei mai activi susținători ai dezvoltării OSINT, a contribuit la reformarea intelligence-ului american şi la dezvoltarea unei noi perspective asupra exploatării surselor deschise, editând numeroase studii şi implicându-se în procesul de pregătire şi specializare în OSINT la nivel național şi internațional.
- **Uniunea Europeană** – cooperarea **Agenției Europene de Apărare** cu organizații de prestigiu din domeniul intelligence (**Jane's**[8], **Reuser's Information Services**[9]), precum şi activitatea pe segmentul

[8] http://www.janes.com/consulting/OSINT.html
[9] http://www.reuser.biz/Website/index.html, http://osint.reuser.biz/#Browsers.

de training a unor companii sau asociaţii nonprofit precum **Infosphere AB**[10], **Sandstone**, **Risk UK**[11], **EUROSINT Forum** etc., urmăresc atât creşterea nivelului de pregătire a specialiştilor OSINT din comunităţile de informaţii ale statelor membre, cât şi crearea resurselor necesare consolidării cadrului instituţional OSINT, după modelul american.

> Programul de Training OSINT – Metode şi Tehnici (Open Source Intelligence Methods and Techniques Training Programme), derulat în perioada ianuarie-februarie 2010 la Londra şi Washington de Jane's Strategic Advisory Services în cooperare cu Reuser's Information Services, a constat în sesiuni de instruire, cu durata de o săptămână, care au urmărit formarea de competenţe privind:
>
> - abordarea disociată a problemelor specifice activităţii de analiză a informaţiilor;
> - elaborarea de planuri privind soluţionarea acestor probleme;
> - identificarea şi accesarea surselor-cheie;
> - evaluarea şi analiza fluxurilor de informaţii;
> - înţelegerea şi analizarea predispoziţiilor în selectarea surselor;
> - sintetizarea informaţiilor, analiza de sursă;
> - elaborarea de produse de intelligence.[12]

România – OSINT ca disciplină academică

La nivelul ţării noastre, cursul universitar de master „Analiza Informaţiilor", organizat începând cu anul 2008 de Facultatea de Sociologie şi Asistenţă Socială din cadrul Universităţii Bucureşti în parteneriat cu **Serviciul Român de Informaţii**, este unul din proiectele care urmăresc formarea unui corp de experţi în domeniul analizei de intelligence, în cadrul căreia Open Source Intelligence ocupă un segment bine determinat şi structurat.

Importanţa cursurilor rezultă concomitent din sporirea rolului reprezentanţilor mediului academic în instruirea şi perfecţionarea specialiştilor în intelligence din surse deschise, cât şi din consolidarea diverselor tipuri de parteneriate în domeniul educativ şi de cercetare, prin includerea în categoriile de public-ţintă a angajaţilor din cadrul instituţiilor de stat, reprezentanţilor societăţii civile şi mediului privat.

---

[10] http://www.infosphere.se/extra/pod/?id=91&module_instance=1&action=pod_show.
[11] http://www.risk-uk.com.
[12] http://www.janes.com/consulting/OSINT.html.

Principiul organizării masterului este imperativul formării unei comunități ştiințifice destinate promovării culturii intelligence-ului colaborativ, fapt relevat de structurarea cursurilor în două grupuri de module, al căror conținut a fost asigurat de cadre didactice din cadrul Facultății de Sociologie şi de traineri ai altor instituții competente.

3. Concluzii

Însuşirea cunoştințelor teoretice necesare orientării în spațiul surselor deschise, alături de dobândirea însuşirilor / competențelor cerute de desfăşurarea practică a activității OSINT reprezintă un segment din ce în ce mai important în intelligence-ul contemporan, în condițiile în care recentele modificări de paradigmă şi diminuarea ponderii modelelor tradiționale trasează noi coordonate conceptuale şi de acțiune la nivel global.

Trainingurile OSINT derulate în prezent la nivelul celor mai dezvoltate comunități de informații sau în format colaborativ, inter-instituțional şi inter-statal, reuşesc să asigure, într-o măsură semnificativă, saltul calitativ al resurselor umane din cadrul organizațiilor de intelligence în prevenirea şi combaterea eficientă a noilor forme de amenințări la adresa securității.

Bibliografie

1. Guțu, Dorina, *New Media*, Editura „Tritonic", Bucureşti, 2007.
2. Truyens, Johan, *Developing Open Source Capabilities*, EDA Bulletin, nr. 9, iulie 2008.
3. http://www.reuser.biz.
4. http://www.eda.europa.eu.
5. http://www.janes.com.
6. http://theosintgroup.com.
7. http://www.infosphere.se.
8. http://www.risk-uk.com.
9. http://ec.europa.eu.
10. http://www.opensource.gov.
11. http://oss.net.
12. http://theosintgroup.com.
13. http://www.sandstone.lu.
14. http://www.eurosint.eu.
15. http//:www.europolitics.info.
16. http://www.dni.gov.

Validarea surselor, fundament al OSINT

Dan BARBU
Sanda GAVRILĂ
Serviciul Român de Informații
e-mail: **ani@sri.ro**

Abstract

Nowadays, evaluating open source credibility is a MUST due to huge amount of available data, as well as to the ever increasing costs of classified data collection. In an ocean of multiple intelligence sources, including the Internet, analysts must be able to identify reliable sources. The alternative is to evaluate each and every piece of information gathered from any kind of source of intelligence interest. Since analysts cannot be specialists on multiple subjects / topics, they have to rely on those open sources that provide them all the useful information they need. A credible source offers „reasonable grounds for being believed".

Keywords: sources' validation, content analysis, intelligence cycle.

Pentru a-şi menține competitivitatea, orice entitate organizațională încearcă să răspundă provocărilor mediului în care îşi desfăşoară activitatea, să anticipeze evoluțiile viitoare şi să identifice trendurile, să-şi cunoască adversarii şi resursele de care dispun, astfel încât managementul organizației să adopte decizii pro-active. În acest scop, colectează şi procesează informații care fundamentează deciziile respective, informații obținute din surse deschise sau din surse secrete.

Prevalența orientării către sursele deschise a fost determinată atât de rațiuni economice (costuri mai mici), dar şi de revoluția tehnologiei informației şi a comunicațiilor, care a avut ca rezultat dezvoltarea şi extinderea exponențială a Internetului, principalul vector al boomului informațional.

În prezent, s-a ajuns la consens în privința importanței surselor deschise de informare pentru procesul de intelligence, însă, cu toate acestea, există opinii diferite cu privire la modul de evaluare a credibilității lor.

Din cauza diversității surselor deschise de informare, validarea informațiilor nu este practică. De aceea, majoritatea organizațiilor, atât din

mediul de business, cât şi din comunitatea de intelligence, s-a orientat către validarea surselor, stabilindu-şi propriile seturi de criterii.

În mod curent, se face confuzie între termenii validitate şi credibilitate. Validitatea este un atribut al informației. De asemenea, descrie informația ca fiind, simultan, relevantă şi semnificativă. O informație validată reprezintă acea informație a cărei acurateţe poate fi verificată[1].

Deşi este importantă pentru comunitatea de intelligence, validarea descrie mai degrabă informația decât sursa, iar singură nu poate măsura credibilitatea acesteia. Astfel, validitatea informației este principalul aspect vizat de analişti.

Analiştii examinează consistența informației şi o verifică cu altele deja validate. Cu toate că datele validate pot conduce la surse credibile, *obiectivul ar trebui să fie identificarea surselor ce pot fi validate, astfel încât toate informațiile diseminate de către acestea să nu mai fie supuse procesului de evaluare*[2].

Validarea unei surse poate oferi unele măsuri de protecție împotriva dezinformării, dar este puțin probabil să combată o campanie de dezinformare elaborată şi executată prin intermediul organizațiilor sub acoperire şi al agenților de influență. De altfel, un domeniu de preocupare este reprezentat de posibilitatea ca un adversar să plaseze un material prin intermediul surselor deschise, cu intenția de a dezinforma analiştii OSINT.

Criterii şi metode de validare a surselor deschise de informare

În funcție de suportul de difuzare, conținut şi modul de diseminare, sursele deschise de informare pot fi clasificate în două mari categorii, fiecare dintre acestea impunând metode specifice de validare:

---

[1] Potrivit lui Robert Steele, conceptul de OSINT validat (OSINT-V) se referă la OSINT care a fost confirmat de surse secrete. În accepțiunea NATO, OSINT-V reprezintă o informație căreia i se poate atribui un grad înalt de certitudine. Poate fi produsă de un analist multisursă din serviciile de informații, cu acces la surse secrete, ce activează în structurile unui stat sau ale unei coaliții. Totodată, poate proveni dintr-o sursă deschisă sigură, care nu ridică semne de întrebare în privința validării.

[2] Această modalitate de lucru este impusă şi de expertiza necesară analistului OSINT pentru a califica informațiile drept valide, varietatea subiectelor / tematicilor tratate de sursele deschise de informații, volatilitatea mediului de securitate şi lipsa timpului făcând imposibilă specializarea în toate domeniile vizate.

- **Surse deschise clasice**

- publicaţii periodice (ziare, reviste), cărţi (de specialitate, de telefoane, „Pagini aurii", anuare), materiale documentare (broşuri, studii), hărţi, fotografii;
- „literatura gri" – totalitatea materialelor care nu sunt disponibile prin intermediul canalelor tradiţionale de publicare, distribuţie sau control biografic;

> Datele oficiale – rapoarte guvernamentale, bugete, statistici demografice, audieri, dezbateri legislative, conferinţe de presă, discursuri, dar şi informaţiile din medii profesionale şi academice – conferinţe, simpozioane, documente elaborate de asociaţii profesionale, lucrări academice şi ale experţilor din diverse domenii, se încadrează în această categorie[3].

- transmisiile audiovideo în eter (radio, TV).

- **Surse deschise online**

- Denumite generic new media şi reprezentând *orice produs media digital care este interactiv şi distribuit prin reţele informatice* sau *totalitatea textelor, sunetelor, imaginilor şi elementelor grafice prelucrate pe computer şi reunite în baze de date* (enciclopedii electronice, bloguri, comunităţi virtuale, social networks, files-sharing, ediţii electronice ale presei tradiţionale, portaluri informaţionale, lumi virtuale, forumuri, biblioteci digitale etc.).

Spre deosebire de cazul mass-mediei clasice (unde există un volum controlabil de informaţii; identitatea şi agenda emiţătorului sunt cunoscute; este folosit modelul clasic al comunicării un emiţător / mai mulţi receptori), validarea unei surse online presupune abordări diferite, datorate în primul rând diversităţii şi specificului lor.

În cazul evaluării unei surse deschise clasice (studii, cărţi, publicaţii periodice etc.) există avantajul evaluării anterioare a acestora de către cercetători, editori sau bibliotecari. Aproape toate sursele de acest tip au fost evaluate într-un fel sau altul înainte ca analistul OSINT să intre în contact cu ele.

Criteriile de evaluare a surselor deschise tradiţionale pot fi folosite drept ghid şi pentru evaluarea surselor online.

---

[3] Furnizori de „literatură gri" sunt institutele de cercetare, think-tank-urile, corporaţiile, guvernele, partidele politice, mediile academice.

I. Evaluare inițială

Autorul

• Unde lucrează şi ce activitate a desfăşurat? Ce afiliere are? Ce educație / pregătire profesională are? Ce alte articole a scris? Subiectul abordat în materialul vizat face parte din aria de expertiză a autorului?

• Ați mai întâlnit numele autorului? A fost citat de alte surse? Există referințe biografice despre el? Autorii reputați sunt citați frecvent de specialişti / cercetători.

• Este autorul asociat cu o instituție / organizație reputată? Dacă da, care sunt valorile şi obiectivele acesteia?

Data publicării

• Materialul este de actualitate?

• Sursa difuzoare diseminează materiale noi? Care este frecvența publicării? Dacă subiectul face parte dintr-un domeniu dinamic, cu o dezvoltare rapidă, verificați caracterul de noutate al acestuia.

Număr de ediții

• Materialul este publicat / difuzat în premieră sau reprezintă o variantă actualizată? Dacă este actualizat, sursa respectivă acordă o atenție deosebită noutăților din domeniul abordat, fiind preocupată să reflecte schimbările apărute şi să-şi armonizeze conținutul?

Existența mai multor ediții ale unei lucrării indică faptul că aceasta a devenit un standard în domeniu.

Editor

• Verificați editorul. Dacă lucrarea vizată este publicată de editura unei universități, în cele mai multe cazuri reprezintă o lucrare cu caracter ştiințific. Cu toate acestea, chiar dacă editorul este o instituție reputată, calitatea lucrării nu este garantată. În schimb, se poate afirma că editorul apreciază lucrarea / sursa respectivă.

Titlul publicației

• Poate indica dacă este o publicație ştiințifică sau dedicată publicului larg. Distincția este foarte importantă, deoarece relevă gradul de complexitate al ideilor expuse.

II. Analiza de conținut

Citiți prefața lucrărilor pentru a determina intențiile autorului în demersul de realizare a acesteia. În cazul cărților, verificați cuprinsul

lucrării pentru a vă face o imagine de ansamblu asupra conținutului, precum şi referințele (note bibliografice). Includerea bibliografiei cu respectarea standardelor academice denotă atenția acordată de autor lucrării sale.

Audiența vizată

• Determinați cărui tip de audiență i se adresează materialul / sursa: unui public avizat sau publicului larg.

Modul de reflectare

• Materialul este informativ, de opinie sau propagandă? Faptele pot fi verificate cu uşurință, dar opiniile, deşi se bazează pe fapte, reprezintă interpretarea acestora.

• Informațiile sunt documentate sau pot fi combătute? Există dovezi care să susțină informațiile? Notați erorile sau omisiunile.

• Ideile şi argumentele prezentate sunt similare celor pe care le-ați mai întâlnit? Cu cât un autor se detaşează de opiniile celorlalți specialişti în domeniul abordat, cu atât mai critici trebuie să fiți față de ideile acestuia.

• Autorul este obiectiv, imparțial? Verificați dacă foloseşte un limbaj care are drept scop inducerea unor stări emoționale.

Gradul de acoperire a temelor abordate

• Verificați dacă sursa consolidează idei vehiculate anterior sau aduce informații noi, ori dacă subiectul este tratat superficial.

• Determinați dacă materialul reprezintă sursa primară sau dacă reprezintă o preluare, deoarece sursele primare ar trebui folosite în procesul de documentare.

Aspect

• Este publicația organizată în mod logic? Secțiunile principale sunt prezentate distinct?

Recenzii / prezentări

• Identificați recenzii / prezentări ale surselor / materialelor. Este recenzia pozitivă? Sursa este descrisă ca fiind obiectivă, ori lucrarea ca fiind o contribuție valoroasă în domeniul abordat?

În lucrarea sa „Authoritative Guide to Evaluating Information on the Internet", Alison Cooke, reputată specialistă în căutarea pe Internet, susține ideea folosirii criteriilor de evaluare şi validare a surselor deschise tradiționale şi în procesul de validare a surselor online, cu unele variații.

De fapt, variațiile reprezintă acele metode şi tehnici necesare pentru a stabili identitatea autorului, proprietarul sursei, locația serverului

de hosting, afilierea, apartenența la comunități online, software-ul folosit, e-mailul autorului, traficul sursei şi proveniența audienței etc.

Extinderea Internetului şi apariția aplicațiilor Web 2.0, a căror implementare a condus la transformarea World Wide Web într-un mediu interactiv, a avut drept consecințe un număr imens de website-uri corporate / personale, bloguri, forumuri, popularitatea fără precedent a rețelelor sociale (sute de milioane de conturi), dar şi creşterea alertă a conținutului generat de utilizatori şi diversitatea limbilor şi a pachetelor în care este livrată informația.

Grafic

Deşi asistăm la creşterea constantă a volumului de informații, determinată în principal de dezvoltarea mediului virtual, realitatea a demonstrat că nivelul informațiilor relevante a rămas aproape acelaşi, însă efortul pentru decelarea lor este mult mai mare.

O asemenea abundență informațională are însă şi aspecte negative: în mediul Internet nu există filtre. Datorită faptului că oricine poate scrie o pagină Web, regăsim documente a căror calitate variază foarte mult, având autori / proveniență diversă (copii, studenți, profesori, cercetători, structuri guvernamentale, promotori ai teoriei conspirației). Rezultatul este acela că resurse excelente pot fi alăturate unora îndoielnice.

Astfel, principalele dificultățile întâmpinate în procesul de identificare şi validare a surselor online sunt generate de caracteristicile Internetului şi facilitățile oferite de acest mediu, respectiv anonimatul relativ al utilizatorilor şi (re)transmiterea virală a unor informații ce pot fi relevante.

Totodată, este necesară filtrarea conținutului pentru a elimina informațiile care se repetă, permisivitatea mediului online în privința preluării conținutului conducând la copiere şi postarea acestuia fără menționarea autorului sau sub o formă modificată. În acest sens, se impune verificarea tuturor surselor de referință oferite, şi compararea materialelor pentru a identifica asemănările / diferențele care pot indica sursa / autorul primar.

Etape ale procesului de validare, specifice surselor online:

- verificarea url-ului sursei – poate releva caracterul personal al acesteia (includerea în url a numelui) sau ajută la evaluarea credibilității sursei (coroborați domeniul de înregistrare – de exemplu: .com, .eu, mil, .gov, .net, .tk, .org – cu conținutul publicat);

- evaluarea designului sursei (elaborat sau simplu) şi a softului utilizat – oferă indicii cu privire la sumele cheltuite şi implicit la valoarea / importanța pe care o are pentru proprietar;
- verificarea adresei sponsorilor sau paginile către care trimit eventualele materiale (banner) publicitare;
- determinarea frecvenței postării articolelor (unele surse postează ora şi data publicării articolelor);
- verificarea aspectului paginii în trecut (prin utilizarea instrumentului „Wayback Machine");
- identificarea serverului (hosting privat, public, gratuit sau cu plată) – prin serviciul gratuit http://www.whois.net;
- traficul înregistrat şi datele privind proveniența utilizatorilor – www.alexa.com, www.quarkbase.com;
- mesajele transmise (sunt originale sau preluate – de unde?) şi audiența vizată – relevă orientarea şi, posibil, obiectivele;
- verificarea codului sursă al paginii – poate conține informații suplimentare, inclusiv e-mailul autorului;
- folosirea instrumentelor oferite de Google pentru identificarea linkurilor către sursa vizată – în căsuța dedicată căutărilor scrieți sintaxa link to: www.sursa.com;
- cercetarea mediului online pentru identificarea utilizatorilor (după ID) care postează / accesează sursa – utilă pentru regăsirea conturilor şi mesajelor lor postate pe alte surse, pentru a stabili relațiile dintre acestea şi, eventual, afilierea la diverse rețele de bloguri, trusturi media, grupări politice sau mişcări extremiste / teroriste;
- monitorizarea comentariilor postate de utilizatori, pentru identificarea mesajelor editate / şterse de către administrator / moderator – relevă blocarea conținutului care contravine ideologiei pe care sursa o promovează;
- cercetarea mediului online şi a bazelor de date disponibile pentru regăsirea referințelor despre sursă / utilizatori sau a autorilor identificați.

Analizarea cronologiei unor evenimente şi a traficului înregistrat de anumite site-uri în intervalul anterior producerii acestora poate releva existența unui tipar de acțiune (traficul sau numărul de mesaje postate scade / creşte brusc înaintea unui atentat terorist), a cărui corelare cu alte elemente şi informații din surse secrete poate ajuta la instituirea unor măsuri preventive.

Concluzii

OSINT plasează omul în centrul procesului de intelligence, eficiența sa depinzând de capacitatea „profesionistului" de a extrage dintr-un volum mare de informații conținutul relevant şi de a identifica şi valida sursele disponibile (fie clasice, fie *new media*), fără a fi nevoit să evalueze fiecare informație colectată.

Bibliografie:

1. Dyèvre, Axel, *Intelligence cooperation: The OSINT option*, octombrie 2008.
2. Guțu, Dorina, *New Media*, Editura „Tritonic", Bucureşti 2007.
3. Norman, Dax R., *How To Identify Credible Sources On The Web*, accesibil la adresa http://sites.google.com/site/daxrnorman2/.
4. Steele, Robert David, *Open Source Intelligence (OSINT) – Draft Chapter for The Handbook of Intelligence Studies*",accesibil la adresa oss.net.
5. Tekir, Selma, *Open Source Intelligence Analysis: A Methodological Approach (Paperback)*.
6. „NATO OSINT Handbook 2001".
7. „NATO OSINT Reader".
8. „NATO Intelligence Exploitation of the Internet".
9. http://www.europolitics.info/dossiers/defence-security/intelligence-cooperation-the-osint-option-art151325-52.html.
10. http://kentsimperative.blogspot.com/2008/09/crowdsourcing-osint.html.
11. http://en.citizendium.org/wiki/OSINT#cite_ref-6/.
12. http://www.library.jhu.edu/researchhelp/general/evaluating/index.html.
13. http://unfccc.int/essential_background/library/items/1420.php.
14. http://www.library.cornell.edu/olinuris/ref/research/skill26.htm.

Integrarea intelligence-ului modern din perspectiva politicilor de securitate națională

Cristina-Ioana AMZA
Masterand „Analiza Informațiilor”,
Facultatea de Sociologie şi Asistență Socială, Universitatea din Bucureşti
e-mail: **amza.cristina@yahoo.com**

„You will know the truth, and the truth will set you free” [1]
Allan Dulles

Abstract

Starting by approaching the subject of intelligence analysis and the role that it plays in national security policy making, the main center of attention will focus on applying the theoretical knowledge on the selected study case represented by post-communist Romania, after being part of the North Atlantic Treaty Organization and a full member in the European Union. As far as the research goes in the field of intelligence, we can bring to attention two major views that summarize our debate: we have the field of public debate and the elaboration of reports about the intelligence services activity on one hand, and a series of studies and academic writings from a historical point of view, mainly about the gathering and failure of intelligence, on the other hand.

The actual merger of the concept of intelligence, as well as security policy, with the Romanian example, will be done in a holistic approach, beginning by analyzing the global context, discussing those elements of national specificity, so that we can establish in the end the role and means which transforms the intelligence product into a reliable policy in direct influence with the process of policy making.

Keywords: intelligence, intelligence analysis, public policy, national security policy, intelligence product.

[1] Verset biblic preluat de Allan Dulles, fost director al Central Intelligence Agency pe perioada desfăşurării mandatului preşedintelui Dwight Eisenhower, devenit ulterior motto.

I. Introducere

Pornind de la mottoul adoptat de Allan Dulles, fost director al Central Intelligence Agency, cercetarea de față își propune să aducă o clarificare într-un domeniu relativ complex, aflat la intersecția mai multor arii tematice şi care prin însuşi complexitatea sa reprezintă o provocare atât în ceea ce priveşte abordarea epistemologică, din punctul de vedere al metodologiei de cercetare, cât şi din punctul de vedere al importanței şi interdependenței cu alte domenii din aria ştiințelor sociale. Intelligence-ul, ca domeniu de cercetare va reprezenta punctul de pornire şi elementul integrator în care se va încadra componenta de analiză a informațiilor precum şi rolul acesteia în procesul de elaborare al politicilor publice.

Printre primele aspecte pe care le voi avea în vedere în lucrarea de față, se referă la contextul socio-politic în care ne încadrăm cercetarea. Lumea în care analiza informațiilor s-a dezvoltat, după cel de-al Doilea Război Mondial, este o lume schimbată, vorbim despre un proces complex, integrator şi generator în relație cu o a doua latură, cea de creare a politicilor publice. Este atât evidentă cât şi justificată o nouă perspectivă, un unghi de analiză şi înțelegere în acord cu noile tipuri de amenințări şi care să fie structurat într-o manieră ce poate veni în întâmpinarea amenințărilor la adresa securității cât şi a siguranței atât pe arena internațională, cât şi la nivel național.

I. 1. Delimitarea ariei tematice: În momentul în care abordăm un subiect de cercetare de tipul analizei informațiilor, se cere făcută o lămurire în ceea ce priveşte aria tematică în care se încadrează. Studiul de față își propune să abordeze atât latura de activitate de informații, latură specifică Studiilor Strategice, cât şi o latură ce se încadrează în aria tematică a Studiilor de Securitate şi anume, crearea de politici de securitate, ambele arii dispunând în acelaşi timp de dimensiunea de Relații Internaționale întrucât subiectul cercetării nu poate fi abordat în afara unui context global şi separat de evenimentele de pe arena internațională, deoarece, în mod esențial, discutăm despre un sistem deschis la influențele externe. Aria tematică reprezentată de către Studiile de Securitate trebuie înțeleasă conceptual „în special datorită influenței teoriei relațiilor internaționale [...] mai degrabă ca un domeniu pluridisciplinar. De aceea, analizele strict istorice sau în spiritul geopoliticii clasice nu sunt suficiente [...]. Lor trebuie să li se adauge printre altele, studiul politicilor, instituțiilor şi mecanismelor de planificare strategică, al scenariilor folosite în construirea strategiilor, dar şi al

dezbaterilor teoretice privind natura şi dinamica relaţiilor internaţionale şi sociale."[2]

În ceea ce priveşte analiza informaţiilor, aria tematică la care facem referire este cea a Studiilor Strategice, această arie fiind de asemenea, „aşa cum notează, de pildă, Booth şi Herring (1994), [...] nu într-o disciplină de sine stătătoare, fiind de fapt un sub domeniu al relaţiilor politice internaţionale de care sunt legate atât prin tradiţie, cât şi metodologii de cercetare."[3] Luând ca punct de pornire „pentru a situa normativ atât studiile de securitate, cât şi studiile strategice în interiorul disciplinei relaţiilor internaţionale"[4] conceptualizările preluate de către Bíro de la Richard Betts[5] putem integra studiile strategice utilizând „metafora cercurilor concentrice"[6]. Totuşi, pentru a putea determina exact unde se află analiza informaţiilor în aceste arii tematice, trebuie să facem referire şi la componenta ce aparţine cu precădere ştiinţelor sociale (sociologie şi psihologie) pentru că ne confruntăm cu „diferite categorii de fenomene cărora li se aplică termenul intelligence; acestea includ anumite informaţii, activităţi şi organizaţii."[7]

I. 2. Noutatea problematicii studiate: Atât la nivelul literaturii de specialitate internaţionale, cât şi la nivelul României, nu putem discuta, decât cu câteva excepţii, despre o conceptualizare şi teoretizare a domeniului intelligence-ului. „Deşi culegerea de informaţii devine un domeniu de studiu ştiinţific recunoscut, mai ales în lumea occidentală, teoretizarea pe marginea acestuia rămâne într-un stadiu incipient."[8] Încercarea de a explica relaţia complexă ce se stabileşte între ştiinţele sociale şi intelligence, este insuficient surprinsă la nivelul cercetărilor în domeniu, ba chiar „insuficient investigată până în prezent."[9] Deşi, până

[2] Luciana Alexandra Ghica, Marian Zulean, „O agendă pentru dezvoltarea studiilor de securitate" în *Politica de securitate naţională; Concepte, instituţii, procese*, Editura Polirom, Iaşi, 2007, p. 29.
[3] Daniel Bíro, „Studiile strategice", în Politica de securitate naţională; Concepte, instituţii, procese, Editura Polirom, Iaşi, 2007, p. 122.
[4] Ibidem.
[5] Richard K. Betts, „Should Strategic Studies Survive?" în World Politics, Vol. 50, No. 1, 1997, pp. 7-33.
[6] Daniel Bíro, op. cit.
[7] Abram Shulsky, Gary Schmitt, *Războiul tăcut; Introducere în universul informaţiilor secrete*, Editura Polirom, Iaşi, 2008, p. 23.
[8] Idem, p. 22.
[9] Idem, p. 11.

la un anumit punct, „e vorba de aceeaşi întreprindere intelectuală, cu prelungiri înspre rafinamentul şi profunzimea analizei, calitatea şi acurateţea sa intelectuală în modul de utilizare a metodelor deductive sau inductive, potenţialul de extrapolare a exemplelor istorice, în general a aplicării unor raţionamente specifice ştiinţelor sociale”[10], distincţia principală ce se conturează între cele două discipline se concretizează în latura practică, de acţiune propriu – zisă a activităţii de informaţii cu rolul de a avertiza şi acţiona în cazul riscurilor la adresa securităţii, spre deosebire de ştiinţele sociale ce pot doar anticipa şi analiza o eventuală situaţie de criză. Problema care aduce însă un plus de noutate în câmpul studiilor despre activitatea de informaţii, este însăşi relaţia dintre analiză sau mai degrabă, produsul finit al analizei şi modul în care acesta influenţează procesul de elaborare al strategiei de securitate a României precum şi al altor politici publice privind securitatea. La nivelul lucrărilor internaţionale, Mark Lowenthal[11] stabileşte premisele abordării intelligence-ului drept sursă fundamentală în crearea politicilor de securitate.

II. Cadrul metodologic şi enunţarea tezei de cercetare

Metoda de cercetare utilizată în mod preponderent este de natură calitativă – analiza surselor bibliografice – orientată atât descriptiv cât şi explicativ, generând o înţelegere profundă şi detaliată a realităţii analizate. Metodele de cercetare sunt de fapt cele ce consolidează şi dau forma lucrării, fiind totodată şi cele ce asigură acurateţea din perspectivă epistemologică, astfel că ne-am axat cu precădere asupra analizei de conţinut[12] fiind metoda care pune împreună elemente definitorii pentru a contura un fenomen în ansamblul său structural şi care se pretează în momentul în care discutăm despre politici publice, metode şi tehnici de analiza informaţiilor, precum şi asupra analizei comparative[13] cu ajutorul căreia putem pune în echilibru contextele socio-politice atât la nivelul arenei internaţionale, cât şi la nivelul României, observând astfel dacă direcţia în care îşi canalizează comunitatea internaţională eforturile către prevenire este

[10] Abram Shulsky, Gary Schmitt, op. cit., p. 11.
[11] Mark Lowenthal, *Intelligence: from secrets to policy*, CQ Press, 2008.
[12] Emile Durkheim, *Regulile metodei sociologice*, Editura Ştiintifică, Bucureşti, 1974, pp. 124-137.
[13] Henri Stahl, *Teoria şi practica investigaţiilor sociale*, Vol. 1, Editura Ştiinţifică, Bucureşti, 1974, pp. 338-339.

în acord cu activitatea de informații desfăşurată pe teritoriul statului român precum şi modul în care există colaborare între structurile de informații la nivel regional. Teza lucrării se conturează pe mai multe aspecte. Procesul de elaborare al politicilor publice, cu precădere, cele de securitate, este un proces amplu, dinamic şi interconectat cu alte sub-discipline din acelaşi domeniu de cercetare. Pornind de la acest aspect, vom discuta despre implicarea produsului finit al analizei informațiilor în procesul laborios de policy making.

III. Definirea domeniului activității de informații

Demersul de a încerca să stabilim parametrii esențiali în ceea ce priveşte procesul de intelligence trebuie precedat de analizarea diferitelor categorii de fenomene şi activități cărora le atribuim în sens generic acest concept. Pe lângă această clarificare, inițial vom defini domeniul şi propriu-zis ce presupune activitatea de informații pornind de la relația: activitate de informații – analiza informațiilor – intelligence. În genere, „indiferent de raza de acțiune, activitățile serviciilor de informații pot fi clasificate în patru categorii, menționate de obicei ca fiind «componente ale domeniului informațiilor»: culegerea, analiza, acțiunile secrete / sub acoperire şi contrainformațiile."[14] Având de-a face cu însăşi echivocul în încercarea de a defini securitatea națională, Shulsky şi Schmitt pun în balanță existența altor organizații, pe lângă guvernele naționale, cu atribuții în domeniul securității şi informațiilor. În ceea ce priveşte cazul României, atenția se concentrează în raport cu existența unei reticențe fată de aceste servicii, dat fiind faptul că avem de-a face cu reminiscențele regimului comunist şi formele sale de control prin intermediul Securității şi a serviciilor secrete. Hans Born consideră că „dacă serviciilor de protecție şi de informații le sunt încredințate misiuni ce cuprind alte aspecte ale vieții cotidiene – de exemplu transportul în comun, comunicarea prin internet sau educația – există pericolul ca prea multe aspecte ale societății să devină obiecte de „securizat", lucru ce poate transforma statul într-un „stat securist"."[15] Tocmai din acest motiv, controlul democratic asupra serviciilor, dar şi menținerea acestora apropiate de decidenți, reprezintă de fapt, limita în care definim domeniul şi atribuțiile activității de intelligence.

---

[14] Abram Shulsky, Gary Schmitt, op. cit., p. 33.

[15] Hans Born, „Controlul democratic al serviciilor de informații", în *Politica de securitate națională; Concepte, instituții, procese*, Iaşi, Polirom, 2007, p. 191.

IV. Tipuri de analiză a informațiilor şi rolul acestora

IV. 1. Analiza operațională (caz): Cele două forme majore în care produsul analizei informațiilor se clasifică, sunt reprezentate de analiza strategică şi analiza operațională (sau de caz). Prima formă pe care o abordăm şi anume, analiza operațională, „este preocupată de evenimente curente sau cu o desfăşurare iminentă. Aceasta se foloseşte pentru a determina capacitatea curentă sau proiectată în viitor a unui program sau a unei acțiuni într-o formă perpetuă şi nu oferă previziuni pe termen lung."[16] Bruce Berkowitz remarcă faptul că în procesul de analiza informațiilor „majoritatea activităților de intelligence vin în susținerea şi dezvoltarea analizei operaționale."[17] Pentru a putea oferi o perspectivă integrantă, analiza operațională constă în identificarea la nivel local, în teren, a incidentelor ce aduc atingere siguranței naționale sau realizarea statisticilor pentru a stabili modurile eficiente de identificare şi prevenire. Acest tip de analiză este folosit cu precădere pentru a ajuta ofițerul de informații în instrumentarea cu succes a cazurilor cu care se confruntă, dar şi pentru a asigura cunoaşterea dimensiunilor reale ale fenomenului ce aduce atingere securității statului, în vederea adoptării unor măsuri preventive.

„Intelligence-ul operațional este utilizat pentru a planifica folosirea resurselor şi a duce la bun sfârşit misiunea. Importanța sa este majoră atât în ceea ce priveşte acțiunile militare, cât şi cele politice."[18] Cu toate acestea, analiza operațională este folosită doar în anumite cazuri, fiind văzută ca un anumit tip de cunoaştere din perspectiva informațiilor, „observarea prin metode sofisticate, supravegherea precum şi filajul, sunt considerate adesea componente ale analizei operaționale (informații operaționale sau informații-acțiune)."[19]

Analiza operațională foloseşte tehnici care se concentrează pe dezvoltarea de ipoteze, reconstituirea derulării fiecărei activități ce aduce atingere statului de drept, identificării unei serii de infracțiuni conexe, înțelegerea rețelelor infracționale şi analizarea domeniului şi a modelelor activității infracționale.

---

[16] *Intelligence threat handbook*, Published by The Interagency OPSEC Support Staff, april 1996, p. 2.

[17] Bruce D. Berkowitz, Allan E. Goodman, *Strategic Intelligence for American National Security*, Princeton University Press, May 1991, pp. 6-29.

[18] David Charters, Anthony Stuart Farson, Glenn P. Hastedt, *Intelligence analysis and assessment*, Published by Taylor & Francis, 1996, p. 170.

[19] Michael Herman, *Intelligence services in the information age: theory and practice*, Published by Routledge, 2001, pp. IX-X.

IV. 2. Analiza strategică: Analiza strategică se referă la modalităţile şi metodele de exercitare a puterii (resurse sau mijloace) pe care conducerea unei entităţi politice le are la dispoziţie prin exercitarea controlului asupra unor evenimente caracterizate de un set de circumstanţe, în vederea atingerii anumitor obiective.[20] Acest tip de analiză oferă o privire de ansamblu asupra activităţilor ce contravin siguranţei şi securităţii naţionale şi urmăreşte să măsoare gradul de ameninţare pe care aceste activităţi săvârşite de diferite grupuri, îl supun asupra jurisdicţiei, atât la nivelul prezentului, cât şi în viitor. Obiectul analizei strategice este reprezentat de obţinerea informaţiilor necesare pentru activitatea de conducere a activităţii, formularea profilului specific, verificarea şi dezvoltarea procedurilor şi metodelor de prevenire.

În contrast cu analiza operaţională, intelligence-ul strategic include toate activităţile care nu sunt orientate prioritar către acţiunea cu care se confruntă serviciile de informaţii la momentul curent, ci care urmăresc examinarea unor subiecte pe termen lung, „astfel că, analiza strategică oferă avertismente privind ameninţările iminente la adresa securităţii naţionale şi stabileşte modele pe termen lung în domeniul de interes al conducerii politice. Intelligence-ul strategic are importanţă politică pentru că poate contura şi ghida politicile publice."[21] Din aceeaşi perspectivă discută şi McDowell definirea analizei strategice drept „o formă specifică de cercetare care se adresează oricărei problematici indiferent de întindere şi detaliu, necesară pentru a descrie ameninţări, riscuri şi oportunităţi într-o manieră ce poate determina crearea politicilor publice."[22]

Un alt aspect pe care Michael Handel îl subliniază este că de fapt „calitatea rezultatelor obţinute în domeniul intelligence-ului a previziunilor strategice, în mod particular, depinde de găsirea soluţiilor la probleme puse de factorul uman, care de multe ori contrazice soluţiile tehnologice."[23]

---

[20] Daniel Biro, „Studiile strategice" în *Politica de securitate naţională: concepte, instituţii, procese*, Editura Polirom, Iaşi, 2007, p. 125.

[21] Richard L. Russell, *Sharpening strategic intelligence: why the CIA gets it wrong, and what needs to be done to get it right*, Published by Cambridge University Press, 2007, p. 5.

[22] Peter C. Oleson, recenzie la Don McDowell, *Strategic intelligence: A Handbook for practitioners, managers and users*, Lanham, 2009, in: Studies in Intelligence, Vol. 53, No. 3, 2009, p. 27.

[23] Michael I. Handel, Richard Betts, Thomas Mahnken, *Paradoxes of strategic intelligence: essays in honor of Michael I. Handel*, Published by Routledge, 2003, p. 7.

V. Culegerea informațiilor – la intersecția dintre HUMINT şi TECHINT

Culegerea informațiilor se clasifică în funcție de diversele metode de culegere, astfel că acestea se pot clasifica în trei mari tipuri de metode: 1) culegerea informațiilor din surse umane (la care se face referire drept spionaj sau humint), 2) culegerea prin metode tehnice (informații tehnice sau techint), 3) culegerea informațiilor din surse deschise.[24] În viziunea publicului larg, HUMINT-ul este sinonim cu activitatea de spionaj şi activități clandestine, „de fapt, în realitate, majoritatea informațiilor din surse umane sunt colectate prin activități conspirate desfăşurate de către diplomați şi ataşați militari. [...] HUMINT-ul include atât activități conspirate, sensibile şi clandestine precum şi ofițerii care exploatează, controlează, supervizează şi susțin aceste surse."[25] Începând cu jumătatea secolului al XX-lea, atât la nivelul dezbaterilor academice, cât şi în practica serviciilor de informații, s-a discutat în mod continuu privind rolul şi importanța jucată atât de humint cât şi de techint în procesul de intelligence. „Pe de-o parte sunt cei care consideră culegerea informațiilor din surse tehnice primordială, existând probabilitatea de a continua să-şi sporească însemnătatea rolului pe măsură ce tehnologia progresează. Pe de altă parte, sunt cei care cred că importanța culegerii informațiilor din surse tehnice a fost exagerată, în detrimentul spionajului tradițional şi că trebuie restabilit acest echilibru."[26]

Culegerea de informații prin mijloace OSINT, componentă operațională a activității informative, reprezintă o etapă deosebită a tuturor serviciilor informative, constituind principala componentă în misiunile ce le revin în vederea realizării produselor finite de informații care pot contribui în mod relevant, prin disponibilitatea lor imediată şi caracterul lor foarte divers, la fundamentarea deciziilor în domeniul securității naționale.

În principiu, se poate discuta despre „complementaritatea humint şi techint"[27] deoarece atât în mod individual, cât şi ca un întreg, acestea pot oferi informații esențiale decidenților şi presupun de fapt integrarea într-un tot finit.

---

[24] Abram Shulsky, Gary Schmitt, op. cit., p. 35.
[25] Intelligence threat handbook, op. cit., pp. 2-4 – 2-5.
[26] Abram Shulsky, Gary Schmitt, op. cit., p. 68.
[27] Olivier Forcade, Sebastian Laurent, *Serviciile secrete. Puterea şi informația în lumea modernă*, Editura „Cartier", Chişinău, 2008, p. 78.

VI. Integrarea intelligence-ului finit în cadrul politicilor de securitate naţională

Aşa cum notează în mod cât mai cuprinzător Abram Shulsky şi Gary Schmitt, produsul analitic final „este reprezentat de orice mijloc, de la un raport oficial la o scurtă conversaţie, prin care un analist de informaţii transmite date prelucrate factorilor de decizie sau comandanţilor militari ce au nevoie de ele şi le pot utiliza."[28] Autorii realizează o clasificare a tipurilor de produse de intelligence, astfel că vom discuta despre: a) informaţii curente, b) informaţii de bază şi c) estimări informative. Cu toate acestea, clasificarea iniţială aparţine lui Sherman Kent şi se referă la forma curentă caracteristică reporterilor a informaţiilor, forma descriptivă de bază şi forma speculativ-estimativă, arătând că de fapt acest tip de produse finale fac referire la prezent, trecut şi viitor.[29]

Importanţa produsului analitic atât în ceea ce priveşte acţiunile propriu-zise ale serviciilor de informaţii, dar şi în elaborarea rapoartelor se concretizează prin însăşi forma şi atenţia cu care acestea sunt elaborate. Pentru analistul de intelligence, „este cât se poate de clar că produsul finit nu este îndreptat în mod neapărat către conducerea acţiunilor diplomatice sau militare, cât este un „multiplicator de forte". Tocmai de aceea, în situaţia în care avem analiză secundară, aceasta aduce un plus de valoare deciziilor privind securitatea naţională şi afacerile externe precum şi pentru activităţile diplomatice şi militare."[30]

VII. Politicile de securitate naţională şi rolul lor în cadrul politicilor publice

O politică publică poate fi de asemenea concepută şi ca o reţea de decizii şi strategii, interconectate, privind alegerea obiectivelor, a mijloacelor şi a resurselor alocate pentru atingerea acelor obiective în situaţii specifice.[31] Securitatea naţională în ansamblul său, rămâne unul dintre bunurile publice asigurate de către stat, printr-o serie de decizii, strategii şi procese, grupate per total sub eticheta de politica de securitate

[28] Abram Shulsky, Gary Schmitt, op. cit., p. 100.
[29] Sherman Kent, *Strategic intelligence for American world policy*, Published by Princeton University Press, 1953, pp. 7-8.
[30] Michael Turner, *Why secret intelligence fails*, Published by Brassey's, 2005, p. 104.
[31] Adrian Miroiu, *Introducere în analiza politicilor publice*, Editura „Punct", Bucureşti, 2001, p. 13.

națională. Deşi, chiar şi în acest domeniu se discută despre „privatizarea securității, securitatea națională rămâne un bun neexclusivist şi nerival, de care beneficiază toți cetățenii. Astfel, politica de securitate națională poate fi considerată o politică publică."[32] Totuşi, procesul de formulare a politicilor publice este de-a dreptul complex şi are implicații atât asupra dimensiunii, proceselor, mecanismelor şi actorilor, într-o rețea de relații conexe.

Analiza politicilor publice este de fapt o disciplină care utilizează multiple metode de cercetare şi de argumentare pentru a produce şi transforma informația relevantă pentru politici pentru a rezolva probleme publice.[33] În esență, pentru a înțelege cât mai bine de ce strategiile de securitate şi politicile de securitate în general sunt probleme-cheie în crearea politicilor publice, Marian Zulean defineşte politica de securitate națională „ca un ansamblu de decizii ce privesc structurarea unei viziuni despre securitatea națională şi interesele naționale, determinarea unor obiective strategice şi elaborarea unor strategii naționale, dar şi implementarea şi evaluarea acelor strategii."[34] Cu toate acestea, prima distincție ce se impune este cea între politica de securitate şi strategia de securitate. Zulean notează că distincția fundamentală între cele două concepte constă tocmai în faptul că „politica de securitate se referă la procesul de stabilire a obiectivelor majore ale unui stat, în timp ce strategiile se referă la modalitățile de realizare a acelor obiective. În plus, politica de securitate cuprinde, ca marcă distinctivă, o componentă politică: nivelul instituțional de decizie politico-militară."[35] Cea de-a doua distincție pe care autorul o are în vedere şi care se cere făcută înainte de a putea analiza comparativ strategiile de securitate, este cea dintre politica de securitate şi politica de apărare, ce are ca punct de plecare însuşi scopul final al acestor politici („securitatea națiunii pentru prima, ori apărarea împotriva unui inamic extern, pentru a doua."[36]), precum şi mijloacele folosite în atingerea scopului propus: „în timp ce apărarea națională se bazează pe mijloace militare, securitatea națională angajează toate resursele naționale."[37]

---

[32] Marian Zulean, op. cit., p. 34.
[33] William Dunn, *Policy Analysis: Perspectives, Concepts, and Methods* (Public Policy Studies, Vol 6), JAI Press, New York, 1986, p. 60.
[34] Idem, p. 41.
[35] Idem, p. 42.
[36] Idem, p. 43.
[37] Ibidem.

Pe lângă aceste aspecte, în crearea şi implementarea acestor politici de securitate, trebuie să ţinem cont de Sistemul de Planificare, Programare, Bugetare şi Evaluare (SPPBE) care prin prima latură a mecanismului, faza de programare „realizează legătura dintre strategiile naţionale, direcţiile de acţiune în domeniul apărării, misiunile forţelor armate şi resursele alocate în cadrul fazei de bugetare pentru realizarea acestora."[38] Importanţa implementării acestui sistem venit pe fondul reformei din armata României este dată de faptul că SPPBE reprezintă „un instrument care oferă cadrul general de îmbunătăţire a procesului de luare a deciziilor la toate nivelurile."[39]

Urmărind totalitatea elementelor care intră în alcătuirea procesului de policy making, parcursul produsului finit de intelligence constă în trecerea de pe masa analiştilor de informaţii, către decidenţi şi comisii specializate care îl vor integra în politicile României de securitate, atât sub forma unor legi, propuneri de proiecte sau chiar strategii. „Ca practică, elaborarea strategiei de securitate naţională în România a evoluat de la delegarea dreptului de elaborare a proiectului către instituţii, precum Ministerul Apărării Naţionale, către o largă consultare a societăţii civile."[40] Ceea ce am încercat să ilustrăm în parcursul cercetării de faţă este că rolul rapoartelor de informaţii este unul integrator ce oferă posibilitatea înţelegerii vulnerabilităţilor apărării României, în ansamblul lor.

VIII. Concluzii

Dacă la nivelul studiilor internaţionale putem discuta despre un demers de durată în studierea intelligence-ului ca disciplină specifică ştiinţelor sociale şi nu ca obiect de activitate şi de pregătire profesională a ofiţerilor de informaţii, în peisajul românesc şi în abordarea studiului nostru de caz, resursele sunt limitate. Noutatea subiectului de cercetare propus derivă chiar din necesitatea existenţei unei astfel de abordări relativ profunde asupra legăturii ce se stabileşte între mecanismele de culegere, evaluare şi transformare a informaţiilor în produse finite, urmărind parcursul

[38] Dan Gavrilă, Mihai Iancu, „Procesul de planificare, programare, bugetare şi evaluare în Armata României", în *Politica de securitate naţională; Concepte, instituţii, procese*, Ediura „Polirom", Iaşi, 2007, p. 173.
[39] Idem, p. 186.
[40] Marian Zulean, „Strategia de securitate naţională" în *Politica de securitate naţională; Concepte, instituţii, procese*, Editura „Polirom", Iaşi, 2007, p. 51.

pe care aceste produse îl traversează până pe masa decidenților militari şi politici, pentru ca în final să fie integrat în sistemul mai amplu al politicii de securitate națională.

Vorbindu-se tot mai des la nivelul Uniunii Europene despre crearea unei comunități regionale de intelligence şi despre cooperare între state în domeniul informațiilor, un astfel de studiu s-a impus şi a încercat să aducă o lămurire pe un teren arid, dominat de perspective istorice sau conspiraționiste în privința procesului prin care analiza informațiilor ajunge să contribuie la crearea politicilor de securitate națională în România postcomunistă.

Bibliografie

1. Berkowitz Bruce D., Allan E. Goodman, *Strategic Intelligence for American National Security*, Princeton University Press, May 1991.

2. Betts Richard K., „Should Strategic Studies Survive?" in *World Politics*, Vol. 50, No. 1, 1997.

3. Bíro Daniel, „Studiile strategice", în *Politica de securitate națională*; *Concepte, instituții, procese*, Editura „Polirom", Iaşi, 2007.

4. Born Hans, „Controlul democratic al serviciilor de informatii", în *Politica de securitate națională; Concepte, instituții, procese*, Editura „Polirom", Iaşi, 2007.

5. Charters David, Anthony Stuart Farson, Glenn P. Hastedt, *Intelligence analysis and assessment*, Published by Taylor & Francis, 1996.

6. Dunn William, *Policy Analysis: Perspectives, Concepts, and Methods* (Public Policy Studies, Vol 6), JAI Press, New York, 1986.

7. Durkheim Emile, *Regulile metodei sociologice*, Editura Ştiințifică, Bucureşti, 1974.

8. Forcade Olivier, Sebastian Laurent, *Serviciile secrete. Puterea şi informația în lumea modernă*, Editura „Cartier", Chişinău, 2008.

9. Gavrilă Jan, Mihai Iancu, „Procesul de planificare, programare, bugetare şi evaluare în Armata României", în *Politica de securitate națională; Concepte, instituții, procese*, Editura „Polirom", Iaşi, 2007.

10. Ghica Luciana Alexandra, Marian Zulean, „O agendă pentru dezvoltarea studiilor de securitate", în *Politica de securitate națională; Concepte, instituții, procese*, Editura „Polirom", Iaşi, 2007.

11. Handel Michael I., Richard Betts, Thomas Mahnken, *Paradoxes of strategic intelligence: essays in honor of Michael I. Handel*, Published by Routledge, 2003.

12. Herman Michael, *Intelligence services in the information age: theory and practice*, Published by Routledge, 2001.

13. *Intelligence threat handbook*, Published by The Interagency OPSEC Support Staff, april 1996.

14. Kent Sherman, *Strategic intelligence for American world policy*, Published by Princeton University Press, 1953.

15. Lowenthal Mark, *Intelligence: from secrets to policy*, CQ Press, 2008.

16. Miroiu Adrian, *Introducere în analiza politicilor publice*, Editura „Punct", Bucureşti, 2001.

17. Oleson Peter C., Recenzie la Don McDowell, *Strategic intelligence: A Handbook for practitioners, managers and users*, Lanham, 2009, în „Studies in Intelligence", Vol. 53, No. 3, 2009.

18. Russell Richard L., *Sharpening strategic intelligence: why the CIA gets it wrong, and what needs to be done to get it right*, Published by Cambridge University Press, 2007.

19. Shulsky Abram, Gary Schmitt, *Războiul tăcut; Introducere în universul informațiilor secrete*, Editura „Polirom", Iaşi, 2008.

20. Stahl Henri, *Teoria şi practica investigațiilor sociale*, Vol. 1, Editura Ştiințifică, Bucureşti, 1974.

21. Turner Michael, *Why secret intelligence fails*, Published by Brassey's, 2005.

22. Zulean Marian, „Strategia de securitate națională" în *Politica de securitate națională; Concepte, instituții, procese*, Editura „Polirom", Iaşi, 2007.

Analiza de intelligence la orizontul anului 2020: perspectiva comunității de informații a Statelor Unite ale Americii

Dr. Horațiu Virgil BLIDARU
Serviciul Român de Informații
e-mail: **horatiu_virgil@yahoo.com**
Sorina Ramona NICA
Serviciul Român de Informații
e-mail: **sorinailiescu2004@yahoo.com**

Abstract

The profession of intelligence analysis faces major challenges deriving from a rapidly changing security and intelligence environment. In this context, it is the responsibility of intelligence organizations to create an environment that provides access to traditional and new analytic tools, fosters effective and rapid learning, rewards innovation, and promotes critical thinking.

The aim of this paper is to make a synthesis of the results of the ***Future of Intelligence Analysis Project****, an eighteen-month study of the Center for International and Security Studies at Maryland, realized by analysts and managers of the United States Intelligence Community and experts from NGOs. The project was focused on intelligence analysis and organized its research around the themes of analyst education, recruitment, training, management, organization and retention. The authors used the year 2020 as a notional date of reference because individuals currently entering the analytic workforce will be seasoned analysts of that moment.*

The main conclusion of the report was that, if current practices continue, the Intelligence Community of 2020 will experience an imbalance between the demand for effective overall intelligence analysis and the outputs of its various analytic communities. In order to provide the analytic outputs that the coming environment will require, the study calls for an integrated analytical culture and establishing the basis for the profession of intelligence analyst across the Intelligence Community.

Keywords: intelligence analysis, national security, intelligence community.

Printre factorii care au făcut posibile tragicele evenimente din data de 11 septembrie 2001 se numără şi un „eşec de imaginaţie" al Comunităţii de Informaţii (*Intelligence Community*, IC) americane, atribuit analiştilor de intelligence. Comisiile speciale de investigaţie ale legislativului[1], dar şi cele constituite la nivelul principalelor agenţii de intelligence, au reliefat o serie de erori analitice premergătoare atentatelor din New York şi Washington şi au emis recomandări de optimizare a acestei componente – apreciată ca fiind din ce în ce mai importantă – a activităţii de informaţii pentru securitate naţională.

În ultimii ani, în Statele Unite ale Americii au fost realizate mai multe cercetări vizând optimizarea analizei de intelligence, comandate de către diferite elemente componente ale IC ori realizate de către institute de cercetare ori entităţi din sfera societăţii civile cu expertiză în domeniu. Unul dintre cele mai consistente studii, realizat de o echipă coordonată de dr. Rob Johnston, cercetător în cadrul Centrului pentru Studiul Informaţiilor *(Center for Study of Intelligence)* din subordinea Agenţiei Centrale de Informaţii (*Central Intelligence Agency*, CIA)[2], a fost publicat la Washington în anul 2005, cu titlul „Cultura analitică în comunitatea informativă a Statelor Unite ale Americii" *(Analytical Culture in the US American Intelligence Community)*[3].

---

[1] Raportul Comisiei Naţionale privind atacurile teroriste îndreptate împotriva Statelor Unite *(the National Commission on Terrorist Attacks Upon the United States),* disponibil pe http://www.9-11commission.gov/report/911Report.pdf; Raportul Comisiei privind capabilităţile informative ale Statelor Unite referitoare la armele de distrugere în masă (the *Commission on the Intelligence Capabilities of the United States regarding Weapons of Mass Distruction)*, http://www.wmd.gov /report/wmd_report.pdf.

[2] CSI a fost înfiinţat în 1974, din dorinţa Directorului Informaţiilor Centrale, James Schlesinger, de a crea în cadrul CIA o organizaţie care să reunească cei mai buni intelectuali disponibili pentru a analiza probleme de intelligence. Centrul, în care îşi desfăşoară activitatea istorici şi practicieni cu experienţă, încearcă să desprindă învăţăminte din operaţiile trecute, explorează nevoile şi aşteptările consumatorilor de informaţii şi stimulează dezbateri pe marginea problemelor actuale şi de perspectivă ale activităţii de informaţii. În acest scop, CSI editează revista *Studies in Intelligence* şi publică cărţi şi monografii care acoperă aspecte istorice, operaţionale, doctrinare şi teoretice ale profesiei de ofiţer de informaţii. Totodată, administrează Muzeul CIA. A se vedea https://www.cia.gov/library/center-for-the-study-of-intelligence/index.html.

[3] https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publucations/books-and-monographs/analytic-cuture-in-the-u-s-intelligence-community/analytic_culture_report.pdf. Documentul a fost postat pe 16 martie 2007.

Pe 10 martie 2006 Centrul pentru Studii Internaţionale şi de Securitate din cadrul Şcolii de Politici Publice a Universităţii din Maryland *(Center for International and Security Studies at Maryland)*[4] a publicat raportul final al proiectului „Viitorul analizei de intelligence" (The *Future of Intelligence Analysis*), comandat de Asistentul Directorului Adjunct al Informaţiilor Naţionale pentru Educaţie şi Instruire *(Assistant Deputy Director of National Intelligence for Education and Training)*[5].

> Poziţia de Director al Informaţiilor Naţionale (*Director of National* Intelligence, DNI) a fost creată prin Legea privind Reforma Informaţiilor şi Prevenirea Terorismului (*Intelligence Reform and Terrorism Prevention Act*, IRTPA) semnată de preşedintele George W. Bush în data de 17 decembrie 2004, în baza recomandării formulate în Raportul Comisiei 9/11, dat publicităţii în luna februarie 2004. DNI este şeful IC, orientează şi supraveghezează implementarea Programului Naţional de Informaţii şi este principalul consilier pe probleme de informaţii de securitate naţională al preşedintelui, Consiliului Naţional de Securitate şi Consiliului de Securitate Internă.

Proiectul în cauză, derulat pe parcursul a 18 luni de către un colectiv de analişti şi manageri din cadrul principalelor elemente componente ale IC[6], în parteneriat cu experţi din sectorul neguvernamental, s-a axat

---

[4] În cadrul centrului se derulează Programul Metode Avansate pentru Securitate Cooperativă, având drept teme de cercetare managementul armelor nucleare şi energiei nucleare, normele de reglementare ale utilizării spaţiului, supravegherea cercetărilor care implică agenţi patogeni periculoşi, dinamici locale ale conflictelor civile şi reconstrucţia post-conflict, securitatea cibernetică, schimbările climatice şi geoingineria. Detalii disponibile la http://www.cissm.umd.edu.

[5] Carson K. Eoyang, numit în această funcţie la 1 mai 2006. Cumulând şi funcţia de Cancelar al Universităţii Naţionale de Informaţii, titularul acestei poziţii are responsabilitatea de a construi relaţii de cooperare între şcolile / centrele de pregătire ale IC şi instituţiile civile şi de a dezvolta un program de instruire şi dezvoltare profesională unitar în domeniul activităţii de intelligence.

[6] Biroul Directorului Informaţiilor Naţionale *(Office of the Director of National Intelligence,* ODNI), Agenţia Centrală de Informaţii, Agenţia de Informaţii a Apărării *(Defense Intelligence Agency*, DIA), Agenţia Naţională de Securitate, Agenţia Naţională de Informaţii Geospaţiale *(National Geospatial Intelligence Agency*, NGIA), Biroul Informaţiilor Navale *(Office of Naval Intelligence,* ONI), Informaţiile Militare *(Army Intelligence)*, Centrul Naţional de Informaţii al Forţelor Terestre *(National Ground Intelligence Center)*, Colegiul Mixt de Informaţii Militare *(Joint Military Intelligence)*, Şcoala Sherman Kent pentru Analiza de Intelligence *(Sherman Kent School for Intelligence Analysis)*, Centrul Naţional pentru Informaţii Aeriene şi Spaţiale *(National Air and Space Intelligence Center)*, Cartierul General al Puşcaşilor Marini *(Headquarters Marine Corps)*, Activitatea de Informaţii a Puşcaşilor Marini *(Marine Corps Intelligence Activity,* MCIA), Centrul Naţional de Informaţii Maritime *(National Maritime Intelligence Center)*, Departamentul pentru Securitate Internă *(Department of Homeland Security*, DHS), Biroul Federal de Informaţii *(Federal Bureau of Information*, FBI) şi Garda de Coastă *(U.S. Coast Guard).*

pe investigarea a şase componente esențiale ale formării analiştilor de intelligence profesionişti – educație, recrutare, instruire, management, organizare şi fidelizare, în scopul formulării de recomandări menite să asigure IC americane, la orizontul anului 2020, un corp de analişti de intelligence performant, capabil să gestioneze provocările unui mediu de securitate complex.

Demersul de cercetare a fost organizat într-un format interactiv, pe patru ateliere în cadrul cărora reprezentanții agențiilor de informații au purtat discuții cu experți din domeniile economic, academic şi cercetare, urmărind identificarea de răspunsuri la întrebările: Ce abilități, expertiză, metodologii şi relații vor permite analiştilor să furnizeze produse analitice înalt calitative, oportune, atât cu privire la amenințările emergente, cât şi la cele bine definite, la nivelurile strategic şi tactic? Ce fel de persoane ar trebui recrutate pentru profesia de analist de intelligence? Ce fel de instruire profesională trebuie să asigure IC analiştilor pe parcursul carierei? Pot fi identificate seturi de bune practici valabile la nivelul IC, având în vedere varietatea misiunilor elementelor componente? În ce măsură reuşeşte IC să fidelizeze analişti de vârf? Există lecții pe care IC le poate prelua din practica altor domenii, precum cel de afaceri?

Dacă inițial studiul şi-a propus să identifice trăsăturile care conduc la performanța analitică individuală, ulterior s-a considerat că o perspectivă de abordare organizațională este mai utilă în perspectiva identificării unor modalități de optimizare a analizei de intelligence. Cercetarea a urmărit să identifice care vor fi exigențele analitice în lumea anului 2020, pentru a proiecta structura IC astfel încât să facă față acestora. Punctul de referință menționat a fost ales întrucât autorii cercetării au apreciat faptul că, la momentul respectiv, analiştii de intelligence angajați ulterior momentului 9/11 vor atinge maturitatea profesională deplină.

Autorii studiului au optat pentru o perspectivă multi-agenție, angrenând în proiect reprezentanți ai majorității elementelor componente ale IC şi axându-se pe studiul „ciclului de viață" al analiştilor *analyst „life-cycle"*: educație, recrutare, fidelizare, instruire, management, leadership şi climatul organizațional în care analiştii îşi desfăşoară activitatea.

Raportul final, revizuit de un panel de reputați experți în domeniul securității naționale, ce i-a inclus pe Richard Danzig, fost Secretar al Marinei, John Gannon, fost preşedinte al Consiliului Național de Informații *(National Intelligence Council)* şi fost director de personal al Comitetului Special al Camerei Reprezentanților pentru Securitate Internă *(House Select*

Committee on Homeland Security), John M. McConnell, viceamiral în retragere, fost director al Agenției Naționale de Securitate (*National Security Agency*, NSA) şi John E. McLaughlin, fost director al CIA, oferă o radiografie detaliată a viitorului analizei de intelligence din perspectivă americană, în concordanță cu evoluțiile prognozate ale unor amenințări la adresa securității din ce în ce mai fluide şi difuze ca natură.

Proiectul „Viitorul analizei de intelligence" a pornit de la o serie de premise devenite axiome în „lumea de după 11 septembrie 2001"[7].

Schimbarea radicală a naturii amenințărilor la adresa securității. După încheierea Războiului Rece, agențiile de intelligence s-au confruntat cu emergența unor noi amenințări la adresa securității naționale generate de o plajă variată de entități, care a inclus actori nonstatali de genul grupărilor teroriste transnaționale. Mare parte dintre aceştia au valorificat în interes propriu efectele globalizării, periclitând în modalități netradiționale securitatea Statelor Unite ale Americii. În acelaşi timp, tendințe globale precum explozia demografică, urbanizarea, pandemia HIV, diminuarea resurselor de apă potabilă în anumite zone ale planetei, au contribuit la accentuarea instabilității internaționale[8]. În acest cadru, fixarea unui set clar de priorități pentru activitățile de culegere şi analiză a informațiilor a devenit extrem de dificil de realizat.

Modificarea aşteptărilor decidenților politici față de serviciile de informații. Principala sarcină a agențiilor de informații o constituie punerea la dispoziția decidenților a unor informații oportune, obiective, independente de considerentele sau tendințele politice, bazate pe toate sursele disponibile (de la cele deschise la cele specifice, secrete), sau, parafrazându-l pe fostul director al CIA din perioada 1997-2004, George Tenet, „de a spune puterii adevărul, chiar dacă aceasta nu doreşte întotdeauna să îl audă". Analiştilor de intelligence le revine misiunea de a da un sens evoluțiilor mediului de securitate global, de a identifica amenințările potențiale la adresa securității naționale şi de a elabora produse analitice adecvate pentru decidenții politici. În acest demers, în afara utilizării surselor secrete tradiționale,

[7] Parafrazare a titlului lucrării fostului premier rus Evgehni Primakov, tradusă în limba română la Editura Institutul Cultural Român în anul 2003.

[8] A se vedea scenariile alternative prezentate de către Consiliul Național de Informații în *Mapping the Global Future: Report of the National Intelligence Council's 2020 Project Based on consultations With Nongovernment Experts Around the World,* Government Printing Office, December 2004. Disponibil la adresa http://www.cia.gov/nic/NIC_globaltrend2020.html.

analiştii de intelligence trebuie să extragă cunoştinţe cu relevanţă în planul securităţii naţionale dintr-o cantitate impresionată de informaţii din surse deschise.

> Potrivit estimărilor serviciilor de informaţii americane, un procent important din totalul informaţiilor obţinute (estimat la 80-90%) provine din sursele deschise. Pentru a ilustra această teză, istoricul Sherman Kent, devenit ulterior un reputat analist CIA, a solicitat în anul 1951 unui grup de cinci istorici ai Universităţii Yale să întocmească un material documentar cu privire la compoziţia, structura de comandă, dispunerea personalului şi a tehnicii de luptă a armatei americane până la nivelul divizie, însoţită de o descriere a capabilităţilor navale şi aeriene, fără a folosi nici un fel de surse clasificate. După o muncă de câteva luni, istoricii i-au predat lui Kent un material de câteva sute de pagini, însoţit de o sinteză de 30 de pagini. Potrivit estimărilor lui Kent, aproximativ 90% din conţinutul raportului era exact. Din dispoziţia expresă a preşedintelui Harry Truman CIA a clasificat ulterior toate copiile a ceea ce a rămas cunoscut în istoria serviciilor de informaţii din perioada Războiului Rece drept „Raportul Yale".

Rapiditatea evoluţiilor mediului de securitate global a făcut ca atât informaţia, cât şi înţelegerea analitică a acesteia, să devină critice. În acest cadru, activitatea de organizare şi culegere a informaţiilor de securitate naţională a inclus, drept ingredient obligatoriu, colaborarea sporită între diferitele componente ale IC, cât şi cu alte instituţii care concură la realizarea securităţii naţionale. Împărtăşirea cunoştinţelor *(knowledge sharing)*, concept ce include atât schimbul de informaţii, cât şi cel de expertiză, a devenit un element esenţial al analizei de intelligence. Aşa cum specialiştii în boli infecţioase din comunitatea medicală recurg la prevenire ca principala modalitate de stopare a pandemiilor, analiştii de intelligence pun accent pe anticiparea şi prevenirea ameninţărilor la adresa securităţii.

Proliferarea ameninţărilor potenţiale a schimbat, totodată, aşteptările decidenţilor politici faţă de produsele informaţionale. Politicienii nu doar pretind ca IC să le pună la dispoziţie noi tipuri de informaţii cu privire la noi tipuri de ameninţări, rezultate din surse variate şi prezentate în modalităţi inedite, dar au posibilitatea de a compara produsele analitice cu informaţiile obţinute din multe alte surse. Drept consecinţă, munca analiştilor de intelligence se desfăşoară într-un mediu mai competitiv decât oricând, iar competiţia va continua să se intensifice în viitor.

Raportul dintre beneficiar şi serviciul de informaţii este esenţial pentru finalitatea misiunilor încredinţate acestuia prin lege. Poziţia factorilor

de decizie față de produsele informaționale care le parvin de la serviciile de informații poate îmbrăca o plajă largă de nuanțe, de la atribuirea unui rol determinant informațiilor furnizate de serviciile secrete, până la minimalizarea acestora. Referindu-se la acest aspect, Allan Goodman, responsabil de Informarea Prezidențială Zilnică *(President's Daily Brief, PDB)*[9] în Administrația Jimmy Carter afirma: „unii factori politici nu citesc, unii nu vor citi, iar alții nu pot citi". De altfel, în literatura de specialitate este prezentată, cu titlul de exemplu, de cum nu trebuie să se deruleze relația dintre şeful statului şi directorul serviciului de informații, următoarea anecdotă: în 1996, un avion de mici dimensiuni s-a lovit accidental de clădirea Casei Albe. Trimişi de preşedintele Bill Clinton să afle cine se afla la manşa avionului, agenții Serviciului Secret i-au raportat preşedintelui SUA că acesta era directorul CIA, care, dorind să fie primit în audiență, nu a găsit o altă modalitate. Este cunoscut faptul că în cei opt ani de mandat, preşedintele Clinton s-a întâlnit cu principalul responsabil al Comunității de Informații americane de numai câteva ori.

Focalizarea pe analizele pe termen scurt (short-term analysis), în detrimentul celor pe termen mediu şi lung (mid- and long-term analysis). Într-un mediu de securitate fluid, metodele tradiționale ale activității de intelligence sunt inadecvate. Dacă observarea prin mijloace tehnice teleghidate, interceptarea electromagnetică şi penetrarea secretă erau suficiente pentru a stabili ordinea de bătaie într-un război tradițional sau a detecta un atac masiv prin surprindere, în cazul unui conflict civil sau al terorismului biologic, astfel de metode nu conduc la rezultatele scontate. Într-o lume în care amenințările la adresa securității sunt tot mai difuze, cele nonmilitare neconvenționale fiind interconectate cu cele pur militare, IC va trebui să înceteze să mai producă analize menite să răspundă unor misiuni specifice, în cadrul unui sistem analitic în care secretul şi segregarea eforturilor vor continua să primeze în detrimentul schimbului de cunoştințe şi unității eforturilor.

După data de 11 septembrie 2001, IC a fost criticată în mod repetat pentru eşecul de a fi împărtăşit informații critice – vulnerabilitate cu care

[9] PDB este un document strict secret (descris drept „cel mai sensibil document clasificat al administrației") a cărui elaborare s-a aflat, tradițional, în responsabilitatea directorului CIA, deşi la elaborarea sa contribuie şi alte agenții de informații. După înființarea poziției de DNI, sarcina prezentării acestei informări responsabilului de la Casă Albă a revenit „țarului" comunității informative.

agenţiile americane de informaţii continuă să se confrunte la nouă ani după atentatele din New York şi Washington, potrivit dezvăluirilor serialului „Top Secret America", publicat în prestigiosul cotidian „Washington Post"[10]. Pentru a fi eficientă în viitor, IC trebuie să îşi dezvolte, în paralel cu actuala structură ierarhică, reţele colaborative care să integreze experţi din sectorul privat şi academic, în vederea elaborării de analize interdisciplinare. Magnitudinea schimbărilor survenite în mediul de securitate intern şi internaţional impune analiştilor agenţiilor de intelligence să schimbe informaţii cu omologi din alte componente ale IC, dar şi cu organizaţii externe, practică ce intră în conflict cu însăşi cultura secretului ce caracterizează agenţiile de intelligence.

Solicitările presante pentru culegerea de informaţii pe termen scurt, analiza, producţia şi diseminarea acestora, distrage atenţia de la importante ameninţări emergente la adresa securităţii, ce necesită perspective de abordare diferite. Evoluţiile mediului de securitate au oferit însă agenţiilor de intelligence şi o *„fereastră de oportunitate" (window of opportunity)* pentru implementarea unor schimbări semnificative, menite să asigure un plus de eficienţă. Şocul produs de atentatele din 9/11 a determinat atât responsabilii politici, cât şi pe cei din cadrul IC, să analizeze critic perspectivele tradiţionale de abordare a activităţii de intelligence. Mark Lowenthal, fost Director Adjunct al Informaţiilor Centrale pentru Analiză şi Producţie, evidenţia că IC se confruntă cu „oportunităţi insurmontabile", dorind să evidenţieze, prin această sintagmă, dificultăţile inerente pe care le implică efortul de reformare a unui ansamblu de organizaţii disparate, prin măsuri de sus în jos, chiar şi atunci când majoritatea actorilor implicaţi recunosc că schimbările sunt necesare.

Din păcate, „fereastra de oportunitate" are un caracter temporar. Pe de o parte, ea incumbă riscul schimbării de dragul schimbării, iar pe de altă parte există posibilitatea ca până şi cele mai bine elaborate iniţiative de reformare să eşueze în absenţa unei voinţe firme, în condiţiile în care marile birocraţii, din categoria cărora fac parte şi agenţiile de intelligence, manifestă o puternică capacitate de rezistenţă la schimbare. În opinia autorilor proiectului de cercetare acesta este motivul pentru care, deşi Legea pentru Reformarea Activităţii de Informaţii şi Prevenirea Terorismului a

[10] Dana Priest, William Arkin, *A hidden world, growing beyond control,* „Washington Post", July 19, 2010; Idem, *National Security Inc.,* „Washington Post", July 20, 2010; Idem, *The secrets next door*, „Washington Post", July 21, 2010.

introdus modificări de substanță la nivelul IC, finalitatea acestora este discutabilă dacă agențiile de intelligence nu își vor schimba modul cotidian de lucru.

În absența modificării practicilor curente, Comunitatea de Informații a anului 2020 se va confrunta cu un dezechilibru între necesitatea unei analize de intelligence integrate eficiente şi perspectivele individuale ale diferitelor structuri analitice din cadrul elementelor componente ale IC. Pentru a preveni o astfel de evoluție, raportul „Viitorul analizei de intelligence" pledează pentru o „cultură integrată" la nivelul IC, menită să asigure operaționalizarea capabilităților analitice solicitate de evoluțiile mediului de securitate. Constatările / recomandările proiectului acoperă patru paliere: cultura IC; leadership, management şi dinamica carierei, educație şi instruire şi respectiv implementarea strategiilor.

Cultura analitică

„Comunitatea de Informații a SUA este comunitatea care nu este" a fost una dintre constatările inițiale ale cercetării *(Community that Isn't)*, întrucât include o serie de organizații aproape autonome, ale căror modalități de operare diferă radical. Diversitatea analitică la nivelul IC reflectă fragmentarea de ansamblu a sistemului de informații. O astfel de perspectivă intră în contradicție cu nevoia unei deschideri tot mai largi în ceea ce priveşte schimbul de cunoştințe necesar realizării unor analize eficiente cu privire la o paletă largă de amenințări.

Natura fragmentară a IC a fost percepută drept un impediment considerabil în calea schimbării. Faptul că fiecare agenție dispune de propria cultură organizațională generează atât efecte psihologice, cât şi practice. În plan psihologic, analiştii se percep pe sine drept analişti CIA, FBI, NSA etc., ceea ce accentuează mai degrabă diferențele decât similaritățile şi alimentează competiția între agenții şi nu cooperarea. În plan practic, diferitele culturi organizaționale conduc la proceduri şi politici incompatibile. Indicatori precum terminologia utilizată, descrierea pozițiilor şi criteriile de performanță, variază considerabil de la o agenție la alta. Agențiile nu culeg informații împreună şi nu schimbă informații sistematic, ceea ce face cooperarea dificilă, chiar dacă analiştii o doresc.

Iată de ce participanții la proiect au apreciat că *dezvoltarea unei culturi analitice unitare la nivelul IC* constituie un pas important în asigurarea capacității de a face față cu succes provocărilor viitorului.

O astfel de cultură s-ar caracteriza, printre altele, prin dorința de a gândi „în afara tiparului" *(„outside the box")*, capacitatea de asumare a riscurilor, abilitatea de a percepe politicile guvernamentale ca variabile independente în analiza unor subiecte de interes şi recunoaşterea faptului că lumea viitorului va conține un număr în continuă creştere de amenințări dispersate, de scală mică, ce necesită o atenție sporită pentru a putea fi prevenite. O astfel de cultură compozită ar trebui să încurajeze analiştii să se autoorganizeze şi stabilească rețele de comunicare în interiorul şi în afara IC.

Un astfel de obiectiv poate fi atins în primul rând prin *profesionalizarea comunității analitice.* Activitățile analiştilor de intelligence din diferitele elemente ale IC prezintă suficiente similitudini pentru a putea fi incluse într-o profesie. Faptul că analiştii nu se percep pe sine în acest mod se datorează mai degrabă evoluției istorice a IC decât unor factori inerenți specificului activității. Apartenența la aceeaşi profesie nu este sinonimă cu conformitatea. Pentru analiştii de intelligence profesionişti este esențial să îşi păstreze capacitatea actuală de a realiza analize competitive.

Comparația utilizată pentru descrierea locului analizei de intelligence în ansamblul IC este extrem de sugestivă. În opinia autorilor raportului, analiştii de intelligence reprezintă pentru arhitectura de informații ceea ce medicii constituie pentru sistemul de sănătate. Toți medicii se consideră pe sine drept membri ai corpului de angajați din sistemul de sănătate. Cu toții se percep, de asemenea, ca aparținând unui subsistem specific, deşi abilitățile pe care le practică diferă considerabil, până în punctul în care abilitățile lor nu sunt întotdeauna transferabile între specializări. Spre exemplu, un neurochirurg nu poate înlocui un chirurg cardiolog, deşi ambii posedă aceeaşi instruire şi educație, apreciază şi înțeleg contribuția muncii celuilalt[11].

Întrucât analiza de intelligence este o specializare a intelligence-ului suficient de complexă pentru a fi percepută ca o profesie în sine, autorii studiului au propus IC să adopte o serie de elemente distinctive ale acesteia, care includ: o doctrină comună şi o descriere standardizată a posturilor; un limbaj profesional; standarde de etică profesională; programe de instruire comune şi specifice; capabilități instituționale de a analiza eşecurile şi

[11] Pentru detalii privind comparația între cele două profesii, a se vedea Stephen Marrin and Jonathan D. Clemente, „Modeling an Intelligence Analysis Profession on Medicine", *International Journal of Intelligence and Counterintelligence*, 18/4 (Winter 2005-2006): 707-729.

succesele şi de a implementa cele mai bune practici; un sistem de rotire a analiştilor în interiorul IC.

Raportul a recomandat elaborarea, sub coordonarea Directorului Informațiilor Naționale, a unor declarații de principii pentru IC în ansamblu şi respectiv comunitatea analitică, a unei doctrine analitice comune şi a unor descrieri standardizate a pozițiilor analitice. Într-o etapă ulterioară, s-a apreciat drept necesară elaborarea unui cod etic al profesiei, constituirea unei structuri care să desprindă lecții de învățat, atât din erori, cât şi din succese şi să asigure diseminarea acestora la nivelul IC, dezvoltarea unui jargon menit să îmbunătățească comunicarea interagenții, precum şi instituirea unui sistem standardizat de evaluare a performanței. Standardele profesionale nu previn apariția unei crize, concluzionează autorii cercetării, dar ele ajută organizația să stabilească unde a greşit şi asigură cadrul orientativ pentru măsuri corective.

Alte recomandări au vizat creşterea colaborării dintre agenții prin elaborarea unei doctrine a IC pentru schimbul de informații, instituirea unui sistem de rotire în funcție pentru analişti şi înființarea unui centru, cu o componentă virtuală, în cadrul căruia analiştii să poată testa noi idei fără teama de potențiale consecințe negative, lecțiile desprinse din aceste „jocuri de idei" urmând a fi înregistrate şi distribuite către toate structurile analitice ale IC.

O altă constatare a studiului a privit caracterul limitat al comunicării dintre analiştii IC şi experții din afara acesteia. Cu privire la acest aspect, autorii au pornit de la premisa că importanța în creştere a informațiilor culese din surse deschise va impune IC să împărtăşească anumite informații / cunoştințe cu experți din domeniile economic, academic şi cercetare. În acest scop, IC ar trebui să aibă în vedere extinderea capacității analiştilor de a se consulta cu specialişti din sectorul neguvernamental atunci când analizează amenințări ori alte subiecte de interes ce nu implică dimensiuni militare, pentru a îmbunătăți procesul analitic cu perspective culturale diversificate. Recomandarea autorilor studiului a fost aceea de standardizare a capacității de relaționare externă a analiştilor, prin elaborarea unei doctrine a IC care să faciliteze colaborarea, prezervând totodată normele de protecție a surselor şi metodelor specifice.

> Unele agenții din cadrul IC întrețin contacte strânse cu reprezentanți ai comunității academice, iar experiența pozitivă a acestora poate servi ca model pentru extinderea unor astfel de programe. Un exemplu de funcționare cu bune rezultate a unui program de dimensiuni globale îl constituie *Global Futures Forum,* lansat de către

> CIA la sfârşitul anului 2005[12]. În afara IC există suficienți experți dornici să se angajeze în astfel de parteneriate, dar agențiile de informații trebuie să îşi modifice unele din practicile de securitate existente pentru a beneficia de expertiză externă. În acelaşi scop, se impune depăşirea unui bias legat de timpul petrecut în afara IC, analiştii apreciind că mutarea în afara IC dăunează carierei.

Politicile de rotire în funcție ar trebui să includă, în afara transferului în interiorul IC, posibilitatea părăsirii temporare a agenției de intelligence, inclusiv în stagii sabatice. Totodată, s-ar impune finanțarea de studii în străinătate, pentru învățarea limbilor străine ori asimilarea de cunoştințe cu privire la alte culturi. Alte măsuri de optimizare propuse au vizat: încurajarea revizuirii produselor analitice de către experți din afara IC, în condițiile în care, în mod curent, analizele sunt transmise spre evaluare managerilor, care, în unele situații, au mai puține cunoştințe cu privire la obiectul analizei decât analiştii; implicarea sporită a centrelor de cercetare academică şi companiilor private în activități cu relevanță în domeniul securității naționale, în vederea îmbunătățirii perspectivelor, metodologiilor şi expertizei analitice; încurajarea analiştilor să stabilească legături cu „lumea exterioară".

O zonă distinctă a recomandărilor a vizat modificarea de către IC a actualelor sisteme de securitate şi tehnologice. Procedurile de securitate fizică şi de acordare a accesului la informații clasificate diferă, în anumite privințe considerabil, între elementele componente ale IC şi sunt incompatibile cu cele folosite de parteneri guvernamentali de la nivel statal şi local, ceea ce afectează negativ recrutarea analiştilor. Aceşti factori, împreună cu absența unor standarde comune ale tehnologiei informaționale, îngreunează considerabil schimbul de cunoştințe. De cele mai multe ori, personalul însărcinat cu protejarea securității informațiilor în interiorul IC nu înțelege necesitatea schimbului de informații ori nu conştientizează că a venit momentul pentru amplificarea substanțială a acestuia. De prea puține ori însă cei care fixează agenda de securitate sunt analiştii orice culegătorii de informații.

---

[12] Comunitate de informații multinațională, multidisciplinară, ce reuneşte experți în intelligence, securitate națională şi din sectorul nonguvernamental din 35 de țări, care lucrează împreună în cadrul unor comunități de interese pentru subiecte comune, precum: terorism şi contraterorism, radicalizare, traficuri ilicite, proliferare, avertizare timpurie, organizarea activității de intelligence, prevenirea genocidului, pandemii, schimbările de mediu şi resurse, state eşuate. Detalii disponibile la https://www.cia.gov/offices-of-cia/intelligence-analysis/organization-1/gfp.html.

Practic, la data studiului, ca şi la momentul 9/11, unui analist dintr-o anumită agenție îi era imposibil să afle dacă alți analişti din terțe agenții lucrează la o problemă specifică. Problemele de interoperabilitate a sistemelor IT contribuie la această situație. Indiscutabil, securitatea este necesară, dar actualul sistem de securitate trebuie ajustat, au concluzionat autorii studiului. Spre exemplu, este puțin probabil că aplicanții pentru un post de analist au disponibilitatea de a aştepta – uneori până la 18 luni – pentru obținerea autorizației de securitate.

Pentru depăşirea barierelor descrise, raportul a recomandat ca ODNI să identifice o modalitate de a audita activitatea analiştilor şi a determina parametrii de securitate a ceea ce aceştia pot şi trebuie să facă şi, ulterior, să dezvolte şi monitorizeze implementarea de standarde tehnologice, de securitate şi clasificare unitare şi interoperabile la nivelul IC.

Conducere, management şi dinamica carierei

Raportul de cercetare a reliefat că practicile de recrutare diferă substanțial în interiorul IC. Fiecare agenție dispune de propriul sistem de selecție a personalului. O standardizare nu există nici în ceea ce priveşte evaluarea personalului. În unele agenții de intelligence, managerii nu au oportunitatea de a-i întâlni pe analişti anterior angajării. Dacă în unele situații mărimea organizației justifică această stare de fapt, în cazul corpului analitic al majorității componentelor IC perspectiva de încadrare ar trebui să fie mult mai personalizată.

La nivelul IC nu există situații centralizate referitoare la calitatea resurselor umane disponibile la nivelul celor 16 elemente componente. În absența unei radiografii a capitalului intelectual existent, practic este imposibil de proiectat o politică de resurse umane raportată la evoluțiile curente şi prognozate ale mediului de securitate. De altfel, dată fiind natura difuză a amenințărilor la adresa securității, formarea unui corp de analişti de dimensiuni adecvate este extrem de dificil de realizat. În mod evident, IC nu poate angaja specialişti în toate limbile străine şi experți cu privire la fiecare regiune ori grup etnic din lume. Istoria recentă a probat faptul că spațiile generatoare de amenințări în anii 1990 nu au constituit priorități pentru decidenții politici. De aici imperativul de a identifica în prealabil şi a utiliza la momentul necesar experți nonguvernamentali şi foşti analişti de intelligence, într-o manieră organizată. Necesitatea extinderii bazinului de recrutare a analiştilor a fost evidențiată majoritatea practicienilor intervievați, care au atenționat că dacă IC va continua să angajeze aceleaşi tipuri de indivizi, va continua să producă aceleaşi tipuri de analize.

Pe acest palier, raportul a recomandat *instituirea unor politici de resurse umane compatibile* la nivelul IC, apreciind faptul că practicienii din domeniu resimt nevoia unor standarde comune de recrutare, angajare, certificare, instruire şi promovare. Atingerea principalului obiectiv al IC, acela de a avea o forță de muncă de excepție, nu se poate realiza în absența unor standarde clare, care să aibă drept punct de pornire o listă de atribute analitice dezirabile.

Trăsături	***Fundal educațional***	***Calificări***
Curiozitate nativă	Abilități de învățare a limbilor străine	Capacitate de exprimare în scris
Gândire clară	Perspectiva clientului / utilizatorului	Bun comunicator verbal
Gândire critică	Specializare de fond (funcțională sau regională)	Bună capacitate de expunere
Gândire intuitivă	Încorporarea politicilor Statelor Unite ca variabile independente	Abilități de rezolvare de probleme
Spirit de echipă	Cunoştințe de istorie	Abilități IT
Capacitatea de a „vedea dincolo de evidențe”	Înțelegerea diferenței dintre intelligence şi politică	Capacitatea de translatare a întrebărilor politice în întrebări de intelligence
Identificarea de patternuri complexe	Stagii peste hotare	Abilități de cercetare
Autodisciplină		Abilități sociale
Abilitatea de a gestiona incertitudinea		Cunoaşterea propriei organizații şi a IC
Abilitatea de a elabora scenarii alternative		Bune abilități interpersonale
Etică / integritate		
Flexibilitate / adaptabilitate		
Capacitate de învățare rapidă		
Imaginație		
Recunoaşterea propriilor biasuri		
Acceptarea criticii		

Competențele unui analist de intelligence profesionist (identificate de membrii IC în cadrul atelierelor subsumate proiectului „Viitorul analizei de intelligence”)

Pentru realizarea acestui deziderat, IC ar trebui să accentueze în procesul de recrutare a analiştilor brandul profesiei şi nu pe cel al agenţiei de intelligence. La momentul cercetării puţine agenţii componente ale IC dispunea de o identificare pozitivă a brandului, majoritatea combinând o recunoaştere scăzută a brandului cu departamente de resurse umane neperformante.

O altă recomandare a vizat instituirea unui sistem unitar de promovare a analiştilor la nivelul IC. Unii dintre experţii intervievaţi s-au pronunţat în favoarea introducerii unei perioade de licenţiere a analiştilor, distinctă de perioada de probă, finalizată printr-un examen care să le acorde dreptul de a profesa.

Întrucât au constatat că mare parte din analiştii recent încadraţi au aşteptări nerealiste cu privire la activitatea cotidiană şi contribuţia posibilă la procesul de fundamentare a deciziei, autorii studiului au propus organizarea unor programe interne, pe parcursul cărora să fie înlăturate prejudecăţile şi stereotipurile cu privire la profesia de analist de intelligence.

Elaborarea de standarde de concediere a fost o măsură propusă ca urmare a constatării că o parte dintre cei intervievaţi au susţinut că, în mod curent, analiştii şi managerii promovează ierarhic indiferent de modul în care îşi îndeplinesc atribuţiile, neexistând nici un mecanism instituţional de îndepărtare a analiştilor neproductivi, percepuţi drept „o povară".

Alte recomandări au vizat: angajarea unui număr adecvat de analişti, care să permită dezvoltarea carierei, instruirea şi rotaţia (fără a fi necesară instruirea standardizată a tuturor analiştilor, potenţial generatoare de efecte negative sau plafonarea vârstei la angajare); constituirea unei baze de date a capitalului intelectual disponibil la nivelul IC şi dezvoltarea de programe care să identifice în avans şi să permită utilizarea, funcţie de necesităţi, a unor experţi nonguvernamentali şi foşti analişti de intelligence.

Instituirea unor repere clare ale carierei profesionale este de natură a creşte fidelizarea analiştilor de intelligence. Expectaţiile analiştilor angajaţi în prezent de către IC diferă considerabil de cele ale forţei de muncă existente şi, pe cale de consecinţă, IC va trebui să se transforme pentru a oferi acele posturi care corespund aşteptărilor.

Participanţii la proiectul de cercetare au vehiculat o rază a pierderilor de 4-5% pentru analiştii având mai puţin de cinci ani experienţă în cadrul IC. În absenţa unor date statistice referitoare la procentul de demisii în rândul analiştilor cu o vechime de peste cinci ani, autorii raportului nu au

putut concluziona cu privire la calitatea resursei umane pierdute, pentru a stabili dacă aceasta include vârfurile ori pe cei pe care IC preferă să îi piardă. Un factor important care alimentează ieşirile din sistem îl constituie salarizarea superioară din sectorul privat.

Autorii raportului au recomandat furnizarea de către IC a unor multiple căi de evoluţie în carieră, prevăzute cu standarde clare, inclusiv stimulente pentru schimbarea acestora, funcţie de necesităţile IC şi cerinţe care trebuie atinse pentru promovarea în trepte superioare. Suplimentar, IC ar trebui să creeze programe de mentorat, să extindă programele de perfecţionare internă şi să încurajeze rotirea analiştilor în interiorul IC, inclusiv prin includerea stagiilor în alte posturi printre condiţiile de promovare în carieră.

Îmbunătăţirea leadershipului şi managementului componentei analitice a activităţii de intelligence este o condiţie esenţială a unei construcţii analitice eficiente. Managerii sunt, într-o măsură determinantă, responsabili de calitatea produselor analitice. Prin stilul de conducere şi influenţa exercitată asupra culturii organizaţionale, ei contribuie decisiv la fluctuaţia resursei umane. De calitatea actului managerial depinde dacă un analist va ieşi la pensie în cadrul IC ori o va părăsi după 5-10 ani. La modul ideal, managerii constituie agenţii schimbării în propriile organizaţii.

În prezent, pentru a avansa în carieră analiştii pot opta între a intra în *Senior Analytic Service*[13] – structură creată în anul 2000 pentru a permite o carieră superioară analiştilor cu experienţă, sau pentru a deveni manageri. Drept rezultat, analiştii devin manageri dacă au probat că sunt buni analişti şi nu pentru că au potenţialul de a deveni buni manageri. O incidenţă ridicată se înregistrează şi în privinţa managerilor care nu au experienţă analitică.

Într-un mediu care solicită deja nivele ridicate ale împărtăşirii cunoştinţelor între analişti, managerii trebuie să fie preocupaţi de modalităţi de a încuraja lucrul în echipă şi de a-i recompensa pe analiştii angajaţi în activităţi colaborative. Ei ar trebui, totodată, să creeze un climat în care argumentele analiştilor cu opinii divergente faţă de cele ale majorităţii să poată fi auzite. Există însă şi manageri care caută să controleze integral informaţia care părăseşte structura din care fac parte, pornind de la percepţia că, evitând să îşi asume riscuri, îşi maximizează şansele de promovare.

---

[13] Jack Davis, *Improving CIA Analytic Performance: DI Analytic Priorities,* The Sherman Kent Center for Intelligence Analysis, „Occasional Papers", Volume 1, Number 3, September 2002.

Raportul a recomandat IC să îmbunătățească programele educaționale şi de instruire pentru manageri existente, inclusiv prin instruirea continuă la toate nivelurile şi introducerea unor sisteme de recompensare adecvate. Totodată, se impune *schimbarea modului de evaluare a performanței, prin mutarea accentului de la cantitatea producției analitice spre calitatea analizelor.* Întrucât managerii sunt evaluați în baza numărului de rapoarte produse de analiştii din subordine, managerii manifestă tendința de a utiliza acelaşi standard pentru a-şi evalua subordonații. Acest mod de raportare conduce la dilema „tiraniei producției": analiştii dispun de puțin timp pentru a reflecta la analize, datorită presiunii pentru producerea de rapoarte. Birocrația cotidiană, formularea de răspunsuri la întrebări punctuale şi preocuparea constantă de încadrare în termene, erodează capacitatea analitică şi distrag atenția analiştilor de la problemele esențiale.

Educație şi instruire

În urma demersurilor de cercetare, a fost identificată o nevoie stringentă de dezvoltare a unor programe educaționale şi de instruire menite nu doar să îmbunătățească activitatea de analiză, ci şi să profesionalizeze forța de muncă analitică. Educația şi instruirea nu se numără printre prioritățile IC a fost una din constatările studiului, iar faptul că managerii nu au beneficiat de o instruire consistentă pe parcursul propriilor cariere a alimentat acest bias.

De regulă managerii apreciază că, întrucât majoritatea subordonaților lor sunt suprasolicitați profesional, este inadecvat să ofere analiştilor timp pentru instruire şi educație. Pe parcursul studiului a mai reieşit faptul că responsabilii IC pun accent pe avantajele pe termen scurt ale stării de fapt existente, ignorând beneficiile pe termen lung ale unei forțe de muncă analitice mai bine pregătite.

Tradițional, analiştii sunt educați în universități şi instruiți ulterior de către agențiile care îi angajează în conformitate cu programe specifice. În procesul de formare a unui analist de intelligence profesionist linia de demarcație între educație şi instruire este însă dificil de trasat. Din perspectiva autorilor raportului, este mai util să percepi educația şi instruirea ca parte a unui continuum, decât ca activități separate.

Întrucât analiştii de intelligence sunt membrii unei profesii, pentru şcolile de politici publice, relații internaționale ori ştiințe politice ar fi adecvat să ofere curricule în „analiza informației" atât la nivel de licență, cât şi de studii aprofundate, astfel de programe îmbinând instruirea cu educația. Mare parte din experții intervievați au apreciat drept fundament adecvat

pentru profesia de analist de intelligence o educație solidă în domenii precum relații internaționale, științe politice, istorie, economie, literatură, jurnalism sau alte discipline umaniste.

În cadrul atelierului dedicat Educației Analiștilor de Intelligence, a reieșit faptul că programele universitare care pregătesc studenții pentru a deveni analiști de intelligence diferă considerabil în ceea ce privește obiectivele și conținuturile învățării. O astfel de stare de fapt prezintă și avantaje, luând în considerare paleta variată de abilități și cunoștințe de care IC are nevoie pentru corpul analitic.

Dincolo de rolul direct în îmbunătățirea eficienței componentei analitice a activității de intelligence, educația și instruirea ar trebui să constituie mecanismele predominante pentru profesionalizarea analiștilor și consolidarea unei culturi a IC. Universitatea Națională de Informații *(National Intelligence University)*, creată de către ODNI la recomandarea Comisiei pentru capabilitățile de informații ale Statelor Unite cu privire la armele de distrugere în masă, a fost considerată instrumentul ideal pentru a coordona toate programele educaționale și de instruire la nivelul IC și armoniza programele specifice agențiilor cu cele oferite de universități.

Pe acest palier, recomandările raportului au inclus: încurajarea a cât mai multor inițiative de instruire la nivelul IC în ansamblu și deschiderea programelor derulate în cadrul agențiilor către analiști din alte agenții; instituirea unui program obligatoriu de inițiere comună pentru toți analiștii IC, în primele șase luni de la angajare, care să includă discipline precum etică și tehnici de informații, având rolul de a induce valori organizaționale comune; dezvoltarea unui sistem educațional și de instruire coordonat la nivelul IC, prin care educația și instruirea să devină etape standard ale carierelor analiștilor; introducerea obligativității parcurgerii unor cursuri de instruire ca și condiție pentru promovare; instituirea unor condiții de educare continuă la nivelul comunității analitice; extinderea la nivelul IC a programului „oficer-in-residence”[14] al CIA, prin care ofițeri ai Agenției sunt

[14] În cadrul programului înființat în anul 1985, având drept obiectiv promovarea unei mai bune înțelegeri a rolului și misiunilor agențiilor de intelligence și consolidarea cooperării cu mediul academic, CIA a sponsorizat prezența anuală a unui număr de 8-12 ofițeri în instituții de învățământ superior, pentru a desfășura activități didactice și de cercetare. Programul a acoperit până în prezent peste 50 de instituții academice civile și militare, printre care Harvard, Princeton, Georgetown etc. Detalii disponibile la https://www.cia.gov/library/center-for-the-study-of-intelligence/academic-relations/ officer-in-residence-program.html.

plasați ca profesori asociați în universități civile, în scopul depistării tinerilor cu abilități analitice şi orientării educației acestora spre zone de interes, care să le faciliteze angajarea în instituție şi evaluarea posibilității utilizării unor cadre didactice universitare pentru a susține cursuri în cadrul Universității Naționale de Informații.

Totodată, s-a propus utilizarea constructivă de către IC a timpului necesar avizării pentru acces la informații clasificate a celor vizați pentru a fi încadrați în poziții analitice prin angrenarea în programe educaționale şi de instruire inițială neclasificate şi extinderea Programului Centre de Excelență Academică în Studii de Securitate Națională al Comunității de Informații (*Intelligence Community Centers of Academic Excellence in National Security Studies Program*, IC CAE).

> Programul menționat a fost inițiat în anul 2005, în conformitate cu Planul Strategic pentru Capitalul Uman *(Strategic Human Capital Plan)* al IC[15], anexă la Strategia Națională de Informații a SUA *(National Intelligence Strategy)*[16], ca răspuns la nevoia în creştere a agențiilor americane de informații de specialişti capabili să promoveze obiective de securitate națională într-un mediu intern şi internațional caracterizat printr-o dinamică accentuată.
>
> IC CAE este divizat în patru componente, având obiective particularizate:
>
> - preuniversitară / liceală – vizează creşterea interesului față de IC şi a procentului de tineri care i-au în considerare o carieră în domeniul intelligence, prin organizarea de colocvii, seminare, vizite de documentare (spre exemplu, la Muzeul Internațional al Spionajului), conferințe, mentorat;
> - universitară – urmăreşte dezvoltarea unui curriculum specific, obținerea expertizei acumulate la nivelul facultăților prin activități sabatice / de cercetare în cadrul consorțiilor, asigurarea de burse în străinătate, sponsorizarea participării studenților la colocvii, conferințe şi seminare locale şi naționale;
> - infrastructură – crearea de centre specializate în cadrul colegiilor / universităților; furnizarea de expertiză;
> - asigurarea de cărți, magazine şi alte materiale cu privire la IC;
> - coordonarea şi evaluarea programului;
> - relaționare – are drept obiectiv stabilirea de linii directoare şi criterii de selecție pentru aplicanți şi susținerea instituțiilor de învățământ /

[15] Disponibil la adresa http://www.fas.org/irp/dni/humancapital.pdf.
[16] Disponibil la adresa http://www.dni.gov/reports/2009_NIS.pdf.

cercetare participante în dezvoltarea curriculum-ului în domeniul securității naționale.

Implementarea strategiilor

Pentru a asigura finalitatea practică a cercetării, raportul „Viitorul analizei de intelligence" a subliniat necesitatea *dezvoltării unor strategii de implementare* a măsurilor de optimizare propuse, atenționând cu privire la posibilitatea întâmpinării unei rezistențe semnificative la nivelul majorității elementelor componente ale IC. Autorii studiului au recunoscut faptul că parte din recomandările formulate au fost identificate şi în cercetări anterioare, fără a fi însă implementate. Pentru a evita repetarea unei astfel de situații, raportul a recomandat dezvoltarea unui mecanism care să exercite o presiune continuă în vederea schimbării, apreciind că recurgerea la o entitate externă care să cuantifice obiectiv progresele înregistrate este mai eficientă decât exercitarea monitorizării de către structuri ale IC.

Dintre recomandările pe acest palier, menționăm: studierea tendințelor generale de evoluție din afara comunității analitice care oferă oportunități de îmbunătățire a procesului analitic; reevaluarea raporturilor dintre ofițerii care culeg informații şi analişti, pentru a identifica modalități suplimentare de îmbunătățire a procesului analitic; investigarea motivelor pentru care inițiativele trecute vizând îmbunătățirea analizei de intelligence nu au fost implementate; continuarea cercetărilor privind cele mai bune practici de angajare şi promovare la nivelul IC.

Concluzii

Evenimentele politice şi sociale neprevăzute şi neaşteptate ale ultimului deceniu, pe de o parte şi impactul dramatic al inovațiilor tehnologice, pe de alta, au schimbat radical conținutul şi metodele cercetării strategice în domeniul intelligence. Analizele şi scenariile consolidate pe parcursul Războiului Rece au devenit, brusc, desuete. Comunitățile de Informații au fost nevoite să îşi redefinească obiectivele şi metodele, pentru a răspunde nevoilor decidenților politici şi îşi menține credibilitatea în percepția publică. Atacurile din data de 11 septembrie 2001 au ridicat serioase întrebări în ceea ce priveşte capacitatea agențiilor de intelligence de a interpreta corect impresionantul volum de informații culese. „Eşecul de intelligence" *(intelligence failure)* a accentuat, imperativ, necesitatea integrării eforturilor analitice şi analizele parțiale ale diferitelor componente

ale IC într-un tablou comprehensiv al ameninţărilor la adresa securităţii naţionale. Drept rezultat, Comunitatea de Informaţii a iniţiat o reexaminare critică a misiunilor şi metodelor, în scopul combaterii reţelelor teroriste transanţionale cu reţele de intelligence transnaţionale.

Intelligence-ul transnaţional prin networking (crearea unei reţele în vederea schimbului de informaţii, experienţă şi bune practici), constituie în prezent o realitate, urmare a dezvoltării accelerate a tehnologiei informaţiilor şi noilor tehnici de integrare a informaţiilor obţinute din surse deschise şi secrete. Pentru a-şi realiza eficient misiunea de prevenire a ameninţărilor la adresa securităţii, agenţiile de intelligence au nevoie de o profesionalizare continuă a capabilităţilor analitice disponibile, de noi instrumente analitice, inovatoare şi de o abordare centrată pe împărtăşirea cunoaşterii şi gândire intuitivă.

Bibliografie

1. Best Richard, „The Director of National Intelligence and Intelligence Analysis", Congressional Research Service, *CRS Issue Brief for Congress*, February 2005.

2. „Creative Strategic Intelligence Analysis and Decision Making Within the Elements of National Power", *Proteus Futures Workshop Hosted by the Center for Strategic Leadership,* United States Army War College, August 14-16, 2007.

3. Davis Jack, „Improving CIA Analytical Performance: Strategic Warning", Sherman Kent Center for Intelligence Analysis, *Occasional Papers*, 1 (1), 2002.

4. Davis Jack, „If Surprise is Inevitable, What Role for Analysis?", Sherman Kent Center for Intelligence Analysis, *Occasional Papers*, 2 (1), 2003.

5. Davis Jack, „Tensions in Analyst-Policymaker Relations: Opinions, Facts, and Evidence", Sherman Center for Intelligence Analysis, *Ocassional Papers*, 2 (2), 2003.

6. Johnson Rob, *Analytic Culture in the US Intelligence Community: An Ethnographic Study.* Washington, DC: Center for the Study of Intelligence, 2005.

7. Hedley John Hollister, „Learning from Intelligence Failures", *International Journal of Intelligence and Counterintelligence*, 18 (3): 435- 450, 2005.

8. Heuer Jr., Richards J., „Limits of Intelligence Analysis". *Orbis* 49 (1): 75-94, 2004.

9. Heuer Jr., J. Richards, *The Psychology of Intelligence Analysis*, Center Washington, DC: U.S. Government Printing Office, 1999.

10. Lahneman J. William, *National Intelligence Agencies and Transnational Threats: The Need for a New Intelligence Paradigm*, Center for International and Security Studies, University of Maryland, College Park, January 27, 2008.

11. Lahneman J. William, *The future of Intelligence Analysis. Final Report*, University of Maryland, March 10, 2006.

12. *New Frontiers of Intelligence Analysis: Shared Threats, Diverse Perspectives, New Communities,* A publication of the Global Futures Partnership of the Sherman Kent School for Intelligence Analysis, Link Campus University of Malta, Gino Germani Center for Comparative Studies of Modernization and Development, Rome, Italy, 31 March - 2 April 2004.

Responsabilizarea socială – soluție a securității societale

Dr. Cristian CIUPERCĂ
Academia Națională de Informații „Mihai Viteazul”
e-mail: **cristiciuperca@yahoo.com**
Conf. univ. dr. Ella Magdalena CIUPERCĂ
Academia Națională de Informații „Mihai Viteazul”
e-mail: **ellaciuperca@yahoo.com**

Abstract

In a post-modern, post-industrial, post capitalist and informational society, to understand the meaning of responsibility is not a philosophical or obsolete action, but a crucial one in a society which should recognize its limited resources. In this paper, I will approach this issue from several perspectives, as responsibility is also present at individual, family, group and societal level. The problem of responsibility is discussed in close connection with the issue of ethics and morality, cooperation and self-sacrifice, social solidarity and so on. Unlike individual and collective responsibilities which are conceptualized, rather, in terms of liability to certain activities undertaken by the group or by an individual, social responsibility is described, especially in terms of obligations of a social group to society.

Further, with the theoretical substantiation of the social responsibility and also of the community dilemma, I will analyse, from a sociological perspective, a dramatic situation which our country is facing: the emigration of medical workers, a human resource, specialised after important individual effort and significant collective investment. Amid a low social responsibility of the authorities, „the medical desertification” of Romania is increasingly obvious and the effects of emigration of medical staff are more and more acute in Romanian social life.

Keywords: individual responsability, social responsability, migration.

Introducere

Anul acesta, în martie, Adunarea Generală a Colegiului Medicilor din România s-a reunit pentru a dezbate o temă de mare actualitate în societatea contemporană: „Responsabilitatea socială şi individuală în sistemul de sănătate românesc". Opțiunea pentru această temă este cu atât mai potrivită cu cât traiectoria vieții medicale în România ultimilor ani este tot mai sinuoasă. Tragedia morții bebeluşilor la Maternitatea Giuleşti este doar unul dintre motivele care au determinat tot mai mulți medici să se raporteze la problematica responsabilității sociale. Referindu-se la această tragedie, şeful Secției Clinice de Obstetrică Ginecologie II „Dominic Stanca" din Cluj Napoca, conf. univ. dr. Dan Mihu, observa că „…este nevoie ca sistemului sanitar să i se acorde mai multă importanță, din toate punctele de vedere. Activitatea care se desfăşoară în sistemul de sănătate are o responsabilitate socială majoră şi se exercită cu mult stres."

Iată doar câteva întemeieri pentru a demara o analiză temeinică pentru problematica responsabilității sociale. De altfel, departe de a fi un efort mai degrabă desuet sau filosofic, înțelegerea semnificației responsabilității are o importanță crucială într-o societate care trebuie să conştientizeze caracterul limitat al resurselor de care dispune şi importanța alegerii comportamentului cel mai eficient în condițiile date.

Discuția referitoare la responsabilitatea socială presupune o abordare interdisciplinară determinată de multidimensionalitatea conceptului şi planurile de reverberație ale acestuia: responsabilitatea este în egală măsură prezentă la nivel individual, familial, grupal şi societal şi este discutată în strânsă legătură cu problematica eticii şi moralei, a cooperării şi a sacrificiului de sine, a solidarității sociale etc.

Semnificația responsabilității individuale şi sociale

În debutul acestui studiu este necesar să diferențiem palierele responsabilității sociale, pentru a decela şi explicita semnificația responsabilității individuale, colective şi sociale.

Conform DEX, responsabilitatea este „obligația de a efectua un lucru, de a răspunde, de a da socoteală de ceva, de a accepta şi suporta consecințele; răspundere; atitudine conştientă, simț de răspundere pentru obligațiile sociale; sarcină, răspundere pe care şi-o asumă cineva" (http://dexonline.ro/definitie/responsabilitate). Definițiile precedente sunt în acord cu Fingarette (1966), care aprecia că responsabilitatea individuală este

emergentă unor situații în care o persoană se comportă „conform moralei", „este responsabilă pentru o acțiune deja petrecută" sau „ce urmează a fi realizată" sau chiar pentru „o gamă întreagă de posibile acțiuni". Pe de altă parte, individul poate să fie „desemnat ca responsabil", „să fie considerat responsabil", „să accepte responsabilitatea" etc.

Diferențierile existente între cele două tipuri de situații sunt evidente: a desemna pe cineva ca responsabil pentru o situație nu echivalează cu asumarea responsabilității şi nici cu acceptarea vinovăției. De multe ori, cazurile de acest tip se înscriu în sfera situațiilor descrise popular prin responsabilitatea acarului Păun. Ion Păun a fost un acar considerat unicul responsabil pentru o ciocnire între două trenuri în 1923 în județul Buzău, soldat cu 66 de morți şi 105 răniți, şi, de atunci, „acarul Păun" este un clişeu echivalat cu „țap ispăşitor" şi desemnează persoana asupra căreia se deviază responsabilitățile altora.

În 1979, Thomas Zenisek observa că semnificația termenului nu este întotdeauna aceeaşi pentru toată lumea. Dacă pentru anumite persoane, responsabilitatea se circumscrie aspectului legal, pentru alții semnifică un comportament corect din punct de vedere etic, iar pentru alții este echivalent cu „a fi responsabil pentru" sau cu „contribuțiile de caritate", cu legitimitatea sau chiar cu datoria fiduciară. Chiar şi antonimele acestor concepte, respectiv „iresponsabilitatea" sau „nonresponsabilitatea" prezintă o multilateralitate de semnificații (Terreberry, 1968, 11-13).

O nuanțare introdusă de specialişti are în vedere caracteristicile persoanelor desemnate ca fiind responsabile sau nu într-o anumită circumstanță. De exemplu, integritatea fizică şi psihologică a unei persoane nu este obligatoriu să coreleze cu responsabilitatea. Managerii unei firme care produce țigări pot intra în această categorie pentru că, în ciuda sănătății acestora, nu îşi asumă responsabilitatea pentru contribuția pe care o au la permanentizarea şi răspândirea pe scară largă a unui viciu atât de nociv.

De obicei, responsabilitatea individuală desemnează o trăsătură de caracter a unei persoane, dar aşa cum, pe bună dreptate, observa Kallen (1942) semnificația conceptului s-a schimbat pe măsură ce societatea însăşi s-a schimbat. Teoriile referitoare la responsabilitatea socială sunt, de obicei, reflexia epocii în care au fost formulate. Deşi pare creat de societatea civilă, conceptul de responsabilitate are rădăcini teologice, fiind discutat adesea în strânsă legătură cu problematica liberului arbitru.

Societatea contemporană, numită postmodernă, postindustrială, postcapitalistă, a cunoaşterii, informaţională ş.a.m.d. are un potenţial de transformare nebănuit care se reflectă în modificări fără precedent în toate domeniile de activitate. Aşa cum afirma Peter Druker (1999), „lumea care va rezulta din prezenta rearanjare a valorilor, credinţelor, structurilor economice şi sociale, a conceptelor şi sistemelor politice, cu alte cuvinte a concepţiilor asupra lumii, va fi diferită de ceea ce şi-ar putea imagina oricine astăzi".

Metamorfoza societăţii poate reprezenta o explicaţie pentru faptul că, în ultimul secol, în sfera responsabilităţii, interesul s-a deplasat de la concepţia individualistă către sfera colectivă sau socială. Ca şi în cazul responsabilităţii personale, noţiunea de responsabilitate colectivă se referă la răspunderea agenţilor morali (colectivi) care au acţionat în sensul deteriorării lumii. Focalizarea interesului către sfera responsabilităţii colective şi a gradului de justeţe în asignarea acesteia se justifică, în mare măsură, prin dorinţa exegeţilor de a răspunde unei întrebări cruciale şi dramatice: este poporul german vinovat şi responsbil pentru atrocităţile regimului hitlerist? Karl Jaspers (1961), Hannah Arendt (1987), H.D. Lewis (1948), Sanford Levinson (1974), Richard Wasserstrom (1971) au fost doar o parte a celor care au discutat, în acest context, problematica responsabilităţii sociale.

Dar preocupările specialiştilor (May, 1987, 1992, McGary, 1986, Friedman, 1980, Appiah, 1987) în această direcţie au fost alimentate şi de alte momente din istorie precum masacrul My Lai în Războiul din Vietnam, pentru cazuri înfricoşătoare întipărite în memoria socială precum uciderea lui Kitty Genovese (o femeie din New York înjunghiată în faţa casei sale, care probabil ar fi fost salvată dacă măcar unul dintre cei aproximativ 40 de vecini care sesizaseră incidentul ar fi sunat la poliţie imediat) sau pentru situaţii specifice rasismului sau sexismului.

Numitorul comun al acestor puncte de vedere au fost preocupările referitoare la justeţea asignării responsabilităţii către grup în întregul său sau către părţi ale acestuia, atunci când daunele sunt produse de un număr limitat dintre membrii săi. Prin urmare, polemicile referitoare la responsabilitatea colectivă au inclus şi dezbateri precum:

- ✓ Este posibil ca grupul, ca şi entitate diferită de membrii săi, să producă vătămări în sensul dictat de morală?
- ✓ Are grupul, ca organism colectiv, intenţii?

✓ Se poate discuta despre responsabilitatea colectivă a unui grup atunci când doar o mică parte a membrilor săi au fost implicați în evenimente neplăcute?

✓ Dacă da, în ce condiții şi cu referire la ce tip de grup? Este corectă asignarea responsabilității colective unui grup asimilat unei juxtapuneri oarecare de indivizi? Unui grup de interes? Unei entități corporatiste?

✓ Dacă se asignează responsabilitatea colectivă în astfel de situații, este tratamentul celorlalți membri corect?

✓ Cum se poate evita responsabilizarea întregului grup şi totodată să fie prevenite evoluțiile asemănătoare în viitor?

Se consideră că acțiunea colectivă este determinată de credințele sau dorințele unui colectiv în întregul său, indiferent dacă acestea sunt valabile sau explicabile pentru fiecare individ în parte (Corlett, 2001, 575), iar responsabilitatea colectivă este pusă în legătură cu comportamentul colectiv.

În general, față de problemele grave, fundamentale ale umanității, precum foametea, conflictele, explozia demografică etc., există percepția că nu pot fi rezolvate de către indivizi singulari. Atunci când se discută de probleme de acest tip, oamenii nu se simt responsabili. Dar, în acelaşi mod în care lipsa de reacție a individului îl face pe acesta parțial responsabil pentru răul produs, la fel inacțiunea colectivă a unui grup de persoane ar trebui să le facă pe persoanele aparținând acelui grup responsabile pentru răul pe care ar fi trebuit să îl prevină. Responsabilizarea membrilor grupului este o primă condiție a formării unor structuri motivate să acționeze colectiv. Alte premise importante ale acelor structuri care acționează colectiv sunt leadershipul, solidaritatea şi comunicarea interpersonală între membri.

O excepție o reprezintă situația membrilor grupului stigmatizat care s-au opus deschis practicilor reprobabile ale comunității (Feinberg, 1968, French, 1998, McGary, 1986, Lucas, 1993, Moody-Adams, 1994).

Spre deosebire de responsabilitatea individuală şi cea colectivă care sunt conceptualizate, mai degrabă, în termenii răspunderii față de anumite activități realizate de către grup sau individ, responsabilitatea socială este descrisă, în special, în termenii obligațiilor pe care un grup social le are față de societate. Ca şi termen specific ştiințelor sociale, responsabilitatea socială are o istorie relativ recentă, dar cu o ascensiune radicală, deşi în literatura domeniului sunt evidențiate poziții, uneori disonante ale specialiştilor.

De exemplu, Neil Chamberlain (1953, 13) definea *responsabilitatea socială* ca fiind caracteristică activităților pe care ne aşteptăm ca liderii

anumitor entități să le întreprindă în situații bine definite. Fiind o consecință a unor activități anterioare, responsabilitatea socială „poate fi satisfăcută doar prin realizarea obligațiilor fiecărui individ în parte, nu de către societate în ansamblul său". Pe de altă parte, responsabilitatea socială este considerată a fi, mai degrabă, apanajul managerilor şi liderilor instituțiilor care pot contribui la binele colectiv, fie acestea guvern, organizații nonprofit, corporații economice sau individ.

Responsabilitatea socială poate fi negativă (atunci când un anumit actor social nu este învinovățit de o anumită vină sau slăbiciune) sau pozitivă (atunci când entitatea respectivă acționează proactiv, în beneficiul colectivității).

Asumarea responsabilității sociale a evidențiat că, în timp, apar numeroase efecte pozitive, atât la nivelul actorului socioeconomic care s-a implicat în respectivele activități, cât şi la nivelul întregii comunități. De exemplu, în țările care valorizează cooperarea şi încrederea între actorii implicați şi în care capitalul uman şi social (capacitatea oamenilor de a lucra împreună pentru scopuri comune şi conexiunile care se formează între aceştia) este considerat o resursă de bază a societății se înregistrează cea mai ridicată prosperitate. Cu toate acestea, oponenții responsabilității sociale consideră că focalizarea asupra acestei probleme conduce la perturbarea atingerii obiectivelor organizaționale principale prin mutarea atenției de la rolul esențial al acestora (Carpenter, Bauer, & Erdogan, 2009).

Dilema comunității şi responsabilitatea socială în domeniul medical. Statistica migrației în domeniul sănătății şi efectele sale

Ecologul Garrett Hardin (1968) a prezentat un scenariu în stil biblic ce ne permite să înțelegem consecințele tragice ale modului în care gândesc şi acționează membrii unei comunități, respectiv indivizii ce beneficiază deopotrivă de resursele de care dispun. Scenariul respectiv se petrece într-un sat ale cărui pășuni pot hrăni 100 de oi. Astfel fiecare păstor ştie câte oi are dreptul să crească. Dar unul dintre aceştia se gândeşte să mai cumpere o oaie fără ştirea celorlalți. Din păcate, toți păstorii gândesc la fel: o oaie cumpărată fără aprobarea celorlalți nu poate modifica prea mult situația – probabil nici nu se va observa. Aşa că, în scurtă vreme, animalele, înmulțite excesiv, ajung să sufere de foame, se îmbolnăvesc şi mor, iar păstorii ajung, cu toții, într-o stare de sărăcie lucie. Astfel, este ilustrată traiectoria modului

în care urmărirea exclusivă a interesului personal se dovedeşte a fi o strategie dezastruoasă.

În literatura psihosociologică această modalitate de comportament a fost denumită tragedia comunității şi constă în tendința de a valorifica resursele comunității în favoarea interesului personal al individului. Juxtapunerea intereselor individuale egoiste conduce la exploatarea extremă a resurselor. Pierderile înregistrate se suprapun, se acumulează, până când este prea târziu şi nu se mai poate face nimic, iar interesele individuale ajung să se întoarcă împotriva comunității, dar şi a individului însuşi.

Este evidentă conexiunea dintre responsabilitate socială şi problematica dilemei comunității. Pedepsirea comportamentelor egoiste, recompensarea celor dezirabile şi reglarea imediată a acestora, comunicarea eficientă între membrii grupului, o educație care să genereze emergența unor norme sociale pozitive sunt câteva dintre modalitățile de prevenire a epuizării resurselor şi de amplificare a responsabilității sociale.

Având ca premisă ideea conform căreia capitalul uman reprezintă cea mai valoroasă resursă a unei comunități, vom analiza în continuare, din perspectivă sociologică, o situație dramatică cu care se confruntă țara noastră: emigrarea personalului medical. Risipa acestei resurse extrem de valoroase, formate în urma a foarte mulți ani de studiu individual şi de investiție colectivă, precum şi uşurința cu care este tratată această problematică trebuie analizată în acord cu fundamentarea anterioară a paradigmelor responsabilității sociale şi a dilemei comunității.

Deşi odată cu accesul în Uniunea Europeană, a fost introdus dreptul bolnavilor de a migra la rândul lor şi de a se trata în oricare dintre țările uniunii, este de presupus că, motive obiective vor bara accesul de masă la astfel de practici. Prin urmare, indiferența cu care este tratată această problemă şi lipsa de responsabilitate socială a autorităților se va răzbuna curând, urmând cadrele delimitate de paradigma dilemei comunității: copii şi nepoții decidenților de astăzi vor fi, cel mai probabil, în imposibilitatea de a se trata în România, vor locui într-un mediu puțin igienic şi vor relaționa cu oameni care pot purta germenii a diferite maladii din vina unor tratamente fie nepotrivite, fie superficiale.

În demersul de înțelegere a mecanismelor care declanşează acest fenomen vom face apel la teoriile care disting între factorii de respingere (push) din țara de origine şi de atracție (pull) în țara țintă a emigrării. În timp ce dorința de a scăpa de sărăcie, de realizare sau a familiei

reprezintă factori de respingere, disponibilitatea slujbelor în țara gazdă poate fi un factor facilitator al migrației. În prezent, abordările teoretice asupra migrației pornesc de la ideea că orice fenomen macrosocial constă, pe fond, în juxtapunerea acțiunilor individuale. Cu alte cuvinte, migrația nu este rezultatul acțiunii colective a unui grup, ci reprezintă suma deciziilor luate de indivizi raționali care au capacitatea de a evalua costurile, beneficiile şi riscurile implicate de un asemenea act şi se informează pentru a lua decizii pertinente din acest punct de vedere. Concomitent, studiile teoretice şi empirice referitoare la migrație abordează problematica efectelor sau consecințelor acesteia, fiind discutat impactul asupra populației de origine, asupra populației de destinație și asupra migranților înşişi.

În domeniul sănătății din țara noastră, cifrele migrației ilustrează o situație tot mai dramatică. Personalul medical din România este tot mai interesat de soluțiile de viață oferite de alte țări. Încă din 2008, migrația medicilor pe țară depăşise 2%, respectiv standardul pe care Organizația Mondială a Sănătății îl echivalează cu un cod roşu în domeniu, iar peste 4% dintre medici (în numărul total de medici fiind incluşi şi absolvenții de medicină care nu profesează) solicitaseră recunoaşterea actelor de studii în vederea emigrării. De altfel, până în prezent au emigrat cca. 15% din numărul total al medicilor din România. În consecință, în România un medic ar trebui să aibă în grijă peste 647 de pacienți, iar o asistentă medicală ar trebui să aibă în grijă peste 200 de persoane (http://www.adevarul.ro/actualitate/eveniment/medici-exod-studiu_0_315568791.html).

Aceste cifre avertizează, în primul rând, asupra posibilității iminente de faliment a sistemului medical, din cauza lipsei de personal. Aşa cum afirma Preşedintele Colegiului Medicilor din România, prof. dr. Vasile Astărăstoaie: „Vom avea unități sanitare cu rol de muzeu, prin care vor trece pacienți ca vizitatori, întrucât nu vor exista persoane calificate care să-i trateze" (http://www.mediafax.ro/social/migratia-medicilor-din-romania-considerata-alarmanta-de-oms-3170525). În 2007, cca. 70% dintre directorii Autorităților de Sănătate Publică din România se plâng de faptul că județele lor se confruntă cu o lipsă de personal din cauza migrației, iar 60% din totalul managerilor unităților sanitare din România recunosc că există probleme din cauza acestui fenomen (www.mediafax.ro). Un studiu recent realizat de Federația „Solidaritatea Sanitară" arată că aproximativ 70% dintre salariații din domeniul medical iau în considerare posibilitatea de a migra pentru muncă, 38 % dintre aceştia fiind hotărâți să muncească

în străinătate. Cei mai mulţi dintre cei care doresc să emigreze sunt profesionişti, au între 30 şi 39 de ani, cu o vechime de peste 10 de ani în specialitate (http://www.adevarul.ro/actualitate/eveniment/medici-exod-studiu_0_315568791.html).

Preşedintele Colegiului Medicilor explica decizia migranţilor astfel: „Calitatea unui sistem depinde de calitatea medicilor care lucrează în el. Printre cauzele migraţiei medicilor români se numără veniturile mici pe care le obţin doctorii, mijloacele mult mai performante pe care le au în unităţile sanitare din străinătate, dar şi poziţia socială a acestora. Dacă în România medicul este privit ca un simplu funcţionar, în străinătate el are cu totul alt statut" (http://www.mediafax.ro/social/migratia-medicilor-din-romania-considerata-alarmanta-de-oms-3170525).

„Desertificarea medicală" cu care încă se confruntă ţări foarte dezvoltate ale Europei de Vest, precum Marea Britanie, Franta, Germania, au determinat autorităţile respective să demareze încă din 2003-2004 o campanie de recrutare în Europa Răsăriteană, inclusiv România, constituind un puternic factor de atracţie către zonele respective. Din punct de vedere material, ofertele făcute medicilor sunt greu de contracarat cu resursele de care dispune ţara noastră. De exemplu, satele din Franţa sunt dispuse să cheltuiască până la 40 000 de euro pentru fiecare medic român adus în regiune, în timp ce Marea Britanie propune unui medic specialist un salariu de aproximativ 2 000 de lire pe săptămână (http://www.sanatateatv.ro/stiri-medicale/astarastoae-legea-salarizarii-unice-va-creste-migratia-medicilor/).

Ipoteza pe care o propun este că mulţi dintre aceştia nu ar fi părăsit ţara dacă ar fi avut asigurat cel puţin un trai decent în România. În mod asemănător, Rectorul Universităţii de Medicină şi Farmacie (UMF) „Iuliu Haţieganu", prof. univ. dr. Constantin Ciuce, consideră că, în ciuda salariilor extrem de ofertante, migraţia medicilor „ar putea fi diminuată dacă ar exista responsabilitate politică faţă de viitorul acestei naţiuni. Pentru aceasta ar trebui să fie create, prioritar, condiţii adecvate de muncă personalului sanitar, să dispară lipsurile din spitale, să fie recâştigată demnitatea profesiei medicale, munca medicilor să fie apreciată corespunzător complexităţii ei şi nu subfinanţată de către CAS, medicii să fie plătiţi corespunzător, iar imaginea lor să nu fie terfelită de neaveniţi." (http://www.paginamedicala.ro/stiri-medicale/Migratia-medicilor-ar-putea-fi-diminuata_8599/).

Comitetul Privat de Medicină Europeană a atras atenția comunității europene că trebuie gândită o altă politică, menită să statueze reguli privitoare la migrația medicilor pe teritoriul Europei, pentru că, altfel, va exista o criză de personal în anumite țări ale Uniunii Europene (http://www.romedic.ro/fenomenul-mondial-al-migratiei-medicilor-devine-ingrijorator-0N1998).

Dar efectele migrației se fac simțite în mai multe sfere ale socialului, iar studierea extensivă a fenomenului este necesară pentru a fundamenta intervenția prin măsuri de responsabilizare socială, politică publică şi strategiile de dezvoltare locală care să combată efectele deja create.

Personalul medical care alege să lucreze în străinătate este preponderent tânăr. Deşi poate să pară patetic, este foarte important să ne gândim la copiii pe care această populație i-ar fi avut. De altfel, ponderea populației tinere cu vârste între 18-40 de ani este de 36% din populația țării, iar în populația care a emigrat legal după 1991 această categorie deține 55%. Între cele două recensăminte, 1992 şi 2002, ponderea populației fertile în totalul migrației a reprezentat 62%. Avem motive să ne gândim la declinul demografic al României şi la îmbătrânirea populației? Statistica răspunde afirmativ.

A gândi soluții pentru rezolvarea problemei forței de muncă pare a fi un demers sisific. În lipsa unor resurse materiale competitive, posibilitățile de suplinire a lipsei forței de muncă nu pot să aibă în vedere decât flexibilizarea pieței muncii, analizarea oportunităților de prelungire a vieții active şi, poate cel mai probabil, transformarea treptată a țării noastre din țară sursă a migrației în țară țintă a acesteia. Construirea unor politici publice care să vizeze atragerea personalului calificat din Republica Moldova, Ucraina sau alte țări din exteriorul UE ar trebui să devină priorități ale agendei factorilor decizionali.

De altfel, şi alte țări au traversat o astfel de situație. Spania, Portugalia, Italia, ulterior țările integrate în UE în 2004, respectiv Slovacia, Polonia, Ungaria, s-au transformat, odată cu creşterea nivelului veniturilor şi a nivelului de trai, din țări sursă ale migrației în țări destinație pentru migrație. Analizele desfăşurate în perioada 1991-1995 asupra a 15 țări europene au demonstrat aportul pe care imigrația l-a avut în producerea de bunăstare pentru țara gazdă, fiecare procent de imigrare în plus reflectându-se în creşterea PIB-ul respectivei societăți cu 1,25% sau cu 1,5% (www.pstalker.com).

Concluzie

În condițiile unei responsabilități sociale scăzute manifestată de autorități față de problematica „desertificării medicale" a României, problema emigrației personalului medical devine din ce în ce mai acută, iar efectele sale sunt tot mai frecvente în spațiul social. Am arătat anterior că scăderea calității corpului medical este cel mai dramatic efect, deoarece tot mai mulți specialiști competenți şi cu experiență sunt atraşi, conform studiilor sociologice, către alte orizonturi. Concomitent, nu poate fi neglijată scăderea numerică a corpului medical, pe fondul problemelor economice. Toate acestea conduc la apariția unor disfuncții dezastruoase pentru pacienți: imposibilitatea fizică de a presta servicii de calitate, lipsa unei expertize de specialitate corespunzătoare, creşterea considerabilă a stresului asociat desfăşurării profesiei, diminuarea motivației. Cazurile de malpraxis (?) sunt tot mai frecvente şi par să nu mai mire prea multe persoane, fiind considerate, mai degrabă, simptome ale unui sistem aflat în moarte clinică din cauza lipsei oxigenului – resursa umană. Pe fondul inexistenței unor politici publice care să rezolve situația creată, însuşi personalul medical alege, în parametrii dilemei comunității, comportamentul egoist, respectiv renunță la responsabilitatea socială caracteristică profesiei, abdică de la rolul comunitar şi aleg drumul îngust al responsabilității individuale şi familiale... sau poate doar supraviețuirea.

Ipoteza pe care o propune acest studiu este că responsabilitatea socială nu poate să apară decât după ce nevoile individuale fundamentale au fost satisfăcute. De aceea migrația personalului medical nu este dependentă de veniturile foarte mari pe care le propun țările dezvoltate, ci de lipsa oricăror mijloace în România. Prin asigurarea unui trai decent, chiar dacă inferior celui din străinătate, se permite activarea mecanismelor responsabilității sociale şi, probabil, migrația în domeniu, s-ar înscrie pe o traiectorie descendentă.

Bibliografie

1. Appiah, A., „Racism and Moral Pollution", *Philosophical Forum*, 18, 1987.

2. Arendt, H. „Collective Responsibility", în J. Bernhauer (ed.), *Amor Mundi*, Dordrecht: M. Nijhoff, 1987.

3. Carpenter, M., Bauer, T. & Erdogan, B., „Principles of Management". Nyack, NY: Flat World Knowledge, 2009.

4. Corlett, J. A., „Collective Moral Responsibility", *Journal of Social Philosophy*, 32, 2001.

5. Drucker, P. F., *Societatea postcapitalistă.* Bucureşti: Editura Image, 1999.

6. Feinberg, J., „Collective Responsibility", *Journal of Philosophy*, 65, 1968.

7. Fingarette, H., „Responsibility", *Mind*, 75 (297), 1966.

8. French, P., „Collective and Corporate Responsibility", New York: Columbia University Press, 1984.

9. Friedman, M. & May L., „Harming Women as a Group", *Social Theory and Practice*, 11, 1985.

10. Hardin, G., „The Tragedy of the Commons", *Science*, 162, 1243-1248, 1968.

11. Jaspers, K., „The Question of German Guilt", New York: Capricorn, 1961.

12. Kallen, H. M., „Source Responsibility", *Ethics*, 52 (3), 1942.

13. Levinson, S., „Responsibility for Crimes of War", în M. Cohen et al., *War and Moral Responsibility*, Princeton: Princeton University Press, 1974.

14. Lewis, H. D., „Collective Responsibility", *Philosophy*, 24, 1948.

15. Lucas, J. R., „Responsibility", Oxford: Clarendon Press, 1993.

16. May, L., „Sharing Responsibility", Chicago: University of Chicago Press, 1992.

17. McGray, H., „Morality and Collective Liability", *Journal of Value Inquiry*, 20, 1986.

18. Moody-Adams, M., „Culture, Responsibility and Affected Ignorance", *Ethics*, 104, 1994.

19. Terreberry, S., „The Evolution of Organizational Environment", *Administrative Science Quarterly*, 12(4), 1968.

20. Wasserstrom, R., „The Relevance of Nuremberg", *Philosophy and Public Affairs*, 1, 1971.

21. Zenisek, T. J., „Source Corporate Social Responsibility: A Conceptualization Based on Organizational Literature", *The Academy of Management Review*, 4 (3), 1979.

Surse online

1. Fundația Soros. *Migrație şi dezvoltare*, activități, metodologie, rezultate. Disponibil la http://www.soros.ro/ro/program_articol.php?articol=54, accesat la 05.11.2008.

2. http://dexonline.ro/definitie/responsabilitate, accesat la 01.10.2010.

3. http://webcache.googleusercontent.com/search?q=cache:35WfQlZNRfUJ:www.cmr.ro/content/blogsection/13/44/+responsabilitate+sociala+spitale+unita

ti+sanitare+medici+spital+%22responsabilitate+sociala%22+-responsabil&cd=9&hl=ro&ct=clnk&gl=ro, accesat la 01.10.2010.

4. http://webcache.googleusercontent.com/search?q=cache:Weky2Q5nzSsJ:www.paginamedicala.ro/stiri-medicale/Deficit-de-personal-la-neonatologia-Spitalului-clujean-_Octavian-Fodor__8790/+responsabilitate+sociala+spitale+unitati+sanitare+medici+spital+%22responsabilitate+sociala%22+-responsabil&cd=1&hl=ro&ct=clnk&gl=ro, accesat la 01.10.2010.

5. http://www.adevarul.ro/actualitate/eveniment/medici-exod-studiu_0_315568791.html, accesat la 05.11.2009.

6. http://www.mediafax.ro/social/migratia-medicilor-din-romania-considerata-alarmanta-de-oms-3170525), accesat la 05.11.2009.

7. http://www.paginamedicala.ro/stiri-medicale/Migratia-medicilor-ar-putea-fi-diminuata_8599/, accesat la 05.11.2009.

8. http://www.responsabilitatesociala.ro/ce-este-csr.html, accesat la 01.10.2010.

9. http://www.romedic.ro/fenomenul-mondial-al-migratiei-medicilor-devine-ingrijorator-0N1998, accesat la 05.11.2009.

10. http://www.sanatateatv.ro/stiri-medicale/astarastoae-legea-salarizarii-unice-va-creste-migratia-medicilor/, accesat la 05.11.2009.

11. http://www.ziaruldebacau.ro/ziarul/2010/08/25/acarul-paun-si-asistenta-florentina.html, accesat la 01.10.2010.

12. Stalkerts Guide to International Migration. Disponibil la http://www.pstalker.com/migration/mg_immig_1.htm, accesat la 05.11.2008.

13. www.mediafax.ro, accesat la 05.11.2009.

Evoluții în domeniul securității naționale. Conceptualizarea şi operaționalizarea rezilienței în societățile cu democrație consolidată

Drd. Gabriela TRANCIUC
Serviciul Român de Informații
e-mail: **gtranciuc@dcti.ro**
Drd. Ionel NIȚU
Serviciul Român de Informații
e-mail: **ionelnitu@sri.ro**

Abstract

Resilience has become a very complex concept, especially when referred to national security. Against the background of dynamic security challenges, consolidated democracies have understood the role of resilient, active institutions and societies and developed strategies and mechanisms to ensure efficient cooperation, response and recovery in crisis situations at the national level. The aim of this paper is to underline the importance of resilience in ensuring national security, by providing an analysis of the origin and evolution of the concept, the approach of different nations to resilience, as well as the role of intelligence analysis and foresight in the implementation of the concept.

Keywords: national security, resilience, intelligence, foresight, strategic analysis

Introducere

Mediul de securitate global se află în continuă transformare. Modalitățile de răspuns la provocările de securitate au cunoscut, de asemenea, evoluții semnificative în ultima decadă. Riscurile contemporane au determinat schimbări ale modelelor de guvernare şi ale conceptului de securitate şi au generat noi idei privind implicarea societății civile în asigurarea securității naționale, fiind astfel introdus conceptul de reziliență. Consolidarea capacității de răspuns şi adaptare în fața riscurilor cronice nu mai reprezintă un apanaj exclusiv al instituțiilor statului, iar comunitatea şi sectorul privat dobândesc un rol primordial în asigurarea rezilienței. Acest concept începe

să fie tot mai des utilizat în discursul factorilor de decizie occidentali şi în studiile de securitate, iar state precum SUA, Canada, Marea Britanie, Israel l-au inclus deja în propriile strategii de securitate ca obiectiv esențial.

Acest articol îşi propune să atragă atenția asupra semnificației rezilienței în cadrul strategiei de securitate națională, pornind de la definiția şi evoluția conceptului şi punând accent pe diferite abordări ale unor democrații consolidate precum SUA şi Marea Britanie. Lucrarea prezintă în final modul în care serviciile de informații pot contribui la implementarea conceptului, prin asigurarea prognozei şi avertizării timpurii asupra riscurilor şi nevoilor de pregătire pentru situații de criză.

Evoluția mediului de securitate şi necesitatea rezilienței

Ultimul deceniu a fost marcat de o frecvență crescută a crizelor în mediul de securitate, cu manifestări în varii domenii, rezultat şi al accentuării competiției între actorii internaționali interesați în maximizarea propriilor poziții în arena mondială, precum şi al multiplicării rolului actorilor nonstatali în influențarea evoluțiilor globale.

Principalelor provocări actuale ale mediului de securitate generate de conflicte, tensiuni regionale, instabilitate, state eşuate, li se adaugă amenințările asimetrice devenite deja tradiționale (terorismul internațional, proliferarea armelor de distrugere în masă, criminalitatea organizată transfrontalieră), a căror principală caracteristică este reprezentată de faptul că nu pot fi evidențiate individual. Granița volatilă şi difuză dintre acestea determină creşterea gradului de relaționare şi interconectare şi generează, implicit, dificultăți de cunoaştere şi anticipare din partea instituțiilor de stat ori a organismelor internaționale, iar ulterior de prevenire şi combatere atât pe dimensiunea internă, cât şi pe cea externă.

Au apărut, de asemenea, noi amenințări precum cele economice, de mediu, cibernetice, schimbările climatice sau cele privind resursele şi infrastructura. Noul model al amenințării este, în general, neconvențional, dinamic, uneori chiar aleatoriu şi neliniar în incidență, fără constrângeri sau reguli de angajare – altfel spus: asimetric. Acesta nu dispune de o doctrină proprie, este dificil de cuantificat şi prognozat şi este susținut de o diversitate de entități. Inamicii de ieri au fost în mod predominant de tip simetric: statici, predictibili, omogeni, ierarhici, rigizi şi rezistenți la schimbare. Duşmanii de astăzi sunt de tipul asimetric: dinamici,

imprevizibili, fluizi, interconectați, auto-organizați, care se adaptează şi evoluează în mod constant[1].

Majoritatea crizelor, conflictelor ori provocărilor de securitate au avut un caracter virulent şi efecte puternice de contagiune ori incidență asupra altor regiuni (de exemplu, declanşarea războiului împotriva terorismului la nivel global, urmare a evenimentelor din 9/11) şi, uneori, au afectat țări ori regiuni care, până la momentul respectiv, se considerau „imune" (de exemplu, actuala criză economico-financiară mondială, care a debutat sub forma unei crizei a creditelor sub-prime în SUA). Totodată, multe din noile provocări au avut drept caracteristică faptul că au apărut în mod surprinzător (de exemplu „criza gazelor", rezultat al diferendului ruso-ucrainean privind prețul de livrare şi tranzitul gazelor prin Ucraina).

Implicit, configurația actuală a mediului de securitate a generat modificări în doctrinele şi activitățile instituțiilor de securitate națională, **reziliența** fiind unul dintre conceptele cele mai dezbătute şi uzitate. Având în vedere că eliminarea surprizelor este imposibilă, guvernele şi alte organizații au nevoie de mecanisme sistematice pentru a-şi consolida capacitatea de a răspunde, cu pierderi minime, unor crize majore şi de a declanşa o reacție rapidă şi eficientă. Reziliența reprezintă răspunsul la dinamismul extrem al lumii.

Originea şi evoluția conceptului

Utilizat în mai multe domenii (medical, tehnic, economic, sociologic), termenul reziliență provine din limba latină, din cuvintele „salire" (a sări) şi „resilire" (a sări înapoi)[2] sau „resalire" (a sări din nou)[3], putând fi definit drept **capacitatea de refacere după un eveniment disruptiv sau revenirea la o stare inițială**.

În fizică, reziliența este conexată capacității materialelor de a-şi reveni la forma şi dimensiunile inițiale: „proprietatea materialelor de a-şi

[1] Schreier Fred, *Transforming Intelligence Services. Making Them Smarter, More Agile, More Effective and More Efficient*, Study Group Information, National Defence Academy and Austrian Ministry of Defence and Sports in cooperation with Geneva Centre for the Democratic Control and Armed Forces, Viena şi Geneva, ianuarie 2010, p.13.

[2] Friborg, O. et al., *Resilience in relation to personality and intelligence*, International Journal of Methods in Psyhiatric Research, 14(1), 2005.

[3] Menon, K. U., *National Resilience: From Bouncing Back to Prevention*, Ethos, Jan-Mar 2005.

recăpăta forma şi dimensiunile după o deformare mecanică."[4] Aplicată sistemelor sociale / comunităților, reziliența se referă la „capacitatea unui sistem de a absorbi perturbațiile şi de a se reorganiza pe măsură ce se derulează schimbarea, astfel încât să-şi păstreze în mod esențial aceleaşi funcțiuni, structură, identitate şi feedbackuri."[5]

Conceptul a fost consacrat în psihologie, începând din anii '50 (conceptul de *ego resiliency* al lui Jack şi Jeanne Block) şi continuând cu studiile privind schizofrenia ale lui Norman Garmezy (anii '70), care au revelat modul în care copii cu părinți schizofrenici au fost capabili să se dezvolte, în ciuda condițiilor potrivnice. Termenul a fost folosit pentru prima dată în anii '70 de psihologul american Emmy Werner pentru a desemna abilitatea pe care au arătat-o indivizii de a se dezvolta cu succes, în medii în care o asemenea evoluție ar fi fost în mod normal puțin probabilă. Conceptul de reziliență a fost popularizat de omul de ştiință francez Boris Cyrulnik în Franța şi larg îmbrățişat de psihiatrii americani, în anii '90.[6] Cercetătorii au încercat să descopere factorii protectori care explică adaptarea la situații adverse, în psihologie, **reziliența fiind înțeleasă ca abilitatea de a face față şi de a se recupera în urma unor evenimente adverse sau abilitatea de a supraviețui şi a se dezvolta în fața adversității şi a schimbării**.

Reziliența poate acționa pe trei paliere fundamentale[7]:

• la nivel individual (ego-reziliența – capacitatea individului de a se adapta în mod adecvat la factorii de stres interni şi externi);

• la nivelul comunității (reziliența comunității, care presupune consolidarea culturii de securitate şi a simțului civic, prin programe integrate);

• la nivel național (reziliența națională – necesită dezvoltarea unor strategii cuprinzătoare coerente, promovarea cooperării transsectoriale şi dezvoltarea parteneriatelor public-private).

---

[4] *Webster's New World Dictionary*, fourth edition, Wiley Publishing, Inc, 2008, Cleveland, Ohio.

[5] Walker B. H. et al., Resilience, adaptability, and transformability in social-ecological systems, Ecology and Society, 9(2), 2004.

[6] http://en.wikipedia.org/wiki/Psychological_resilience (22.10.2010).

[7] Romanoschi C., *Management of Resilience in Terrorism Age*, The 32nd International Scientific Conference „Modern Technologies in the 21st Century", Military Technical Academy, Bucharest, 1-2 November, 2007.

Este important de subliniat că reziliența este diferită de rezistență – încercarea de a preveni şi a opri derularea unor evenimente disruptive. Strategiile de rezistență includ în general măsuri fizice, ca de exemplu împiedicarea teroriştilor de a urca la bordul unei aeronave. Reziliența este un concept mai larg şi presupune inclusiv posibilitatea ca rezistența să nu fie întotdeauna eficientă, asigurând, însă, accesul la resurse alternative.[8]

Conceptul de reziliență a fost preluat relativ recent în studiile de securitate. La începutul anilor '90 termenul era aproape necunoscut, dar evoluția amenințărilor de securitate, în special a celor asimetrice, a condus la conştientizarea necesității pregătirii instituțiilor naționale şi a societății pentru gestionarea situațiilor de criză majore.

Conceptul presupune o abordare comprehensivă, atât din punct de vedere al resurselor, cât şi din punct de vedere strategic. Guvernul nu mai este principalul garant al rezilienței, devine doar un facilitator al acesteia, un rol important revenind comunității. Planificarea urgențelor civile nu se mai bazează exclusiv pe o politică *top-down*, ci îmbină şi dimensiunea *bottom-up*, cu un punct de convergență la mijloc. Societatea, comunitatea sunt principalul referent al securității şi principalul actor. Abordarea locală predomină, în sensul dezvoltării inițiale a unor capabilități la acest nivel prin programe cuprinzătoare şi apoi suplimentarea prin capabilități la nivel guvernamental. Se face trecerea de la guvernarea oamenilor la guvernarea cu oamenii, către aşa numitul „stat relațional", definit drept un sistem de guvernare care întreprinde lucruri cu oameni, în opoziție cu a face lucruri pentru oameni.[9]

Mai multe studii au încercat să dezvolte modele conceptuale ale rezilienței, pornind de la o serie de caracteristici care fundamentează un sistem rezilient eficient. Astfel, pentru a reduce la minim vulnerabilitățile comunității în caz de criză majoră, este sugerată (Godschalk) îndeplinirea următoarelor condiții:

• redundanța: sisteme proiectate cu multiple noduri, pentru a se asigura că, afectarea unei componente a acestuia nu conduce la căderea întregului sistem;

---

[8] Longstaff P. H. et al, *Building Resilient Communities: A Preliminary Framework for Assessment*, Homeland Security Affairs, Volume VI, no 3, September 2010.

[9] Mulgan Geoff, *The Birth of the Relational State*, February 2010, Young Foundation, UK, http://www.youngfoundation.org/policy/tips/the-birth-relational-state (22.10.2010).

• diversitatea: componente ori noduri multiple versus un nod central, pentru a asigura protecția împotriva unei amenințări specifice unui anume amplasament;

• autonomia: capabilitatea de a opera independent, în afara unui control extern;

• forța: puterea de a rezista unei forțe neprevăzute sau unui atac neprevăzut;

• interdependența: sistem integrat de componente, pentru a se susține reciproc;

• adaptabilitatea: capacitatea de a învăța din experiență şi flexibilitatea de face schimbarea necesară;

• colaborarea: oportunități multiple şi avantaje pentru o participare largă a celor interesați.[10]

Longstaff *et al* propune un model de reziliență a comunității bazat pe analiza resurselor disponibile şi a rezistenței, capacității de adaptare în utilizarea acestora. Elementele cheie ale funcționării eficiente a unui sistem de reziliență colectivă includ: eficiența, redundanța (asigurarea unor sisteme paralele) şi diversitatea, alături de memoria instituțională, învățarea inovativă şi interconectare.

Inexistența unui model agreat privind implementarea conceptului de reziliență a permis fiecărui stat dezvoltarea propriului mecanism pentru gestionarea situațiilor de criză, pe baza unor priorități particularizate la specificul amenințărilor securitare şi în funcție de resursele disponibile.

Abordări naționale privind conceptul de reziliență

Terorismul a constituit principalul factor declanşator al implementării conceptului de reziliență în cadrul eforturilor mai largi de prevenire şi contracarare a amenințărilor asimetrice. După atacurile teroriste din SUA (2001) şi Anglia (2005), conceptul a devenit o componentă esențială a strategiilor de securitate națională ale acestor state. De asemenea, Israelul, prin natura amenințărilor la adresa securității sale, Canada şi, recent, statele din Asia de Sud-Est (Singapore) promovează conceptul la nivel național şi în cadrul cooperării internaționale.

[10] http://www.adpc.net/v2007/Programs/EWS/CCR/downloads/CCRConceptsandPracticesofResilience.pdf (23.10.2010).

Atenția va fi concentrată în special asupra SUA şi Marii Britanii, care au dezvoltat sisteme instituționale complexe pentru implementarea conceptului de reziliență, dar care au avut abordări diferite din punct de vedere strategic. În ambele cazuri, reziliența este abordată holistic, având ca scop asigurarea securității naționale cu toate mijloacele disponibile şi prin implicarea întregii societăți, inclusiv a mediului academic şi a sectorului privat.

SUA, în urma evenimentelor din 11 septembrie 2001, au promovat o politică concentrată pe securitatea internă/securitatea cetățenilor, urmând o abordare bazată pe modificări strategic conceptuale, dar şi pe schimbări instituționale. Astfel, pe 1 martie 2003, a fost înființat *Department of Homeland Security*, reunind 22 de agenții guvernamentale şi aproximativ 180.000 de angajați. De asemenea, au fost create structuri cu misiuni relevante pentru reziliență, precum: *Homeland Security Advisory System* – pentru a disemina informația privind riscul de atac terorist; *Citizen Corps* – pentru a consolida capacitatea de răspuns a comunității prin educație, pregătire şi voluntariat.

Schimbările structurale au fost dublate de consolidarea cadrului strategic. *The National Strategy for Homeland Security*, actualizată ulterior, promova ideea că protejarea națiunii nu se poate baza exclusiv pe resursele publice, ci pe eforturile tuturor americanilor. Strategia includea considerații strategice privind cooperarea între guvenul federal, state, sectorul privat şi cetățeni în anticiparea atacurilor teroriste sau a dezastrelor naturale cu impact major. Pe baza strategiei, a fost dezvoltat un sistem complex *(the National Response Framework)* de pregătire şi răspuns la crize, cu planuri şi măsuri detaliate până la cel mai jos nivel local.[11] Participarea şi responsabilizarea reprezintă cele două direcții de acțiune principale urmărite pentru îmbunătățirea rezilienței.

Semnificația conceptului de reziliență națională este evidențiată şi de noua strategie de securitate a SUA (mai 2010), în care aceasta reprezintă o componentă fundamentală. Este considerată prima strategie de securitate a SUA care integrează conceptul de securitate internă[12]. Reziliența este definită ca „abilitatea de a se adapta la condiții în schimbare, de a se pregăti

[11] http://www.dhs.gov/index.shtm (23.10.2010).

[12] Brennan John, *Securing the Homeland by Renewing American Strength, Resilience and Values*, Remarks by Assistant to the President for Homeland Security and Counterterrorism at CSIS, May 26, 2010, http://www.whitehouse.gov/the-press-office/remarks-assistant-president-homeland-security-and-counterterrorism-john-brennan-csi (23.10.2010).

pentru, a rezista şi a se replia rapid în situaţii de criză" şi este plasată în cadrul primului obiectiv de securitate – „strengthen security and resilience at home". Implementarea acestui obiectiv de securitate presupune planificarea şi construirea unor capabilităţi cheie pentru situaţii de urgenţă, la nivel guvernamental şi regional, dezvoltarea unor programe de pregătire integrate, parteneriate public-private pentru asigurarea unor capabilităţi critice de rezervă *(redundant systems)*, informarea publică asupra riscurilor şi situaţiilor de urgenţă.[13]

În viziunea *Department of Homeland Security*, conform documentului strategic *Quadrennial Homeland Security Review 2010*, reziliența reprezintă un concept cuprinzător care integrează managementul riscului şi include serviciile de informaţii, guvernul, ONG, zona privată, academică şi cetăţenii. Reziliența este înțeleasă ca abilitatea de a rezista, a se replia sau de a se adapta cu succes la ameninţări ori la schimbări.[14]

În opinia unui reprezentant al departamentului american de securitate internă[15] prezent la o conferinţă internaţională, în SUA, *homeland security* începe cu *hometown security*. O societatea activă în prevenirea riscurilor şi gestionarea crizelor este o societate „reziliantă". În SUA, cetăţenii conştientizează mai mult riscurile care-i vizează personal, ca indivizi, nu ca societate (spre exemplu, problematica utilizării armelor de foc sau cea a accidentelor auto). Trebuie investit mult în pregătirea populaţiei, similar perioadei din cel de-al Doilea Război Mondial, când au fost derulate multiple campanii publicitare sau de informare, cu diferenţa că oamenii trebuie învăţaţi nu ce să facă în anumite situaţii, ci de ce să se ferească.

Reziliența reprezintă, de asemenea, capacitatea de coordonare a răspunsurilor, capacitatea de interconectare (pentru a oferi un răspuns adecvat), respectiv capacitatea de a înțelege un risc şi de a răspunde. Există şi reziliență activă – care ar însemna nu doar să înțelegi, să te adaptezi, ci să te opui în mod activ răului.

Marea Britanie promovează, de asemenea, o abordare cuprinzătoare a conceptului de reziliență. Spre deosebire de SUA, care a creat o nouă structură pentru gestionarea situaţiilor de urgenţă pe teritoriul

[13] http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf (23.10.2010).
[14] *Quadrennial Homeland Security Review*, US Department of Homeland Security, February 2010, www.dhs.gov/xabout/gc_1208534155450.shtm (24.10.2010).
[15] Conform regulii Chatham House, identitatea acestuia nu poate fi dezvăluită.

național, Marea Britanie a preferat consolidarea conceptuală în cadrul instituțional deja existent (UK Cabinet Office, Home Office). După 11 septembrie, guvernul a promovat o strategie de combatere a terorismului – CONTEST, construită pe două cuvinte cheie „protect" şi „prepare". În zona de acțiune al celui de al doilea termen: „prepare" se dezvoltă două concepte importante: „civil contingency" şi „resilience". În această țară, „reziliența" a fost instituționalizată, devenind o adevărată componentă a sistemului de protecție antiterorism: „termenul *reziliență* a fost ales pentru a indica necesitatea unei capacități extinse de infrastructură, flexibilă şi diseminată, pentru a absorbi perturbațiile într-o manieră reglementată, distinctă şi complementară *managementului situațiilor de urgență*, reactiv, ocazional şi sub control centralizat, ca şi activităților tradiționale ale structurilor de informații şi securitate".[16]

Conceptul de reziliență a fost preluat în ultima strategie de securitate națională (octombrie 2010), care extinde paleta riscurilor de securitate națională de la cele teroriste la atacuri cibernetice, agresiuni militare, dezastre naturale sau provocate. Vechiul concept al managementului de risc este de asemenea consolidat, prin adăugarea unei componente esențiale: implicarea cetățenilor. Este clar evidențiată ideea că asigurarea securității nu este doar obligația administrației centrale, ci a societății ca întreg. Primul obiectiv major al strategiei de securitate britanică este asigurarea securității şi rezilienței UK („ensuring a secure and resilient UK"), iar pe parcursul documentului este accentuată importanța rezilienței naționale („place greater emphasis on domestic resilience") în contextul unui climat global de securitate dinamic.[17] Este subliniat faptul că nu toate riscurile pot fi prevenite, dar pentru a răspunde acestora este necesară consolidarea rezilienței la nivel național şi local.

> „To ensure that we are able to recover quickly when risks turn into actual damage to our interests, we have to promote resilience, both locally and nationally. Ensuring that the public is fully informed of the risks we face is a critical part of this approach. To support national and local

[16] Cornish, Paul, *Domestic Security, Civil Contigencies and Resilience in the United Kingdom*, Chatham House, June 2007, http://www.chathamhouse.org.uk/files/9380_0607ukresilience.pdf (24.10.2010).

[17] *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, October 2010, http://www.cabinetoffice.gov.uk/newsroom/news_releases/2010/101018-national-security-strategy.aspx (24.10.2010).

> resilience, we will continue to publish a National Risk Register which sets out the more immediate risks of civil emergencies occurring in the UK." (*A Strong Britain in an Age of Uncertainty:The National Security Strategy*, p. 25)

O atenție deosebită este acordată cooperării intersectoriale şi rezilienței la nivelul comunității. În scopul îmbunătățirii capacității locale de a răspunde la situații de urgență, la nivel guvernamental a fost elaborat *National Risk Register of Civil Emergencies*, care include un capitol dedicat riscurilor (cu puncte de contact ale instituțiilor responsabile de gestionarea acestora) şi o secțiune cu direcții de acțiune pentru familii, comunitate, organizații (cu accent pe *business continuity management*).[18] De asemenea, sunt dezvoltate planuri locale (există un *Community Risk Register*), forumuri de reziliență pentru cooperarea inter-agenții şi schimbul de informații la nivel local.

Astfel, viziunea Marii Britanii asupra rezilienței porneşte de la o strategie de management al riscului care să furnizeze cea mai bună abordare în vederea luării deciziilor referitoare la investițiile necesare privind capacitatea de rezistență în condițiile unor resurse limitate şi este bazată pe prioritizarea riscurilor conform probabilității materializării lor şi a impactului la nivel național. Sunt vizate investiții prioritare în capabilități pentru prevenire, pregătire, răspuns şi refacere, care sunt cele mai eficiente în reducerea riscurilor. Este adoptată o abordare cuprinzătoare privind „toate riscurile" evitând duplicarea şi separarea, prin realizarea unor diferențe artificiale între capacitățile privind dezastrele provocate intenționat (fie urmare a terorismului, fie a altor infracțiuni grave) şi capabilitățile în caz de dezastre provocate de fenomene naturale. Dimensiunea ascendentă în sensul dezvoltării inițiale a unor capabilități locale şi apoi suplimentarea, prin capabilități la nivel guvernamental este încurajată, în acelaşi timp cu promovarea cooperării în echipe de lucru, în măsura posibilului, în toate sectoarele – public, privat, voluntar şi comunitar, şi la toate nivelurile – local, sub-național, național şi internațional, precum şi intensificarea împărtăşirii informației, inclusiv o creştere a numărului informațiilor disponibile public privind riscurile. Alături de accentul pus pe reziliența comunității, mediul de afaceri este susținut. O atenție sporită este acordată capacității de rezistență a infrastructurii critice naționale, îmbunătățirii

[18] *National Risk Register of Civil Emergencies*, 2010 edition, UK Cabinet Office, http://www.cabinetoffice.gov.uk/media/348986/nationalriskregister-2010.pdf (24.10.2010).

capacității autorităților locale de răspuns, dezvoltării şi menținerii capacității generice de a soluționa o diversitate de evenimente, consolidării programelor de activitate privind riscurile interne cele mai importante.

Sintetizând, modelul complex dezvoltat de Marea Britanie este fundamentat pe îmbinarea a trei planuri:

• îmbunătățirea managementului crizei şi a structurilor de planificare la nivel local, regional şi național, incluzând avertizări pe termen scurt, evaluări pe termen mediu-lung asupra riscurilor şi a comunicării riscurilor;

• relații de cooperare transsectorială şi acorduri cu partenerii externi şi agențiile internaționale interguvernamentale;

• mecanisme de evaluare a progreselor şi reacției.

Rolul intelligence – prognoza şi avertizarea strategică

Reziliența reprezintă un concept cuprinzător, care nu trebuie să excludă rolul serviciilor informații, în special modul în care analiza strategică poate contribui la consolidarea capacității unui stat de a răspunde provocărilor de securitate şi de a asigura o reacție rapidă şi eficientă la nivelul instituțiilor de stat şi al cetățenilor.

O funcție importantă a activității de intelligence este aceea de a avertiza din timp cu privire la tendințele de manifestare ale unor amenințări şi factori de risc la adresa securității naționale, în scopul de a reduce efectul de surpriză (de a elimina starea de incertitudine), respectiv de a sprijini fundamentarea unor decizii, politici şi strategii preventive sau de acțiune postfactum[19]. Modul în care este îndeplinită această funcție reprezintă un indicator relevant de evaluare a performanței serviciilor de informații.

Analiza de intelligence nu poate previziona, însă, cu exactitate toate scenariile viitorului. Sursele incertitudinii sunt variate, acestea derivând din nesiguranța „naturală" (incertitudinea inerentă), determinată de posibilitatea apariției unor fenomene nondeterminate (aleatorii); existența unor „goluri de cunoaştere" asupra țintei vizate (incertitudinea epistemică); operațiuni de manipulare şi dezinformare inițiate de alte state ori servicii de informații străine (incertitudinea indusă).

Dacă acestea sunt câteva din sursele incertitudinii, demersul de a realiza avertizări şi analize predictive este cu atât mai dificil, pentru

[19] Lowenthal, Mark, *Intelligence. From Secrets to Policy,* Second edition, A division of Congressional Quarterly Inc. Washington, D.C.

că majoritatea sistemelor dinamice din mediul de securitate (intern şi extern) se caracterizează prin nonlinearitate (relaţiile cauză-efect nefiind proporţionale).

La toate acestea se adaugă limitele şi constrângerile inerente oricărui proces de analiză / prognoză, care sunt de multe tipuri, de la cele de ordin psihologic, cultural ori lingvistic, la cele date de integrarea dificilă a fluxurilor mari de date.

Dificultatea de a prevedea schimbările nonlineare *(black swan*[20]*)* este dublată de faptul că procesarea şi interpretarea informaţiilor este inevitabil afectată de limitele cognitive şi mentale ale furnizorilor produselor informaţionale. Astfel, utilizarea de tipare mentale[21] pentru a „transporta" elementele de noutate în zona familiarului / inteligibilului poate să contribuie substanţial la alcătuirea unei reprezentări distorsionate asupra lumii exterioare, în timp ce natura imperfectă a memoriei şi capacităţii cognitive umane ar putea determina întârzieri de acţiune şi, implicit, pierderea unei oportunităţi în context strategic[22].

Pe de altă parte, limitele cognitive individuale sunt replicate şi întărite în contextul instituţional specific domeniului *intelligence*. Astfel, trasarea unor direcţii (priorităţi informative) de colectare a informaţiilor necesită o anumită „viziune" asupra a ceea ce trebuie căutat, iar principiul compartimentării forţează analiştii să formuleze predicţii pe baza unor informaţii reduse, în comparaţie cu cele existente la nivelul întregii organizaţii[23].

După cum observă Heuer, analiştii – după cum fac şi politicienii – percep lumea printr-o „lentilă" sau un „ecran" care canalizează şi

[20] Conceptul, avansat în literatura de specialitate de Nassim Taleb, desemnează acele evenimente care apar în mod neaşteptat, care au un impact foarte mare şi care depăşesc aşteptările normale. Pentru Taleb, evenimentele din 9/11 sunt un exemplu elocvent de *black swan* („lebădă neagră").

[21] Herbert Simon a introdus în literatura de specialitate conceptul de „raţionare limitată" (*bounded rationality*), ca expresie a capacităţii reduse a minţii umane de a asimila complexitatea realităţii, respectiv a tendinţei oamenilor de a-şi construi modele mentale simplificate ale realităţii, cărora le suprapun informaţiile primite ulterior, fără să le verifice întotdeauna compatibilitatea cu propriul sistem de gândire.

[22] Freedman, Lawrence, *The Revolution in Strategic Affairs*, Adelphi Paper, nr. 318/1998, International Institute for Strategic Studies, London.

[23] Fruhling, Stephan, Uncertainty, Forecasting and the Difficulty of Strategy, Taylor & Francis Group, 2006.

focalizează şi, prin urmare, poate distorsiona imaginile văzute[24]. Alţii autori (precum Roger George) avertizează că „în timp ce concepţiile pot fi de ajutor în selectarea datelor obţinute, ele devin călcâiul lui Ahile pentru strategii profesionişti sau analiştii serviciilor de informaţii, atunci când nu mai corespund cu noile dinamici internaţionale. Capacitatea de a realiza când o concepţie devine învechită şi are nevoie de revizuire poate reprezenta un test pentru orgoliul celui mai bun expert."[25]

Multe dintre convingerile analiştilor şi ale beneficiarilor sunt influenţate de stereotipuri şi prejudecăţi. Nu de puţine ori, percepţiile acestora sunt alimentate de discuţiile de grup şi influenţele sociale, ajungând să se conformeze gândirii generale sau „gândirii de grup" (aşa cum a fost definită de Janis).[26]

Cu toate acestea, instituţiile componente ale sistemului de securitate trebuie să fie capabile să evalueze corect probabilitatea şi impactul diferitelor evenimente sau fenomene şi să aprecieze în mod adecvat modalităţile de răspuns.

Din această perspectivă, componenta analitică a procesului de intelligence (incluzând în acest concept şi funcţia de avertizare şi prognoză) a traversat o perioadă de continuă transformare şi adaptare de paradigmă. Multiplicarea în progresie geometrică a datelor şi accesul tot mai mare şi în timp real la informaţii au contribuit la consolidarea importanţei analizei de intelligence în procesul de fundamentare a politicilor unui stat, respectiv de valorificare a oportunităţilor de realizare a unor interese de securitate naţională.

Analiza de intelligence a devenit un factor determinant în obţinerea de avantaje în domeniul securităţii naţionale, în raport cu alţi competitori. În acest sens, esenţiale au devenit comprimarea timpului de reacţie, respectiv de prelucrare a datelor, astfel încât produsul de intelligence să fie disponibil la timp pentru a fi util în fundamentarea unor politici ori strategii naţionale pe termen mediu şi lung. Alte variabile sunt: capacitatea de interpretare /

---

[24]Heuer, Richards Jr., *Psychology of Intelligence Analysis*, Washington D.C., Central Intelligence Agency for the Study of Intelligence, 1999, http://www.cia.gov./csi/books/19104.

[25] Apud Russell, L. Richard, Competitive Analysis: Techniques for Better Gauging Enemy Political Intentions and Military Capabilities, în Jonson K. Loch (ed.), The Oxford Handbook of National Security Intelligence, Oxford, University Press, 2010, pp. 375 – 388.

[26] Janis, Irving, Victims of groupthink; a psyhological study of foreign-policy decisions and fiascoes, Boston, Houghton, Mifflin, 1972.

integrare a datelor cu accent pe analiza multisursă şi abordarea multidisciplinară a problemelor de interes strategic, precum şi forma corespunzătoare a produselor informative prin utilizarea oportună a unor metode şi tehnici analitice în varii situaţii, astfel încât să fie eliminate situaţiile în care analiza eşuează din cauza limitelor inerente subiectivităţii factorului uman implicat în procesul analitic.

Clark susţine că manifestările oricărui sistem pot fi anticipate prin analiza fenomenelor sale convergente (care determină existenţa unei predicţii) şi care sunt guvernate de legea cauză-efect, dar şi a fenomenelor divergente (care inhibă predicţia). Potrivit acestuia, formularea corectă a predicţiei este condiţionată de identificarea forţelor care acţionează asupra unei entităţi, atât în prezent cât şi estimativ, de previzionarea schimbărilor survenite în acestea de-a lungul timpului, respectiv de suficienţa argumentării în formularea opiniei.[27]

Necesitatea de a elimina incertitudinea caracteristică domeniului *intelligence* a impus (la nivel teoretic şi în plan acţional) dezvoltarea unor modele capabile să avertizeze cu privire la posibilitatea producerii unor evenimente cu impact major asupra stării de securitate în plan intern sau internaţional.

Reducerea stării de incertitudine (inerentă sau epistemică) prin intermediul prognozei este condiţionată de identificarea factorilor cheie[28] care acţionează asupra problemei vizate (componentele spaţială şi temporală; mecanismele declanşatoare; modalităţile şi formele de manifestare; factori favorizanţi ori inhibatori; probabilitatea de apariţie / manifestare; potenţialul impact asupra securităţii naţionale etc.), cu ajutorul cărora sunt formulate proiecţii / scenarii de evoluţie şi sunt trasate modalităţi de contracarare a posibilelor efecte[29]. În esenţă, obiectivul prognozei este acela de a fundamenta adoptarea, în prezent, a acelor decizii capabile să prevină materializarea evoluţiei indezirabile a unor factori de risc, în viitor.

---

[27] Clark, M. Robert, *Intelligence Analysis: A Target – Centric Approach,* CQ Press, Washington D.C., 2007, p.184.

[28] Analistul american Jack Davis denumeşte factorii identificaţi ca fiind *„premise de influenţă în activitatea de informaţii”*, având un rol important în structurarea unor relaţii de tipul cauză-efect care să determine probabilitatea de manifestare a unui scenariu previzionat (Davis, Jack, *Strategic Warning: If Surprise is inevitable, What Role for Analysis*, Sherman Kent Center for Intelligence Analysis, Occasional, Papers, Vol. 2, No. 1/2003).

[29] Davis, Jack, *Strategic Warning: If Surprise is inevitable, What Role for Analysis*, Sherman Kent Center for Intelligence Analysis, Occasional, Papers, Vol. 2, No. 1/2003.

În pofida limitelor şi constrângerilor analitice, având în vedere că eliminarea surprizei este imposibilă, guvernele şi alte organizaţii au nevoie de mecanisme sistematice şi de încredere în vederea identificării oportunităţilor şi provocărilor existente, anticipării apariţiei lor, evaluării obiective şi prioritizării acestora, comunicării efective cu liderii şi alţi factori de decizie, monitorizării atente a problemelor critice persistente. Prin abordarea cuprinzătoare a fiecăruia dintre aceste domenii, este posibilă dezvoltarea evaluării de risc şi a capacităţilor de avertizare care vor limita incertitudinea, creşterea rezilienţei şi a flexibilităţii, ceea ce va ajuta liderii şi organizaţiile să gestioneze schimbările strategice. Rolul intelligence-ului este evident în acest sens, activitatea serviciilor constituind o capabilitate complementară în capacitatea naţională de consolidare a rezilienţei în faţa şocurilor viitorului. Intelligence-ul devine o componentă esenţială a parteneriatului cu societatea în asigurarea securităţii naţionale.

Concluzii

Reziliența prezintă relevanță în domeniul securității naționale, în special din perspectiva asigurării capacității de a trăi cât mai normal sub amenințare, gândind în avans soluții de repliere şi construind sisteme care pot să-şi păstreze funcționalitatea în condiții adverse.

În pofida progresului semnificativ, cercetările care au ca obiect „reziliența" sunt, totuşi, doar la început. Pe măsură ce apar noi inițiative şi se finalizează noi proiecte, se detaşează cu pregnanță şi unele limite ale acestora: ambiguitate în definiții şi în terminologia folosită, ceea ce îngreunează înțelegerea şi operaționalizarea acestora, precum şi în evaluarea şi valorificarea rezultatelor, eterogenitate în ceea ce priveşte experiența riscului şi competențele indivizilor considerați rezilienți, utilitatea conceptului teoretic, lipsa unui model de aplicare la diferite niveluri etc.

Cu toate acestea, reziliența rămâne un concept esențial în asigurarea securității naționale, în special pe componenta combaterii riscurilor asimetrice imprevizibile transnaționale, precum terorismul, proliferarea armelor de distrugere în masă etc., a riscurilor provocate sau non-artificiale (dezastre naturale, pandemii etc.).

Preocupările de conceptualizare şi operaționalizare a rezilienței lipsesc, din păcate, în România, atât la nivel guvernamental (central şi local), cât şi în mediul academic sau în cadrul comunității. Abordările statelor cu democrație consolidată, precum SUA şi Marea Britanie, pot

reprezenta modelele de urmat, particularizând implementarea conceptului de reziliență la specificul național. O condiție esențială pentru acest demers o va reprezenta, însă, consolidarea culturii de securitate şi a simțului civic, iar dezvoltarea unor programe coerente în acest sens va contribui fundamental la avansarea unui concept de reziliență cuprinzător, care să se bazeze pe un parteneriat solid, de încredere, între guvern, servicii de informații, mediul academic, sectorul privat, comunitățile locale.

Bibliografie

1. Brennan John, *Securing the Homeland by Renewing American Strength, Resilience and Values*, Remarks by Assistant to the President for Homeland Security and Counterterrorism at CSIS, May 26, 2010, http://www.whitehouse.gov/the-press-office/remarks-assistant-president-homeland-security-and-counterterrorism-john-brennan-csi (23.10.2010).

2. Clark M. Robert, *Intelligence Analysis: A Target- Centric Approach,* CQ Press, Washington D.C., 2007.

3. Cornish Paul, *Domestic Security, Civil Contigencies and Resilience in the United Kingdom*, Chatham House, June 2007, http://www. chathamhouse.org.uk/files/9380_0607ukresilience.pdf (24.10.2010).

4. Davis Jack, *Strategic Warning: If Surprise is inevitable, What Role for Analysis*, Sherman Kent Center for Intelligence Analysis, Occasional, Papers, Vol. 2, No. 1/2003.

5. Freedman Lawrence, *The Revolution in Strategic Affairs*, Adelphi Paper, nr.318/1998, International Institute for Strategic Studies, London.

6. Friborg O. et al., *Resilience in relation to personality and intelligence*, International Journal of Methods in Psyhiatric Research, 14(1), 2005.

7. Fruhling Stephan, *Uncertainty, Forecasting and the Difficulty of Strategy*, Taylor & Francis Group, 2006.

8. Heuer Richards Jr., *Psychology of Intelligence Analysis*, Washington D.C., Central Intelligence Agency for the Study of Intelligence, 1999, http://www.cia.gov./csi/books/19104.

9. Janis Irving, *Victims of groupthink; a psyhological study of foreign-policy decisions and fiascoes*, Boston, Houghton, Mifflin, 1972.

10. Longstaff P. H. et al, *Building Resilient Communities: A Preliminary Framework for Assessment*, Homeland Security Affairs, Volume VI, no 3, September 2010.

11. Lowenthal Mark, *Intelligence. From Secrets to Policy*, Second edition, A division of Congressional Quarterly Inc. Washington, D.C.

12. Menon K. U., *National Resilience: From Bouncing Back to Prevention*, Ethos, Jan-Mar 2005.

13. Mulgan Geoff, *The Birth of the Relational State*, February 2010, Young Foundation, UK, http://www.youngfoundation.org/policy/tips/the-birth-relational-state (22.10.2010).

14. Romanoschi C., *Management of Resilience in Terrorism Age*, The 32nd International Scientific Conference „Modern Technologies in the 21st Century", Military Technical Academy, Bucharest, 1-2 November, 2007.

15. Russell, L. Richard, *Competitive Analysis: Techniques for Better Gauging Enemy Political Intentions and Military Capabilities*, în Jonson K. Loch (ed.), The Oxford Handbook of National Security Intelligence, Oxford, University Press, 2010.

16. Schreier Fred, *Transforming Intelligence Services. Making Them Smarter, More Agile, More Effective and More Efficient*, Study Group Information, National Defence Academy and Austrian Ministry of Defence and Sports in cooperation with Geneva Centre for the Democratic Control and Armed Forces, Viena şi Geneva, ianuarie 2010, p. 13.

17. Walker B. H. et al., *Resilience, adaptability, and transformability in social-ecological systems*, Ecology and Society, 9(2), 2004.

18. *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, October 2010, http://www.cabinetoffice.gov.uk/newsroom/news_releases/2010/101018-national-security-strategy.aspx (24.10.2010).

19. *National Risk Register of Civil Emergencies*, 2010 edition, UK Cabinet Office, http://www.cabinetoffice.gov.uk/media/348986/nationalriskregister-2010.pdf (24.10.2010).

20. *Quadrennial Homeland Security Review*, US Department of Homeland Security, February 2010, www.dhs.gov/xabout/gc_1208534155450.shtm (24.10.2010).

21. *Webster's New World Dictionary*, fourth edition, Wiley Publishing, Inc, 2008, Cleveland, Ohio.

22. http://en.wikipedia.org/wiki/Psychological_resilience (22.10.2010).

23. http://www.adpc.net/v2007/Programs/EWS/CCR/downloads/ CCR ConceptsandPracticesofResilience.pdf (23.10.2010).

24. http://www.dhs.gov/index.shtm (23.10.2010).
http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf (23.10.2010).

Securitate şi dezvoltare durabilă – Informaţii strategice privind mediul înconjurător (II) –

Ana Ligia LEAUA
Serviciul Român de Informaţii
e-mail: **analigialeaua@yahoo.com**

Abstract

The research on environment and security, while limited, has brought attention to the growing salience of non-conventional security threats. It has also stimulated discussion on issues of environment and human security. It appears that this latter discussion may provide a useful framework within which to address development issues, particularly since it recognises that environmental problems must be analysed from a broad perspective that encompasses economic, political, cultural and demographic systems. It, thus, emphasises the extent to which understanding the context is crucial to successful development and security strategies. Undertaking research on the role that environmental degradation plays in contributing to insecurity also assists in clarifying what other factors may be important contributors to insecurity and conflict. For example, research on environment and security often strengthens the conclusion that poverty is a key factor in causing tension, unrest and, eventually, conflict. In short, linking environmental change to a broad concept of security is a useful and insightful approach to many contemporary problems.

Keywords: Environment, human security and sustainable development, environment and conflict, environmental security, environmental and security risk, environmental security policies.

SECURITATEA MEDIULUI ŞI INTELLIGENCE STRATEGIC

Într-un sens foarte general, statul asigură securitatea prin adoptarea şi aplicarea legilor, redistribuirea resurselor, asigurarea bunurilor publice, susţinerea serviciilor militare şi de informaţii şi încheierea de alianţe strategice. În baza acestei concepţii a statului, două tipuri de întrebări au apărut în literatura de specialitate privind securitatea mediului. Prima

întrebare, „Este necesară integrarea preocupărilor legate de mediu în activitățile instituțiilor militare şi de informații, şi dacă da, cum?, s-a bucurat de o atenție specială în SUA şi în unele state europene. Cea de-a doua întrebare se axează, deseori, pe presupusele vulnerabilități cu care se confruntă state aflate în curs de dezvoltare: „Cum se poate şi cum ar trebui structurată capacitatea statului, astfel încât problemele legate de securitatea mediului să fie soluționate eficient?".

Lipsa de alimente, apă şi energie pot avea un impact dur şi catastrofal asupra securității statelor. Cu toate acestea, structurile tradiționale de securitate nu sunt pregătite pentru a face față provocărilor globale, cum ar fi deficiența resurselor, care depăşeşte limitele geografice, disciplinare şi instituționale. Deoarece riscurile legate de diminuarea resurselor sunt sistemice şi neliniare, acestea devin insesizabile atunci când fragmente dintr-un sistem extins sunt analizate separat. Deşi există o cantitate mare de informații referitoare la hrană, apă şi, respectiv, energie, este disponibil un număr redus de date privind conexiunile dintre acestea. Gradul ridicat de specializare, predominant atât în sectorul public, cât şi în cel privat, este parțial responsabil de această carență, împiedicând înțelegerea problemei.

Prin urmare, apare necesitatea unor noi abordări privind obținerea şi utilizarea informațiilor. Se preferă informațiile colectate din multiple surse în locul acumulării datelor într-un model unic, determinat. Devine un imperativ utilizarea „informațiilor colective", cu ajutorul cărora sintetizăm şi deducem sensul informațiilor, şi nu doar le colectăm. Politicile de securitate trebuie să se bazeze pe prognoze strategice, pe cunoaşterea sistemelor şi regiunilor vulnerabile, înainte să aibă loc schimbările catastrofale de mediu, şi modul de ameliorare sau evitare a celor mai grave consecințe.

„Ecosistemele" adaptabile de cunoaştere care realizează conexiunea între datele provenind din diverse zone, ca răspuns la aceste probleme sistemice şi interdependente, pot astfel să completeze cadrele existente de securitate. Un exemplu al acestei abordări poate fi *Programul pentru Energie Globală & Ecosistemul Strategic al Mediului*[1], elaborat de Departamentul american pentru Energie. Această inițiativă este un parteneriat internațional în care participanții contribuie prin individualizarea

[1] Cunoscut drept Global EESE, ce funcționează pe o platformă „on-line" şi „face-to-face" (www.globaleese.org/).

riscurilor şi insecurităţilor în cadrul evaluărilor privind energia globală şi provocările la adresa mediului înconjurător.

1. Instituţiile de securitate tradiţională şi mediul înconjurător

Există două modalităţi în care factorii de mediu şi instituţiile militare şi de informaţii au fost conectate. Prima are legătură cu modul în care schimbarea mediului ar putea ameninţa interesele de securitate naţională şi, astfel, devine relevant pentru mandatele convenţionale ale acestor instituţii. Cea de-a doua are legătură cu modul în care activităţile acestor instituţii afectează mediul şi, de asemenea, cu modul în care resursele şi capacităţile lor ar putea fi utilizate pentru implementarea şi susţinerea politicii de mediu. Prevederile de securitate – oricum ar fi ele concepute – sunt, în general, considerate ca responsabilitate primară a statului. În îndeplinirea acestei atribuţii, statul colaborează cu serviciile militare şi de informaţii, iar studiile de securitate tind să se concentreze asupra acestor instituţii deoarece, deseori, securitatea a fost definită ca protejând integritatea teritorială şi independenţa politică a statului împotriva ameninţărilor externe directe. Însă, pe măsură ce conceptul de securitate se extinde, alte aspecte ale statului necesită atenţie.

Desigur, statul a fost întotdeauna mandatat să asigure securitatea în interiorul graniţelor sale, unde ameninţările includ, printre altele, crimele, corupţia, conflictele interetnice şi tensiunile între mediul rural şi cel urban. Pentru a face faţă conflictelor civile, statul se bazează pe legi imparţiale şi pe aplicarea eficientă a acestora, pe capacitatea sa de a redistribui resursele şi de a furniza bunuri publice şi pe o mulţime de mecanisme de management al conflictelor. De asemenea, statul trebuie să fie îndeajuns de solid pentru a se adapta noilor provocări. O serie de state create în cea de-a doua jumătate a secolului XX au fost supuse presiunilor pentru asigurarea securităţii interne. Este posibil ca acestea să ducă lipsă de legitimitate sau resurse sau să fie afectate de corupţie. În situaţiile în care degradarea mediului este severă, sărăcia este extinsă, corupţia este endemică, iar statul este relativ nou şi duce lipsă de legitimitate şi expertiză, pot apărea violenţe şi conflicte civile.

În mod clar este necesară consolidarea capacităţilor statului. Atunci când statele nu sunt capabile să asigure securitatea, ele pot apela la comunitatea internaţională (sau pot alege să intervină), însă entităţile externe au rareori motivaţia, resursele şi autoritatea de a gestiona un conflict intern. De la terminarea Războiului Rece, ONU a derulat o serie de misiuni

umanitare[2], o tendință care este posibil să continue, însă rezultatele nu au fost foarte bune. Acest lucru se întâmplă în mare parte deoarece un stat eşuat sau care este într-un război civil creează numeroase probleme complexe.[3] Este oportună găsirea unor modalități de consolidare a capacităților statului pentru a putea gestiona un conflict intern, pentru a se adapta schimbărilor de situație, de a participa la inițiative multilaterale şi de a contribui la consolidarea organizațiilor regionale.

Cu toate acestea, există o înțelegere redusă a ceea ce înseamnă, de fapt, consolidarea capacității statului şi a modului în care se poate realiza aceasta. Resursele limitate trebuie canalizate către acele sectoare în care pot avea cel mai bun efect – dar care sunt acestea? Nu există o formulă verificată şi demonstrată care să ghideze activitățile comunității internaționale.

În contextul securității mediului sunt extrem de importante pregătirea, schimbul de informații, crearea de baze de date şi asigurarea accesului la tehnologii ecologice. De asemenea, este esențială descoperirea unor modalități de reducere a sărăciei, de îmbunătățire a sistemului de sănătate şi educație. Mai mult, este esențial ca toate formele de asistență să fie elaborate cu participarea beneficiarilor pentru a se asigura faptul că exigențele, obiceiurile şi valorile locale sunt luate în considerare la adoptarea soluțiilor.

În primul rând, consolidarea capacității statului pentru a putea gestiona un conflict şi pentru a asigura securitatea trebuie să vină din interior. Nu există un model singular de stat ideal care să poată fi folosit. Contextul este esențial – diferențele care variază de la resurse şi climat la obiceiurile tradiționale şi comportament pot afecta caracterul individual al statului. Cu toate acestea, actorii externi subliniază importanța politicilor participative, statului de drept, echității şi respectării drepturilor omului. Acestea sunt elemente comune binecunoscute ale statelor prospere.

În al doilea rând, aparatul de stat este o sursă importantă de prestigiu, sănătate şi putere – cea mai mare parte a conflictului intern reprezentând, de fapt, rezultatul tentativei de capturare a statului. Odată ce statul a fost ocupat, oficialii săi pot folosi armata, serviciile de informații şi poliția pentru a-şi păstra poziția privilegiată. Pentru evitarea acestei situații, este importantă consolidarea capacității societății civile, precum şi cea

[2] http://www.un.org/en/humanitarian/

[3] Rotberg, Robert I. (ed.), *When States Fail: Causes and Consequences*, Princeton University Press, 2003.

a statului. Cetățenii trebuie să își cunoască drepturile, să-şi poată exprima temerile şi să poată participa liber la formularea politicilor şi legilor care îi afectează.

În cele din urmă, deşi în conformitate cu legislația internațională statele au autoritatea suverană în interiorul granițelor lor, ele sunt afectate de o multitudine de forțe transnaționale şi internaționale pe care acestea nu pot spera să le controleze pe cont propriu. Astfel, încurajarea participării la organizațiile regionale şi globale, care într-o măsură mai mare reuşesc să gestioneze aceste forțe, reprezintă o componentă importantă în consolidarea eficientă a statului.

În cadrul securității mediului, există un număr de roluri pentru armată şi serviciile de informații. Unele dintre acestea se înscriu perfect în mandatele convenționale ale acestor instituții, în timp ce altele le obligă să treacă în noi domenii de activitate. În SUA[4] şi alte câteva state membre NATO s-au depus eforturi pentru integrarea problemelor de mediu la nivelul acestor instituții specializate de securitate. Acest lucru este justificat, parțial, de dorința de a proteja bugetele pentru apărare de reducerile de după Războiul Rece şi de a reforma imaginea negativă pe care o au aceste instituții în comunitatea de mediu. Însă, este, de asemenea, un răspuns la conştientizarea tot mai mare a faptului că necesitățile de securitate se schimbă pe măsură ce tehnologia uneşte întreaga lume, iar omenirea se confruntă cu noi provocări transnaționale şi de mediu.[5] Aceste eforturi trebuie încurajate şi promovate în țările în curs de dezvoltare, însă trebuie recunoscute limitele acestora. Există anumite rețineri în instituțiile de apărare şi multe temeri justificate în ceea ce priveşte utilitatea şi competența acestora.

Pe măsură ce conceptul de securitate de extinde, ne este amintit faptul că garantul fundamental al securității în lumea noastră este statul. Deşi actorii nonstatali joacă un rol important, care trebuie recunoscut şi încurajat, consolidarea capacității statului rămâne extrem de importantă. Întrebarea ce apare foarte des este cea referitoare la modalitatea de realizare a acestei consolidări. În mare măsură, statele prospere trebuie consolidate din interior.

---

[4] În anul 2009, CIA a înființat „Centrul privind schimbările climatice şi securitatea națională" (The Center on Climate Change and National Security), care are drept obiectiv impactul asupra securității naționale a fenomenelor legate de deşertificare, deplasarea populațiilor, schimbărilelimatice, problemelee mediu, concurența privind resursele energetice.

[5] „Meeting 21st Century Transnational Challenges: Building a Global Intelligence Paradigm", CENTRAL INTELLIGENCE AGENCY, 2009.

Însă, comunitatea internațională poate ajuta prin evidențierea importanței statului de drept, politicilor participative şi respectării drepturilor omului. Aceasta poate acționa pentru a se asigura că şi societatea civilă beneficiază de putere. De asemenea, poate accentua importanța organizațiilor regionale şi globale în elaborarea unor soluții colaborative la probleme comune şi în dezvoltarea unor regimuri bazate pe aşteptări şi informații comune care facilitează alte forme de interacțiune reciproc avantajoase.

2. Informații strategice privind mediul

Probabil că nu este surprinzător faptul că identificarea unei noi amenințări nu are drept consecință o reacție eficientă. Este nevoie de mai mult timp pentru ca țările să înțeleagă importanța strategică a noilor amenințări la adresa intereselor lor vitale şi să reorganizeze prioritățile existente. Este nevoie de şi mai mult timp pentru a dezvolta instrumente eficiente de reacție. Sistemele de securitate constituite din certitudinile strategice ale Războiului Rece s-au luptat să răspundă unui nou mediu strategic fluid în care sursele de amenințare se transformă constant. Însă, acest lucru se schimbă. În rândul marilor puteri, acestea se concentrează, în prezent, mai puțin asupra puterii altor state şi mai mult asupra necesității combaterii instabilității şi statelor necontrolate, pentru a asigura securitatea energetică, a preveni dezvoltarea „spațiilor neguvernate" vulnerabile în fața abuzurilor teroriştilor şi membrilor grupărilor de crimă organizată şi aborda conflictele interne care pot dezvolta şi susține terorismul internațional.

Combaterea acestor amenințări necesită un tip extrem de diferit de aparat de securitate caracterizat de trei abordări:

- **preventivă**: acordarea unei importanțe mai mari guvernării eficiente, prevenirii conflictelor şi stabilizării țărilor după apariția unor conflicte şi crize;
- **integrată**: necesitatea „unor abordări guvernamentale cuprinzătoare" care să îmbine capacitățile militare, diplomatice, de dezvoltare şi cele ale sistemului juridic;
- **convergente**: asigurarea faptului că, la stabilirea priorităților, sunt evaluate complementaritățile între diferitele obiective politice şi instrumente (de exemplu, avantajele economice, de dezvoltare şi securitate ale combaterii exploatărilor forestiere ilegale).

Aceste principii devin, de asemenea, cunoscute pe parcursul abordărilor politice „de dezvoltare durabilă" şi, din mai multe puncte de

vedere, politica de securitate devine similară celorlalte domenii ale politicii internaționale. În centrul acestei provocări se află modalitatea de motivare a investițiilor consistente de capital financiar şi politic pentru prevenirea pe termen lung a conflictelor şi reducerea instabilității.

În pofida preponderenței eforturilor depuse de guvern în ceea ce priveşte obținerea de informații operaționale şi tactice, cele mai necesare informații sunt cele referitoare la tendințele pe termen lung şi ideile asupra modului în care „lumea din jurul nostru" va arăta în viitor. Chiar şi atunci când analizele strategice au inclus factorii de mediu, acestea au aplicat modele economice sau politice care este posibil să nu fie corespunzătoare pentru problemele ecologice complexe şi s-au bazat pe identificarea a ceea ce pare a fi „cel mai probabil lucru" din perspectiva informațiilor acceptate la scară largă.

Condițiile de mediu tind să reprezinte rezultate neintenționate ale acțiunii colective şi, astfel, sunt probabil mai puțin vizibile. Surprizele strategice, precum problemele de mediu emergente, au apărut, în general, atunci când este disponibil un volum mare de informații pentru a răspunde situației, totuşi riscurile nu au fost recunoscute sau abordate de politicieni. Obstacolele în calea unei supravegheri eficiente a securității mediului constau în câțiva factori importanți: căi de transmitere inadecvate a informațiilor la nivelul organizațiilor care împiedică comunicațiile, aşteptările ştiințifice pentru cauzalitate puternică şi conservatorism metodologic, tendința percepției cognitive a riscului în baza experiențelor anterioare şi subestimarea evenimentelor rare.

Chiar şi atunci când sunt disponibile informații, există bariere cognitive în calea recunoaşterii eficiente a posibilelor riscuri. Dacă cineva consideră anticiparea ca un exercițiu în evaluarea riscului, trebuie luată în considerare raportarea la experiențele anterioare. Această tendință, care se aplică atât în cazul percepției riscului, cât şi în cazul construirii instrumentelor metodologice, rezultă în subestimarea probabilităților viitoare în ceea ce priveşte riscurile. Estimările probabilității se bazează pe experiențele anterioare, iar, în general, oamenii nu se aşteaptă la niciun plan pentru acele evenimente pe care nu le-au experimentat foarte mult. Raportările se pot face structural în modul în care sunt construite evaluările, în care doar anumite măsurători şi observații sunt luate în considerare, în timp ce altele sunt, în mare parte, ignorate.

Impactul schimbării mediului asupra stării de securitate este şi mai dificil de coordonat, din cauza apariţiei unui domeniu, al securităţii mediului[6] (care nu are nici măcar propriile jurnale de cercetare) şi a lipsei istorice de cooperare între oamenii de ştiinţă în domeniul mediului şi cei specializaţi în domeniile tradiţionale de securitate. Între politicieni şi comunitatea serviciilor de informaţii această problemă devine una care ţine de „zidurile de protecţie" de securitate istorice menite să prevină accesul neautorizat la informaţii sensibile sau clasificate. Lipsa schimbului de informaţii între şi în interiorul agenţiilor este problematică chiar şi din punctul de vedere al securităţii tradiţionale, însă este extrem de dăunătoare pentru probleme privind ştiinţa mediului care se bazează pe fluxul liber de date unde există expertiză nu în cadrul agenţiilor guvernamentale, ci în rândul comunităţilor internaţionale de cercetători.

Provocările interconectate reprezentate de necesităţile în ceea ce priveşte energia, creşterea populaţiei, lipsa de apă şi alimente, schimbările climatice, pierderea biodiversităţii şi interdependenţa economică reprezintă un posibil „tsunami" pentru întreaga lume. Aceste provocări sunt „neobişnuite" prin faptul că au o dimensiune şi un nivel de complexitate fără precedent în istoria omenirii. Înţelegerea importanţei acestora şi adoptarea unor acţiuni pe măsură se numără printre dilemele noastre comune în ceea ce priveşte securitatea.

Provocările sistemice cu care ne confruntăm includ realităţi demografice: numărul de oameni de pe glob, deja de patru ori mai mare decât în urmă cu doar 100 de ani, urmează să crească din nou cu 35% – adică cu încă 2,4 miliarde de oameni – în următorii 40 de ani[7]. Cea mai mare parte a creşterii populaţiei va avea loc în partea de lume aflată în curs de dezvoltare. Drept consecinţă, consumul energetic la nivel global este de aşteptat să crească cu peste 60% în aceeaşi perioadă de timp[8]. Dependenţa tot mai mare de combustibili solizi în timpul acestei perioade este posibil să copleşească o serie de sisteme critice şi să amplifice schimbările climatice, acidificarea oceanului şi dispariţia unor specii.

În plus, rapoartele indică faptul că activitatea umană la nivel mondial provoacă o pierdere a habitatului şi dispariţia speciilor la o scară nemaivăzută de milioane de ani. Există o teorie ştiinţifică puternic

[6] Barry Buzan, *Popoarele, statele şi teama*, ediţia a doua, Editura Cartier, Chişinău, 2000.
[7] http://www.npg.org/facts/world_pop_year.htm.
[8] http://www.iea.org/textbase/nppdf/free/2010/key_stats_2010.pdf.

argumentată care ne obligă să conştientizăm faptul că sistemul climatic global este condamnat la o creştere importantă a temperaturii, chiar şi în cazul adoptării unor reduceri drastice a emisiilor de gaze.[9] Şi, dacă actualele tendințe în ceea ce priveşte emisiile de gaze continuă pentru următoarele câteva decenii, temperaturile globale este posibil să crească cu 3 până la 5 centigrade, în pofida oricăror acorduri viitoare privind stabilizarea concentrațiilor atmosferice.

Aceste fapte ne plasează pe noi şi civilizația noastră la o răscruce de drumuri în care trebuie să ştim nu doar unde ne aflăm, ci şi consecințele direcțiilor în care alegem să ne îndreptăm. Interacțiunile dintre aceste sisteme – în care o mică perturbare într-un sistem vital conduce la colapsul altuia – prezintă riscuri pentru securitatea noastră comună. Aceste sisteme complexe şi extrem de interconectate sunt imprevizibile şi dominate de posibilitatea unor schimbări mai rapide decât este de aşteptat.

Problemele de mediu nu sunt, neapărat, mai complexe decât condițiile sociopolitice care dau naştere la conflicte violente, însă este mult mai dificil să atribui intenții sau pronosticuri ale gândirii raționale, modului în care se schimbă condițiile. Condițiile de mediu globale sunt inevitabil legate de sistemele social, politic şi economic, care pot, de asemenea, prezenta incertitudini, pe când analiştii ar prefera să studieze sistemele ca o colecție discretă de variabile izolate.

În acest context, acele provocări globale neobişnuite necesită redefinirea conceptelor noastre de securitate cu scopul de a dezvolta această capacitate de culegere a informațiilor strategice. Conceptele de securitate actualizate subliniază înțelegerea vulnerabilităților, punctelor critice şi metodelor de consolidare a rezistenței sistemelor de care civilizațiile – viețile noastre – depind.

Adevărata valoare a activității de culegere a informațiilor strategice nu constă în furnizarea de informații cu privire la ceea ce este, în general, considerat cel mai probabil. Astfel de informații sunt deseori disponibile şi nu asigură capacitățile de avertizare ce permit o pregătire eficientă pentru evenimente posibil dezastruoase. Mai degrabă este mai importantă identificarea lebedelor negre, regăsite uneori, în mod statistic, sub numele de „cozi groase" sau „cozi lungi". Acestea sunt evenimentele puțin probabile dar cu un impact puternic care creează probleme importante atunci

[9] Proceedings of The National Academy of Sciences, *Warmer evening temperatures lower rice yields,* Press Releases, Washington DC, 2004.

când apar. Impactul şi dislocările pe care le produc astfel de evenimente sunt disproporţionate, în mare parte, deoarece nu ne aşteptăm ca ele să apară, iar oamenii subestimează posibilitatea apariţiei lor din cauza faptului că nu au experimentat anterior astfel de situaţii.

Este necesară crearea unei capacităţi de culegere de informaţii strategice neclasificate sau de anticipare şi avertizare pentru problemele cu care ne confruntăm în ceea ce priveşte energia şi securitatea mediului. O astfel de capacitate are ca scop consolidarea abilităţilor pentru recunoaşterea nu doar a pericolelor, ci şi a oportunităţilor, precum şi a posibilelor consecinţe involuntare. Această abordare ar trebui să privească problemele energetice şi de securitate a mediului ca un întreg şi nu să le evalueze separat, deoarece aceste provocări îmbinate reprezintă riscuri de securitate globale care, cu câteva excepţii, nu sunt foarte bine formulate şi înţelese.

Înţelegerea şi anticiparea problemelor de securitate ce reies din cele energetice şi de mediu vor reprezenta instrumente puternice pentru factorii de decizie din guvern şi din sectorul afacerilor.[10] O astfel de capacitate va fi benefică comunităţii de informaţii prin furnizarea informaţiilor şi cunoştinţelor relevante pentru analizele strategice. Deseori, factorilor de decizie le lipsesc datele concrete şi evaluările pragmatice necesare înţelegerii depline a modului în care schimbările din sectoarele energetice sau sistemele de mediu vor afecta alte elemente ale unui alt sector sau sistem, economiile naţionale, instituţiile internaţionale, culturile locale sau rivalităţile regionale.[11] Rapoartele serviciilor de informaţii se concentrează frecvent asupra unei singure probleme, ignorând astfel multe conexiuni între diversele probleme şi principalele grupuri de interese. Este posibil ca factorii de decizie să nu deţină cunoştinţe suficiente în ceea ce priveşte sensibilitatea relaţiilor cheie pentru stabilitatea globală şi regională şi caracterul fragil al interacţiunilor locale cu perturbaţiile de mediu.

În domeniul de intelligence şi al securităţii guvernamentale, informaţiile strategice s-au concentrat, în general, asupra ameninţărilor şi provocărilor considerate externe statului. Sherman Kent[12], un pionier

[10] „Enabling Strategic Intelligence on Energy and Environmental Security Impacts and Consequences", INTERNATIONAL DESIGN TEAM MEETING, Scotland, 2007.

[11] „Energy and Environmental Insecurity – Global strategic assessment 2009", INSTITUTE FOR NATIONAL STRATEGIC STUDIES.

[12] Sherman Kent (06.12.1903-11.03.1986) este istoric şi analist al intelligence-ului american. Profesor de istorie al Universităţii Yale, Kent a iniţiat numeroase metodologii de analiză a intelligence-ului, în timpul celui de-al Doilea Război Mondial. În Statele Unite este cunoscut drept „părintele analizei intelligence-ului".

al activității de analiză din cadrul serviciilor americane de informații, a sugerat că informațiile strategice reprezintă „un tip de cunoştințe pe care un stat trebuie să le aibă în ceea ce priveşte alte state, cu scopul de a se asigura că obiectivele sale nu vor avea de suferit, iar acțiunile sale nu vor eşua deoarece oamenii de stat şi militarii îşi fac planuri şi acționează în necunoştință de cauză".

Definiția lui Sherman Kent pentru informațiile strategice a reprezentat un răspuns bun în timpul Războiului Rece (atunci când a conceput-o), însă trebuie reactualizată pentru mediul de securitate din zilele noastre. În prezent, o capacitate de culegere a informațiilor strategice concentrată doar asupra actorilor şi amenințărilor externe are „paravane" încorporate pentru problemele de securitate evidente şi emergente la scară globală şi de natură sistemică (interdependentă). Fie că ne preocupă rețelele de crimă organizată, fie cele teroriste, conexiunile dintre călătoriile cu avionul şi tiparele de răspândire a agenților patogeni sau temerile interconectate de securitate la nivel global privind energia şi securitatea mediului – un accent limitat la actorii externi şi amenințări ar paraliza dezvoltarea informațiilor strategice.

Forțele energetice şi de mediu sunt atât globale, cât şi interdependente, nici interne, nici externe şi, în general, constituie factori de securitate. Astfel de factori includ presiuni asupra resurselor naturale primare şi zonele de impact din sectoarele de dincolo de cel al resurselor energetice, pentru a include apa, agricultura, bolile, tensiunile sociale, amenințările la adresa legitimității guvernului şi posibilitățile crescute pentru izbucnirea de conflicte internaționale şi epidemii, precum şi revolta populară şi radicalizarea.[13] Astfel, trebuie să analizăm actorii dintr-un punct de vedere extins atunci când abordăm problema securității energetice şi a mediului, pentru a include convingerile, percepțiile, acțiunile şi consecințele involuntare ale multiplilor actori de pe scena mondială.

În prezent, interdependențele înțelese prea puțin şi reacțiile globale creează noi dinamici între părți (economiile naționale şi societăți) şi întreg (ecosistemul global şi reacțiile în ceea ce priveşte mediul). Obiectivele securității tradiționale nu pot înțelege sau anticipa eficient noile amenințări şi preocupări privind securitatea pe care aceste reacții le creează. Mai mult, procesele şi instituțiile de asigurare a securității şi culegere a informațiilor tradiționale sunt proiectate necorespunzător pentru astfel de probleme.

[13] „Scanning the Horizon on Food, Water, Energy, and the Environment", CENTRE FOR STRATEGIC AND INTERNATIONAL STUDIES, 2009.

Un ecosistem emergent de cunoaştere a informațiilor strategice, format din indivizi cu diverse interese, experiențe şi scopuri, ar putea avea efectul rebalansării acestei istorii, sporind importanța acordată separat de guverne, problemelor de securitate energetică şi a mediului.

Un astfel de ecosistem de cunoaştere a informațiilor strategice va conține „o varietate indispensabilă" de expertize şi culturi, care este în egală măsură complexă pentru agenda de securitate a energiei şi mediului. Drept rezultat, sistemul va fi destul de robust din punct de vedere social pentru a aştepta şi corecta eforturile de manipulare a sistemului şi va prezenta o agendă explicită de organizare şi impulsionare a strategilor sistemici sau „generaliştilor care sunt specialiştii întregului".

Rolul catalizatorilor sistemului va fi de „cultivatori" sau „grădinari" care adoptă o abordare de tip ecosistem pentru a stabili conexiuni bazate pe încredere (prin valori, stimulente, normative de construire a unei relații) între grupurile de interese existente. Aceasta va fi cea mai mare valoare a sistemului deoarece va asigura conectivitatea interumană înaintea apariției crizelor şi va consolida relațiile interumane pentru a fi capabile să colaboreze mai rapid şi eficient odată ce adevăratele situații urgente vor fi în derulare, producând astfel informații în baza cărora se pot demara acțiuni atât pentru prevenirea crizelor, cât şi în timpul crizelor.

Din punctul de vedere al unora, acest ecosistem de cunoaştere a informațiilor strategice va fi atât un factor al noilor capacități cât şi un mediu de lucru captivant al viitorului în care indivizii vor putea să înțeleagă şi să anticipeze consecințele strategice. Sistemul ar putea conduce la crearea unor proiecte de demonstrații operaționale importante care ilustrează modul în care actualele tendințe se pot inversa, reducând viitoarele amenințări prin dezvoltarea unor comunități de încredere capabile să abordeze, atât cooperativ, cât şi pragmatic, principalele provocări în ceea ce priveşte energia şi mediul.[14]

În plus, acest ecosistem de cunoaştere a informațiilor strategice poate oferi diferite capacități, inclusiv piețe de anticipare, instrumente de vizualizare, scanări ale mediului şi construirea de scenarii alternative. Unicitatea acestuia va consta într-o rapidă acumulare şi evaluare a informațiilor şi cunoştințelor strategice, prin sisteme de acreditare a informațiilor,

[14] „Strategic intelligence and warning ecosystem", Foresight methodologies Brief series, N-1, 2009, GlobalEESE, Energy and Environmental Security Directorate (EESD), U.S. Department of Energy.

distribuite şi în curs de dezvoltare (precum cele popularizate pe E-Bay, Amazon sau digg.com). In special, acest sistem va face legătura la nivel local, regional şi global între comunităţi, în ceea ce priveşte diversitatea şi expertiza, şi va furniza o sursă credibilă şi mai obiectivă de informaţii decât cea disponibilă prin intermediul instituţiilor guvernamentale şi neguvernamentale ce acţionează doar în domeniul securităţii energiei şi mediului. Ideal, un astfel de ecosistem de cunoaştere va susţine comportamentele de conştientizare a grupului şi va depăşi limitele observate frecvent în cazul unităţilor mici de analişti care operează doar într-o singură organizaţie – un instrument cu o valoare specială atunci când se ia în considerare natura extinsă a provocărilor în ceea ce priveşte securitatea energiei şi a mediului.

Ecosistemul de cunoaştere a informaţiilor strategice va atrage o expertiză variată, precum virusologia, biologia evolutivă, cercetarea reţelelor, economia de dezvoltare, degradarea mediului, gestionarea dezastrelor, ştiinţa politică, relaţiile internaţionale şi diferite metodologii de evaluare a sistemelor dinamice în scopul analizării fenomenelor interdependente de securitate.

Concluzii

Conceptul de securitate naţională folosit, deseori, atât în ştiinţa politică, cât şi în logica populară conţine un număr de presupuneri umane, modalităţi de gândire care trebuie abordate înainte ca noi să înţelegem dificultăţile inerente ale schimbării mediului şi conexiunilor securităţii. Pe scurt, aceste zone cu posibile probleme sunt:

1. complexitatea variabilelor şi natura neliniară a relaţiilor;
2. natura ireversibilă a sistemelor de mediu;
3. considerarea problemelor de mediu ca fiind externe sistemelor politic, economic şi social;
4. atenţia acordată analizelor la nivel de stat impune false diviziuni între factorii de resort;
5. considerarea sistemelor de mediu ca fiind cauzele „naturale” şi originare ale problemelor.

Percepţiile populare ale problemelor de mediu se bazează pe noţiuni potrivit cărora condiţiile de mediu sunt, în mare parte, statice, rămân mai mult sau mai puţin aceleaşi pe parcursul timpului, fiind protejate împotriva interferenţelor externe ale acţiunilor omului sau a altor interferenţe

copleşitoare. Cu toate acestea, astfel de abordări limitează înțelegerea sistemelor de mediu complexe şi neliniare.

Din păcate, diferența dintre nivelul instituțiilor noastre de securitate națională ale secolului XX şi realitățile secolului XXI în ceea ce priveşte securitatea sunt mai mari ca niciodată. Observarea şi înțelegerea instrumentelor de avertizare timpurie nu au fost niciodată mai importante. Totuşi, istoria instituțiilor de securitate națională este una de o profundă inabilitate de adaptare la timp la noile amenințări de securitate. În mod tipic, adaptarea, dacă apare, reprezintă un răspuns reactiv la dezastru după ce a avut loc – aceasta este problema clasică de pregătire continuă de luptă pentru ultimul război.

Integrarea schimbării mediului ca un concept principal, atât prin contribuția la forțarea sistemelor de mediu, cât şi ca posibile soluții de cooperare, reprezintă o prioritate. Un astfel de concept va fi inerent complex, implicând multă incertitudine şi ilustrând scenarii care conțin multiple efecte de reacție inversă şi perturbații în cascadă („efectul de val"). Modelele simple şi o viziune continuă potrivit căreia sistemele de mediu se află în exteriorul activității umane impun bariere artificiale atât pentru înțelegere, cât şi pentru găsirea unor soluții.

Necesitatea unei mai bune anticipări şi avertizări implică nu doar dezvoltarea sistemelor analitice pentru furnizarea de date relevante, ci avem nevoie, de asemenea, de o mai bună înțelegere a vulnerabilităților la nivelul sistemelor critice şi a modului în care aceste vulnerabilități pot fi înțelese ca probleme de securitate. Necesitatea definirii securității mediului şi a metodelor de identificare a insecurității conține similarități cu problemele de securitate anterioare, în timp ce alte atribute ale problemelor de mediu necesită noi instrumente şi abordări. Preocupările în ceea ce priveşte mediul sunt transnaționale şi deseori neintenționate, fiind pline de incertitudini şi necesitând noi comunități de expertiză.

Ideea acestui exercițiu nu este de a furniza răspunsuri imediate şi concrete. Este puțin probabil ca acest lucru să fie posibil din cauza incertitudinii inerente aflată în discuție. Mai degrabă, noi trebuie să asigurăm definiții şi cadre legale funcționale pentru politica de abordare, care să depăşească definițiile din timpul Războiului Rece ce presupun securitatea statului, acțiuni deliberate şi conflicte violente. Dacă ar fi folosite aceste definiții, am analiza greşit regiunile şi perioadele.

Aşa cum comandanții de luptă au nevoie să înțeleagă întreaga dinamică a mediului de confruntare, factorii de decizie au nevoie de o

perspectivă extinsă în ceea ce priveşte posibilele consecinţe pe care le are dinamica globală şi regională asupra securităţii, care afectează problemele energetice şi de mediu.[15] O analiză strategică mai aprofundată va conduce la procese de luare a deciziilor mai bine documentate şi, în cele din urmă, la decizii mai bune. Dezvoltarea capacităţii indispensabile de culegere a informaţiilor strategice ar putea asigura:

- avertizarea timpurie a factorilor de decizie în legătură cu riscurile emergente (înainte ca acestea să devină ameninţări serioase);
- impunerea unui raţionament care transcende zona partizanatului şi grupurile de interese;
- conştientizarea viitoarelor direcţii alternative ale dezvoltării tehnologiilor energetice şi pieţelor internaţionale, a viitoarelor provocări în ceea ce priveşte mediul şi, astfel, a posibilităţii de a acţiona, a adapta şi mai degrabă a configura, decât a reacţiona.

Albert Einstein a observat în mod excepţional că „nu ne putem soluţiona problemele cu aceeaşi gândire care le-a creat". În acest secol, va trebui să depunem eforturi concertate pentru a investi în capacităţile de înţelegere globală, bazându-ne pe o reţea interconectată de minţi pregătite să abordeze aceste provocări cu o nouă gândire.

Bibliografie

1. *Common Security, Uncommon Challenges: Managing Risks in an Age of the Unthinkable*, Carol Dumaine, Geneva, Switzerland, GLOBAL ENERGY&ENVIRONMENT STRATEGIC ECOSYSTEM, US Department Energy, May 2009.

2. *Enabling Strategic Intelligence on Energy and Environmental Security Impacts and Consequences*, INTERNATIONAL DESIGN TEAM MEETING, Scotland, 2007.

3. *Environmental security, abrupt climate change and strategic intelligence*, Chad Michael Briggs, GLOBAL ENERGY&ENVIRONMENT STRATEGIC ECOSYSTEM, US Department Energy, February 2009.

4. *Energy and Environmental Insecurity*, „Global strategic assessment 2009", INSTITUTE FOR NATIONAL STRATEGIC STUDIES.

5. *Environment and Security, Transforming Risks into Cooperation, Environmental risks in South Eastern Europe*, ENVSEC COOPERATION, 2006.

[15] *Introduction to Strategic Intelligence Analysis*, GOVERNMENT TRAINING INC, 2009.

6. *Energy & Environmental Risks: Defining Security and Vulnerability*, INSTITUTE FOR ENVIRONMENTAL SECURITY, 2009.

7. *Environment and Security Policy*, INTERNATIONAL INSTITUTE FOR SUSTAINABLE DEVELOPMENT, 2009.

8. *Inventory of Environment and Security Policies and Practices*, INSTITUTE FOR ENVIRONMENTAL SECURITY, 2007.

9. *Introduction to Strategic Intelligence Analysis*, GOVERNMENT TRAINING INC, 2009.

10. *State-of-the-Art Review On Environment, Security and Development Co-operation*, IUCN, THE WORLD CONSERVATION UNION, 2007.

11. „Scanning the Horizon on Food, Water, Energy, and the Environment", CENTRE FOR STRATEGIC AND INTERNATIONAL STUDIES, 2009.

12. Global monitoring for environment and security (GMES), COMMISSION OF THE EUROPEAN COMMUNITIES, 2008.

13. The Intelligence Community's Neglect of Strategic Intelligence, CENTRAL INTELLIGENCE AGENCY, 2009.

14. „Meeting 21st Century Transnational Challenges: Building a Global Intelligence Paradigm", CENTRAL INTELLIGENCE AGENCY, 2009.

Evoluţii şi perspective „*Afganistan 2014*": un stat democratic sau unul eşuat? O analiză de tip OSINT

Drd. Cristian NIŢĂ
Serviciul Român de Informaţii
e-mail: **cnita@dcti.ro**

Abstract

According to the Report published by World Economic Forum, the most important risks identified for 2010 are the instability in Afghanistan, the problem of Palestinian territories and relation with Israel, as well as the developments in Iraq.

The background from Afghanistan reveals as the biggest present dangers the rapid and uncontrolled disintegration of the security environment inside so-called AfPak, increasing radicalization within Pashto regions from both states and extending anti-American feelings across the area. Despite the fact that international actors declare stability as the premise for Afghan rebuilding, law enforcement, combating insurgency and the fight against corruption are essentials in order to solve the problems of this country, in the context in which there is an evidence the fact that authorities from Kabul are not able to assure their own security for short or long term.

Keywords: AfPak, US strategy, ISAF, Taliban reconciliation, reconciliation abandon.

AfPak – între dezintegrare şi stabilitate

În Afganistan, cel mai mare pericol îl reprezintă dezintegrarea rapidă şi necontrolată a stării de securitate din aşa-numitul *AfPak*, radicalizarea rapidă a regiunilor paştune din cele două state – apariţia fenomenului de *paştunizare* şi extinderea sentimentelor antiamericane din regiune,[1] precum şi continuarea

[1] http://www.cf2r.org/fr/notes-actualite/nouveau-chef-operationnel-pour-les-talibans-afghans.php. În zona paştună din Pakistan exsită patru comandamente militare ale talibanilor afgani: shura regionale stabilită la Gerdi Jangal, în Balutchistan, shura regională din Quetta, condusă de Hafiz Abdul Majid, care are în responsabilitate provinciile din sudul şi vestul Afganistanului, Hafiz Abdul Majid fiind, între altele, şi responsabil pe probleme de informaţii; shura regională din Peshawar, condusă de Abdul Latif Mansour, care se ocupă de estul şi nord-estul Afganistanului; shura regională din Miramshah, al cărui lider este Sirajuddin Haqqani, din clanul Jalaluddin Haqqani, care are în responsabilitate provinciile Paktika, Paktia, Khost, Logar şi Wardak.

activităților CIA în regiunea de graniță dintre Afganistan şi Pakistan, cu sau fără permisiunea autorităților pakistaneze.[2] De altfel, potrivit unui raport publicat de *World Economic Forum*, unul din cele mai importante riscuri identificate în anul 2010 a fost *instabilitatea în Afganistan.*[3]

Numărul atentatelor s-a dublat în Afganistan în anul 2009 față de 2008, în timp ce frecvența celor din Pakistan a crescut, acest stat continuând să servească ca spațiu de antrenament pentru teroriști.

Pentru Pakistan, provocarea majoră este asigurarea unei mai bune guvernări. Aceasta presupune, înainte de toate, intensificarea cooperării între executivul de la Islamabad şi armată, pentru a putea fi stopat fenomenul de talibanizare a țării, stabilizate zonele tribale de la granița cu Afganistanul şi adoptate măsuri pentru realizarea progresului economic. De-a lungul istoriei sale, Pakistanul a folosit deliberat actori nonstatali pentru a duce un război strategic asimetric împotriva unor adversari mai puternici, precum India sau Uniunea Sovietică. Cu toate acestea, în prezent, militanții talibani îşi urmăresc propriile obiective, acționând împotriva intereselor Islamabadului. Analiştii apreciază că, dacă Pakistanul nu va adopta o poziție fermă față de extremiştii islamişti în cel mai scurt timp, ar putea pierde controlul asupra statului. Riscul cel mai mare pentru securitatea regională şi internațională îl reprezintă însă exploatarea instabilității politice şi a insecurității de către *mişcarea Tehrik-i Taliban Pakistan (TTP)*, *ceea ce ar permite pentru prima dată în istorie accesul unei organizații teroriste la un arsenal nuclear dezvoltat şi la tehnologia aferentă acestuia*.[4]

Conform experților, actuala situație politică, socială şi economică a statului pakistanez poate determina luarea în calcul a unui astfel de scenariu sumbru. În contextul în care tranziția spre democrație a Pakistanului este încă fragilă, anchetele penale sunt derulate împotriva unor membri ai Guvernului şi în care se intensifică tensiunile dintre partide, slăbiciunea actualei conduceri a țări este evidentă. Cea mai apăsătoare problemă a stabilității Pakistanului este reprezentată de situația politică a țării. Tranziția spre democrație este fragilă: coaliția condusă de Partidul Poporul din

---

[2] Seth G. Jones, „Take the War to Pakistan", *Rand Corporation*, 04.12.2009; Ahmed Rashid, „Coming up Short on Pakistan", http://www.cf2r.org/fr, 14.12.2009.

[3] „Global Risks 2010. A Global Risk Network Report", *World Economic Forum*, january 2010.

[4] Sumit Ganguly, S. Paul Kapur, „The Sorcerer's Apprentice: Islamist Militancy in South Asia", în *The Washington Quaterly,* ianuarie 2010. Statele Unite ale Americii au anunțat la 1 septembrie 2010 că i-au plasat pe talibanii pakistanezi („Tehrik-e-Taliban") pe lista neagră a organizațiilor teroriste internaționale.

Pakistan (PPP) se bucură de o majoritate parlamentară fragilă şi principalul său aliat, Mişcarea Muttahida Qaumi (MQM), a ameninţat de mai multe ori că se retrage din coaliţie. Dincolo de sfera politică însă, Pakistanul este, de asemenea, un stat cu instabilitate socială pronunţată. Un aspect al acestei instabilităţi se referă la tensiunile partizane şi religioase, precum şi la violenţe. Deşi partidele islamiste se bucură de susţinere populară limitată, aşa cum a fost dovedit în cadrul alegerilor din februarie 2008, Pakistanul rămâne o ţară conservatoare pe ansamblu. În plus, una dintre dificultăţile cu care se confruntă Pakistanul în încercarea de a rezolva diferitele inechităţi socio-economice din ţară este situaţia dificilă macroeconomică.[5] Cota popularităţii preşedintelui Asif Ali Zardari nu a încetat să scadă din cauza corupţiei omniprezente şi a pasivităţii în faţa problemelor economice şi a inundaţiilor catastrofale. În plus, ţara este afectată de numeroasele atentate atribuite în majoritate talibanilor: aproximativ 1 000 de morţi în 2010. Acest greu tribut plătit de pakistanezi unui conflict considerat de către opinia publică ca importat de SUA din Afganistan alimentează un profund sentiment antiamerican.

În acest context dificil, conform unui raport al unui grup de specialişti condus de directorul Centrului pentru Asia de Sud din cadrul Consiliului Atlantic, Shuja Nawaz, deteriorarea relaţiilor dintre Statele Unite şi Pakistan ar putea conduce la o înfrângere a celor două state în războiul din Afganistan.

Shuja Nawaz menţionează că, în contextul în care nu sunt luate măsuri strategice de către ambele tabere, relaţiile SUA-Pakistan pot înregistra o răcire, marcată de neîncredere şi neconcordanţă între poziţia adoptată în mod public şi negocierile private.

Raportul notează faptul că, în timp ce armata pakistaneză a înregistrat succese în ceea ce priveşte eradicarea teroriştilor de pe teritoriul statului, guvernul nu dispune nici de voinţă, nici de capacitatea de a beneficia de susţinere faţă de implementarea unor reforme şi politici pe termen lung.[6]

Serviciile de informaţii pakistaneze (ISI) continuă să antreneze, să finanţeze şi să ofere protecţie talibanilor în Afganistan, în pofida presiunilor SUA, conform unui raport dat publicităţii în iunie 2010 de London School.

[5] „Inerţia democraţiei – Paralizia politică din Pakistan", publicaţie lunară *Janes Intelligence Review*, 07.05.2010.
[6] Publicaţia „The Washington Times", 30.06.2010.

Conform lui Matt Waldman, cercetător la Universitatea Harvard, *„comandanţii talibani afirmă că ISI orchestrează, susţine şi influenţează enorm mişcarea. ISI oferă protecţie atât talibanilor, cât şi reţelei Haqqani (aripa radicală a talibanilor afgani) şi furnizează un sprijin important în antrenament, muniţii, alimente”*. Unii dintre talibanii intervievaţi au afirmat că membri ai ISI au asistat la întâlniri cu consiliul suprem al talibanilor. Una dintre afirmaţiile cel mai surprinzătoare este aceea că preşedintele pakistanez şi un oficial ISI de rang înalt au vizitat în primăvara anului 2010, într-o închisoare secretă din ţară, cinzeci de şefi talibani, cărora le-au declarat că au fost arestaţi numai la presiunile americane. Raportul conchide că, fără o schimbare semnificativă a comportamentului autorităţilor pakistaneze, va fi dificil, dacă nu imposibil, pentru guvernul afgan şi forţele NATO să pună capăt insurgenţei talibane în Afganistan.[7]

Există însă şi semnale care demonstrează o nouă abordare a problematicii talibane de către ISI. După arestarea, în luna februarie 2010, a comandantului taliban Abdul Ghani Baradar, reţinerea unui alt lord al războiului, Maulvi Abdul Kabir, în Pakistan, la sfârşitul aceleiaşi luni, indică o schimbare de atitudine pentru serviciul pakistanez de informaţii (ISI). Timp de mulţi ani, ISI a susţinut insurgenţii din Afganistan, finanţându-i şi antrenându-i. Deşi, în cele din urmă, Pakistanul trebuie să-şi continue relaţia cu talibanii, în prezent, este evident că este pregătit să coopereze cu statele occidentale şi să depună toate eforturile în scopul destabilizării insurgenţilor. În paralel cu arestările operate, ISI şi-a informat partenerii occidentali că doreşte să joace un rol în negocierile cu talibanii. Influenţa saudită a jucat un rol decisiv în cazul acestei schimbări de atitudine. Şeful Direcţiei Generale de Informaţii (GID) din Arabia Saudită, prinţul Moqrin bin Abdulaziz, a întreprins demersuri la Riyadh şi Islamabad pentru a-l convinge pe generalul Ashfaq Kayani, şeful Armatei pakistaneze, să pună capăt sprijinului ISI pentru talibani. Având în vedere importanta susţinere financiară saudită faţă de Armata pakistaneză, demersurile acestuia au avut succes. În timp ce serviciul pakistanez de informaţii (ISI), condus de generalul Ahmed Shuja Pasha, pare decis să destabilizeze forţele talibane, acesta nu mai are aceeaşi disponibilitate în privinţa cooperării cu serviciile secrete occidentale, în special cu CIA. ISI se ocupă singur de interogarea lui Baradar, fără participarea omologilor occidentali, cărora le transmite informaţiile obţinute.

[7] Irina Cristea, „Serviciile de informaţii pakistaneze îi susţin în continuare pe talibani”, agenţia de ştiri „Agerpres”, 14.06.2010.

Până acum, solicitările înaintate de SUA privind participarea americanilor la interogarea lui Baradar şi transferarea acestuia în Afganistan, la închisoarea Bagram, din apropiere de Kabul, au rămas fără răspuns.[8]

Chiar dacă actorii internaţionali susţin că stabilitatea este premisa pentru reconstrucţia Afganistanului, aplicarea legii este condiţia esenţială pentru ca problemele acestei ţări să fie soluţionate, în condiţiile în care este cert că autorităţile de la Kabul nu vor reuşi pe termen scurt şi mediu să-şi asigure singure securitatea.[9] Guvernul Karzai pare incapabil să reconstruiască un stat care să îşi asume răspunderea pentru instaurarea şi menţinerea securităţii, cel puţin în viitorul apropiat. Semne de întrebare sunt şi în ceea ce priveşte dorinţa preşedintelui de a vedea o îmbunătăţire a guvernării provinciale. Preocupat de consolidarea imaginii sale, şeful statului pierde din vedere un aspect extrem de important – legitimitatea statului afgan.[10]

Practic, potrivit experţilor, fără sprijin din exterior, guvernul se va prăbuşi, talibanii vor prelua controlul asupra celei mai mari părţi a ţării, iar conflictele interne se vor agrava, existând riscul revenirii la războiul civil din anii ’90.

În acest context, Coaliţia internaţională trebuie să ţină cont de tensiunile la nivel guvernamental (lipsa de legitimitate a preşedintelui Karzai şi contestarea capacităţii acestuia de a guverna, lipsa de unitate), precum şi de relaţia de rivalitate dintre liderii talibani şi interesele regionale ale statelor vecine Afganistanului.

Având în vedere aceste aspecte, Coaliţia va trebui:

- să îmbine acţiunile pe termen scurt cu cele pe termen lung, astfel încât efectele asupra statului afgan să fie atât cele dorite, cât şi cele promise;
- să adopte şi să implementeze deciziile la nivel central şi local, în mod uniform;
- să ajungă la un echilibru în privinţa aplicării justiţiei şi a obţinerii păcii;
- să nu desconsidere niciuna dintre forţele care acţionează în Afganistan;
- să vizeze satisfacerea unitară a nevoilor întregii populaţii, dar păstrând ajutoarele la nivelul strictului necesar şi fără agravarea condiţiilor de securitate;

---

[8] „Cum a reuşit Arabia Saudită să convingă serviciul pakistanez de informaţii”, publicaţie bilunară *Intelligence Online*, nr. 612, 11.03.2010.

[9] Michael O’Hanlon, Hassina Sherjan, „The Tide May Be Turning In Afghanistan”, *The Brookings Institution*, 16.02.2010.

[10] James Traub, „The Karzai Dilemma”, http://www.foreignpolicy.com/articles/2010/04/13/the_karzai_dilemm.

- să protejeze populația atât față de insurgenți, cât şi față de abuzurile puterii centrale.[11]

Experții pe problematica reconstrucției statale şi contrainsurgenței sunt divizați în două tabere. Unii consideră că Afganistanul nu va fi niciodată un stat stabil şi sigur în absența unui guvern central puternic, capabil să asigure funcțiile statale în toate regiunile. Alții apreciază că Afganistanul este şi a fost întotdeauna o societate descentralizată, motiv pentru care pledează pentru dezvoltarea de instituții locale care să asigure stabilitate. De altfel, experții apreciază că absența unei guvernări puternice a oferit clanurilor ocazia să exploateze tensiunile sociale existente.

În prezent, populația este în expectativă, dezamăgită puternic de comunitatea internațională şi liderii de la Kabul. Însă teama mai mare este dată de viitorul nesigur, când trupele ISAF vor părăsi teritoriul, anii următori fiind critici pentru populația afgană.[12]

Nivelul crescut al incertitudinii cu privire la perspectivele retragerii trupelor ISAF în Afganistan a fost inflamat de apariția ştirii conform căreia geologi americani au identificat rezerve minerale semnificative de litiu, aur, fier, cupru şi cobalt. Potrivit unui document intern al Pentagonului, Afganistanul ar putea deveni „Arabia Saudită a litiului", un material-cheie în industria electronică.

Se prefigurează implementarea unui regim de exploatare excesivă a bogățiilor naturale ale Afganistanului de către companii multinaționale miniere, aceste activități aducând cu ele numeroase efecte negative, între care încurajarea corupției administrației locale şi consecințe ireversibile asupra mediului.[13]

Perioada imediat următoare retragerii trupelor ISAF din Afganistan este privită cu îngrijorare la Washington, opinia generală fiind de părere că afganii sunt imposibil de guvernat în mod centralizat şi eficient. În această situație, războiul din Afganistan poate fi câştigat doar cu condiția asumării riscurilor şi situației complexe specifice acestei țări. Cu toate acestea, trebuie ținut cont şi de faptul că războiul poate fi pierdut uşor, prin

[11] Belfer Center – Matan Chorev şi Jake Sherman – The Prospects For Security And Political Reconciliation In Afghanistan: local, National, And Regional Perspectives / mai 2010.

[12] Stiftung Wissenschaft und Politik - Michael Paul – The Bundeswehr in Afghanistan: A New Focus on Training / mai 2010.

[13] Michael Chossudovsky, „The War is Worth Waging: Afghanistan's Vast Reserves of Minerals and Natural Gas", Global Research, 17.06.2010.

exacerbarea riscurilor imediate.[14] O soluție ar fi implementarea unui model dovedit viabil din punct de vedere istoric: un gen de *democrație descentralizată, în care comunitățile locale (jirga sau shura) să se bucure de o autonomie decizională sporită*.[15]

Potrivit secretarului general al Alianței Nord-Atlantice, Anders Fogh Rasmussen, NATO va începe transferul controlului asupra securității către forțele afgane la începutul anului 2011 sau cel târziu în luna iulie 2011.[16] Rasmussen a declarat că acest proces se va desfăşura cu monitorizarea situației din Afganistan, adăugând că NATO trebuie să-şi consolideze eforturile în direcția pregătirii unui număr de 300 000 de soldați afgani până în octombrie 2011.

La summitul NATO de la Lisabona din noiembrie 2010, termenul-limită al retragerii din Afganistan a fost fixat pentru 2014, urmând ca, până la această dată, transferul sarcinilor de asigurare a stabilității statului către armata şi forțele de ordine afgane să fie făcut gradual, începând cu anul 2011. În acest context, situația din Afganistan trebuie administrată într-un mod diferit, aproape matematic, respectând termenele-limită setate. De asemenea, efortul ISAF trebuie energizat, proactivitatea fiind o responsabilitate a tuturor țărilor membre,[17] în condițiile în care efortul operațional şi coordonarea operațiunilor militare revine în proporție de 70% Pentagonului.[18]

---

[14] Anthony H. Cordesman, fost profesor de „Studii de securitate națională" al Universității Georgetown şi deținătorul funcției de Președinte pe probleme de securitate în cadrul CSIS, „Realism in Afghanistan: Rethinking an Uncertain Case for the War", Center for Strategic & International Studies, 16.06.2010.

[15] Ibidem.

[16] Stephen Biddle, Fotini Christia şi Alexander Their, „Defining Success in Afghanistan", *Foreign Affairs*, july-august 2010.

[17] www.stratfor.com, 12-18.10.2010.

[18] Simona Haiduc, „NATO şi-a stabilit obiective ambițioase pe fondul unor bugete militare de austeritate", în cotidianul *Financiarul* nr. 722, 22.11.2010. Liderii statelor aliate au adoptat măsuri economice, care privează NATO de un sfert din personalul său, reduce numărul comandamentelor sale (de la 11 la 6 sau 7), a agențiilor de susținere logistică (de la 14 la 3) şi a comitetelor sale (de la aproape 400 la 85). Pe fondul gravelor deficite publice, europenii au redus amploarea forțelor lor militare. Bugetul propriu al NATO este consacrat cheltuielilor care răspund intereselor colective ale celor 28 de state membre. Aceste cheltuieli s-au cifrat, de exemplu, în anul 2005, la 1.735 mld. euro. Cei mai mari cinci contributori sunt SUA (29,16%), Germania (19,95%), Marea Britanie (11,59%), Franta (6,40%) şi Italia (7,33%). În acest context, reducerea drastică a capacității de „proiecție" a forțelor militare europene înseamnă pentru Statele Unite că următorul conflict vor trebui să-l gestioneze singure sau aproape singure, Washingtonul fiind astfel obligat să renunțe la aliații săi în cazul unor confruntări globale sau să-şi găsească alții. Faptul că la Casa Albă, europenii sunt din ce în ce mai puțin apreciați, a apărut evident în multe ocazii, mai ales de când s-a instalat actuala administrație, care urmăreşte în mod prioritar întărirea legăturilor cu aliații din Asia (cu scopul de a domina China) şi rezolvarea diferendelor cu Moscova, pe baza intereselor comune.

În pofida numărului foarte mare de trupe ISAF, vulnerabilitatea anumitor regiuni şi rute este pregnantă şi, în special, cea a rutelor pakistaneze pentru transportul suportului logistic necesar şi atacurile recurente ale militanților asupra punctelor de acces de pe teritoriul afgan impun găsirea unei rute alternative. O variantă ar fi tranzitarea Uzbekistanului, în condițiile în care Tokyo şi Taşkent s-au oferit să susțină financiar construirea, respectiv îmbunătățirea şi prelungirea unor linii de cale ferată în Afganistan.

Afganistanul a stabilit anul 2014 drept anul în care țara va deține controlul total asupra securității naționale.

Tentativele forțelor britanice şi americane de extindere a controlului asupra teritoriului afgan în ultimele 12 luni au fost contraproductive şi au condus la o agravare a situației de securitate, a declarat Richard Barrett, şeful misiunii de monitorizare a talibanilor din cadrul ONU.

Analiza lui Barrett coincide cu un raport oficial al Consiliului de Securitate din iunie 2010 care a indicat o escaladare a violențelor din Afganistan în timpul primelor patru luni ale anului 2010. Numărul atacurilor cu bombă a crescut cu peste 90%, comparativ cu aceeaşi perioadă a anului 2009, s-a precizat în raport.[19]

Victoria coaliției ISAF în Afganistan depinde de depăşirea următoarelor **provocări**:

- definirea a ceea ce constituie „victorie" în actualul context geopolitic;
- evaluarea capacităților şi resurselor reale ale insurgenților;
- stabilirea unor termene-limită şi a unei agende tactice realiste ;
- acceptarea contextului sociocultural al societății afgane şi renunțarea la etnocentrismul american;
- dezvoltarea componentei civile în detrimentul aspectelor pur militare.[20]

Obiectivul – cheie al *strategiei contrainsurgente* este obținerea suportului populației afgane. Această strategie se va fundamenta pe patru piloni: creşterea rapidă a numărului forțelor de securitate, îmbunătățirea capacității de guvernare şi responsabilizarea autorităților de la Kabul,

[19] Mark Townsend, Extinderea controlului asupra teritoriului afgan din partea trupelor americane şi britanice a condus la escaladarea conflictului în regiune, în publicația săptămânală „The Observer", 20.06.2010.

[20] S. Frederick Starr, Andrew C. Kuchins, Stephen Benson, Elie Krakowski, Johannes Linn şi Thomas Sanderson, The Key to Success in Afghanistan, Central Asia-Caucasus Institute, 09.06.2010.

preluarea inițiativei împotriva insurgenței şi valorificarea resurselor pentru protejarea populației.[21]

Istoria a demonstrat că eşecul în construirea unei armate naționale de coeziune a condus, adesea, la difuziunea forței statale la nivelul mai multor actori interni, grăbind căderea guvernelor de la Kabul. Intenția de a crea forțe militare specializate s-a materializat în apariția unor miliții cu rolul de a anihila orice amenințare internă ori externă la adresa statului.

La sfârşitul lunii iunie 2010, experții americani declarau că nu există o metodă care să demonstreze cât de pregătite sunt forțele afgane pentru a prelua responsabilitatea privind securitatea de la forțele americane deoarece sistemul utilizat până de curând pentru evaluarea afganilor este nesigur.

Transferul responsabilității pentru asigurarea securității asupra forțelor afgane este unul din punctele cheie ale strategiei preşedintelui american Barack Obama privind războiul împotriva insurgenților talibani.[22] În acelaşi timp, se derulează un curs de reintegrare a mujahedinilor şi de readucere a lor în sistem pentru a lucra şi pentru a fi loiali guvernului afgan. Apoi aceştia sunt antrenați pentru a forma un corp de ofițeri de carieră. Totodată, această inițiativă îi reprezintă mai bine la nivelul armatei pe reprezentanții grupului etnic al paştunilor, majoritar în regiunile de sud şi est. Pentru a fi sustenabilă, armata afgană trebuie să reflecte balanța etnică a țării.

„International Crisis Group" a lansat o serie de recomandări pentru Guvernul de la Kabul şi preşedintele Hamid Karzai, privind:

- *regândirea managementului militar, prin întărirea schemei legislative şi administrative în vederea depolitizării;*

---

[21] „Obama's war in Afghanistan", The International Institute for Strategic Studies, Strategic Comments, Volume 15, Issue 10, decembrie 2009. Generalul William B. Caldwell este comandantul Misiunii NATO de Instruire din Afganistan, responsabilă pentru crearea unităților militare şi de poliție locale. Totodată, acesta coordonează şi Comandamentul Integrat de Transfer al Securității din Afganistan (Combined Security Transition Command – Afghanistan). Înainte de preluarea atribuțiilor din Afganistan, generalul Caldwell a condus prestigiosul centru de cercetare de la Fort Leavenworth, acolo unde se formulează doctrina armatei americane. De altfel, generalul Caldwell este continuatorul unei moşteniri care avea să schimbe decisiv cultura armatei americane, fiind succesorul generalului David Petraeus la Fort Leavenworth. Absolvent al Academiei Militare de la West Point, promoția 1976, generalul Caldwell a mai ocupat funcțiile de comandant al Diviziei 82 Aeropurtată, o unitate de elită a armatei americane, dar şi pe cea de purtător de cuvânt al Forței Multinaționale din Irak, în timpul operațiunii „Iraqi Freedom".

[22] „Sistemul de evaluare al forțelor afgane este viciat, declară experții americani", cotidianul *International Herald Tribune*, 29.06.2010.

- prioritizarea sarcinilor de supraveghere şi a responsabilităţilor la nivelul Ministerului Apărării;

- instituirea unor politici de apărare generale;

- suspendarea programelor de reintegrare şi reconciliere până în momentul în care societatea civilă va fi integrată procesului de consultare pe toate cele trei dimensiuni: executivă, legislativă şi juridică.[23]

Generalul William B. Caldwell, comandantul Misiunii NATO de Instruire din Afganistan (NTM-A)[24], responsabilă pentru crearea unităţilor militare şi de poliţie locale şi comandantul Comandamentului Integrat de Transfer al Securităţii din Afganistan (Combined Security Transition Command – Afghanistan)[25] consideră că cea mai mare problemă a Afganistanului este *analfabetismul*.[26] Doar 20% din populaţie are un grad cât de cât de pregătire. A doua problemă majoră identificată este generalizarea *corupţiei*, care a devenit un mod de viaţă şi este aproape un fenomen cultural. O a treia problemă majoră şi cea mai stringentă este *insurgenţa propriu-zisă a talibanilor*. Obiectivele forţelor de securitate internaţionale / naţionale vizează combaterea eficientă a insurgenţei şi menţinerea ei la un nivel scăzut, condiţie esenţială pentru a garanta stabilitatea guvernării. Guvernarea este foarte importantă pentru a răspunde nevoilor de bază ale societăţii afgane.

Campania de combatere a insurgenţei din Afganistan îşi propune să convingă populaţia afgană să susţină Guvernul central de la Kabul, şi nu guvernele talibane din umbră care există în multe din provinciile ţării. În acest scop, eforturile anticorupţie sunt considerate la fel de importante ca şi capturarea militanţilor, potrivit unor ofiţeri implicaţi în aceste operaţiuni.

Un important ofiţer american a declarat: *„dacă înainte întreaga noastră reţea se concentra asupra capturării şi uciderii membrilor*

[23] „A Force in Fragments: Reconstituting The Afghan National Army", *International Crisis Group*, 12.05.2010.

[24] Decizia privind crearea NTM-A a fost luată la Summit-ul NATO de la Strasbourg-Kehl, pentru instruirea Armatei Naţionale Afgane (ANA) şi a Poliţiei Naţionale Afgane (ANP).

[25] Ion M. Ioniţă, Octavian Manea**, „**Trupe SUA sub comandă românească. Admirabil", în cotidianul *Adevărul* nr. 6194, 21.06.2010, pp. 26-27.

[26] Misiunea NATO de Instruire în Afganistan derulează programe pentru alfabetizarea recruţilor din armată şi poliţie. Apoi, programul continuă în cadrul unităţilor pentru a ridica gradul de alfabetizare şi se speră ca în câţiva ani situaţia să se schimbe semnificativ în cadrul sectorului de securitate afgan. Programul este susţinut de 1200 de profesori afgani.

al-Qaida şi a talibanilor, acum încercăm să obţinem informaţii despre reţelele de corupţie".[27]

Războiul din Afganistan se află deja în cel de al zecelea an de derulare şi, după cum susţine secretarul american al apărării, Robert M. Gates, *„trebuie să se înţeleagă faptul că încă vor mai fi purtate lupte grele"*. Cu toate acestea, conflictul nu este nici etern şi nici fără speranţă.

Pentru a înţelege aceasta, trebuie însă să fie depăşite mai multe prejudecăţi, cum ar fi:

• *„afganii îi urăsc pe invadatori şi îi învinge întotdeauna";*

• *„situaţia din Afganistan este mult mai dificilă decât cea din Irak";*

• *„este obligatoriu să se negocieze cu talibanii";*

• *„nu există nicio strategie de ieşire din situaţia actuală sau de încheiere a conflictului".*

Interesul SUA în acest moment este cel al reintegrării talibanilor insurgenţi în cadrul societăţii afgane.[28] Au existat speculaţii că acest demers face parte din strategia Casei Albe de a se retrage rapid din Afganistan. Administraţia Barack Obama trebuie să conştientizeze faptul că insurgenţii negociază mai degrabă dacă se simt dezavantajaţi pe câmpul de luptă, iar talibanii au câştigat influenţă în Afganistan în ultimii patru ani, astfel încât SUA şi NATO trebuie mai întâi să îi slăbească pentru a putea demara negocieri cu aceştia. Experţii consideră că, în loc să încerce să confere legitimitate liderilor talibani seniori din Pakistan, SUA ar trebui să se axeze pe reconcilierea cu talibanii din Afganistan, mai ales că, în ultimele luni, Islamabadul a acceptat cooperarea pentru a modifica cursul evenimentelor din ţara vecină.[29]

Potrivit lui Mohammad Umer Daudzai, şeful de personal al preşedintelui afgan Hamid Karzai, forţele internaţionale trebuie să înceteze raidurile nocturne derulate asupra caselor rezidenţilor şi să-şi îndepărteze soldaţii din *„viaţa cotidiană a poporului"*, o strategie total diferită de cea a generalului David H. Petraeus, comandantul trupelor de coaliţie din Afganistan, care implică prezenţa soldaţilor în cadrul comunităţilor locale.[30]

---

[27] Thom Shanker, Eric Schmitt, „Serviciile americane de informaţii, implicate în lupta de combatere a corupţiei din Afganistan", în cotidianul *International Herald Tribune*, 14.06.2010.

[28] Hassina Sherjan, „Five Myths About Afghanistan", *Brookings Institution*, 22.03.2010.

[29] Lisa Curtis, „Taliban Reconciliation: Obama Administration Must Be Clear and Firm", *The Heritage Foundation*, 11.03.2010.

[30] David Nakamura, Joshua Partlow, „Şeful de personal al lui Karzai a declarat că Statele Unite trebuie să-şi schimbe strategia din Afganistan", în cotidianul „The Washington Post", 30.08.2010.

La începutul lunii septembrie 2010, grupul nepartizan de experți „Fundația Noua Americă" a publicat un raport în care prezintă o nouă strategie pentru Afganistan, intitulat „O nouă cale spre progres – Regândirea strategiei americane din Afganistan". În raport sunt prezentate cinci recomandări pentru o nouă strategie americană destinată războiului din Afganistan, care să permită o retragere relativ rapidă a forțelor americane, dar nu completă. Printre acestea se numără: concentrarea asupra formării unei coaliții de guvernământ şi a integrării politice, reducerea şi încheierea operațiunilor militare din sudul Afganistanului, acordarea unei atenții sporite grupării al-Qaida şi securității interne, încurajarea dezvoltării economice şi atragerea de investitori regionali şi internaționali.[31]

Conform aprecierii lui Henry Kissinger, generalul David Petraeus poate să câştige războiul din Afganistan, dar nu, în sensul convențional al luptei împotriva unui adversar cu care este posibil să se încheie un acord realizabil. Teoretic poate, în sensul înfrângerii în mod treptat a insurgenței şi a aducerii acesteia în stare de neputință, însă va dura mai mult decât permite sistemul politic american. Cel mai important principiu pe care generalul David Petraeus l-a introdus prin intermediul „doctrinei de Contrainsurgență" poate fi formulat astfel: *„You can't kill your way to victory"*. Oricât ai dori să foloseşti forța militară pentru a obține victoria, aceasta nu poate fi realizată exclusiv prin utilizarea puterii militare. Este necesară implicarea celorlalte dimensiuni şi elemente ale puterii naționale: *guvernare, politică, economie*.

Anunțarea însă a unei date limite pentru retragerea trupelor americane din Afganistan, în contextul în care uzura adversarului reprezintă unul dintre elementele strategiei, permite adversarului să-şi stabilească propriul ritm de luptă şi îi oferă un termen limită. Există necesitatea ca preşedintele Obama să reconsidere acest termen limită şi există nevoia de a regândi modul în care strategia a fost proiectată. A fost schițată pentru a preda responsabilitatea în ceea ce priveşte securitatea unui Guvern afgan la nivel național, ceea ce va fi foarte dificil de realizat, cel puțin conform termenelor limită stabilite. În cazul în care SUA menține aceste termene limită şi obiective nerealiste, principala problemă este aceea că elementele diplomatice şi cele militare ale actualei strategii nu sunt compatibile unele cu celelalte. Strategia militară nu poate fi realizată în termene limită, iar data limită îi încurajează pe adversari să aştepte retragerea trupelor americane.[32]

---

[31] „O nouă strategie americană pentru Afganistan?", www.stratfor.com, 10.09.2010.

[32] Daniel Dombey, „Interviu cu Henry Kissinger", în cotidianul *Financial Times*, 29.06.2010.

Fostul secretar de stat american, Colin Powell, nu crede într-o retragere rapidă a Armatei americane din Afganistan, în pofida grabei Administrației Obama, care doreşte demararea acestui proces din iulie 2011.[33]

Conform statisticii pe primele opt luni ale anului 2010, acesta este deja anul cu cele mai multe decese pentru armata americană în Afganistan, cu 323 de morți, în timp ce Barack Obama şi-a reînnoit promisiunea de începere a retragerii, programată pentru vara anului 2011.

Din cei 80 de soldați străini ucişi în luna august 2010, a treia lună cea mai sângeroasă pentru forțele internaționale în nouă ani de război, 56 provin din Statele Unite. În iunie 2010, au fost ucişi 102 soldați străini – din care 60 de americani – şi 88 în iulie 2010 – din care 65 de americani, potrivit site-ului independent icasualties.org. În anul 2009, au fost ucişi 317 soldați americani.

De altfel, potrivit unei evaluări a Centrului Național pentru Combaterea Terorismului din Statele Unite ale Americii, în anul 2009, intensificarea atacurilor teroriste din Pakistan şi Afganistan a condus la creşterea numărului victimelor în rândul civililor şi a transformat Asia de Sud în principala regiune teroristă a lumii, depăşind Orientul Mijlociu. Conform statisticilor agenției americane, mii de civili – în principal musulmani – continuă să fie ucişi în atacuri extremiste, contribuind la instabilitatea guvernelor adesea sărace sau slabe din regiune.[34]

Potrivit unui raport trimestrial al ONU, în anul 2010, gradul de violență din Afganistan a crescut semnificativ față de anul 2009, înregistrându-se cu 20% mai mulți civili ucişi şi cu 66% mai multe incidente de securitate. Raportul informează că, în primele zece luni ale anului 2010, peste 2 400 de civili au fost ucişi şi 3 800 răniți. În luna august 2010, au fost înregistrate, în medie, trei atacuri sinucigaşe pe săptămână.[35]

Generalul american David Petraeus, care comandă trupele americane şi pe cele ale NATO în Afganistan, a admis la sfârşitul lunii august 2010, la Kabul, că talibanii câştigă teren, dar el vede în pierderile alarmante din rândul soldaților străini o consecință a efortului Statelor Unite în acest război.

---

[33] Andrei Vălan, „Colin Powell: Armata SUA va mai sta mulți ani în Afganistan", agenția de ştiri *Agerpres*, 30.08.2010.

[34] „Situația din Pakistan şi Afganistan transformă Asia de Sud în principala regiune teroristă a lumii", în publicația lunară *Janes Intelligence Review* , 28.04.2010.

[35] Postul de televiziune „CNN International", 24.12.2010.

Conform generalului Petraeus, *„cred că nimeni nu poate contesta faptul că talibanii îşi extind prezenţa. Numărul atacurilor acestora a crescut, manifestare a faptului că, în acelaşi timp, şi noi am sporit resursele şi le-am cucerit o parte din sanctuarele pe care au reuşit să şi le construiască în ultimii ani. Iar când sanctuarele inamicului sunt ameninţate, el ripostează. Am spus de mai multe ori anul acesta (n.a. 2010) că situaţia se va îngreuna pentru forţele internaţionale „înainte de a deveni mai uşoară”.*

De altfel, „Raportul cu privire la progresul către securitate şi stabilitate în Afganistan”, realizat de Pentagon la sfârşitul lunii noiembrie 2010, subliniază că „progresul din regiune este fluctuant, înregistrând victorii modeste din punct de vedere al securităţii, al sistemului de guvernare şi al dezvoltării zonelor prioritare de operaţiuni”[36], generalul David Petraeus, comandant al forţelor americane şi ale NATO din Afganistan, a prezentat un bilanţ pozitiv al strategiei de contrainsurecţie întreprinse. În septembrie 2009, a indicat generalul Petraeus, cei trei stâlpi ai acţiunii conduse de coaliţia internaţională – securitate, guvernare, dezvoltare – prezentau disfuncţionalităţi. În acel moment, „am atins cel mai ridicat nivel de violenţă. Când înmulţiţi operaţiunile, violenţa creşte. Acum, această fază a trecut, iar încrederea afganilor sporeşte. Acest lucru presupune timp”. La sfârşitul anului 2010, progresele sunt „reversibile” şi realizările prevăzute sunt „foarte dificile”, dar situaţia s-a îmbunătăţit prin întărirea efectivelor militare, reorganizarea comandamentului Forţei Internaţionale de Asistenţă pentru Securitate (ISAF) a NATO, dar şi prin intensificarea pregătirii forţelor afgane şi a luptei împotriva corupţiei.[37]

Potrivit afirmaţiilor unor importanţi oficiali din cadrul NATO şi al Pentagonului, generalul David H. Petraeus, comandantul forţelor de coaliţie din Afganistan, a finalizat noile reglementări privind transferul unor responsabilităţi de securitate către forţele afgane, în decursul viitoarelor luni, solicitând trupelor aliate să se retragă progresiv din anumite regiuni, pe măsură ce s-a restabilit pacea în respectivele zone. Reglementările subliniază faptul că, în timp ce unele trupe vor părăsi Afganistanul, în condiţiile în care în zonele protejate de acestea se va restabili pacea, altora le-ar putea fi stabilite alte misiuni pe teritoriul statului. În acest sens, preşedintele afgan doreşte negocierea unui acord de securitate cu Statele

[36] Publicaţia *The Washington Times*, 24.11.2010.
[37] Publicaţia *Le Monde*, 24.11.2010.

Unite, care ar garanta angajamentul acestora în Afganistan după începerea retragerii forțelor americane în iulie 2011.[38]

Petraeus accentuează necesitatea ca trupele aliate să consilieze forțele de securitate afgane în scopul accelerării procesului de pace, la care ar putea lua parte cu succes ofițerii şi soldații din cadrul forțelor de poliție locale.[39]

Statele Unite vor cheltui aproximativ şase miliarde de dolari anual pentru pregătirea şi susținerea trupelor şi forțelor de poliție afgane, după retragerea trupelor combatante în 2011. Cheltuielile estimative ale SUA până în anul 2015, detaliate în cadrul unui document referitor la misiunea NATO de pregătire, reprezintă o confirmare a faptului că securitatea Afganistanului va depinde în mare parte de Statele Unite. Acest fapt ar putea reprezenta o problemă pentru administrația Obama, în contextul în care aceasta continuă să solicite finanțare pentru Afganistan din partea Congresului, într-o perioadă de reduceri a cheltuielilor bugetare.[40]

În contextul afirmației conform căreia retragerea trupelor SUA din Afganistan ar începe în luna iulie 2011, Pakistanul a intervenit pentru a completa ceea ce consideră a fi un vid de securitate în zonă.

Această operațiune este condusă de comandantul armatei pakistaneze, generalul Ashfaq Kiyani şi directorul serviciului pakistanez de informații ISI, generalul-locotenent Ahmed Shuja Pasha. Administrația americană a declarat că intenționează să poarte tratative doar cu acele grupări care încetează violențele, susțin Constituția afgană şi nu mai favorizează al-Qaida. Oficialii americani au menționat că rețeaua Haqqani nu îndeplineşte aceste condiții şi au catalogat perspectiva negocierilor dintre Karzai şi Haqqani drept deranjantă.[41]

O serie de oficiali din cadrul administrației Statelor Unite ale Americii şi un fost ministru afgan, Abdullah Abdullah, şi-au exprimat rezervele cu privire succesul tratativelor intermediate de Pakistan dintre preşedinte afgan Hamid Karzai şi grupările afiliate al-Qaida, susținând că

[38] John CK Daly, „Rerouting Logistics in Afghanistan", ISN Security Watch, 17.05.2010.
[39] Thom Shanker, „Petraeus a finalizat noile reglementări privind transferul securității din Afganistan", în cotidianul *International Herald Tribune*, 31.08.2010.
[40] Desmond Butler, „SUA va finanța pregătirea trupelor afgane", în cotidianul *The Washington Times*, 07.09.2010.
[41] Ashish Kumar Sen, „SUA are o atitudine rezervată cu privire la calitatea de negociator a Pakistanului", în cotidianul *The Washington Times*, 29.06.2010.

Islamabadul încearcă să-şi delege reprezentanţi în cadrul unui viitor Guvern la Kabul.

Afganistan – „statul din umbră"

Desfăşurarea scrutinului pentru camera inferioară (Wolesi Jirga) a Adunării Naţionale de la Kabul, care a avut loc în septembrie 2010, a accentuat instabilitatea politică şi nu a adus beneficii pentru regimul preşedintelui Hamid Karzai şi pentru eforturile de stabilizare a situaţiei interne depuse de coaliţia multinaţională.

Prăbuşirea Băncii Centrale din Kabul la jumătatea lunii septembrie 2010, ca urmare a dovezilor referitoare la deturnările de fonduri operate de fratele preşedintelui afgan, a reprezentat un nou semnal al extinderii fenomenului corupţiei. Anterior scrutinului au existat dovezi privind producerea, în regiunea pakistaneză Peshawar, a mii de cărţi de vot false. În astfel de condiţii, atât speranţele populaţiei afgane, cât şi ale comunităţii internaţionale referitoare la legitimitatea acestui scrutin au fost încă de la început destul de reduse.[42]

Reducerea numărului de incidente (aproximativ 300 faţă de 500, câte s-au înregistrat la scrutinul din 2009) este posibil să facă parte dintr-un proces mai amplu de „manipulare" informaţională a talibanilor, pentru ca electoratul să fie ţinut departe de urne. Se pare că islamiştii au reuşit: potrivit datelor Comisiei Electorale Independente de la Kabul, au fost exprimate aproximativ 3,6 din cele 11,4 milioane de voturi (comparativ cu 6,4 milioane de voturi înregistrate la scrutinul parlamentar din 2005 şi 4,6 milioane – la alegerile prezidenţiale din 2009).

Perspectivele nu sunt deloc optimiste. În condiţiile în care majoritatea dintre cei 2 447 de candidaţi la cele 249 de mandate nu au experienţă în ceea ce priveşte procesul electoral şi cu atât mai puţin procesul de „democratizare", capacitatea lor de a-şi duce la îndeplinire misiunea, dacă vor fi aleşi, a fost pusă sub semnul întrebării. Pe de altă parte, a compara situaţia din Afganistan cu standardele din ţările occidentale reprezintă un proces ineficient.

Este puţin probabil ca rezultatele să afecteze şi mai mult eforturile depuse de ISAF – Forţa Internaţională de Asistenţă de Securitate în vederea

[42] Susi Dennison, „Decision Time for Afghanistan", European Council of Foreign Relations, 17.09.2010.

asigurării stabilității politice. Dar, în cazul decretării „legitimității" scrutinului, administrația Karzai are o nouă provocare de înfruntat: în contextul în care dezaprobarea față de eforturile sale de a negocia cu talibanii şi a coopera cu Pakistanul este susținută, dialogul preşedintelui cu un Parlament în care rivalii săi politici ar putea avea un cuvânt de spus se anunță dificil. Până în prezent, Hamid Karzai „a beneficiat" de un for legislativ puternic din punct de vedere constituțional, prin ralierea mai multor lideri regionali influenți, în tentativa de a preveni configurarea unei opoziții puternice.[43]

Scrutinul nu va aduce schimbări semnificative în plan intern. Devenită singura forță efectivă în multe regiuni, mişcarea talibanilor a început deja să construiască un *„stat din umbră"*. Cu o susținere din partea țărilor europene din ce în ce mai redusă, cu un sprijin al populației locale şi mai scăzut şi fără a avea un partener credibil la Kabul, coaliția multinațională condusă de Statele Unite nu are şanse reale de a înfrânge insurgența. Pentru a reuşi, în locul începerii retragerii militare, în vara anului 2011, SUA ar trebui să suplimenteze din nou numărul de trupe. Devine imperativă, astfel, demararea negocierilor reale cu talibanii, care ar putea constitui o posibilă soluție la conflict.[44]

În prezent, talibanii reprezintă o amenințare serioasă la adresa Guvernului afgan în multe zone din țară şi manifestă o continuă capacitate de a submina securitatea internațională şi eforturile depuse în vederea stabilizării.

Cu toate că gruparea nu va putea să răstoarne guvernul atât timp cât în țară se vor afla trupele ISAF, există şanse mici ca aceasta să poată fi învinsă pe termen scurt.

Prin urmare – în contextul retragerii anticipate a trupelor ISAF din regiune, talibanii reprezintă o amenințare serioasă la adresa viitorului Guvernului afgan pe termen mediu şi lung.[45]

Din această perspectivă, conflictul din Afganistan este departe de a fi încheiat şi se pare că este nevoie ca această afirmație să fie reiterată mai ales în contextul în care mass-media evidențiază *„progrese"* în procesul de reconciliere, ca urmare a discuțiilor purtate de Guvernul de la Kabul cu insurgenții talibani.

---

[43] „Pitfalls in Afghanistan's Parliamentary Elections", www.stratfor.com, 18.09.2010.

[44] Gilles Dorronsoro, „Afghanistan Will Only Get Worse", Carnegie Endowment for International Peace, 14.09.2010.

[45] „Gruparea „Talibani" din Afganistan", periodic *Jane's World Insurgency and Terrorism Review*, 20.08.2010.

Două conflicte se desfăşoară astăzi în Afganistan: cel descris de armata SUA drept *„orientat în direcţia cea bună”*, care are „şanse mari de reuşită” – un război dur, dar însoţit de speranţă; cel definit de numărul tot mai mare de victime în rândul civililor şi militarilor în regiuni altădată sigure (cum ar fi nordul ţării), marcate acum de violenţă şi insecuritate, dar şi de corupţia şi incompetenţa guvernului şi de pesimismul populaţiei.

La o primă vedere, ar părea că anunţul debutului retragerii din Afganistan din iulie 2011, făcut de preşedintele american, Barack Obama, încă din toamna anului 2009, nu poate conduce la o schimbare a situaţiei, existând incertitudine cu privire la disponibilitatea insurgenţilor talibani de a negocia, atâta timp cât pot aştepta, pur şi simplu, retragerea americană. Pe de altă parte, este posibil ca negocierile să continue doar cu „permisiunea” serviciilor de securitate pakistaneze (un exemplu sau, altfel spus, un avertisment în acest sens fiind arestarea, în luna februarie 2010, a liderului taliban Mullah Abdul Ghani Baradar, aflat în proces de negocieri cu guvernul de la Kabul.[46]

„Mai mult timp” este ceea ce au cerut, în ultimii zece ani, susţinătorii campaniei militare din Afganistan, pentru a putea justifica atât suplimentarea numărului de trupe, cât şi cererile de alocare de noi fonduri pentru finanţarea conflictului. Doar „timpul” şi „strategia curentă” pot schimba cursul războiului şi conduce la învingerea definitivă a insurgenţilor talibani. În contextul în care prinde contur ipoteza conform căreia forţele de coaliţie au pierdut de multă vreme capitalul politic câştigat cu afganii – dacă mai era nevoie, o „dovadă” suplimentară a oferit însuşi preşedintele Hamid Karzai, care a confirmat „transporturile de bani gheaţă” dinspre Teheran, realizate în cadrul unui „proces transparent” – condiţiile în teren vor continua să se deterioreze şi pe fondul consolidării influenţei talibane pe întreg teritoriul ţării (situaţia din oraşele Jalalabad şi Kabul s-a înrăutăţit considerabil, în ultimele luni, iar influenţa autorităţilor în regiunile din nord este aproape inexistentă). În aceste condiţii, forţele de coaliţie se vor afla, în anul 2011, într-o şi mai mare dificultate.[47]

---

[46] Andrew Exum, „Smoke and Mirrors in Kabul”, *Foreign Policy,* 22.10.2010; Michael A. Cohen, „What's lurking behind the Pentagon's overly optimistic spinning of the Afghan war?”, *Foreign Policy,* 29.10.2010; Matt Waldman, „Dangerous Liaisons with the Afghan Taliban. The Feasibility and Risks of Negotiations”, United States Institute of Peace, octombrie 2010.

[47] Gilles Dorronsoro, „Think Again: the Afghan Surge”, *Foreign Policy*, 07.10.2010; „The U.S., Iraq and an Iranian Role in Afghanistan”, www.stratfor.com, 18.10.2010.

Soluțiile pe termen mediu şi lung pentru reglementarea situației din Afganistan trebuie să ia în considerare trei principii de acțiune: reforma politică, reconcilierea națională şi mecanisme de diplomație regională, în cadrul unui sistem politic funcțional care să fie capabil să preia sarcina luptei contra insurgenților. În acest context, Statele Unite trebuie să acționeze ca un broker al reconcilierii între toate formațiunile cu miză în societatea afgană. În loc să sprijine formațiunea lui Hamid Karzai, rolul diplomaților americani trebuie să fie acela de arbitru la masa negocierilor. Armata americană trebuie să-şi reconceptualizeze rolul pe acest teatru de război, principalul scop fiind acela de a antrena mai mulți ofițeri de poliție şi militari afgani. De asemenea, forțele de stabilizare (personalități, lideri spirituali şi religioşi) din interiorul comunităților locale trebuie susținute în măsura în care sprijină eforturile pentru pace. Investițiile americane trebuie să se îndrepte spre industria extractivă, agricultură şi infrastructură. Astfel, prin crearea unei baze de dezvoltare sustenabilă, Afganistanul îşi va reduce treptat nevoia de asistență din exterior.[48]

Experții consideră că un aspect ce nu poate fi ignorat în eforturile de stabilizare a țării este reformarea profundă a sistemului judiciar, considerat a fi într-o situație catastrofală. Pentru a submina puterea pe care talibanii încă o au în anumite regiuni ale Afganistanului, putere exprimată prin instituirea unui sistem paralel de judecată *(sharia)*, prin infiltrarea în structura socială din mai multe provincii afgane şi prin continua campanie de intimidare împotriva oricărei persoane ce cooperează cu autoritățile, factorii cu putere de decizie trebuie să adopte o serie de măsuri care cuprind, printre altele, revizuirea Constituției, reducerea nepotismului şi a venalității în sistemul judiciar, profesionalizarea celor care lucrează în acest sistem şi, nu în ultimul rând, eliminarea distorsiunilor cauzate de detențiile secrete, proceduri extrajudiciare aplicate deținuților suspectați de terorism şi metode de interogare care nu sunt în deplină conformitate cu standardele internaționale.[49]

Mai mult, nici evoluțiile la granițe, în special în zona de frontieră AfPAk, nu prezintă motive de a crede că țara se îndreptă spre regăsirea stabilității şi a echilibrului, fenomenul de migrație din aceste zone complicând şi mai mult o situație şi aşa dificilă. Organizațiile militante rivale din zona de frontieră dintre Afganistan şi Pakistan colaborează din ce în ce mai mult în comiterea raidurilor, acțiuni pe care oficialii din domeniul

[48] Richard L. Armitage, „U.S. Strategy for Pakistan and Afghanistan", Council on Foreign Relations, 12.11.2010.
[49] „Reforming Afghanistan's Broken Judiciary", International Crisis Group, 17.11.2010.

militar şi al serviciilor de informaţii le consideră a face parte din tentativa de a redobândi iniţiativa, după luni de zile de atacuri din partea forţelor americane şi aliate. Noile evaluări ale serviciilor de informaţii referitoare la această regiune menţionează că facţiunile insurgente au renunţat la rivalităţile istorice, unindu-şi forţele într-un mod nemaiîntâlnit anterior.

Concluzii

Prevenirea colapsului statal în Afganistan şi administrarea tranziţiei stabile şi de durată în responsabilitatea liderilor afgani ar permite Statelor Unite să alinieze cel mai bine obiectivele de securitate importante din regiune şi, pe termen lung, să sprijine pacea şi integrarea economică a regiunii Asiei de Sud. Statele Unite, împreună cu partenerii NATO-ISAF, trebuie să prioritizeze măsurile care să inducă reforme politice şi economice din partea Guvernului afgan, pentru a reuşi o retragere treptată şi totală din Afganistan în următorii trei ani. După anul 2014, Statele Unite pot oferi sprijin financiar Afganistanului şi pot menţine o forţă militară redusă, capabilă să întreprindă atacuri asupra grupărilor teroriste, să culeagă informaţii şi să ofere sprijin în antrenarea Forţelor de Securitate Afgane. Însă trebuie avut în vedere că o rezolvare durabilă a conflictului din Afganistan reprezintă o provocare extrem de descurajatoare, dat fiind faptul că există un grad mare de neîncredere între părţile implicate, astfel încât diferiţii actori aflaţi în lupta pentru putere sunt motivaţi mai degrabă de interese proprii pe termen scurt, decât de stabilitatea pe termen lung a statului afgan. Suferinţa poporului afgan, ca urmare a celor 30 de ani de război şi efectele adverse manifestate la nivel regional şi global, cauzate de instabilitatea statală ar trebui să fie un factor imperios pentru aliaţii din Afganistan şi pentru susţinătorii internaţionali ai acestora, pentru încheierea unui acord politic sustenabil.

În acest context, întrebările fără răspunsuri evidente care circulă în mediul academic vizează următoarele probleme:

- situaţia la următoarele alegeri din Statele Unite ale Americii, având în vedere promisiunea ce pare din ce în ce mai nefezabilă a preşedintelui Barack Obama privind anul 2011 ca început al retragerii din Afganistan;
- transformările strategiei „COIN" (contrainsurgenţă) a generalului David Petraeus, ulterior publicării documentelor secrete de către site-ul „Wikileaks", luând în considerare că talibanii au acum o „hartă" a strategiei pe care o pot studia şi contracara cu o mai mare eficienţă;[50]

[50] Marc A. Thiessen, „WikiLeaks' Blow to the Surge", American Enterprise Institute for Public Policy Research, 10.08.2010.

- modul în care trupele americane vor câştiga „inimile şi mințile" cetățenilor afgani fără a face aceleaşi greşeli ca în Vietnam, acum 40 ani;[51]

- capacitatea forțelor de ordine locale, de tipul milițiilor, de a lua locul firmelor private de securitate care îşi desfăşoară activitatea în Afganistan.[52]

O posibilă soluție pentru retragerea americană care să nu echivaleze cu o înfrângere în fața talibanilor ar putea fi realizată prin atragerea țărilor interesate ca situația să nu evolueze în sensul restaurării unui guvern taliban. SUA nu este singura forță care încearcă să contureze viitorul Afganistanului: puterile regionale şi cele emergente, Pakistanul, India, Iranul, Rusia şi China îşi urmăresc şi ele propriile interese în această zonă.

- **Rusia** (care se confruntă cu amenințări din partea grupurilor islamiste);

- **India** (conştientă de periculosul suport pe care Pakistanul l-ar primi de la Kabulul controlat de talibani);

- **Iran** (unde teocrația şiită este amenințată de gruparea sunnită Jundullah şi de extremiştii salafişti). Iranul, unde estimările plasează în jur de 2,5 milioane de cetățeni afgani refugiați încă din timpul invaziei sovietice, a început deportările acestora pentru a obține o pârghie de forță în relațiile bilaterale. Conştiente fiind de faptul că o țară pe teritoriul căreia se desfăşoară un teatru de război nu poate face față unui influx de proporții mari de populație, autoritățile de la Teheran încearcă să „convingă" aparatul politic condus de preşedintele Hamid Karzai că soluția pentru securitatea statului rezidă nu la Washington, ci în mâinile conducătorilor din capitala iraniană.[53]

- **Tadjikistan** (țară amenințată de factorul destabilizator al refugiaților afgani şi de grupările extremiste sunnite conduse de Hizb ut-Tahrir);

- **China** (amenințată de uigurii islamişti);

- **Uzbekistan**.

Recunoaşterea intereselor legitime ale acestor țări în ceea ce priveşte Afganistanul ar putea duce la o înțelegere realizată între forțele Statelor Unite, guvernul condus de Hamid Karzai şi talibani. Împărțirea zonelor de control între cei doi actori din urmă ar servi la ameliorarea situației,

[51] Roger Cranse, „The «Hearts and Minds» Guys", *Foreign Policy*, 13.08.2010.

[52] Michael A. Innes, „Afghanistan's «Militia» Problem: Can Local Defense Forces Replace Private Security Firms", The Jamestown Foundation, 12.08.2010.

[53] Ahmad K. Majidyar, Ali Alfoneh, „Iranian Influence in Afghanistan, Refugees as Political Instruments", American Enterprise Institute for Public Policy Research, november 2010.

cu condiția ca sfera de control a talibanilor să nu depăşească Pashtun-ul şi ca aeroporturile din țară să fie exclusiv sub controlul guvernului de la Kabul (pentru a nu permite talibanilor *„exportul"* fundamentalismului).[54]

Până în prezent, angajamentul comunității internaționale în Afganistan s-a bazat pe doi piloni: cel militar şi cel al reconstrucției civile. Ambii sunt indispensabili, însă nu suficienți. Ani la rând a fost neglijat într-un mod nepermis pilonul politic. Analiştii pun accentul pe soluția politică, pe un proces politic. Un proces care să se finalizeze printr-un aranjament în care să se regăsească toate grupurile din Afganistan.

Acest proces de negocieri trebuie, într-adevăr, derulat într-o manieră afgană, însă comunitatea internațională trebuie să-l sprijine. Iar când va veni momentul potrivit, vecinii Afganistanului vor trebui să andoseze rezultatul acestui proces, pentru a-l face stabil. Pentru că şi în cazul acestui aspect critic este valabil ceea ce s-a discutat astăzi în special în cadrul primului modul: avem o şansă la un Afganistan stabil, numai dacă vecinii nu vor exploata Afganistanul – aşa cum s-a întâmplat deseori în trecut – ca locație de derulare a propriilor lor conflicte de interese.

Experții sunt de acord asupra faptului că ne aflăm aici în fața unor mari provocări şi că interese diferite, care se exclud, în parte, reciproc, complică foarte mult situația. Însă, în pofida tuturor divergențelor de interese ale actorilor, există un interes comun.

Nimeni nu îşi poate dori în mod serios ca Afganistanul să se afunde în haos. În ciuda tuturor divergențelor, în ciuda neîncrederii şi a tuturor manevrelor, aici există o convergență obiectivă de interese. Acesta este cel mai mic numitor comun, asupra căruia se pot înțelege toți vecinii, toți actorii regionali.[55]

---

[54] Selig Harrison, „How to Leave Afghanistan Without Losing", *Foreign Policy*, 24.08.2010.

[55] Michael Steiner, însărcinat special al Guvernului federal german pe probleme legate de Afganistan şi Pakistan, „AFPAK – un nod gordian?", www.bnd.de, 16.11.2010, discursul susținut în cadrul celei de-a 11-a ediții a simpozionului internațional organizat de serviciul german de informații externe în data de 28.10.2010, la Hotel Estrel din Berlin.

INSTRUCȚIUNI PENTRU AUTORI

Misiune şi conținut. *Revista Română de Studii de Intelligence (RRSI) este dedicată studiilor de intelligence şi disciplinelor ştiințifice conexe, cu scopul de a facilita crearea unui forum de dezbatere pentru mediile profesional, academic, politic şi public.*

RRSI este o publicație nepartizană şi nonprofit care nu pledează în favoarea sau împotriva vreunei poziții, responsabilitatea pentru ideile prezentate aparținând în exclusivitate autorilor.

Politica de evaluare*. RRSI acceptă doar editoriale, articole şi recenzii care nu au fost anterior publicate.*

Editorii şi redactorii RRSI selectează materialele transmise de autori şi, acolo unde este cazul, le ameliorează prin dialog constructiv, doar cu acceptul acestora din urmă, asigurând astfel corectitudinea şi valoarea ştiințifică a materialelor ce urmează a fi publicate. Evaluarea calității academice a materialelor se face în anonimat ("blind review"), corespondența dintre evaluatori şi autori realizându-se doar prin intermediul e-mailului ani@sri.ro. RRSI garantează că lucrările nu sunt respinse/modificate pentru că ideile exprimate sunt contrarii altor studii publicate anterior sau pozițiilor evaluatorilor, ci doar în cazul în care nu fac dovada cercetării ştiințifice.

RRSI asigură confidențialitatea pentru materialele respinse de la publicare, precum şi pentru modificările aduse acestora.

Pregătirea materialelor pentru publicare

1. Forma de prezentare a lucrării

Articolele propuse spre publicare în RRSI se prezintă atât în format fizic, cât şi în format electronic pe adresa Academiei Naționale de Informații „Mihai Viteazul": Şos. Odăi nr. 20, sector 1, Bucureşti, ani@sri.ro.

Textul trebuie redactat cu caractere Times New Roman de mărimea 12, dublu spațiat. Prima pagină trebuie să conțină titlul lucrării şi afilierea autorului (nume şi prenume, titlu ştiințific, apartenența la o instituție/asociație/organizație, precum şi adresa de e-mail).

Articolul va fi însoțit de un abstract (de până la 100 de cuvinte) şi de cuvinte-cheie (keywords), ambele într-o limbă de circulație internațională.

Toate referințele bibliografice trebuie precizate (parentetic, note de subsol etc.).

Autorii sunt responsabili pentru obținerea oricărei permisiuni referitoare atât la publicarea unor materiale din alte surse, cât şi la respectarea oricăror restricții sau proceduri care țin de locurile de muncă unde activează ori au activat.

Odată publicat, materialul intră în proprietatea RRSI, iar fiecare autor primeşte câte un exemplar al numărului RRSI în care i-a fost publicată contribuția.

Aranjarea în formatul de carte tipărită a textului, figurilor şi tabelelor se face, de regulă, de către personalul de specialitate al Editurii Academiei Naționale de Informații „Mihai Viteazul".

Pentru citate se folosesc ghilimele („ – pentru deschidere şi ” – pentru închidere).

Figurile se numerotează. Titlul figurii se scrie cu un corp mai mic cu 2 pt decât textul de bază, imediat sub aceasta, fără spații, după care se dă explicația figurii, respectiv a graficului şi se precizează sursa, dacă este cazul.

Tabelele dintr-o lucrare trebuie să aibă o prezentare unitară. Se recomandă ca fiecare să fie numerotat şi să aibă un titlu. Titlul se scrie drept 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.

În cazul referințelor bibliografice din text, ordinea datelor este următoarea: numele şi prenumele autorului, titlul, volumul/ediția, editura, localitatea, anul, locul citat. Dacă lucrarea nu are autor, se trec trei steluțe liniare (***) sau numele instituției sub egida căreia a apărut lucrarea.

2. Referințe bibliografice

Bibliografia se plasează la sfârşitul articolului, după anexe.

De regulă, 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.

Titlul lucrării se scrie exact cum este tipărit în publicația citată, cu mențiunea că în cazul limbii române ortografia trebuie actualizată conform normelor Academiei Române.

De regulă, ordinea datelor este următoarea: numele şi prenumele autorului, titlul lucrării, volumul / ediția, editura, localitatea, anul.