Editors

Teodoru ŞTEFAN Irena DUMITRU

INTELLIGENCE IN THE KNOWLEDGE SOCIETY

Proceedings of the XVIIIth International Conference

Bucharest – 2013

Descrierea CIP a Bibliotecii Naţionale a României
Intelligence in the Knowledge Society / editors: Teodoru Ştefan, Irena Dumitru. - Bucureşti : Editura Academiei Naţionale de Informaţii *„Mihai Viteazul”*, 2013
Bibliogr.
ISBN 978-606-532-087-1

I. Ştefan, Teodoru (ed.)
II. Dumitru, Irena (ed.)

316.6

Editura Academiei Naţionale de Informaţii *„Mihai Viteazul”*
Telefon: 021 4106550/1186,1204
Fax: 0213104714

COLECTIVUL DE REDACŢIE

Redactori: Oana SANDU
Valentin NICULA
Tehnoredactare: Alexandra VIZITIU
Coperta: Valentin NICULA

Bun de tipar: 20.09.2013 Apărut: septembrie 2013
Tipărit sub comanda nr. 3973186/10.09.2013

ISBN 978-606-532-087-1

Intelligence in the Knowledge Society
Proceedings of the 18th International Conference

Content

Foreword

From the perspective of intelligence studies, Romania has offered an interesting case as an Eastern European country suffering from a totalitarian past, whose Communist security service had gained quite an ill-reputed fame before 1989. In this specific historical context, the Romanian Intelligence Service had to undergo, immediately after its creation in the early 90s, two parallel reform processes, of democratization and modernization, which made it aware of the need to shed away the legacy of its past and promote an open relationship with the academia and the society as a whole.

In its attempt to contribute to the creation of a security and intelligence culture, the Romanian Intelligence Service, through its National Intelligence Academy, has begun several projects aimed at bridging the gap between the secret world of intelligence and society. The first initiatives of this type were the creation of master programs within the National Intelligence Academy, addressing topics such as terrorism prevention, management of intelligence for national security and the protection of classified information, opened to people from outside the Service, interested or working in the field of national security and the creation of a joint MA program on intelligence analysis between the National Intelligence Academy and the University of Bucharest, designed to train a new generation of intelligence analysts for beneficiaries outside the intelligence community.

Another project was the creation of the National Institute for Intelligence Studies within the National Intelligence Academy, as a research entity focused on promoting and expanding the field of intelligence studies at national and international level. Its foundation was based on the certitude that intelligence is no longer valued for its secret nature and that the academic environment can be a potential partner which can provide weighty expertise. Therefore in a world where threats become more and more interconnected and intelligence

cooperation has moved from an ideal to an everyday reality, the creation of a space where intelligence practitioners and academics can meet and exchange ideas on the best ways to deal with these complex emerging challenges has become increasingly urgent.

In time the idea of providing a forum for discussion inside the Romanian intelligence community and academia, but not restricted to it, has taken the shape of the annual international conference on security and intelligence studies organized by the National Intelligence Academy, which in 2012 has reached its 18th edition.

Nevertheless, the 2012 Conference brought an element of novelty, as for the first time a wide variety of international experts in the field of intelligence and security studies met in Bucharest, to discuss the opportunities and obstacles faced by both the academic and intelligence communities in building an intelligence discipline and a national intelligence school, the intricacies of training intelligence analysts as well as issues related to the need for adaptation and flexibility in intelligence organizations as a means to remain competitive in the ever-changing international environment.

The interdisciplinary character of the papers presented together with the diversity of the problems addressed have contributed to making the debate rich in terms of value, underlying the intimate connection that should exist between the new field of intelligence studies and traditional study areas such as political science, ethics, law, history, psychology and sociology.

Moreover, this event has been a step towards broadening the perspective on national security, a field formerly reserved to state institutions, by allowing intelligence practitioners to engage with representatives of the academia and civil society, setting the stage for wider collaborations aimed at identifying and exchanging best practices in the field.

The conference has also acted as a confidence-building measure between the Romanian intelligence community and the civil society, the debates displaying a high level of transparency and openness. The goal of building a national security and intelligence culture has been brought closer with the creation, through such events, of networks of experts in the field as well as by defining the role which should be played by non-security actors in preserving the current security climate.

From an academic point of view, the debates have contributed to opening new paths of research in intelligence studies, by bringing into the limelight innovations made in the field of intelligence analysis instruments, possible interconnections between academic fields yet unexplored as well as complex intelligence problems transcending national borders.

In structuring this book, we have tried to emphasize all these novel elements, opting for those thematic criteria that emerged as most relevant throughout the debates: *Intelligence Education and Training: an Integrated Perspective, 21st Century Intelligence Analysis: Challenges and Opportunities, Transforming Intelligence Organizations: New Paths, Perpetual Processes, New Technologies: "Cyber-opportunities" or Cyber-threats?, Predictive Analysis: "Crystal Ball" or Scientific Method?, Intelligence: a Crossroad of Sciences.*

By publishing this volume we expect to increase academic and public awareness in the field of intelligence studies, both in Romania and abroad, while at the same time bringing a small, but we hope, significant contribution to the process of building a national security and intelligence culture.

The editors

Intelligence Education: Towards What Ends?

Stephen MARRIN*

Abstract

Intelligence studies and associated degrees in higher education are part of the wild west of academia; a place where there is much opportunity and few rules. It also has a bit of the gold rush thrown in, as academic institutions have taken advantage of the recent increase in funding that has been devoted to the intelligence and security sectors since the 2001 terrorist attacks. Over the past ten years, many new and different kinds of academic intelligence studies programs have been created at both the undergraduate and postgraduate levels. The one kind of degree that has not yet been created is the intelligence studies doctorate. As the doctorate is the 'end' of education, what are the potential benefits and problems associated with the creation of different kinds of intelligence doctorates?

The Beginnings of Intelligence Education

Intelligence education courses and programs were first proposed many years ago. In 1957 retired US Brigadier General Washington Platt recommended that intelligence organizations support the creation of educational programs consisting of "advanced courses, comparable to graduate courses in other professions" for those who wanted to have a career in intelligence[1]. In 1960, Peter Dorando suggested that academic colleges or universities create "a basic course of study in the meaning of intelligence, its significance as the foundation for policy planning and a guide for operations, how it plays those roles and the principles and processes by which it is produced and formulated"[2].

Over twenty years later, in 1983, the first postgraduate degree in intelligence was developed and offered by the US government to intelligence personnel through the Defense Intelligence College. After a number of name changes, the institution which currently offers the very same degree is the US National Intelligence University. A wide variety of courses on intelligence were also taught in colleges and universities, especially in the Washington DC area. By the1980s there were so many courses offered that a number of field surveys of intelligence education were published,[3] and the US government developed programs to support these efforts to teach intelligence[4].

* Lecturer, Brunel University

After the 9/11 terrorist attacks, a wide variety of intelligence education programs sprang up to meet the demand for more focused education and training in this area. Various efforts have been made to provide an overview of this growing field and assess its somewhat haphazard implementation[5]. Additional emphasis has been placed on describing and evaluating the more recent creation of intelligence education programs in the United Kingdom[6]. With the creation of the International Association for Intelligence Education (IAFIE) in 2004, information about teaching intelligence (programs, content, resources, etc) has been extended even further[7].

Intelligence Studies and Intelligence School

All of this work has shown that those who teach intelligence do so for a number of different purposes and from a number of different perspectives. The two main approaches are labelled intelligence studies, which is a way to gain greater understanding and knowledge about all aspects of the intelligence field, and intelligence school, which is a professional or vocational approach to intelligence education.

Intelligence studies degrees are conventional liberal arts degrees which use frames of reference from conventional academic disciplines in order to gain knowledge and understanding about intelligence as a function of government. These frames of reference can include political science, history, anthropology, sociology, communications, media studies, film or literature, and others. Intelligence studies began as an academic complement to the practice of national security intelligence; the contribution that higher education has made to interpreting its past, understanding its present and forecasting its future. The value of intelligence studies is primarily substantive knowledge; to provide the students with an understanding of what intelligence is, and what it has done. Students who take these courses do not have to then go on to work in the field of intelligence. Instead, it could be part of the foundation of knowledge they acquire about government in their university education before they go on to do other things. But these kinds of courses can also provide some useful knowledge for those who might want to become intelligence officers or analysts.

By way of contrast, intelligence school is a professional or vocational approach to intelligence education. A number of academic

programs have been created recently with an applied orientation; to produce practitioners with the knowledge, skills and abilities required for entry into the intelligence community as analysts. Those that do so are like other graduate-level public policy schools who prepare students for careers in government by providing them with knowledge about the field as well as some of the skills associated with it. In the United States, similar degrees are offered at the post-graduate level for entry into the respective professions: Law Schools are for those who want to become lawyers; Medical Schools are for those who want to become doctors; Journalism Schools are for those who want to become journalists; Business Schools are for those who want to go into business, and Education Schools are for those who want to become teachers. Each one of those different kinds of postgraduate degrees has a professional emphasis, and provides a credential that is more professional than it is scholarly. So the term "Intelligence School" is to clearly put the purpose of the education into the scope of the professional rather than the scholarly.

From the student's perspective, the existence of intelligence schools provides a very workable educational option for those who self-identify early as interested in entering the intelligence profession. Most of these practitioner-oriented schools tend to emphasize intelligence analysis because it is the analytic skill-set which is most easily developed in the academic context[8]. Intelligence schools teach students how to collect information, conduct research and evaluate source reliability and validity. In some programs they teach about certain kinds of collection methods like HUMINT or SIGINT, but in others the emphasis remains almost exclusively on open source research. Then they teach students to communicate their analysis effectively through written and verbal formats. Intelligence schools also sometimes teach critical thinking, argumentation, and structured analytic methods or techniques. Regardless of exactly what is taught, though, the emphasis remains on the development of a practitioner skill set.

Combining Intelligence Studies and Intelligence School

Neither intelligence studies nor intelligence school is better than the other. While each approach on its own is good, the combination of an academic approach to intelligence studies with

a practitioner's approach to intelligence school is better[9]. There is value in bringing the practitioner perspective and academic perspective together in the same place: with applied courses layered on top of a conceptual foundation built through acquisition of knowledge about the field. That way the educational institution can meet the needs of both sets of students, the liberal arts students and the pre-professional students, using appropriate knowledge and expertise as it does so. This also centralizes knowledge about the theory and practice of intelligence as a profession so that it can then be disseminated through to government, other parts of academia, the news media, and segments of society in a more structured way than has been done in the past[10].

Intelligence school is the best educational foundation for the core group of generalists who do much of the analytic grunt-work in the intelligence community, and intelligence studies is familiarization with intelligence for everyone else. Real subject matter experts—the specialists--are the anchors of the intelligence community. They have deep knowledge of the subject matter; the language, the culture, the history, and have sometimes lived in the areas that they are subject matter experts on. They provide a conceptual value added to the intelligence analysis product; a depth of knowledge that goes beyond the raw intelligence itself. These kinds of specialists should probably not go to intelligence schools. Instead, they should spend their time gaining additional knowledge and expertise. But intelligence studies courses providing concept and context might also provide value for specialists; to give them the kind of foundation that will prove to be useful for them later on in their careers. The generalists who work in the intelligence community, on the other hand, might have some language ability, some knowledge of culture, some knowledge of history, but their real role in the process is to provide decisionmakers with the best intelligence available on the subject precisely because they do not necessarily have the depth of knowledge or expertise to provide the best interpretation possible. But they do serve a very important purpose. What they need to know and what they need to do is different from what a specialist needs to know and what a specialist needs to do. So the education they need should be different as well; the best education for the specialist might be intelligence studies, and the best education for the generalist might be intelligence school.

A wide variety of different kinds of intelligence-oriented degree programs have been created in academia. There are undergraduate liberal arts degrees that include intelligence courses. There are undergraduate intelligence school degrees. There are undergraduate degrees that combine intelligence studies and intelligence school. There are postgraduate liberal arts degrees that include intelligence courses. There are postgraduate intelligence studies degrees. There are postgraduate intelligence school degrees. There are postgraduate degrees that combine intelligence studies and intelligence school. There are doctoral degrees that include the study of intelligence (conventional PhDs). But there are no intelligence-specific doctoral degrees.

The Ends of Intelligence Education

The PhD and the professional doctorate are the logical 'ends' of intelligence education, with the PhD as the end of intelligence studies and the professional doctorate as the end of intelligence school. The doctorate is the end of the line; there is no academic credential after the doctorate. But there are no doctoral degrees in intelligence. This is not because of lack of interest. There have been discussions in a number of universities about the creation of intelligence studies PhDs or intelligence studies professional doctorates. Nor has it been because of lack of a market. Demand exists from practitioners who want the reputation, prospects for promotion, and other professional benefits associated with a doctoral degree. The degrees have just not yet been created.

The reason the intelligence studies PhD has not been created is because it is not needed in order to create new kinds of knowledge. While PhDs take different forms in different countries, the general purpose of the PhD is "to make an original contribution to knowledge"[11]. A PhD in intelligence studies would have minimal to no unique value added vis-à-vis other bodies of knowledge or existing academic disciplines. It is possible to specialize in intelligence studies at the PhD level within existing academic disciplines (political science, history, anthropology, sociology, philosophy, communications, etc). The only value that an intelligence studies PhD would provide would be a specialization in intelligence studies literature, but it would come at the cost of losing the knowledge foundation and methodologies of the more traditional or conventional academic discipline. The end result would

be a weaker contribution to knowledge than would otherwise have been possible in a more conventional academic discipline. Why create something new that would be weaker than that which already exists?

There is another kind of doctoral degree, though, and that is the professional doctorate. This kind of doctorate can take a number of different forms. It could be for entry into the profession, in the same way that the law degree and medical degree are in the United States. Alternatively, it could be for building new knowledge about intelligence, from the practitioner perspective rather than from the purely academic perspective. This is more of a knowledge building effort like a PhD but done by practitioners for the purpose of building knowledge useful for practitioners.

There is positive potential to both of these forms of the professional doctorate. It would be good for the field to have a solid credential that would facilitate entry into the profession. Get the degree, take the test, and if successful the student would move to the top of the list in terms of entry into government. It would also be good for the field to have the opportunity to build useful knowledge in academia. Despite the appearance of value, however, a closer look reveals that there is minimal value to either kind of professional doctorate.

Professional Doctorate Not Needed for Entry into Profession

The first kind of professional doctorate, used for entry into the profession, would not be useful in an intelligence context because the intelligence field lacks the regulatory framework that exists in other fields. In other professions, professional associations play an important role in establishing and regulating the content of professional degrees. These associations help develop degrees that provide prospective new entrants into that profession with the knowledge, skills, and abilities that they will need to do well as practitioners. Some professions require that credential precisely because the practitioners (through associations) decided that they wanted to regulate the expertise of future practitioners by making sure that they went through a formal process to educate and acculturate themselves into the profession before they actually entered it.

In terms of intelligence, the first problem is that there are no overarching professional associations in the intelligence domain.

There are a variety of intelligence related associations that have been created in recent years, including the International Association for Intelligence Education and the International Intelligence Ethics Association, but neither is currently in a position to be able to create and enforce academic standards, accreditation requirements or certification processes. As conversations developed within IAFIE through the late 2000s, it became clear that intelligence educators do not yet know what should be required, what should be recommended, and what should be eliminated from either intelligence studies courses or intelligence schools. That is because they have not yet linked the content of either approach in intelligence education to the knowledge, skills or abilities required for the appropriate education or training of a proficient intelligence practitioner. Until professional intelligence associations first identify what it is that intelligence education programs should accomplish, and then evaluate how well they are meeting those goals, it will not be possible to synchronize content of a professional doctorate with standards developed by those professional bodies. Right now, those professional associations are still in their formative stages.

In addition, unlike both medicine and law in the US, it is possible to enter the intelligence profession without a professional doctorate. For example, it is possible to enter governmental intelligence organizations with either a bachelor's degree or more frequently a master's degree. Indeed, there are even programs which provide master's degrees to facilitate entry into government. For example, the School of Foreign Service at Georgetown University exists as a platform for getting into the Foreign Service precisely because of the foreign service exam. A doctorate is not required to pass the foreign service exam; instead, all that is needed is a good education. But in the intelligence field there is no exam to teach to for entry into the intelligence profession. As a result, the professional doctorate is not a requirement for entry, and if it were created probably would not help all that much in terms of helping students get jobs in intelligence.

Right now it is an open question as to whether intelligence is actually a profession rather than an occupation or a craft[12]. It may currently lack some important components of what makes a profession a 'profession'. Before intelligence schools and their degrees are going to be accepted as a legitimate feeder stream into

governmental intelligence organizations, it may be necessary for the field to become more professional through the creation of overarching professional associations and more formal standards and practices. In terms of intelligence education, if intelligence programs want their graduates to be seen as capable of doing the work of intelligence officers, they are going to have to make the case that their graduates meet and even exceed basic baseline expectations within government. If they cannot do that, then they will never gain widespread acceptance from hiring authorities. This has to be worked out over time between academic programs, hiring authorities, and professional associations, and the field is just beginning to have those conversations. It is years, probably decades, before the professional doctorate will be a requirement for entry into governmental intelligence organizations, if it ever happens at all.

Professional Doctorate Not Needed to Create New Knowledge

There is also minimal value to the second kind of professional doctorate which involves creating new knowledge by current or former practitioners. In theory, the value of this kind of professional doctorate would come from the opportunity for focused study of a single applied or practitioner-oriented research project that addresses a puzzle or problem with a focus more on the real world aspects of the problem than the more academic interests of the scholar. This would place it somewhere between a master's degree and a PhD, and that could potentially have value.

But it would be of minimal value precisely because a lot of knowledge can be acquired from different kinds of master's degrees. If someone wants to acquire in-depth postgraduate knowledge, that person can enrol in a master's degree program and acquire that knowledge. It is also simple to create interdisciplinary knowledge by enrolling in a master's degree that is interdisciplinary. Or, to specialize even further, one can take different kinds of master's degrees in succession; stack one kind of knowledge on top of another kind of knowledge. Through the dissertations and other projects associated with master's degrees, a current or former practitioner can develop a lot of new, useful knowledge which has value for the professional intelligence domain.

It is also possible to acquire significant amount of professionally-oriented knowledge through a PhD. As a study in Australia found, even though the numbers of professional doctorate programs has increased, "the numbers of students in these programs remain relatively low. In contrast, the PhD…has blossomed with increasing numbers of students in professional fields of study"[13]. The authors then go on to suggest that the professional doctorate has been less popular than expected because the PhD can have a professional orientation, is more flexible than many people believe, and as a result "candidates in professional fields prefer to complete PhDs." In fact, the development of the "new route PhD" in the UK which incorporates a taught component and makes it more like a PhD in the US makes specifying the unique value of the professional doctorate even more difficult[14].

What distinguishes the professional doctorate from other kinds of degrees is its engagement with the professional discipline rather than the academic discipline[15]. As a result, one of the differences between those students who choose to do a professional doctorate rather than a PhD has to do with the role they envision playing in the future. As British researchers Jerry Wellington and Pat Sikes point out, few professional doctorate students "see themselves as professional scholars, but many of them would wish to be seen, as a result of their professional doctorate, as being scholarly professionals—perhaps more would see themselves as 'researching professionals' once the doctorate had finished"[16]. Cardiff University, for example, suggests that students who see themselves as professional scholars think about choosing the PhD, and those who see themselves as scholarly professionals think about choosing the professional doctorate[17].

But in reality there may not be much of a difference between these two perspectives. Wellington and Sikes conclude that the unique value of the professional doctorate relative to the PhD does not have to do with the knowledge created, but rather the meaning that knowledge production has for the individual student. As they put it: "the skills developed in a professional doctorate are not perceived as being directly relevant to professional practice or to improving practice, but as helping students to reflect on and illuminate their practice and the practice in the institution where they work. In other words, the doctorate is seen as being largely of benefit to the individual rather than the profession as a whole"[18].

For that reason, the professional doctorate may be shifting to a 'practitioner doctorate' instead. In addition, as Janne Malfroy points out, professional doctorates only infrequently engage with professional organizations, and encounter much hostility in the workplace[19]. As a result, she suggests a reconceptualization of the purpose and value of the professional doctorate by emphasizing an individual's professional practice and change to professional identity or practice as key to its value proposition. Since this redefines a professional doctorate in such a way as to eliminate both the profession and the workplace, the end result is minimal to no unique value to the professional doctorate in terms of knowledge creation that cannot be created via either a PhD on the one hand or master's degrees on the other hand.

Professional Doctorate Could Create a Reputational Risk for Existing Programs

A final problem relates to the perception of rigor and programmatic quality. The creation of a weak professional doctorate would pose reputational problems to both new and existing intelligence degrees. There is a general concern about the quality of professional doctorates most everywhere because there is not a lot of different between a rigorous master's degree and a professional doctorate with minimal requirements. The danger is that the professional doctorate is seen as nothing other than a master's degree (or two master's degrees) in different form. For example, as one student in a professional doctorate program has pointed out: "I think that a lot of the so-called professional doctorates are bogus. When you look at the entry standards, the time required to complete, and the content of what the student has to produce, and what the professional doctorates are, as far as I'm concerned they are glorified master's programs and as much as anything they are just becoming money making ventures. I mean there are a lot of master's and master's honours programs that are as rigorous and more rigorous than some of the so called professional doctorates. …I'm just very skeptical about it"[20].

This is not an isolated concern. As Burton Bollag observes, "professional doctorates, which take less time than the PhD, are spreading fast—as are concerns about their uneven quality"[21]. Bollag then quotes a chancellor of a university as saying that "for the last

15
or 20 years, we've been under pressure to take what is basically a master's degree and call it a doctorate." Bollag also points out that an accreditation organization suggested that "there seems to be no obvious consistency among the various degrees as to the length of study; rigor, substance, or content of the program; or the ultimate utility of the degree to the person who earns it." This may be because, as Jeroen Huisman and Rahani Naidoo point out, "the development of professional doctorates…cannot be disconnected from the universities' income generation policies"[22]. Professional doctorates may be of financial value to the educational institutions which offer them, and may have professional advantages for the student who enrols in them, but the end result may be "a competitive rush to the bottom"[23].

An additional complication is that developing a weak professional doctorate at a reputable university could pose reputational problems for existing intelligence degree programs. Intelligence studies has academic credibility when linked to academia's traditional academic disciplines such as history, political science, or other social sciences. But intelligence studies on its own or in its applied form has struggled to acquire academic credibility. The risk of creating a professional doctorate is that the concerns about rigor and credibility shift to the existing master's and doctoral programs on the same subjects being done at the same institution in more conventional context.

Recommendation: Do Not Create New Intelligence Doctorates

Despite the potential value that intelligence doctorates appear to possess on first glance, it may be better to not create them at all. Perception of quality matters and—as John Taylor points out—many academics and some professionals believe that any doctorate other than a PhD "is, at best, an inferior award and, at worst, jeopardises the whole meaning and understanding of a doctorate"[24]. As a result, the downside risk associated with the creation of a new professional doctorate program would outweigh potential benefits. Rather than develop either a specific intelligence studies PhD or professional doctorate in intelligence, it would make more sense to bolster the proper ends of intelligence education: the conventional PhD for intelligence studies, and the master's degree for intelligence school.

References

[1] Washington Platt, *Strategic Intelligence Production: Basic Principles* (New York: Praeger, 1957), pp. 256-258.
[2] Peter J. Dorando, "For College Courses in Intelligence", *Studies in Intelligence*, Vol. 4, No. 3, 1960, pp. A15-A19.
[3] Marjorie W. Cline (ed.), *Teaching Intelligence in the mid-1980s: A Survey of College and University Courses on the Subject of Intelligence* (Washington, DC: National Intelligence Study Center, 1985); Hayden Peake, *The Reader's Guide to Intelligence Periodicals* (Washington, DC: National Intelligence Book Center, 1989).
[4] US Central Intelligence Agency, *Symposium on Teaching Intelligence,* October 1-2, 1993 (Washington, DC: Center for the Study of Intelligence, 1994); Ernest May, "Studying and Teaching Intelligence", *Studies in Intelligence*, Vol. 38, No. 5, 1995, pp. 1-5; US Joint Military Intelligence College, *Teaching Intelligence at Colleges and Universities. Conference Proceedings* (Washington, DC: Center for Strategic Intelligence Research. 18 June 1999); US Joint Military Intelligence College, "A Flourishing Craft: Teaching Intelligence Studies", in Russell G. Swenson (ed.), *Papers Prepared for the 18 June 1999 JMIC Conference on Teaching Intelligence Studies at Colleges and Universities* (Washington, DC: Center for Strategic Intelligence Research, June 1999).
[5] Martin Rudner, "Intelligence Studies in Higher Education: Capacity-Building to Meet Societal Demand", *International Journal of Intelligence and Counterintelligence,* Vol. 22, No. 1, Spring 2009, pp. 110-130; Peter Monaghan, "Intelligence Studies", *Chronicle of Higher Education*, 20 March, 2009; William Spracher. "Teaching Intelligence in the United States, the United Kingdom, and Canada" in Robert A. Denemark (ed.), *International Studies Encyclopedia* (Malden, MA: Wiley-Blackwell, 2010), pp. 6779-6800; Stephen Campbell, "A Survey of the U.S. Market for Intelligence Education", *International Journal of Intelligence and Counterintelligence,* Vol. 24, No. 2, Summer 2011, pp. 307-337.
[6] Michael S. Goodman, "Studying and Teaching About Intelligence: The Approach in the United Kingdom", *Studies in Intelligence* Vol. 50, No. 2, 2006, pp. 57-65; Philip H. J. Davies, "Assessment BASE: Simulating National Intelligence Assessment in a Graduate Course", *International Journal of Intelligence and Counterintelligence*, Vol. 19, No. 4, Winter 2006–2007, pp. 721–736; Michael S. Goodman and Sir David Omand, "What Analysts Need to Understand: The King's Intelligence Studies Program", *Studies in Intelligence,* Vol. 52, No. 4, Dec. 2008, pp. 1-12.
[7] Mark Lowenthal, "Intelligence as a Profession: IAFIE Sets Its Sights", *American Intelligence Journal*, Summer 2006, pp. 41–42.
[8] See chapter titled "Improving Intelligence Analysis through Training and Education" in Stephen Marrin, *Improving Intelligence Analysis: Bridging the Gap between Scholarship and Practice* (London: Routledge, 2011); Stephen Marrin. "Training and Educating US Intelligence Analysts", *International Journal of Intelligence and Counterintelligence*, Vol. 22, No. 1, Winter 2008-2009, pp. 131-146; James Breckenridge, "Designing Effective Teaching and Learning

Environments for a New Generation of Analysts", *International Journal of Intelligence and Counterintelligence*, Vol. 23, No. 2, Summer 2010, pp. 307-323; Michael Landon-Murray, "Social Science and Intelligence Analysis: The Role of Intelligence Education", *Journal of Applied Security Research*, Vol. 6, No. 4, 2011, pp. 491-528; Kristan J. Wheaton. "Teaching Strategic Intelligence Through Games", *International Journal of Intelligence and Counterintelligence,* Vol. 24, No. 2, Summer 2011, pp. 367-382; Timothy Walton, *Challenges in Intelligence Analysis: Lessons from 1300 BCE to the Present* (New York: Cambridge University Press, 2010); Thomas W. Shreeve, *Experiences to Go: Teaching with Intelligence Case Studies* (Washington, DC: Joint Military Intelligence College, September 2004); Ernest R. May and Philip D. Zelikow (eds.), *Dealing with Dictators: Dilemmas of U.S. Diplomacy and Intelligence Analysis, 1945–1990. BCSIA Studies in International Security* (Cambridge, MA: The MIT Press, 2006).

[9] This has been described as an intelligence studies equivalent to a Reece's Peanut Butter Cup solution; the combination of chocolate and peanut butter - the best of both worlds - like a Reece's Peanut Butter Cup.

[10] Stephen Marrin, "Intelligence Studies Centers: Making Scholarship on Intelligence Analysis Useful", *Intelligence and National Security*, Vol. 27, No. 3, June 2012, pp. 398-422.

[11] John Hockey, "The Social Science PhD: A Literature Review", *Studies in Higher Education*, Vol. 16, No. 3, 1991, pp. 319-332.

[12] Stephen Marrin and Jonathan Clemente, "Modelling an Intelligence Analysis Profession on Medicine", *International Journal of Intelligence and Counterintelligence*, Vol. 19, No. 4, Winter 2006–2007, pp. 642–665; George Allen, "The Professionalization of Intelligence", *Studies in Intelligence,* Vol. 26, No. 1, Spring 1985, pp. 23–31, reprinted in Douglas H. Dearth and R. Thomas Godden (eds.), *Strategic Intelligence: Theory and Application*, 2nd ed. (Washington, DC: Joint Military Intelligence Training Center (JMITC), 1995.

[13] Terry Evans, Peter Macauley, Margot Pearson and Karen Tregenza, "Why Do A "Prof Doc" When You Can Do a PhD?", *Fifth International Conference on Professional Doctorates*, Higher Education Academy, UK, 2005.

[14] Chris Park, "New Variant PhD: The Changing Nature of the Doctorate in the UK", *Journal of Higher Education Policy and Management*, Vol. 27, No. 2, July 2005, pp. 189-207; "New Route PhD Programme Handbook 2012-2013", Brunel University, 2012.

[15] Jeroen Huisman and Rajani Naidoo, "The Professional Doctorate: From Anglo-Saxon to European Challenges", *Higher Education Management and Policy,* Vol. 18, No. 2, 2006, p. 57.

[16] Jerry Wellington and Pat Sikes, "'A Doctorate in a Tight Compartment': Why Do Students Choose a Professional Doctorate and What Impact Does it Have on Their Personal and Professional Lives?", *Studies in Higher Education*, Vol. 31, No. 6, December 2006, p. 725.

[17] "PhD or Professional Doctorate", Cardiff University School of Nursing and Midwifery Studies, Cardiff University, available at http://www.cardiff.ac.uk/sonms/degreeprogrammes/postgraduateresearch/phd-or-profdoc.html
[18] Wellington and Sikes, "A Doctorate in a Tight Compartment", p. 733.
[19] Janne Malfroy, "Conceptualization of a Professional Doctorate Program: Focusing on Practice and Change", *The Australian Educational Researcher*, Vol. 31, No. 2, August 2004, p. 63.
[20] Ruth Neumann, "Doctoral Differences: Professional Doctorates and PhDs Compared", *Journal of Higher Education, Policy, and Management*, Vol. 27, No. 2, July 2005, p. 184.
[21] Burton Bollag, "Credential Creep" *Chronicle of Higher Education*, 22 June 2007, available at http://chronicle.com/weekly/v53/i42/42a01001.htm
[22] Jeroen Huisman and Rajani Naidoo, "The Professional Doctorate: From Anglo-Saxon to European Challenges", *Higher Education Management and Policy,* Vol. 18, No. 2, 2006, p. 55.
[23] *Ibid.*
[24] John Taylor, "Quality and Standards: The Challenge of the Professional Doctorate", *Higher Education in Europe*, Vol. 33, Issue 1, 2008, pp. 65-87. As cited in: Rebecca Attwood, "Scholars Remain Unconvinced About the Value of Professional Doctorates", *Times Higher Education*, 14 August 2008.

Some Major Challenges Academic Intelligence, and Intelligence Education and Training Are Confronted with

Florin DIACONU[*]

Abstract

For almost twenty years, the author of this study has continuously worked for some of the most prestigious academic institutions in Romania, dealing with both Political Science and International Relations: the Institute for Political Science and International Relations of the Romanian Academy, the Political Science Department/Faculty of the Bucharest University (teaching here Geopolitics, Praxis of International Relations, Strategic Studies, Introduction to International Relations, and Seapower in International Relations), and the Romanian Diplomatic Institute (here my work is one with direct research responsibilities concerning some of the most significant political-military balances of power and evolutions at regional and global levels, but also the foreign policy of the U.S. and Great Britain, and significant evolutions of the large scale conflict some authors and political leaders call Global War on Terror – GWOT). Along these many years of research and teaching, the author of this study was directly confronted (sometimes together with his students) with several significant challenges, relevant for a debate focusing the attention on the main topics of our panel (a panel called 'Towards a Science of Intelligence at the Beginning of the 3rd Millennium'). A very brief list of such intellectual challenges compulsorily includes several elements: the need to predict elements of the future, with very limited pieces of information/intelligence, and against a quite strong academic tradition stating that Political Science analyze and do not offer predictions; the necessity to operate with pieces of information/intelligence which are neither completely accurate, nor really complete; the need to extensively use contradictory pieces of information/intelligence; and the need to operate a clear distinction separating realities and wishful thinking. All these will be presented accompanied by some significant details and examples.

Along the pages of this very condensed presentation the central meaning of *Intelligence* – seen both as a process and as a product (or final result) – is that available in a notorious work, *The Craft of Intelligence*, written several decades ago by Allen Dulles. The former Director of the Central Intelligence Agency (CIA) wrote in 1963, almost two years after the moment when he had retired, quoting a statement

[*] Associate Professor, Political Science Faculty, Bucharest University
Senior Researcher, Romanian Diplomatic Institute
Director, Hans J. Morgenthau Center for Strategic Studies, Applied Geopolitics and Security Studies

addressed to the U.S. government by the task force on Intelligence Activities of the second Herbert Hoover Commission, that "Intelligence deals with all the things which should be known in advance of initiating a course of action". Dulles deliberately and strongly emphasized the fact that this very modern definition is strongly resembling the ideas of the ancient Chinese author Sun Tzu, who wrote about foreknowledge (seen as a major element of good Strategic Intelligence) that it represents "the reason the enlightened prince and the wise general conquer the enemy wherever they move"[1]. The common denominator of the definitions of Intelligence issued by both Sun Tzu and Allen Dulles is obvious:

- *Intelligence is a tool* decision-makers, both civilian and military, strongly need, clearly anytime and anywhere;
- *Intelligence is made up of various strata and elements (a structure we might describe as being a non-homogenous mix)*, a feature really important mainly when and if all these pieces of knowledge, put together, enhance the chances of the decision-maker to make really effective decisions;
- Intelligence represents a really significant process and/or result almost only in a *highly competitive environment*, as International Relations are in most occasions;
- The political and strategic value of Intelligence becomes *more obvious in case of major political-military conflict*.

All these features Intelligence perennially has are connected, in a way or another, even if not very obviously and not in a continuous way, with *some* activities of academic institutions of all sorts (and I have to strongly underline that two types of such institutions are most heavily taken into account here – research entities and universities whose *main* activities are *neither* academic Intelligence, *nor* Intelligence education and training).

A supplementary methodological explanation is necessary here, I think. In several occasions, I deliberately decided to use strong – and sometimes quite well-known – historical examples. Such an approach might be legitimately questioned by a large share of the audience, for a very simple reason: in the end, Intelligence (as a process) is the ability of individuals and groups to collect and interpret elements of the ongoing realities, in order to offer the decision-makers a tool enhancing their chance to reach really effective decisions. In such a situation, as long as the decision-making process is taking place *now*, what's the use of exploring

moments belonging to a *very* distant past? Of course, *there is no direct use* of doing this. But, at least in the context of BA and MA programs in universities, *history generally offers a lot of examples and situations useful in shaping, consolidating and testing emerging professional skills of several sorts*. And, if the young Army officer studies the campaigns of Hannibal, even if now elephants, heavy cavalry and archers are not used any more, it might be useful, I think, to start educating young students along the very long path potentially leading them to a professional career in the field of Intelligence by making them solve more and more complex Intelligence problems present in many historical episodes. *The method has an obvious extra merit: we already know which the decisions were, based on analyzing the elements of Intelligence we are using (better or worse than our distant ancestors did) in a procedure which is just an exercise, risk free in terms of cost and consequences*. If such an interpretation is accepted, the quite large number of historical examples in this brief study is not going to disturb anyone (I hope).

There are *many* major challenges connected, in a way or another, to using – or generating – Intelligence in academic contexts. *Lacking really adequate resources is one of them*. *Very* often, in almost all my previous and present jobs I have been confronted with not having something really important: either enough time to accomplish really desirable results; or enough literature to explore; or free access, in real time, to coherent sets of pieces of information to be processed in order to generate completely sound analytical or predictive final products of all sorts. But such hardships and shortcomings, even if very important in generating major obstacles along the path of successful research, *are not* the main topic of my presentation. And this happens just because I am fully aware – together (or at least so I presume) with some of my colleagues and with some of my former students present here, today – that lacking enough time or lacking adequate amounts of other vital resources is a *very* usual feature of the activity of almost any individual and group, almost anytime and almost anywhere. That is why I will try, along the next few minutes, to explore, in some occasions by means of presenting a number of significant examples, four major intellectual challenges the *civilian* Romanian academic environment has to cope with, when it is involved in generating products which have *some* academic Intelligence elements, or in Intelligence education and training activities of all sorts.

Challenge no. 1: Problems Associated with (or Generated by) Predicting the Future

There is a really serious tradition of *predicting some significant elements of the future* in the Western culture. At the beginning of the 16th century, for example, a gifted, interesting and innovative, but at that time quite obscure Italian author, Niccolo Machiavelli, wrote a lot about some politically significant issues clearly belonging to a *very* distant future, many generations away: first of all, the grand design of uniting the entire Italian peninsula in a single mighty state able to balance, in case of need, France and the German Empire; and secondly, the idea of establishing, maintaining and operating what we call today *national armies*[2], institutional structures shaped, up to a certain point, in direct contradiction with the notoriously potent – and sometimes astonishingly successful – tradition of the mercenary armies[3].

Quite clearly, when we make predictions, we *naturally tend to focus the attention on some issues, accidentally or deliberately neglecting (or placing in a cone of shadow) other aspects*. The problem is that, at least sometimes, the topics not properly explored prove themselves to be *very* important, and in quite many occasions *more* significant, in the long run, than some of the realities whose evolution is explored with a lot of attention and details. Let us see an example of this sort: In the opening stages of the two decades separating World War I and World War II, an Italian author became one the forefathers of strategic bombing. Douhet stated that, in just a few years, the traditional way of waging war, together with the relatively stable balance(s) of power at regional, continental and global level will be significantly altered by massive formations of bombers[4]. Anyhow, his prediction – broadly stating that victory will mean, more and more, a skilful and massive use of the concentrated power of large and very large bomber formations (several hundred or even 1,000 planes strong) – neglected at least two major realities correlated, historically, with the astonishing success of strategic bombing. The first reality Douhet almost naturally ignored is the basic fact that, the stronger the pressure of strategic bombing becomes, the stronger becomes, as well, the will of the foe to protect, in different ways, what we call today COGs of all sorts (for example, if we speak about vital industries, simply by abandoning the habit of concentrating them in huge centers; de-concentrating vital sectors of strategically significant industries proved itself to be a successful

method to annihilate the mighty devastating power of Allied strategic bombing in the case of Germany, in World War II, and the same method is now replicated again by the Iranians, who deliberately avoided to place all their nuclear facilities in the same region). A second major reality Douhet ignored is the clearly quickly changing nature of war. Along several centuries of *modern* European and global historical evolution, most wars were fought by states, whose competitors were other states. I mean by this that, in a way or another, traditional war is naturally dominated by a strong *symmetry* – state versus state, regular army versus regular army, national economy (dominated by massive industrial facilities) versus national economy (dominated also by almost similar massive industrial facilities). But, more recently, *several* really massive strategic bombing campaigns aimed to destroy targets of a more non-regular, more volatile and more elusive nature, within the general framework of conflicts not any more dominated by symmetry: such targets were, sometimes, improvised logistical services operating a multitude of tiny and non-regular routes and a huge variety of transportation devices (the case of the so-called Ho Chi Minh trail in Vietnam and Laos), or tiny groups of irregulars – former guerrilla fighters, terrorists, highly motivated leaders obsessed by their desire to harm as much as possible the Western world and, above all, the U.S. (the case of Afghanistan in the late stages of 2001 and early stages of 2002). In these both occasions, no massive targets of *traditional* sort were available, no irreplaceable damages could be inflicted by even the most destructive and skilled bombing raids[5]. But, of course, Douhet could not have been able to predict such developments, simply because he focused on the very logic of strategic bombing, not on massive and quick changes of the very nature of war.

For better understanding the fact that *realities and trends can dramatically change, badly damaging the chance to use very simple, 'linear' predictions*, let us evaluate another simple and significant example. At this very moment, if we try to analyze, because of very obvious and very serious reasons, different constitutive elements of the national power of several political actors in the Arab-Persian Gulf Area, we can easily identify an almost general pattern: Iran is more potent than any of its Arab competitors (in terms of Gross Domestic Product, of labor force, of military personnel, of total number of airports of all sorts – including heliports and airports with unpaved runways, etc), but clearly less powerful than all the countries belonging to the Gulf Cooperation

Council (GCC) put together. At the same time, other figures really significant for both a better understanding of national power of different states in the region, and for a better understanding of significant trends of the balance of power in the area do not necessarily belong to this general (or at least really widespread) pattern. To be more precise, we might be tempted to take into account the predictive value of the resources poured by different states into education. If we do this, we are confronted with a situation in which national education seems to be a significant priority for Tehran (4.7 % of the GDP), while most of the GCC have significantly smaller percentages of the GDP used in education: 2.9 % for Bahrain, 3.5 % for Qatar, 3.8 % for Kuwait, 3,9 % for Oman, a very low 1.2 % for the United Arab Emirates and only one country, Saudi Arabia, with a percentage larger than that used by Iran in education – 5.6 %[6]. Such figures might be the foundation for a prediction stating that, in the future, at least some of the fragilities and vulnerabilities of Iran might be compensated, up to a certain point, simply by pouring more resources in the educational system. But such a prediction *might* easily be badly mistaken, because of at least three major reasons:

- First of all, these figures do not seem to take into account the potentially significant role of private efforts in education (made by more or less wealthy families, by larger communities, by local and Western NGOs).
- Secondly, it is not at all clear which the real effectiveness of such budgetary efforts is. We might easily imagine that, at least in some occasions, a significant percentage of the cash used by both Iran and the Arab states in the Gulf area for education are poured into strictly religious schools (mainly in the countryside), with a very limited role in developing and strengthening vital elements of the national power.
- And thirdly, *we cannot accurately forecast how these percentages are going to evolve.* And it is only a matter of political will to sharply increase (or, on the contrary, to decrease or to maintain at a quite low level) the amount of cash poured into the educational system. To better understand such a problem, it is obvious that, increasing resources available to the educational system with only 8 to 9 % a year, a country spending now only 2.9 % of its GDP for education might reach, in at most 10 years, 5.8 % of its GDP, a significantly higher percentage than that used by Iran at this very moment.

At the end of this segment of my presentation, it might be useful to underline the fact that, in *some* of the institutional contexts in which I have been involved, for shorter or longer terms, there was (and still is) another significant obstacle to be bypassed, as well: a *strong belief* that political science (together with other social sciences of all sorts) is a mental tool, a set of methods, an academic discipline *aiming to analyze and not aiming (or maybe not even fit) to predict*. Such a belief, well or less well founded, academically, has a major flow: it simply dissolves, from the very beginning, the chance to develop, starting with early stages of the teaching/learning processes, the ability of students to build and test sound predictions; and we have to remember that this very ability is enormously useful in almost any *political* context dealing with various facets of power on the international arena, and also in very many *institutional* contexts of all sorts (including those directly and massively involved in Intelligence work).

Challenge no. 2: Problems Associated with (or Generated by) Not Very Accurate and Incomplete Sets of Information/Intelligence

Some other important problems and difficulties are to be coped with, in many occasions, when we are using clearly *not complete sets of data/pieces of information/pieces of Intelligence*, mainly present in *most* of the open sources we almost daily are using in research work and in teaching and learning processes. One potent example of this type is the way in which even very serious authors in the Middle Ages, vital for *any* serious effort attempting to explore the deeds of really charismatic and definitely important political and military leaders offer the analyst an adequate amount of details. We have to emphasize the basic fact that we are not speaking here about ordinary details we might ignore without major problems of any sort, but about basic data and figures we badly need to generate really accurate evaluations. Let us explore, for example, a notorious biography, that of Charles the Great (Charlemagne), the founding father of the medieval political idea (and tradition) of empire in Western Europe. Eginhard, the author of this notorious biography, is, quite clearly, the embodiment of many of the best features cultural life – and bureaucratic environment/institutions – in his era could

generate. His work has several important qualities no one can deny: it is adequately short; it does not mix, usually, naked truth with political correctness of that distant past; it does not exaggerate either the charisma of Charlemagne, or the difficulties he was confronted with; it does not focus the attention only on the core regions of the empire, but it presents, with some vivid details, the political and strategic realities or the geographic periphery of the Carolingian state as well; in many occasions, it offers many figures (for example, how long were some wars, how many the combat casualties and collateral casualties of some campaigns were). But, in spite of all these positive assets, *Vita Karoli Magni*[7] is *not* at all a *really* complete source of *strategic Intelligence*. For example, the text tells almost nothing about several very significant issues. We can easily list several really important realities and data of this sort, clearly stating that, without these pieces of Intelligence, we cannot deliver a really accurate and really complete evaluation of the strategic effectiveness of Charlemagne:

- The text does not present, in most occasions, accurate and complete data (figures) concerning the manpower used by the Carolingian state and by its foes in different wars.
- The text does not offer accurate and complete figures, vital for any effort attempting to estimate the aggregate costs of the wars and, in the end, of imperial expansion and of operating the empire;
- The text does not offer precise and complete data concerning the combat casualty ratio for both Carolingian armies and the armies of the enemies of the Carolingian state.
- The text does not offer complete data (figures) concerning the way in which reinforcements were raised and used in order to make some campaigns gain extra momentum.
- The text does not offer complete sets of data concerning the chronology of events, not allowing us to find out, for example, how large and how difficult was the effort of the Carolingian empire to fight several wars concomitantly.

Another example might put some useful extra emphasis on this very type of problem. Let us imagine, again, that we are trying to analyze various other facets of the general balance of power in the Arab-Persian Gulf area, a topic we already have talked about. One of the potentially significant items we can use as a solid element within the foundation of a sound estimate is the total number of airports of different types (major ones with very long paved runways, minor

ones without paved runways, and heliports) states in the area have and can use for both civilian and military aircraft. A clearly serious open source of Intelligence, the *World Factbook* generated and updated by the Central Intelligence Agency (CIA) offers us a lot of useful figures dealing with this very issue (see *Table 1: Airports in the Arab-Persian Gulf Area*).

Table 1. Airports in the Arab-Persian Gulf area, according to the CIA's *World Factbook*[8]

Country	Total number of airports of all sorts (plus separate figure for heliports)	Significant details (how many of them with paved runways; how many of them with runways longer than 3,047 meters)
Iran	324 plus 21 heliports	324 airports; 136 of them with paved runways, 42 of them with runways longer than 3,047 meters; plus 21 heliports
Iraq	104 plus 20 heliports	104 airports, 75 of them with paved runways, 20 of them longer than 3,047 meters; plus 20 heliports
Bahrain	4 plus 1 heliport	4 airports, all of them with paved runways, 3 of them with runways longer than 3,047 meters; plus 1 heliport
Kuwait	7 plus 4 heliports	7 airports, 4 of them with paved runways, 1 of them with runway longer than 3,047 meters; plus 4 heliports
Oman	130 plus 3 heliports	130 airports, only 12 of them with paved runways, 6 of them with runways longer than 3,047 meters; plus 3 heliports
Qatar	6 plus 1 heliport	6 airports, 4 of them with paved runways, 3 of these with runways longer than 3,047 meters; plus 1 heliport
Saudi Arabia	216 plus 10 heliports	216 airports, 80 of them with paved runways, 33 of these with runways longer than 3,047 meters; plus 10 heliports
United Arab Emirates	42 plus 5 heliports	42 airports, 25 of them with paved runways, 12 of these with runways longer than 3,047 meters; plus 5 heliports
Yemen	57 plus 0 heliports	57 airports, only 17 of them with paved runways, only 4 of these with runways longer than 3,047 meters; no reported heliports

Unfortunately, these data, even if they are many enough and quite detailed, are not entirely fit for our task, simply because they are *not* complete pieces of information/pieces of Intelligence. I mean by this that the figures quoted here *do not* tell us anything, at all, about *several* significant issues. Among these, we might list at least these elements:

- How many of these airports are regularly used;
- How many of them are close to significant inhabited areas;
- How many of them are close to major land transportation routes, enabling the operators to quickly replace fuel, spare parts, and ammunition;
- How many of them with adequate logistic infrastructure, making them fit for extensive and/or continuous use;
- How many of them with adequate logistic infrastructure, making them fit for moderately intensive combat operations;
- How many of them with adequate logistic infrastructure, making them really fit for intensive combat operations of all sorts;
- How many of them with hangars strong enough to protect transport and combat aircraft in case of moderately intensive air or missile attacks;
- How many of them with hangars strong enough to protect transport and combat aircraft in case of really intensive air or missile attacks;
- For how many of them the operating entities/states do have all necessary skilled manpower, to operate them 24 hours a day.

With a tremendous amount of effort, the average non-professional Intelligence analyst, working with limited resources within the academic environment, can fill in *some* of the gaps. But, let us face the truth, not all of them. So that, in situations like this, the analyst – together with the political decision-maker he might be working for – face a *difficult choice,* or better said a *painful dilemma*: either to go on with data clearly not complete (a quite risky course of action, potentially leading to analytical and decisional mistakes/failures), or not to go on (a risky attitude as well, because decisions *have* to be taken, as long as the pace of evolutions on both the domestic and international arenas is now more and more accelerated, if we compare it with the average pace of events in the even quite recent past).

Challenge no. 3: Problems Associated with (or Generated by) the Need to Use Contradictory Pieces of Information/Intelligence

In some occasions (not at all very many, to put it bluntly), the *Intelligence analyst* (sometimes *very* professional, in other occasions behaving in a more 'amateurish' way; sometimes confronted with *very* strict responsibilities and deadlines, in other occasions having the possibility to fix his/her own research agenda, but also the pace and the depth of the effort to be done) has the tremendous chance to use coherent (non-contradictory) sets of information/Intelligence, in which all available elements converge in almost the same direction, even if the details may significantly differ. In many other occasions, this user-friendly chance simply does not exist.

Let us explore, for a better understanding of this very issue, *the intensely contradictory nature of pieces of Intelligence/information which, put together, tell us about ongoing realities in Afghanistan*. We operate with a huge amount of open sources, describing, with a lot of vivid details, two sets of realities. The more you read, the stronger becomes the feeling that you are operating with elements of Intelligence generated not by a single country, but by two vastly different countries, placed on two vastly different planets. There is, first of all, a significant amount of news, media reports, official statements and official reports stating that, even with some difficulties, there is a serious and steady amount of progress in Afghanistan. Such an *optimistic* evaluation is, in the end, one of the key elements acting as a solid foundation for the already adopted decision of NATO, to put and end to the military presence of the Alliance in Afghanistan in just a couple of years from now. But there is another reality as well, clearly less optimistic: an Afghanistan where logistics are now made more and more difficult by the badly deteriorating security and stability in many Pakistani regions; an Afghanistan where, quite recently, the plane of the U.S. Chairman of the Joint Chiefs of Staff (JCS) was attacked, within the heavily defended perimeter of Bagram air base, with missiles, by insurgents (mostly probably battle-hardened veterans, possibly knowing the area for years, maybe from the era of the war against Soviet invasion); an Afghanistan where, at this very moment, regions and provinces (including many administrative units in the central and

northern parts of the country) which seemed to be soundly pacified and pretty stable a few years ago are the arena of increased insurgent activities of all sorts (from propaganda to implementing, by force, traditional Muslim law, to open attacks against NATO troops and against Afghan governmental forces and Afghan provincial officials loyal to Kabul); an Afghanistan where U.S. and other NATO military contingents are confronted with a sharp increase of the so-called 'insider attacks', launched by insurgents who managed to join the Afghan army or police and now they are deliberately attacking their Western trainers and combat partners.

At any given moment, we *have to* operate with pieces of information/Intelligence belonging to *both* categories listed above, even if putting together elements which seem not to have too much in common is not at all a very easy intellectual task.

But, let us face this reality, *an intensely contradictory nature of various pieces of information/Intelligence is a quite common feature of many strategically significant realities/environments/examples, almost anytime and almost anywhere.* In order to offer only one very brief example proving (or at least attempting to support) such a statement, let us remember how a quite accurate author, Arrianus, described the way in which the army of Alexander the Great came back to the central regions of the huge and recently established empire, after a long and successfully set of campaigns and raids in India, clearly beyond the borders of the former Persian state. The veteran members of the Macedonian phalanx, inherited by Alexander from his father, were probably the best, bravest and most effective infantrymen of the era we are speaking about. Well trained and well armed, they had been able to conquer, without any major problem, accompanied by a very limited number of heavy cavalrymen, roughly half of Asia. But, traveling on foot through the hot sands of the Persian wastelands, the courage of these veteran fighters almost completely evaporated. Tired, lacking food and water, the mighty warriors started to commit suicide in larger and larger numbers, and Alexander had to personally intervene in order to restore the morale of the troops[9]. This very example properly illuminates the method we might use in almost any situation pushing us to operate with a lot of contradictory pieces of Intelligence: *we simply accept that they can, all of them, be both valid and true. And we try to put them together at work, in order to shape a dynamic image of ongoing processes and realities, in which 'positive' elements or trends*

simply coexist with 'negative' ones. In such a situation, the analytical effort is to be accompanied by a set of recommendations with at least two basic features:

- To identify means potentially enabling the decision maker(s) we might work for to boost, to develop or at least to protect the 'positive' elements of the 'puzzle';
- And to identify means potentially enabling the decision maker(s) we might work for to eliminate (or at least to significantly and deliberately diminish the impact of) the 'negative' elements of the same 'puzzle'.

Challenge no. 4: Problems Associated with (or Generated by) the Need to Operate a Very Clear Distinction Separating Realities and Illusions (Wishful Thinking)

A problem some of us are confronted with is the basic fact that the average individual – and also the average research group or university learning group (class) – is intellectually operating within an environment shaped by tremendously potent *ideological* influences of all sorts. Many of my students, for example, are heavily imbibed by the very idea that the value of international *institutions* and international *principles* is, at any given moment, really huge. In such a context, almost any attempt to make them smoothly and rationally process a massive amount of tiny pieces of information/Intelligence able to generate, put together, a detailed and broad picture of the ongoing trends concerning the way in which power is present and works on the world arena is severely hampered, many times from the very beginning. It is not their fault, at all. Such students, many of them really bright, are, simply, what we could call 'prisoners' of the Idealist-Liberal school of International Relations, whose ideas, values, authors and works make the students I am speaking about clearly unable (or simply unwilling) to take into account the basic fact that, for a better understanding of *some* issues, Realism[10] might be a better method/option than Idealism.

In a way or another, this very type of problem is an old one. Let us remember, for example, the way in which *political correctness* was the thinking pattern which made German strategic planners completely unable to take into consideration *some* of the harsh

realities of the Russian front. The Germans overemphasized, first of all, *some* of the elements they thought that the campaign in France (1940) showed as being potentially decisive. One of them was the speed of the advance of tank units. In Russia, where modern roads were very few, the speed of the armored units was clearly lower, and the problems the logistical services were confronted with were by far much larger. Climate conditions were also not the same. But these mistakes, even if significant, were not lethal for the German war effort. It was, in the end, the official state doctrine, the official ideology of Nazi Germany which made even some professional military commanders and planners (and, above all, the political decision-makers) not able to take into account two of the most important ingredients of the German failure and of the Soviet successes. One of them was the fact that the average Soviet soldier, even if poorly led and poorly trained and equipped (at least in 1941) was very well motivated[11]. The second element strategic planners and military commanders on the German side ignored, because of obvious ideological reasons, was the ability of Soviet engineers to design, and the ability of Soviet industry to build, quickly and in really great numbers, modern weapons, including an armored fighting vehicle better than any German armor in 1941: the notorious T 34. In this situation, dominant ideology made the German commanders and planners to think that the Soviets will be quickly defeated, even easier than the French had been. This proved itself to be a very dangerous illusion, a moment when wishful thinking was directly leading to a major military disaster, at least in the long run.

These two examples, even if are many decades apart (and, *more important*, separated by really *immense* ideological and political regime differences), have a very strong common denominator: both of them clearly show that, at least in some occasions, *mixing Intelligence work with ideologies (or with strong ideological beliefs) can directly lead to a decreased ability to operate a clear distinction separating realities and wishful thinking*.

Conclusions

For some of the members of the so distinguished audience I am speaking to, some of the ideas and challenges presented along the previous pages might be acceptable and interesting; for some others,

not at all. But, in almost *any* occasion I can imagine, we might identify, *together* (even if with vastly different professional backgrounds and vastly different institutional affiliations and professional careers), a common conclusion: *civilian* academic institutions are to be regarded as major *potential* partners in almost *any* serious Intelligence activity, *mainly* when dealing with *open sources* of all sorts. But *developing* the institutional capabilities of *civilian* academic institutions in the field of Intelligence is an activity which clearly needs a lot of resources. Some of them are, of course, not a matter of *direct* concern for teachers and researchers (like myself), but an obvious responsibility of major political decision makers. But there is something we can do, together, in a smooth and effective way, not at all consuming too vast resources: *simply interacting in as many occasions as possible, in various projects of all sorts*. This way, *professional compatibility and confidence is more and more consolidated* and, above all, various intellectual avenues can be properly explored by both civilian academic institutions and Intelligence services (and their highly specialized research units). Simply shaping and testing such *ad-hoc joint task forces* is an extraordinary result, simply pushing *all* persons and institutions involved to be more flexible, more imaginative, more effective, both in strictly academic research and in generating intellectual results which are, at least in some occasions, *potent* or even *vital* Intelligence products.

References

[1] Allen Dulles, *The Craft of Intelligence* (New York, Evanston, and London: Harper & Row Publishers, 1963), p. 9.

[2] For the role of Machiavelli in developing modern strategic thought, but also for those ideas of him we call here predictions of a distant future see Felix Gilbert, "Machiavelli: The Renaissance of the Art of War", in Peter Paret (ed.), *Makers of Modern Strategy from Machiavelli to the Nuclear Age* (Princeton, N.J.: Princeton University Press, 1986), pp. 11-31.

[3] For a quite brief, but *very* clear presentation of both the roots and the consequences of the massive presence of mercenaries, for several centuries, in European political-military affairs see Michael Howard, *Războiul în istoria Europei* (Timişoara: Editura Sedona, 1997), pp. 29-48 (the entire 2nd chapter, called "Wars of Mercenaries").

[4] For the ideas of Douhet, see several fragments in Simion Pitea, Gheorghe Tudor (eds.), *Pagini din gândirea militară universală,* Volume III - *De la Războiul Crimeii la Cel De-al Doilea Război Mondial* (Bucharest: Editura Militară, 1988),

pp. 164-191, and also David Macisaac, "Voices from the Central Blue: The Air Power Theorists", in Peter Paret (ed.), *Makers of Modern Strategy*, pp. 624-647.

[5] For the *very* limited – and clearly disappointing, from a certain perspective – results of the U.S. strategic bombing in Vietnam and Laos, see George Donelson Moss, *Vietnam: An American Ordeal* (Englewood Cliffs, N.J: Prentice Hall, 1990), pp. 203-211; and for the failure of the B-52 (mainly flying from Diego Garcia) to destroy the Taliban and al Qaeda tiny groups of fighters and leaders, see Seth G. Jones, *In the graveyard of empires: America's war in Afghanistan* (New York, London: W.W. Norton & Company, 2010), pp. 94-108.

[6] For these figures see *The World Factbook*, CIA, available at www.cia.gov/library/publications/the-world-factbook/.

[7] Eginhard, *Vita Karoli Magni / Viaţa lui Carol cel Mare* (Bucharest: Editura Vremea, 2001).

[8] For the figures used in this table, see *The World Factbook*.

[9] For this episode, see several ancient authors, and mainly Flavius Arrianus, *Expediţia lui Alexandru cel Mare în Asia* (Bucharest: Editura Ştiinţifică, 1966), VI, 26, pp. 1-5.

[10] For a condensed but detailed presentation of Realism see, for example, Jack Donnelly, *Realism and International Relations* (Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore, Sao Paulo: Cambridge University Press, 2000).

[11] For ignoring such impressive and strategically significant assets of the Soviets, plus for other major mistakes of the German strategic planners and political decision-makers, see Erich von Manstein, *Victorii pierdute* (Bucharest: Editura Elit), pp. 167-169.

Intelligence Analysis for the 21st Century: Skills, Tradecraft and Training

Julian RICHARDS*

Abstract

One of the most difficult aspects of establishing and developing an effective national intelligence capability is the question of how to define the activity of intelligence analysis, and how to codify it in terms that traditional human resources and learning institutions understand. So far, there have been various attempts within intelligence institutions to describe the activity in terms of a range of "competencies" and "skills", with the former representing a set of behaviours and aptitudes that intelligence analysts would be expected to display, and the latter representing more specific activities which can be learnt and measured.

Focusing on the British, and, to a lesser extent, the US experiences, this paper looks at the way in which skills and competency frameworks have been developed at the institutional level, and asks the question as to how effective these have been in establishing a clear baseline for defining the role of intelligence analysis, and for defining the teaching and learning programmes to accompany it. The paper also takes a critical look at the range of training and education activities currently in place in the UK for intelligence analysts.

In this paper, I explore the key questions that face managers and strategists in the 21st century when thinking about the human factors in the intelligence business. Questions that have always been asked in the intelligence business, and which are no less pressing today, include: how can we be sure that we are recruiting the right people into our intelligence business to be able to tackle the threats that we face today? With what skills do they need to be equipped, and how can we best develop those skills with training and other development activities? How would we define the intelligence tradecraft today, and how is it changing in the 21st century?

Why Attempt to Codify and Measure Intelligence Analysis?

Perhaps the first question that could reasonably be asked is: why should we attempt to codify and measure intelligence analysis? Some might argue that the intelligence function is an inherently

* Lecturer, University of Buckingham

amorphous and instinctive activity, and does not lend itself very well to being counted and measured. In short, perhaps it is more art than science. I believe that the answer to this question is that, while we can have some sympathy with a view of intelligence analysis as being a mercurial and indefinable activity, the day-to-day business of governments and intelligence agencies means that some degree of structure needs to be put in place around the activity[1]. This is important for two reasons. Firstly, a government needs to be sure that it is conducting its intelligence activity in the most effective and efficient way, and that it is not liable to suffer any more intelligence surprises than are absolutely necessary. Secondly, the staff who make up the intelligence function need to be given the opportunity for career development much as any other staff, and it is difficult for this to happen if their core activity cannot be measured in any way.

For the intelligence business itself, therefore, the need to make some progress in codifying and measuring the intelligence activity can be broken down into four requirements. Firstly, the intelligence business needs to be able to set appropriate entry requirements for new staff coming into the business. To do this, it needs to have a fundamental understanding of the core skills and capabilities that an entry-level analyst needs before they enter the building. In the UK, the general approach in recent years is that entry-level analysts need to be educated at least to Bachelor's degree level, but that they do not need any specific skills beyond that, since the intelligence agency will train them in the specific mechanics of the business once they join (essentially, in intelligence "tradecraft"). It is assumed that education to degree level – regardless of the subject of the degree – imbues the candidate with a general level of capability in analysis and assessment of complex and large amounts of information.

Interestingly, there is some evidence in recent months that UK policy is moving towards a recognition that, for the more technical elements of the business, such as, for example, intelligence in the cyber-realm, training and education of a more vocational nature might be needed. In 2012, De Montfort University in the UK launched the first Apprenticeship (Foundation level degree) for cyber-security analysts entering the intelligence business. This may mean that degree-level analysts are no longer the default, as has been the case for some years. It also reflects the manner in which intelligence analysis tradecraft is changing and diversifying in the 21st century.

The second requirement concerns that of advancement for analysts once they join the business. In order to be able to attract the best and brightest candidates and keep them in the business for as long as possible (and, indeed, to prevent them moving out to more attractive options elsewhere), such candidates have to be offered a compelling career path that allows them to advance upwards. To be able to promote the best analysts at the appropriate time – and to do so fairly and equitably - there has to be some system for codifying and measuring the skills required at the higher level and the degree to which a candidate is able to demonstrate them.

Thirdly, most areas of government and the private sector now operate systems of annual staff assessment and appraisal, often linked to pay and promotion. These systems vary enormously in nature and complexity between organisations, but all require some degree of annual assessment of a staff member's performance and the skill level they have attained, whether this is done quantitatively or qualitatively, or both. Intelligence analysts are no different from other members of staff in this respect, and are thus not immune from the assessment process.

Finally, and related to the third requirement, not only does the performance of individual analysts need to be measured in some way in order to allow assessment and consideration of suitability for advancement, but the performance of the intelligence function as a whole also needs to be measured and assessed. For the intelligence business, continued success is very much a dynamic picture, and a moving target. As technologies, threats and the tradecraft of targets mutate and develop, so must the overall skills disposition and capabilities of the intelligence business to deliver the new and developing tradecraft of intelligence. Measurement of performance is therefore a collective as well as an individual requirement.

Defining Intelligence Analysis?

There has been a great deal of debate over the years as to whether intelligence analysis can best be termed a science or an art. Indeed, whole conferences have been devoted to the question on both sides of the Atlantic. The author can attest to having spent some time analysing this issue. In my recent book on the subject, I concluded that:

Scientific and structured methods of analysis and data-handling are essential, and there is much that can be learnt and copied from the natural and social sciences, particularly the latter since intelligence is, after all, a question of analysing and predicting human behaviour. At the same time, not only are human beings frustratingly indeterministic in their behaviour more often than not, but intelligence targets are frequently – by their very nature – elusive, evasive and keen on employing deception and obfuscation.....Add to this the frequent problem of incomplete coverage of a target's activities, and it is clear that intelligence analysis can never be a precise science[2].

In this way, the answer to the question as to whether intelligence analysis is an art or a science is that it is "both and neither"[3]. The difficulty is partly the nature of the beast, as implied above, namely that intelligence analysis is a study of the activities of human beings, but with some added complications that make it even more difficult and unpredictable than tasks faced by many other social scientists.

The other issue, however, is that "intelligence analysis" actually encompasses a very wide range of activities which vary somewhat in their nature. Some of these activities are fairly technical and mechanical in nature, and lend themselves to quantitative assessment measures. Many of the basic data handling skills, for example, such as capabilities in exploiting and manipulating intelligence data sets, can fall into this category. At the other end of the spectrum, certain "raw" analysis and assessment activities occupy the realm of less quantifiable skills such as perception and overcoming bias, and are as much to do with judgement, and, in some cases, experience. These lend themselves to more qualitative assessment mechanisms.

There are various analogies that can be drawn in attempting to conceptualise this situation. One I particularly like is the analogy of learning to play a musical instrument, and assessing a student's performance as they move through the levels. Playing an instrument such as the piano is an inherently artistic endeavour. Assessing things like feeling and expression is not something that can be done using quantitative measures, however, but is more a question of just listening to how someone plays. At the same time, to become a really

good pianist usually involves a great deal of technical work in areas such as theory and composition. Some of these things can be measured more quantitatively – you can assess how many mistakes a pianist makes in playing scales or other formatted exercises. If a pianist is good in one area but not the other – for example, if they are technically very proficient but lacking somewhat in style and expression – then we might say they were a good pianist, but not a great one. It is the combination of the two, and our assessment thereof, that allows us to consider just how good a pianist we are hearing.

Another analogy is that of different academic subjects. Scientific and technical subjects such as Mathematics can be assessed using quantitative measures, such as numbers of "correct" answers to specific tasks. Subjects in the Humanities field have to use more qualitative measures, such as an assessment of an essay, since it is not so easy to say what is correct and what is wrong, but rather how someone goes about the task. In exactly the same way, intelligence analysis usually covers a range of technical and less technical tasks, and so the assessment of them has to cover both quantitative and qualitative mechanisms.

In this way, Marrin and Clemente were partially right in saying that, certainly prior to the post-9/11 period, "no official standards exist to endure the competency of individual analysts"[4]. Since that time, however, this no longer holds entirely true, certainly in the US or the UK, where the strategic shock of the 9/11 attacks and subsequent terrorist incidents have caused the intelligence business to focus sharply on whether they have the right disposition of analysts in their organisations, and whether those analysts are best suited to the change in threat that has unfolded in the post-Cold War period. In certain parts of the intelligence business, a great deal of work has gone into what are loosely called "career frameworks", within which the skills of specific roles across different levels have been identified and codified. In very general terms, these frameworks tend to identify that there are two dimensions to each staff member's capabilities (or more precisely, to the requirements of the role that the staff member occupies). In the UK these are usually delineated between "Competencies" (which tend to be generic capabilities and dispositions, which are generally difficult to measure other than in qualitative ways, such as "teamworking"); and "Skills" (which are

more readily measurable in quantitative terms, or using structured tests). Using our piano-playing analogy, these represent the difference between feeling and expression; and technical proficiency. Some parts of the intelligence business will use slightly different words and frameworks for these elements of a staff member's capabilities, but the general principles tend to apply.

Interestingly, the question of where "analysis" fits into this framework in its most raw form has been a difficult one, and has tended more towards the "competency" rather than "skill" end of the spectrum. Thus, someone can be assessed as having good analytical skills in a qualitative way by looking at such things as evidence portfolios describing how they went about tackling particular tasks, but they cannot really be tested in a mechanical way to determine their skill in this area.

The skills and competencies framework is mirrored in many other areas of social science and human resources. One example is Facione's description of what makes a capability in "critical thinking", which, like intelligence analysis, seems to encompass both measurable and more amorphous elements. Facione settled on a dual framework of "dispositions" (general tendencies which a good critical thinker will tend to display, such as being "truth-seeking" or "open minded"); and "skills" (which are more measurable activities such as the deployment of inference, interpretation or evaluation in specific tasks)[5].

Pitfalls in Measurement

With these thoughts in mind, we start to move towards a situation where the job of an intelligence analyst can be broken down into different categories and activities, and these can be described in terms of both competencies (generally measured qualitatively) and skills (generally measured quantitatively). These, in turn, can be set at different levels for different jobs and levels of proficiency, allowing some "headroom" for analysts to move along a range of career pathways and envisage how their career can develop in positive directions over a longer period.

This all seems fine and many intelligence organisations have put effort into codifying and measuring their analytical workforces in this way, but there are pitfalls in this process. The biggest one, and

the one that many institutions arguably fall into most easily in the modern era, is that the business of codifying and measuring skill levels and career pathways becomes a massive industry in itself, eating up time and resources which might be better spent actually doing intelligence analysis.

A flavour of this pitfall can be tasted in David Moore's framework: "Species of Competencies for Intelligence Analysis"[6]. In this paper, Moore reproduces an analysis developed earlier by himself and Lisa Krizan around "functional core competencies for intelligence analysis"[7]. This breaks the dual formula of competencies and skills down yet further into the four dimensions of abilities; characteristics; knowledge; and skills. The paper overlays these dimensions with a recognition that analysis can comprise different types of activity, which Moore and Krizan describe through a process of "speciation" delivering the four categories of descriptive; explanatory; interpretative; and estimative intelligence analysis. Different analysts will be fulfilling these different roles at different times, and some may specialise in one or other of these roles in the course of their career. For each, different skills and competencies might be needed, since someone who is very good interpreting tactical intelligence for its meaning, for example, may not be so good at estimating long-term outcomes in strategic situations, and so on.

In Moore's analysis, further definition around this framework is provided by breaking each "species" of intelligence analysis down into a comprehensive set of descriptors and requirements, and measures of success. This is useful and very logical, but I would argue that it contains within it a large pitfall. This is that, as this codification becomes more detailed and forensic, it starts to cross a line into the territory of a very onerous and bureaucratic exercise, which runs the risk of levying very considerable administrative demands on intelligence analysts and their managers if the system is to be operated and refreshed successfully. The "interpretive" intelligence analysis type, for example, breaks down into 7 descriptors, and 42 requirements. The measures of success fall into 3 categories, which further break down into 11 separate measures. While these are very instructive, the process of codifying these against specific job requirements, then working out and delivering

accurate measurement and assessment mechanisms on an ongoing basis for each intelligence analyst and their managers, entails a very considerable administrative overhead on the business of intelligence. Inevitably, the analysts themselves will become very wrapped up in this industry and this can cause a dangerous distraction from their core business of delivering intelligence.

Conclusions

Clearly, as a corollary to this argument, I would not propose that we make no effort in capturing what skills and competencies an intelligence analyst needs, and to assess how well they are meeting these requirements on an individual and institutional level. To do otherwise would be entirely negligent in the modern context. What I am arguing, however, is that there are very delicate balances to be struck between designing and delivering a useful assessment mechanism, and not going overboard in complexity and bureaucracy, as too many government institutions in particular are rather prone to do. To get this balance wrong ultimately affects intelligence performance very adversely, to say nothing of staff morale.

I have established in this paper firstly that "intelligence analysis" as a function involves a wide array of activities, some of which are quite technical, while others are somewhat qualitative and more difficult to assess. There are elements of both science and art in intelligence analysis, when looking at it across the whole spectrum, and this remains very true as the central tradecraft of intelligence changes and diversifies in the modern era. The "cyber" realm illustrates many of these points, since it is, at one level, intensely technical and scientific, while at another level the same qualitative requirements of assessing and analysing complex data still apply in the same way that they always did.

I have also established that there are very good human resources reasons for needing an appropriate codification and assessment mechanism applied to the intelligence workforce, both for the individual staff members themselves in terms of developing careers, and for the institution in terms of making sure it has the right disposition of analysts and is best equipped to deal with the evolving threat picture. The basic concept of competencies and skills provides an initial framework for such mechanisms.

For the intelligence organisation, an appropriately balanced system of codifying and assessing intelligence analysts' competencies and skills allows for more structured and precise planning to be undertaken in the area of training programmes. In accordance with the dual system of competencies and skills, training programmes in the UK and elsewhere have offered a range of different activities and exercises to address the various different elements of the picture.

Skills-based training is delivered in the shape of technical courses and workshops addressing specific technical capabilities, often provided by external training providers on a generic basis. Project-based training, in which "learning on the job" is simulated, can also be provided. An example of this is an internship or summer student placement within an intelligence organisation, to undertake a particular project. On a more developed level, the new Apprenticeship/Foundation Degree programme in cybersecurity promises to be the harbinger of a move away from a general liberal arts education as a default starting point for some intelligence analysts at least. Many of the older members of the organisation will remind us that this takes us back to the technical apprenticeships of many years ago! They remind us that perhaps nothing is new under the sun!

Competency-based training is, first and foremost, provided by the staff member's external education. This is why, in the UK at any rate, a degree was considered to be an entry requirement for all analysts as it provided a general level of competency in such areas as analysis and assessment, regardless of the subject taken. As mentioned above, this may no longer be the default position as some analysts are required to undertake much more technically complex activities. Meanwhile, a plethora of management skills and workshops, and "brain training" exercises and activities are likely to remain a central part of training programmes within the intelligence organisation, to develop what are sometimes called "soft skills" such as teamworking and leadership, or indeed critical thinking and judgement. Many of these activities will be harder to measure in terms of their outputs other than in very qualitative, evidence portfolio-based ways, but they will be no less critical to overall development of analysts despite this fact.

There are many moving parts in this whole picture, and, as illustrated, if perspective is lost and balances are not struck, a very inefficient and inappropriate system can be put in place which undermines the business. It is also worth noting that the threat environment is moving so quickly and so dynamically, that flexibility to change and develop programmes is likely to be critical for all intelligence organisations in the coming years, and this will apply to skills development as much as to anything else.

References

[1] At this stage it is worth noting that the "intelligence business" can comprise not only governmental actors but also private companies.
[2] Julian Richards, *The Art and Science of Intelligence Analysis (*Oxford: Oxford University Press, 2011), p.172.
[3] *Ibid.*
[4] Stephen Marrin and Jonathan D. Clemente, "Modelling an Intelligence Analysis Profession on Medicine, *International Journal of Intelligence and Counterintelligence*, Vol. 19, No. 4, 2006, p. 642.
[5] Peter A. Facione, *Critical Thinking: What it is and Why it Counts* (Milbrae, CA: California Academic Press, 1998, updated 2009), URL http://www.insight assessment.com, P. 10.
[6] David T. Moore, "Species of Competencies for Intelligence Analysis", *Defense Intelligence Journal*, Vol. 11, No. 2, 2002.
[7] David T. Moore and Lisa Krizan, "Intelligence Analysis: Does NSA have what it takes?", *Cryptologic Quarterly*, Vol. 20, No. 2, 2001.

Building Up a Discipline. The Case of Romania

Karin MEGHEŞAN[*]
Andreea CUCUTĂ[*]

Abstract

It is no doubt that intelligence is many things and unfortunately intelligence is defined in many ways, too often very different from one to another. The main purpose of this article is to briefly examine the need of establishing a community-wide intelligence understanding and education framework that meets the needs of intelligence professionals on all levels (military or civilian) and to analyze what the differences between professional development, education, and training are. Is intelligence an art, a craft, a profession? Will it be possible to be a science or just an applied discipline? If we talk about intelligence as academic discipline what should be the core issues of any curricula and how could we keep a fair theoretical balance between the various multidisciplinary approaches? From our point of view we cannot talk about any revolution, or reform in intelligence activity and organization without starting from the grassroots - the human resource.

Having as a starting point the intelligence culture, the existence of a common language or a unitary understanding of our world we will try to briefly present some of the concerns linked to the process of education and training – concerns present on the agenda of secret services. To exemplify we will use general and specific issues of our institution.

Whatever the controversies, the various conceptual approaches, the changes in substance and form of the intelligence activity, there is a single aspect that intelligence professionals, historians, political scientists, sociologists and political decision/makers agree upon: the quick, deep and endless changes of the global environment requires flexibility, accuracy, a high capacity to predict, action and above all structures able to cope with the new requirements in intelligence. But what could we do to better educate, train, and form young people in order to acquire superior abilities to enable them to cope with the new challenges in international environment?

The rapid and quick changes of the world we were used to had the inevitable effect of institutional transformations and reconstructions.

The analysis of these changes and their causal connections highlights the global concerns of the last decade: cultural and economic discrepancies, asymmetric conflicts, unpredictable threats, increasingly dangerous non-military threats and a necessity to rethink security in non-military terms, global and regional interests, and new spaces of geopolitical interest.

[*] Lecturer, "Mihai Viteazul" National Intelligence Academy
[*] Asistant Lecturer, "Mihai Viteazul" National Intelligence Academy

We are not only witnesses of these changes. We are part of the global chain of these changes, together with the institutions where we develop our activity, be they private or state-owned, multinational, transnational or national.

In the past years, debates on intelligence have focused on the necessity of restructuring intelligence services; this necessity comes as an effect of the change in the security paradigm. For the first time in the last five, six decades, the activities of the secret services (which from now on we will call intelligence activity) is considered an integral part of governing, a fundamental activity of any decisional process. For the first time in the past years it has become widely recognized that meeting the targets of national interest largely depends on the functional capacity of intelligence services. Even though studies and research have almost completely covered the issue of institutional reconfiguration of intelligence activities, there is still a topic of major interest that is still under debate: intelligence education.

First of all we should carry out an analysis regarding the interest in intelligence education. As mentioned forward in the study there are two coordinates which, for now, the literature covers unitarily even though in our opinion they should be tackled separately.

Indeed there is an intelligence education meant for "civilians" - we talk about people who have no connection whatsoever with intelligence services, and in this case we start from the idea that "a knowledgeable public is a vital perquisite for mobilizing and sustaining broad societal interest and support for national security policies in democracies"[1].

Creating an intelligence academic culture comes from the necessity to better understand this domain of activity. Intelligence activities are stereotypically perceived by citizens. And such stereotypes turn out to be extremely resilient due primarily to commercial, mass, popular culture mentioned at the beginning of the article. The spy stereotype[2], gender stereotypes (the image of *femme fatale* of the female spy[3] is still present in the collective memory) and the image of intelligence services induced through fiction (movies, novels, even documentaries) have had the most unexpected effects felt just today. In my point of view, introducing new intelligence subjects in civil universities curricula represents a huge advantage even so more important that the ones presented in the literature[4].

Young people today, fascinated by 'the world of espionage' as it appears in works of fiction are those who will occupy key positions in the state, military and civil decision making processes. Their expectations of the intelligence role and missions were formed under the influence of popular culture industry, and for that reason expanding the international relations and political sciences curricula with intelligence dedicated courses represents a real need for improving the intelligence-decision relation. As Amy B. Zegart[5] observed, unexpected explosion of mixes of espionage myth and reality had two important effects on policy in the field: first of all the construction of cognitive schemata that easily slides between the ideas that intelligence organizations are considered to be omnipotent but in the event of a situation such as *focus event*[6] they might be considered to be incompetent. Without much exaggeration we believe that famous revealing of officers' identities or illegal activities have been caused by a shallow understanding of the role and tradition of intelligence.

A second coordinate of intelligence studies is the one regarding professional education and training- an intelligence education and training meant for those designated to provide Information – it strictly refers to those educated and trained to become future intelligence officers.

Romania is among the few countries where the educational pattern is based on its own security system resources and sources. Education and training are carried out within the three stages of the Bologna system and it effectively and originally blends the general knowledge students must possess with a theoretical and practical training by improving and refining their native abilities. From our point of view intelligence education needs to become part of security and intelligence culture, and this security and intelligence culture should represent the common language for all levels of society – the ordinary citizen, the political elite, or the professional in intelligence.

Without getting into too many details the academic education within RIS academy is mainly based on those subjects which are considered to be the scientific base of an intelligence officer. Having presented some general aspects about our understanding regarding civilians and professionals' education and training, we'd like to mention some specific aspects about our Academy. *MV*NIA is a military institution of higher education (in Romania the services

within the national intelligence community are mainly military) and the Academy trains officers for all these structures. As far as civilians are concerned we have MA for civil society.

Our intelligence studies incorporates a wide spectrum of conceptual-theoretical perspectives and subject matter. The university curricula is a clear proof that "Interdisciplinary became, indeed, a veritable hallmark of Intelligence Studies"[7] and it has both subjects such as: psychology, sociology, political sciences (international relations, compared politics, governmental mechanisms, decision making), history, languages, geo-politics and diplomacy, logics, semantics and other subjects necessary for a better understanding of intelligence- history, decision making politics, foreign politics, human rights, and security institutions. Yet, we should not forget that more than half of our education and training is focused on practical activities, and all above mentioned subjects are taught through the eye of an intelligence officer.

Analyzing the curricula we can easily notice that the Romanian pattern meets all the requirements for a successful intelligence approach that the literature mentions. We would like to mention Thomas's four approaches[8] (historical/biographical approach, the functional and the discipline methodologies proposed by Wesley Wark: the research project, historical project, the definitional project, fourth perspective (that is, using case studies to test the theoretical deliberations), memoirs, civil liberties project, investigative journalism, and popular culture project.

The theoretical and practical professional training, even though based on these interdisciplinary approaches still relies on the **transmission of knowledge and expertise from experts to novices**. From this point of view training in our country relies on what Jeffrey Cooper[9] called "a guild structure" that "recruits, trains, and inculcates members in distinct rituals and arcane". Cooper says that each intelligence subject (and by that the author means that each INT - military, civilian, intelligence specific law-enforcement, foreign intelligence etc) recruit their officers by inoculating **their own culture**. More often than not such differences of culture lead to future rivalries which later on will lead in their turn to issues in respecting the need to share principle. Within the Academy we believe that such conflicts are dealt with successfully. Our experience

of 20 years has taught us how to train young intelligence officers for different beneficiaries within our national defense structure by offering them a joint training ground in understanding intelligence, a common language – a sort of linguistic inter-operability, a higher ability to correctly perceive and understand their place and role within the national defense structure. Ultimately the sense of belonging to different structures creates an esprit de corp of the Romanian intelligence triggering a very powerful feeling of loyalty which goes on beyond their respective structures.

Concluding our analysis regarding intelligence education and training we can say that intelligence can be taught in a wide variety of ways. Even though the curricula in our institution do meet the requirements we believe that the difficulties on an international level in defining intelligence clearly influence the educational process in our country. In our opinion the concept of inter-disciplinarity within intelligence lacks certain methodological approaches. Primarily we are talking about the undergraduate studies where students come to the Academy bearing only a general yet superficial knowledge from high-school!

Why Intelligence Education?

If you ask a high school graduate (and not only) what is the first thing that crosses their mind when they think of an intelligence officer they will answer “James Bond” or “The Recruit”. Most of the times, the adrenaline and the spectacular define the intelligence activity in the eyes of the youth. Which is not bad; on the contrary, attracted by the spectacular, many young people will dream of a career in intelligence. But there will come up problems that may or may not find a solution during their educational and professional training. One of them is the intellectual quality of these young people. At 18-19 it is almost impossible to conceive the perfect balance between talent, loyalty, hard work, calling, that are so necessary for a good professional in intelligence activity. Once involved in the specific educational mechanisms, there comes another problem: finding the proper methods to reduce frustration and intellectual dead-end. More often than not, these phenomena appear when the young generations realize that their “James Bond” expectations match neither the realities of intelligence activity, nor the requirements and offers of the academic intelligence education.

And at this point we can mention those responsible with academic activity, those responsible with turning these young people into professionals in intelligence.

The public perception of intelligence as an integral and indispensable role of good governing raised an increased academic interest in this profession. Civil society is more and more interested in aspects related to intelligence. The need for specialists in intelligence is felt not only in the state sector, but also in the private one. From the requirements of initial training in the field we have reached the requirements of a continuous training by organizing master's and doctoral studies in intelligence. Through these educational offers we opened new opportunities for collaboration and communication between civil society and intelligence services.

Each nation-state has chosen its own avenue in training, educating and specializing its own personnel involved in intelligence activity. In general, most of the states that chose to offer initial and professional training through post-university courses in centers belonging to intelligence services follow specific short-term training courses, function of the specific field of activity. On the one hand, this educational program ensures the transfer of knowledge from former officers to "young apprentices in intelligence", but on the other hand it has a great disadvantage. Too strict a specialization may become a hindrance when speaking about flexibility, and intelligence education aiming strictly at specialized issues is only a piece (though a very important one) of a much more complex puzzle. Specialized education within agencies is focused on developing aptitudes, specific competencies, increasing students' "natural talent" through intensive training. This kind of approach cannot meet regular standards, because each service has its own responsibilities in security and intelligence, its own needs for personnel, and most of the times there are significant differences both in the means and methods used and personnel and in activity strategies.

Despite all these shortcomings, training within own educational systems fully serves the needs of the respective services. There are voices in the USA[10] saying that this kind of training and the lack of common strategies and capabilities of professional development in intelligence field resulted in gaps in the field of inter-agency cooperation. Sidney Fuchs considers that training within own educational systems has weakened the efficiency

of the American intelligence community in training young officers and low rank managers for activities that are specific to joint operations and inter-agency cooperation[11].

In general, intelligence services focus on the basic and further professional training in two major fields: intelligence gathering and intelligence analysis, leaving aside the aspects that may contribute to a better officer qualification. These aspects are generally related to the evolution of national and international political systems, international policies, and concerns in the field of security, understanding the mechanisms of internal and international political decisions, in other words it is about education with a view to gathering extensive knowledge in political sciences and international relations. Intelligence education must not be strictly centered on intelligence services. Cooperation, collaboration, partnership – they all imply the existence of a common national and international language. Intelligence education needs to become part of security and intelligence culture, and this security and intelligence culture should represent the common language for all levels of society – the ordinary citizen, the political elite, or the professional in intelligence.

How Do We Carry Out Intelligence Education/Study?

The common answer would be: starting from the intelligence cycle (in Romanian it is often referred to as intelligence flux). This answer though does not offer an ideal solution, given the fact that the classical intelligence cycle is largely disputed nowadays[12] and is sometimes different from agency to agency. Another hypothesis is the one starting from the concept of intelligence and how we may define it. Defining intelligence is far more controversial than the intelligence cycle. For this reason, the approaches in intelligence studies or education vary according to the understanding of the concept of intelligence.

For us it is difficult to deal with this concept, since in Romanian there is no linguistic equivalent. In the literature regarding political theory, in strategy and state politics, *intelligence* is used with the meaning of "knowledge referring to events, tendencies, and personalities that may affect the observer or the country, institution, governmental service for which the observer works, in an imminent situation or one that is perceived as imminent. This information identifies, describes and defines situations that require or seem

to require taking certain decisions"[13]. Essentially, it means activities of gathering and analyzing intelligence in order to support the political process – that is to fundament or to adjust national security strategies.

Wesley Wark, an esteemed academic in intelligence established difficulties in making intelligence an academic discipline. Intelligence education is tackled from various points of view by Anglo-Saxons themselves (Americans and Brits), or even within the same intelligence community[14]. The literature[15] in the field is extremely useful in pointing the right avenues to follow for a competitive intelligence education offering solutions, approaches, weak points and lessons learnt. The educational needs in intelligence are obvious in all analyses dedicated to the processes of restructuring and increasing the performance of intelligence services. Two studies on the necessity of qualitative intellectual modifications of the human capital come to attention: Loch K. Johnson, *The CIA's Weakest Link: Forget James Bond. What Our Intelligence Agencies Need Are More Professors*[16] and Richard J. Aldrich, *The Name Is Bond. Professor Bond*[17] .

Lessons Learnt – The Current Approach of Intelligence

The Anglo-Saxon concerns in intelligence training and education bears the generic name **Intelligence Education and Training – IET**. These concerns can be met in the studies and research published in peer-reviewed magazines such as: *International Journal of Intelligence and Counter Intelligence, Studies in Intelligence, Intelligence and National Security*. Their councils are made up of renowned professors specialized in intelligence, such as: Peter Jackson – Aberystwyth University, William M. Nolte – Maryland University, Richard R. Valcourt – American Military University, Mark M. Lowenthal – The Intelligence and Security Academy, Arthur S. Hulnick – Boston University.

Debates referring to finding a balance between professional training and development and education led to the creation of an international association called International Association for Intelligence Education, **IAFIE**. The creation of this international association is another proof of the necessity for a common denominator both in professional education and training, and in the didactic programs and curricula that ensure further learning. The subjects debated in this association's workshops included topics of interest for Romania:

- Is there a profession such as "intelligence specialist"? At first sight it may seem a certainty, but it is in the classified list? How can we connect intelligence training and education to the realities of the work market?
- Are there in the national classified lists disciplines related to Studies in Intelligence? Can we speak of a distinct branch of study, education and research? Can we speak of this discipline, "Intelligence"? When we speak of Intelligence education do we mean also interdisciplinary, multidisciplinary?
- Do we need a different approach for each educational cycle? Do we refer to the requirements specific to basic training programs, BA, MA and doctoral studies?
- What obligatory disciplines should the studies previous to intelligence specialization cover? For example, in the case of MA or BA programs, what are the obligatory disciplines that a candidate should have studied in the educational cycles preceding university courses?
- Narrowing the gap between the academic community and intelligence should really take place, or is the gap beneficial to maintaining a secret character of intelligence activities?
- What should be the optimal balance between theoreticians and practitioners in creating the professorate?

Conclusions

Controversies, conceptual approaches, basic and formal changes aside, intelligence professionals, historians and sociologists are agreed upon just one aspect: valuable information is as important now as it was 2000 years ago. The never-ending, far-reaching and fast changes in the global landscape call for flexibility, accuracy, enhanced provisional capacity, action, and mainly for structures capable to meet the new intelligence requirements. The academia's interest in intelligence has become manifest by the growing number of further education and master courses in intelligence and security. Most intelligence professionals still tend to underestimate scientific or theoretic approaches to intelligence.

➢ There are multiple advantages in teaching intelligence to civilians.

- Fill the gap between civil society and intelligence services.

- Reveal a "need to know" part of the mystery in order to achieve a better understanding of the intelligence role and missions (sometimes disadvantage).
- Basic intelligence and security education for private sector.
- Ensure the basics for the intelligence and security culture.

➢ On the other hand, education and training for intelligence officers are carried out within the three stages of the Bologna system and it effectively and originally blends the general knowledge students must possess with a theoretical and practical training by improving and refining their native abilities. It also ensures a scientific base and intellectual framework of an intelligence officer.

The academic approach to intelligence, the scientific study on the power and use of intelligence may not be a day-by-day support of action. However, they provide a foundation for doctrinal change, and help the reduction of ineffective bureaucracy within the intelligence agencies. To quote a veteran of the American intelligence community: "the Agencies should focus less on gathering raw information and more on what intelligence really means".

So, tackling intelligence in institutions of higher education can raise some issues.

- Intelligence can be taught in a wide variety of ways.
- The difficulties in defining intelligence (wide spread definition) clearly influence the educational process in our country.
- The concept of interdisciplinary within intelligence lacks certain methodological approaches.
- Too many important issues, too many points of view.

The changes that have taken place in the past years in the international system, as well as the diversification of national security concerns have a less predictable effect on the range of concerns of the intelligence community. 50 years ago, J. F. Kennedy said "don't ask what your country can do for you but ask yourself what you can do for your country." It seems it is not enough to do *anything* and *anyhow* for the country, and moreover it is not enough that *anyone* should do something for the country. Those who want or are called to serve the interests of a country should be thoroughly prepared for the missions they have to carry out. If some of the most powerful intelligence services in the world, such as the American, feel the urge of a qualitative development of university education in the field, creating long-term educational strategies, projecting the future of the

American intelligence community for the next two generations, maybe time has come for Romania as well to creates strategies in intelligence education through its specialized structures, to draw up programs that would help the national intelligence community and the academic community, as well as programs that would lead to achieving the targets of national interest of Romania, be they desirable or vital.

References

[1] Gustavo Diaz-Matey, "Intelligence studies at the dawn of the 21st century: New posibilities and resources for a recent topic in international relations", UNISCI Discussion Papers, University of Salford, May 2005, available at http://www.rieas.gr.

[2] Even using the word spy as a replace for any other term referring to an employee of such governmental secret organizations is also a stereotype. It is a higher advantage to use terms such as *espionage movie* instead of a movie referring to intelligence activities and operations of organizations responsible with national security; *espionage novel* describing the activity of a certain organization in a certain country; *spy* instead of intelligence counter-intelligence, analyst or domestic/foreign officer/agent; *espionage* instead of 'secret or official intelligence gathering about foreign countries in order to build up an informative base necessary to implement foreign policies and overseas covert activities coordination'. The term *spy* (those interested can read an outstanding work *The Spy* by Alain Dwerppe) undoubtedly has certain negative connotations, as well, regarding the activity which often takes place on the borderline of ethical and moral generally accepted limits. Ethics and morals in intelligence activities represent another important issue in literature.

[3] The idea, according which such stereotypes are sometimes accepted and even promoted by the governmental intelligence organizations, is also supported by the image displayed on the official CIA web page under the section dedicated to children- a female cartoon character, dressed in an overcoat, with a bright red lipstick speaking on a phone which is probably hidden in a high heeled shoe. Even though the image is not quite consistent with the stereotypes we have to admit that the message it conveys is clearly targeted to a certain audience and thus we cannot but wonder why don't we do the same thing in Romania? That is having a section dedicated to children within our official web page. Also see "Sex, Spies and Stereotypes", L.A Times online issue, 27 May, 2003 and "Movie Stereotype of Dangerous Spy", Washington Post online issue, 3 July, 2010.

[4] For details regarding intelligence theory and studies see Russell Swenson, "A Flourishing Craft: Teaching Intelligence Studies", Occasional Paper no.5 Joint Military College, 1999; Ernest May, "Studying and Teaching Intelligence", *Studies in Intelligence*, Vol. 38, No. 5, 1995; Loch K. Johnson, "Bricks and Mortar for a Theory of Intelligence", *Comparative Strategy*, Vol. 22, No. 1, 2003.

[5] Amy B. Zegart, "Spytainment: The Real Influence of Fake Spies", *International Journal of Intelligence and Counterintelligence*, Vol. 23, No. 4, pp. 599-622.
[6] Event which triggers deep organizational and political changes. For further details see Thomas Birkland, *After Disaster: Agenda Setting, Public Policy and Focusing Events* (Washington, DC: Georgetown University Press, 1997).
[7] Diaz-Matey, "Intelligence studies at the dawn of the 21st century".
[8] S. T. Thomas, "Assessing Current Intelligence Studies," *International Journal of Intelligence and Counterintelligence*, Vol. 2, No. 2, 1988, p. 239.
[9] Jeffrey R. Cooper, *Curing Analytic Pathologies: Pathways to improve Intelligence Analysis* (Washington, DC: Central Intelligence Agency, 2005).
[10] Sidney E. Fuchs, "The Intelligence Education Framework for the 21st Century", available at www.dni.gov.press.../20060505_3_release.htm.
[11] Sidney Fuchs, International Association for Intelligence Education, 2008.
[12] See Arthur S. Hulnick, "What's Wrong with the Intelligence Cycle", *Intelligence and National Security*, Vol. 21, No. 6, 2006, pp.959-979; and Amos Kovacs, "Using Intelligence", *Intelligence and National Security*, Vol. 12, No. 4, 1977, pp. 145-164.
[13] Ames A. Jordan, W.I Taylor, Jr. Lawrence and J. Korb, *American National Security. Policy and Process* (Baltimore and London: The John Hopkins University Press, 1989).
[14] Wesley Wark, "The Study of Espionage: Past, Present, Future?", *Intelligence and National Security*, Vol. 8, No. 3, 1993, p. 1.
[15] W. Wark, cited work, S.T. Thomas, "Assessing Current Intelligence Studies", *International Journal of Intelligence and Counterintelligence*, Vol. 2, No. 2, 1988, p.239; L. Scott and P. Jackson, "The Study of Intelligence in Theory and Practice", *Intelligence and National Security*, Vol. 19, No.2, 2004, p. 141; Arthur Honig, "A New Direction for Theory Building in Intelligence Studies", *International Journal of Intelligence and Counterintelligence*, Vol. 20, No. 4, pp. 699-713.
[16] Loch K. Johnson, Washington Monthly, July-August 2001, p. 6.
[17] Richard J. Aldrich in S. Tang, *Serviciile de informații și Drepturile Omului în era terorismului global* (Bucharest: Ed. Univers Enciclopedic, 2008), p. 328.

Trusted Relationships Management as an Intelligence Function

Rubén ARCOS*

Abstract

Since the mid-1990s, there is a growing concern about the need of outreach to outside experts to improve the analytic capabilities of the intelligence communities. The rise of the concepts of intelligence reserves and analytic outreach express this reality and, arguably, the emergence of a new paradigm for dealing with a wide array of threats and challenges for societies to which intelligence have to be able to respond effectively and efficiently in a timely manner. However, intelligence services need to hold the understanding of these stakeholders to be able to tap the expertise of outsiders. Consequently, the development of a trusted relationship management capability by intelligence services and the definition of an appropriate strategy are essential to achieve that aim.

Intelligence Reserves, Analytic Outreach and the Need for Trusted Relationships

In mid-1990s, a number of studies in the United States highlighted the need for interacting with outsiders to improve the analytical capabilities of the intelligence enterprise. The *Report of Twentieth Century Fund* (TCF) *Task Force on Future of U.S. Intelligence* recommended fostering interactions between the National Intelligence Council (NIC) and outside experts from academia, think tanks, business and non-governmental organization[1]. Likewise, the *Report of the Council on Foreign Relations* (CFR) *Task Force on the Future of U.S. Intelligence* suggested the creation of an intelligence reserve corps consisting of "former intelligence professionals, academics, and others with particular geographic and/or functional expertise for dealing with unanticipated crises in low-priority areas"[2]. The development of a Civilian Reserve Program was also underscored by the Staff Study of the Permanent Select Committee on Intelligence, *IC21 The Intelligence Community in the 21st Century*, as "the most important aspect of preparing the IC for the future, especially in terms of linguistic and analytic capabilities"[3]. This study provided the recommendation of including non-IC experts from academia

* Professor, Chair of Intelligence Services and Democratic Systems, King Juan Carlos University

and business for providing "ongoing information on warning and trends and to be utilized during crises to augment IC assets"[4]. Similarly, the Report of the Commission on the Roles and Capabilities of the United States Intelligence Community, *Preparing for the 21st Century: An Appraisal of U.S. Intelligence,* stressed the need for making use of expertise outside the Intelligence Community:

> "Intelligence agencies should more often take the initiative to sponsor open conferences on international topics, make direct and regular use of outside consultants, establish regular "peer review" by outside experts for major assessments and estimates, and contract out research on unclassified aspects of analytical problems or the maintenance of reference data bases. Analysts should systematically be able to consult outside experts on particular issues without undue bureaucratic hindrance"[5].

This growing awareness about the need of tapping the expertise of outsiders has ended up becoming an intelligence directive. The role of academia and other non-intelligence communities, such as think tanks, industry, non-governmental organizations and scientific world, has become normalized by the Intelligence Community Directive (ICD) Number 205. In response to recommendations of the Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, that encouraged Community analysts to broaden their information horizons and expanding their use of outside experts, the Director of National Intelligence (DNI), Mike McConnell, issued an ICD on Analytic Outreach. It is defined as:

> The open, overt, and deliberate act of an IC analyst engaging with an individual outside the IC to explore ideas and alternate perspectives, gain new insights, generate new knowledge, or obtain new information. It is conducted in accordance with fiscal, procurement, security, counterintelligence, operational and other laws, regulations, policies and procedures applicable to the IC and the analysts' individual organizations[6] .

This IC-wide policy directs intelligence analysts to network at home and abroad for developing trusted relationships:

> These trusted relationships could include, as appropriate, experts in academia; think tanks; industry; nongovernmental organizations; the scientific world (e.g., U.S. government laboratories, national academies, national research councils, and Federally Funded Research and Development Centers); state, local, and tribal

> governments; other non-Intelligence Community U.S. government agencies; and elsewhere. These communities allow the IC to expand its knowledge base, share burdens, challenge assumptions and cultural biases, and encourage innovative thinking[7].

Regarding responsibilities, the Directive gives instructions to establish a coordinator for analytic outreach in each service of the IC, in order to "act as a catalyst, advocate, and locus of expertise for conducting outreach activities, and help coordinate and de-conflict outreach efforts to eliminate unnecessary duplication within and among organizations". According to ICD 205, the Analytic Outreach Coordinator also has duties of liaison on security, counterintelligence, and outreach tradecraft training issues, dissemination of information regarding outreach events and reporting on the results of outreach activities, as well as on the state of outreach in their organizations on an annual basis. Likewise, the Subcommittee on Analytic Outreach of the National Intelligence Analysis and Production Board is appointed "the principal coordinating body in the IC with respect to analytic outreach initiatives and interagency collaboration", and the Bureau of Intelligence and Research (INR) is directed to be "the Executive Agent of the DNI to promote, facilitate, and implement Community-wide outreach"[8].

The utmost importance of relationships of trust within the System was also stressed by the preliminary findings report of the Project on National Security Reform:

> FINDING: The effective flow of information and knowledge is facilitated through networks of trust. Trust within the national security system is irregular, causing information and knowledge between departments to be uneven and unpredictable. (Knowledge Management).

Trust must be built among different parties within a system to create reasonable expectations of reciprocity in sharing information and knowledge. Trust tends to emerge between highly committed individuals on an ad hoc basis and within personal relationships[9].

The Canadian Security Intelligence Service (CSIS) has also established an Academic Outreach Program in the same year[10]. In Spain the National Intelligence Centre's launched (CNI) Intelligence Culture Initiative in mid-2000, being one of its objectives to allow intelligence services to benefit from the knowledge and experience of scholars in relevant issues and matters of interest for intelligence services[11]. In June 2012, the second edition of the International Workshop on Intelligence (IWI) took place at King Juan Carlos

University with the main objective of bringing together international experts in field of Intelligence to explore the issue of analytic outreach. Regarding trusted relationships, academic scholars from the United States, United Kingdom, Spain and representatives of the CNI, the Intelligence System of the Portuguese Republic (SIRP) and the "Mihai Viteazul" National Intelligence Academy (Romania) reached the following conclusion:

> Trusted relationships management emerge as an Intelligence function under the new intelligence paradigm. The effectiveness of intelligence services to reach out to academic scholars and other non-IC stakeholders depends on the capability of the intelligence services to build and manage the trust of outside experts. The meetings between practitioners and scholars, their exchange of ideas, and the discussion of topics of interest should be institutionalized[12].

Accordingly, to be able to both tapping expertise from outsiders and creating an information and knowledge sharing culture across the intelligence enterprise, the services shall develop a trusted relationships management capability that defines and implements a strategy for achieving these goals at the IC level and between the Community and their external stakeholders. Communication (symbolic and behavioral) shall play a relevant role to that end. Communication is a vital ingredient for organizations to the extent that without communication there would be no organization[13]. The same principle might be stated for the case of Intelligence Communities, if by community should be understood coordinated set of intelligence organizations sharing information and working as a unit to achieve common planned objectives according to a strategy.

Trust-building and Stakeholder Management[14]

The Stakeholder theory and a stakeholder management approach to outreach can be useful for building trusted relationships and tapping the expertise from outsiders.

Encouraging and building trust between organizations and their stakeholders is a key driver of success for both companies and public institutions. Beyond short-term objectives, companies need to build relationships and maintain the support of their customers and other stakeholders for keeping being competitive. However, trust should never be assumed or taken for granted since it is a perishable asset that needs to be cultivated and sustained[15]. As Robert Boutilier has

pointed out, mistrust from stakeholders can reduce the degree of access to resources, such as raw materials, employees, financing, suppliers and clients. Thus, those companies that secure a superior access to valuable, scarce, no substitutable resources will achieve a competitive advantage over others[16].

According to the stakeholder theory, organizations have stakeholders, that is: "groups and individuals who can affect, or are affected by, the achievement of an organization's mission"[17]. Stakeholders hold stakes, something of value other want or need[18]. Then, stakes connect those individuals or groups with the organization and can be tangible (e.g., funds) or intangible (e.g., support)[19].On the other hand, stakeholders have interest in a matter, issue or concern, being "cognitively involved to obtain, review, think about, and formulate attitudes and behavioral intentions about the matter"[20]. It could be said that, stakeholders and stakeseekers (those who want the stake held by other) are categories or roles exerted in relationships of influence. Consequently, the degree of a stake's value will determine the ability of stakeholders to influence organizations' decisions and performance. Obviously, there are differences between kinds of stakeholders since not all of them have equal degree of power or legitimacy and conflict of interest may exist among stakeholders. Originally, Freeman's stakeholder theory is presented in the framework of business organizations but it also can be applied for nonprofit and governmental organizations. With regard to firms, a generic stakeholder map includes employees, customers, suppliers, government, media, activist groups, and others. Consumers seek the product or service provided by a company and hold resources to get it, so it is established a stake-exchange relationship between both sides. But consumers also can make the decision of not purchasing that company's product or service if, for instance, there is a perception of physical insecurity about it, or dissatisfied customers make negative word-of-mouth comments, then affecting negatively the company's objectives. Regarding governmental agencies, the main purpose of public organization is creating public value "through meeting the organization's mandates and fulfilling its mission" as a result of producing decisions and actions that satisfy a set of functions[21]. As Hal Rainey has asserted, "public agencies are born of and live by the satisfaction of interest that are sufficiently influential to maintain the agencies' political legitimacy and the resources that come with it"[22].

Intelligence services have obvious specific characteristic in relations with other governmental organizations that will shape their approach to stakeholders but like other governmental organizations, intelligence agencies are required to address their mission competently and most of the times efficiently. Intelligence services must satisfy the consumer's requirements, their primary stakeholder, with good intelligence products by understanding his needs. Sometimes the intelligence agency must explain the difficulty to address those needs with the resources at disposal. The augmentation of resources may imply in that case the agency ability to retain general public and media support conducting as a result to political support. And finally, a lack of public perception or understanding of what intelligence mission is and does can neglect this support affecting intelligence organization's mission. Intelligence Services need to develop a stakeholders' relationship management function and programs, therefore.

A map of generic stakeholders of intelligence services includes policymakers, lawmakers, citizens, media, employees, private companies, whether contractors that work for intelligence agencies or not, other organizations that are members of Intelligence Community, and foreign intelligence organizations with which there exist a cooperation relationship.

Concerning policymakers and lawmakers, there is a need for having educated politicians on intelligence issues. The role of educational institutions is essential to that end. Depending on political systems and specific legislation in each democratic country, intelligence has different oversight mechanisms and structures. This includes overseeing intelligence spending of funds and the consistence of intelligence activities with the law[23]. But, intelligence oversight is also affected by many environmental factors, such as media reports and pressure groups. The management of relationships with the legislative branch or institutions that conduct intelligence oversight is essential for building trust.

Regarding citizens, since transparency is a fundamental principle of democracies, it is essential to properly communicate to the general public what intelligence is, what an intelligence agency does, what services it is supposed to provide, how the agency provides these services and carries out its functions, and why its operations require a space of secrecy outside general public accountability. Citizens are affected by the achievement of intelligence mission and objectives and citizens also can grant or deny understanding and support

to intelligence services through exerting influence on their representatives. The executive and legislative branches of government are the representatives of the citizens, acting on their behalf. Educating the public about intelligence issues, process, functions, and so on, becomes crucial for the intelligence missions if, as Hulnick points, it improves the ability to get resources, to serve intelligence consumers, or recruiting human talent[24].

News media inputs are primary elements for the public to judge intelligence organizations. Arguably the only knowledge about intelligence for most citizens comes from media reports. Thus, these inputs determine public trust in intelligence agencies. It also happens that intelligence is front-page news most of the time when there is a failure, or as once President John F. Kennedy asserted at CIA Headquarters: "successes are unheralded, failures are trumpeted". Nevertheless, the latter is not the only point in the intelligence-media relationship, as Robert Dover and Michael S. Goodman have shown in the volume Spinning Intelligence[25]. Another major source that positions intelligence organizations in the general public's minds is the entertainment industry. Movies, television series, video-games, fiction literature, graphic novels, comics, radio programs, and magazines all help to shape citizens' understanding of intelligence organizations. Citizens extract information about intelligence organizations from these sources. Images and narratives constitute symbolic representations that produce meaning and configure intelligence cultural archetypes. Thus, to some extent, these cultural representations constitute frames of reference for non-expert publics, playing a key role in what might be called the "interplay of influences". According to Heath and Palenchar[26], archetypes can determine the quality of relationships between stakeholders and stakeseekers.

Outreach policies position academic experts, think tanks, business and other communities as important stakeholders within the intelligence services' webs of mutually influential relationships.

Among all these communities, academic institutions and experts emerge as key stakeholders for three main reasons: (1) they can shape the opinions and attitudes of Intelligence Community 'stakeholders toward intelligence matters: decision makers, media, the public, and non IC experts; (2) Academia can provide value to the intelligence enterprise as a place to send officials for gathering knowledge, expertise or insights on intelligence needs from academic experts and also to learn methodologies to improve the practice of intelligence analysis[27]; (3) Academic events can provide interaction

environments to bring closer intelligence officials and professionals from different bodies of the intelligence system and outsiders[28]. And these motives, in turn, demand a relationship management strategy for dealing with scholars, especially in the case of new democracies or countries where security and intelligence issues are perceived with an attitude of suspicion or lack of understanding[29].

Relationships Building Between Intelligence Communities and Academic Scholars

Since Academia seems to be a key player for building and managing trusted relationships between the IC and their other stakeholders, a trusted relationship management strategy should include specific programs for this strategic community. As Hallahan has pointed out from the discipline of Public Relations "community can be conceptualized as a group of people who share a common experience, identity of interest and who are joined together through their interaction or communication"[30]. We can refer to a community in the geographic sense (a specific city like Bucharest) and also in the symbolic sense (e.g., the International Academic Community of Intelligence Studies). According to Hallahan,

> Communities define themselves and thus exist outside the context of any particular organization [...] Communities are not merely audiences and are not defined by their stakeholder relationship to the organization. Communities are the umbrella grouping within which various publics might exist and from which groups of people might form to address issues. Communities differ from publics because they organize around common interests, not issues, and are apolitical. Their goal is usually to sustain the group, rather than to effect change [...] Communities have long and well-established histories and people within them routinely interact by sharing a common culture. By contrast, a public created around an issue often has a short-term life span and brings together diverse people whose only commonality is concern about a common problem. As the term is commonly used, a public is considered to be made up of individuals, yet communities can be thought of as being composed of individuals as well as organizations and institutions[31].

From our standpoint, both the concepts of stakeholders and community, as well as both the stakeholder management and the community relations approaches to academic outreach are useful and complementary. Intelligence organizations engage in analytic outreach seek the stake of expertise that specific experts hold and that can

be exchanged or withheld. At the same time, the academic community can alter the IC degree of access to resources of expertise. This is expressed in the concept of social license to operate[32]. According to Burke, since the 1970s, communities have emerged as "the focal point for decision making that affects companies" determining their license to operate and, consequently, "attitudes, expectations, and behavior in communities have to be managed as any other function in the company[33]. And remaining beneath the surface of relationships between companies and communities there is a psychological contract, or the combination of both the explicit and tacit expectations that companies and communities have for each other[34]. Following Burke's ideas for companies and communities, the IC has to develop strategies for its relationship with the Academic Community that can give or deny the IC permission to operate analytic outreach policies with academic scholars. To get the SLO, the IC has to build trust between it and the Academic Community, behaving in a way that promotes that trust, being respectful with community's values and practices, and keeping its actions consistent with its messages. Promoting and building trust is a necessary condition for developing the positive reputation that guarantees the SLO.

The Intelligence Culture Initiative: Promoting Intelligence Studies and Managing Trusted Relationships for Analytic Outreach in Spain[35]

Prior to mid-2000s, the presence of intelligence in Spanish university courses was anecdotic. The causes of this notable absence are diverse, although probably linked to the Spain pre-democratic past, since intelligence is interrelated to the political system to which it serves. The consequence was a general mistrust and a lack of knowledge on intelligence matters by intelligence services' stakeholders. This situation changed considerably due to the implementation of an openness policy by the CNI, through its Intelligence Culture Initiative and the signing of agreements with universities, which has led to the development of Intelligence Studies in Spain. In addition to producing knowledge or culture on intelligence matters, the Initiative has a strategic dimension since it aims to allow the services to reach out for expertise to academic scholars and other non-IC stakeholders, including the business community. To that end, an Intelligence Culture unit has been created inside the CNI.

Since intelligence and information services have traditionally resisted to openness, the effectiveness of analytic outreach depends on the capability of building and managing bidirectional trust between the IC and outsiders. Academic events, workshops and university courses have emerged as interaction environments to bring closer intelligence officials and professionals from different bodies of the intelligence system and outsiders, helping also to overcome a culture of secrecy and mistrust and its replacement for a culture of intelligence.

In December 2006, the Chair Intelligence Services and Democratic Systems of King Juan Carlos University, the Institute of Intelligence for Security and Defense of Carlos III University of Madrid (which were the first universities to sign specific collaboration agreements with the CNI) and Plaza y Valdés Publishers launched the first intelligence academic journal in Spain, *Inteligencia y seguridad: Revista de análisis y prospectiva* (Intelligence and security: Journal of analysis and foresight).

A wide array of academic events, like seminars and conferences, targeted to the general public and aimed at creating an accurate concept and representation of intelligence and intelligence services have been organized since the beginnings of the Initiative, such as conferences on intelligence and national security and on economic and competitive intelligence. However, the first major academic event was the Congress on Intelligence held in October 2008. The second edition of the Congress was held on November 2010, and a third international edition has been programmed for November 2012 at Barcelona. Both editions have brought a number of Spanish and also international experts together to discuss intelligence ethics, history, law, sources and methods, economic and competitive intelligence, and academic research among other topics.

Together with these events, other non-opened events have also been organized. In June 2011, it was launched the International Workshop on Intelligence (IWI) that brings together international experts in intelligence and intelligence studies from academia and intelligence officials. The inaugural workshop was focused on good practices in Intelligence Studies and IWI 2012 was devoted to the issue of analytic outreach.

In 2006, the Chair of Intelligence Services and Democratic Systems also set up the free elective course “Intelligence Services: security and treatment of open sources” for the students of the Faculty of Communication Sciences at King Juan Carlos University.

Intelligence literature production, academic research on intelligence matters, and education and training in intelligence and intelligence analysis are strategic pillars of the Initiative altogether.

A cornerstone of the Initiative is the postgraduate program in Intelligence Analysis. In 2009, King Juan Carlos and Carlos III Universities, with the collaboration of CNI and also the sponsorship of a number of private companies, launched the first edition of MA in Intelligence Analysis, the first academic program in Spain focused on educating and training in intelligence analysis. In 2012, this intelligence analysis postgraduate program was also launched in Barcelona, with the participation of University of Barcelona, and the Autonomous University of Barcelona. This academic postgraduate program constitutes a remarkable advance for the development of intelligence in Spain. The program is structured in modules covering the following topics: principles of intelligence; planning and direction, epistemology applied to intelligence; intelligence collection both from open and human sources; analytic methodologies and techniques; communication, dissemination and protection of intelligence; economic and competitive intelligence. A mandatory internships module is also integrated in the program. The professors are both academics, including scholars from the United Kingdom, the United States, practitioners from private business, military staff and also members of CNI, active or retired. Expressing its nature in the terms suggested by Stephen Marrin, the MA in Intelligence Analysis mixed the intelligence studies and the intelligence school models. Regarding training in intelligence analysis and production, students are instructed in the use of social sciences methods and learn structured analytic techniques. The Master in Intelligence Analysis makes use of simulations for improving the learning experience of students.

A simulation exercise was designed in 2010 for addressing the need of training the students while testing the use of multimedia tools in enhancing the intelligence consumer experience by enriching intelligence reports' communicative features. The simulation allows the students to experience the intelligence production process while role-playing and interacting as information gatherers, analyst and managers addressing a real-time intelligence requirement. From the standpoint of the educator or trainer, it allows to reinforce the concepts and tools taught to the students.

In addition to the events and programs more directly related to the Intelligence Culture Initiative, other public and private universities have begun to launch programs and to organized activities in Spain.

Although there are not comprehensive quantitative reports on the number of published articles, collective volumes and monographs on intelligence as a consequence of the Intelligence Culture Initiative covering the period, the fact is that intelligence literature has increased exponentially during the last decade. The same thing can be stated regarding conferences, workshops and intelligence related events in general. Since these publications and events are open and targeted to general audiences, and some of the activities have been covered by media news, the influence of the initiative on these audiences seems to be a reality. Journalists have also begun to ask for academic intelligence experts to produce news or reports and there is active conversation on intelligence in social media channels. According to a survey published by the journal Inteligencia y seguridad in January 2012, the CNI is, together with the Spanish Armed Forces and the Crown, one of the Spanish institutions best valued by the citizens. However, only a low percentage (between 30 to 40 per cent) declares to have enough knowledge about CNI for expressing an opinion about it, a fact that raises an argument for strengthening the Intelligence Culture Initiative. After an introduction phase, the initiative has reached an ongoing consolidation phase in which there is a growing interest in intelligence and Intelligence Studies from academics, students, business, and departments from the Spanish administration.

As regards the culture inside the Spanish Intelligence Community, and more specifically, the analytic culture, it is difficult to know. The culture of secrecy has been deep-rooted inside intelligence services configuring a markedly stove-piped system that has begun to change only in the last ten years. Both the activities of the CNI, the main intelligence collection and analysis agency in Spain, and those of the other military and law enforcement intelligence services are classified as top secret, according to the Spanish legislation in force. This fact together with the absence of a declassification policy, prevent research activities based on official documentation and historical records of former intelligence organizations that could be used to evaluate changes in analytical practices.

However, since workshops on analytic techniques and other events have been attended by staff from organizations members of the IC, it can be expected to have had an influence at least in providing knowledge on structured analysis. Another challenge remains to be the involvement of decision makers both at the government and business level in activities of the Initiative, while there is a need to educate them on intelligence issues.

References

[1] Allan E. Goodman, Gregory Treverton and Philip Zelikov, *In from the Cold: The Report of the Twentieth Century Fund Task Force on the Future of the U.S. Intelligence* (New York: Twentieth Century Fund, 1996).
[2] Council of Foreign Affairs, *Making Intelligence Smarter: The Future of U.S. Intelligence, Report of an Independent Task Force* (New York: Council of Foreign Affairs, 1996).
[3] Staff Study, Permanent Select Committee on Intelligence, United States House of Representatives, *IC21: Intelligence Community in the 21st Century* (Washington, D.C.: GPO, 1996).
[4] *Ibid*.
[5] Commission on the Roles and Capabilities of the United States Intelligence Community, *Preparing for the 21st Century: An Appraisal of U.S. Intelligence*, March 1996, available at http://www.gpo.gov/fdsys/phg/GPO-INTELLIGENCE/content-detail.html
[6] Director of National Intelligence, *ICD 205 Analytic Outreach*, July 16, 2008.
[7] *Ibid*.
[8] *Ibid.*
[9] Ashton Carter *et al.*, *Project on National Security Reforme-Preliminary Findings,* July 2008, p. 89.
[10] See: http://www.csis-scrs.gc.ca/bts/cdmctrch-eng.asp.
[11] See: http://www.cni.es/es/culturainteligencia/.
[12] Draft document prepared by the author.
[13] See: Everett M. Rogers, *Communication in organizations* (New York: The Free Press, 1976).
[14] Some ideas from this epigraph were included in the paper "Academics as Strategic Stakeholders of Intelligence Organizations: a view from Spain" that was presented at the Academic Intelligence and Security Studies Conference held in November 2011 at Bucharest. It has also been presented and accepted for publication at the *International Journal of Intelligence and Counterintelligence* (forthcoming).
[15] Edmund M. Burke, *Corporate Community Relations: the principle of the neighbor of choice* (Westport, CT: Praeger, 1999).
[16] Robert Boutilier, *A stakeholder approach to issues management* (New York: Business Experts, 2012).
[17] R. Edward Freeman, *Strategic Management: A Stakeholder Approach* (Marshfield, Massachusetts: Pitman, 1984), p. 52.

[18] Robert L. Heath and W. Timothy Coombs, *Today's Public Relations: an introduction* (Thousand Oaks, CA: Sage, 2006), p. 79
[19] W. Timothy Coombs and Sherry J. Holloway, *It's not just PR: Public Relations in Society* (Singapore: Blackwell, 2007), p. 24.
[20] Robert L. Heath and Michael J. Palenchar, *Strategic Issues Management: organizations and public policy challenges*, 2nd edition (Thousand Oaks, CA: Sage, 2009).
[21] John M. Bryson, "What To Do When Stakeholders Matter: A Guide to Stakeholder Identification and Analysis Techniques", Paper presented at the National Public Management Research Conference, 9-11 October 2003, The Georgetown University Public Policy Institute, Washington, D.C., p. 7, available at http://www.governat.eu/files/files/pb_bryson_stakeholder_identification.pdf (accessed 4 August 2011).
[22] Hal G. Rainey, *Understanding and managing public organizations*, 4th edition (San Francisco, CA: Jossey-Bass, 2009).
[23] L. Britt Snider, "Sharing secrets with lawmakers: Congress as a user of intelligence" (1998), in Susan L. Maret and Jan Goldman (eds.), *Government Secrecy: classics and contemporary readings* (Westport, CT: Libraries Unlimited, 2009), p. 522.
[24] Arthur S. Hulnick, *Fixing the spy machine: preparing American Intelligence for the Twenty-First Century* (Westport, CT: Praeger, 1999), p. 185.
[25] Robert Dover and Michael Goodman, "Introduction: Intelligence in the Information Age", in Robert Dover and Michael S. Goodman (eds.), *Spinning Intelligence: why intelligence needs the media, why the media needs intelligence* (London: Hurst & Company, 2009), pp. 1-11.
[26] Robert L. Heath and Michael J. Palenchar, *Strategic Issues Management: organizations and public policy challenges*, 2nd edition (Thousand Oaks, CA: Sage, 2009).
[27] See: Stephen Marrin, *Improving Intelligence Analysis: Bridging the gap between scholarship and practice* (Abingdon, Oxon: Routledge, 2011).
[28] Rubén Arcos and Joan Antón, "Reservas de Inteligencia: hacia una Comunidad ampliada de Inteligencia", *Inteligencia y seguridad: revista de análisis de prospectiva*, No. 8, 2010, pp. 11-38.
[29] Rubén Arcos, "Academics as strategic stakeholders of intelligence organizations: a view from Spain". Paper presented at the Academic Intelligence and Security Studies Conference held in November 2011 at Bucharest.
[30] Kirk Hallahan, "Community and Community Building", in Robert L. Heath (ed.), *Encyclopedia of Public Relations* (Thousand Oaks, CA: Sage, 2005), p. 171.
[31] *Ibid*., p. 172.
[32] Boutilier, *A stakeholder approach,* 2012.
[33] Edmund M. Burke, *Corporate Community Relations: the principle of the neighbor of choice* (Westport, CT: Praeger, 1999).
[34] *Ibid*.
[35] Some findings included in this epigraph can be found in the paper "Assessing the impact of intelligence education and training on the development of intelligence analysis culture in Spain" presented by the author at the International Conference on Intelligence Analysis –ICINTA'12 "From Intelligence to Policy-Making: Intelligence Analysis for Policy Executives" held in June 2012 at Ankara. It also presents contents included in the chapter "Systems of Intelligence: Spain" from the *Routledge Companion to Intelligence Studies* (forthcoming).

Strategic Analysis
Facing the New Challenges

Cristina POSAŞTIUC*

Abstract

The end of the Cold War, as well as the new challenges to national security that emerged in the last two decades led to a reshaping of the intelligence paradigm and, as a consequence, of the intelligence communities' role and objectives.

Both analyst and decision-maker have been forced to rethink their role, as the current environment is rapidly and continuously changing.

Thus, in order to tackle the new risks, the traditional methods have been replaced by new ones focused on knowledge and designed to provide strategic warning.

The pressure exerted by the changes arisen in the context of the World War Two established a novel issue as a study subject: the relationship between information and security, where information is the strategic power resource.

Sherman Kent, who formulated the direction, was also the one who developed the first *intelligence* project and the very concept of strategic analysis as well and who introduced the "Knowledge Is Power" paradigm, taken from Francis Bacon. He promoted the idea that the strategic advantage can be gained through rethinking *intelligence* as academic field. He also advanced the term "strategic thinking", pointing out the distinction between that and *non-range planning* or *forecasting*.

Around 1935, he joined a team of American experts who had the task of creating a national intelligence agency. Within the project, he started a process of analyzing social and political implications, representing, in conceptual terms, a benchmark of current evolutions from the open source point of view.

According to some experts[1], during the Cold War, policymakers were "large consumers" of strategic *intelligence*, that provided necessary support to successfully continue their operations and clearly assess the threats, but also the strengths and weaknesses of the adopted strategies.

As the modern theory of *intelligence* is marked by the impact of uncertainty, the security environment of the 21st century "forces the *intelligence* organizations to adhere to two distinct paradigms in

* Lecturer, "Mihai Viteazul" National Intelligence Academy

order to operate: the traditional one, which involves solving puzzles in the case of common threats against state, and a new one, adapted to transnational threats"[2].

Thus, opposite to Kent's vision, "the urgency" of events - according to John G. Heidenrich[3] - puts the tactical thinking on top of *customers'* priorities, leaving strategic *intelligence* on a second place. Consequently, too elaborated or far away in time analyses tend to be ignored[4].

The theory that an intelligence community could simply become "a knowledge provider" rather than "a producer of information"[5] has been also advanced.

Strategic Culture and Strategic Advantage

Even since the end of the last century, experts have rediscovered the valences of strategic culture as an instrument of analyzing national security policies:

- "the cultural realism" of the Chinese security policy during the Ming Dynasty was explored by Alastair Johnston, who suggested that societal characteristics exerted influence on state behavior over a long period of the human civilization history;
- according to other experts, that studied Germany's and Japan's security policies in the post-Cold War era, the unique character of "anti-militantist" strategic cultures would explain the continuity recorded from 1990 up to present;
- Samuel Huntington's theory was that the "meta-cultural" differences would increase the probability of international conflicts (the idea was used to explain both the events of September 11, 2001 and the war against terrorism).

The end of the Cold War has been interpreted as a major strategic opportunity for states to reconsider their past, present and future. The neo-realists have predicted that the United States, as the only surviving superpower, will be able to establish the new world order, as Russia and the former Soviet republics will be affected by fragmentation of their policies, and China may rise as a real rival to the American hegemony. On the other hand, states which have been "left aside" and subject to constraints after the Cold War, such as Japan and Germany, will normalize their foreign policy by creating an assertive profile rather than focusing on strategic interests, backed by the threat of military force[6].

A decade after the end of the Cold War, critics denounced neo-realism, arguing that it was wrong in predicting major events (such as system changes) and did not adequately describe patterns of national security policies of the new dynamic international system.

In the mid 1990s, criticism on systemic approaches became visible in national security studies. Works elaborated by Bueno de Mesquita and David Lalman, Jack Snyder, Richard Rosecrance and Arthur Stein, and others related to neo-realist trend could not fully explain the major changes in security policy such as the end of the Cold War or the shifts in the balance of power.

Colin Gray defined the strategic culture as "reference to ways of thinking and action, taking into account the force, which derives from the perception of national historical experience, from aspirations to a responsible behavior in national terms" and even from "civic culture and lifestyle". Strategic culture "provides the framework for strategic debates" and serves as an independent determinant of strategic policy patterns. Thus, according to Gray, strategic culture would exercise a semi-permanent influence over security policy[7].

Resources for Strategic Power

The analytical focal point of intelligence communities was changed by globalization and information revolution[8]. Even if the new technology society presented many advantages, the permanent change of benchmarks has resulted in the development of anxiety at the human level and in the difficulty to provide viable development scenarios to customers, at the level of *intelligence* analysts. The unpredictable background was also supported by the diversification and spread of the security threats.

Within this context, not only information is critical, but also its understanding, in order to consistently interpret the new security dynamics. Consequently, even the traditional methods used by analysts can prove, in some circumstances, to be inappropriate and inapplicable in the case of assessments that focus on anticipation and prevention.

The political and social transformations as well as the awareness of the social responsibility in preserving the current model of civilization were all reasons to redefine the security environment. To complicate things, we can say that, in terms of security, some entities may be friends and foes at the same time, depending on the area of interest. The new typology of risks and security interests underlies these changes.

The hectic pace with which events happen puts pressure on both analysts and customers/decision-makers.

The analysts are forced to continually adapt the analytic speech according to developments, sometimes finding themselves overtaken by them.

On the other hand, the decision-makers are pressed by the need for knowledge and also always concerned that they do not have all the pieces of information needed to substantiate the measures they intend to take.

Therefore, we can say that today we are witnessing an unprecedented explosion of tensions, triggered by a growing demand for analytical materials and operative conclusions, designed to promptly manage the emerging situation.

Under these circumstances, the role of security-related information is critical as the experience shows that the resources allocated to prevent a real threat are much lower than those designed to remove potential effects of its materialization.

We can say that this reality has triggered the shift in the customers' interest from diagnostic, explanatory information to estimate information forecasting the changes in the relevant fields.

Strategic Analysis - Definition and Features

In the most common perspective, the economic one, the strategic analysis is one of the elements of the planning process, as its ultimate goal is to provide competitive advantage.

Professor Les Worral at the University of Wolverhampton Business School formulated a comprehensive definition, that shows that strategic analysis is "a theoretically informed understanding of the environment in which an organization is operating, together with an understanding of the organization's interaction with its environment in order to improve organizational efficiency and effectiveness by increasing the organization's capacity to deploy and redeploy its resources intelligently".

Or, more simply, the *BNET Business Dictionary* defined it as "the process of conducting research on the business environment within which an organization operates and on the organization itself, in order to formulate strategy".

Therefore, strategic analysis is only a phase in a process that ends in the adoption of a usually long-term decision, involving the full engagement of all available resources.

As stated above, the demand for analysis to determine and, especially, implement strategies aimed at ensuring an advantage over competitors by adapting, in real time, to changes in political, economic, social, cultural or scientific environment has significantly increased at different decision-making levels.

Analyses of development trends in domestic and international environments, assessments on the probability for risks and threats to materialize as well as their effects are vital information on which policy makers:

- properly define national interest;
- develop an appropriate doctrine and ensure its transposition into practice;
- create a security policy and an opportune military strategy;
- assign appropriate tasks to the security structures.

In the case of strategic analysis, the emphasis is placed on the trend of image and its correlation with the main events occurred in the analyzed period, as well as on highlighting major image vulnerabilities.

The increase in "strategic surprises" and their consequences has determined the analysts to consider that a different approach, connected to the technical possibilities and current knowledge, is needed. The need for anticipatory *intelligence*, as a potential tool for correcting, through timely and fair decisions, the conditions that can lead to serious security risks, has become increasingly obvious.

The so-called *post-mortem report*, which, after 1990s, has become a constant at the level of the US National Intelligence Community, the political decision-making bodies or the powerful local *think-tanks* was one of the instruments that stated the need for a substantial paradigm change. One of the conclusions was that, although representing a major part of the analysis, prediction seems to have a different role depending on the pursued purpose or, especially, on the type of decision to be adopted.

Furthermore, it has become clear that for making prognostic assertions, a coherent system, constantly providing dedicated analyses, is needed.

The pressure exerted on the intelligence communities to use the best tools – either analytical, methodological, or technological - to improve *intelligence* has become increasingly powerful in the sense of sharing with the external environment the knowledge gained in intelligence practice.

Jack Davis (2002) has made a clear distinction between tactical warning (*tactical/incident warning*), very useful to estimate

when, where and how security interests can be affected, and *strategic warning*, as a way to detect the changes in the probability of security threats and mechanisms of occurring.

In the same year, the Joint Military Intelligence College promoted, in an updated form, Cynthia Grabo's 1980 report - the result of an analyst's life - on the need for strategic warning and the way it could be implemented in the current *intelligence*, previously placed in the "secret" category.

Alongside Cynthia M. Grabo's contribution, those of Steve Chan and Davis Bobrow are very important for the Cold War period and they represent, at the same time, the foundation of current attempts to harmonize with the worldwide changes. The shift to security *intelligence* has led to a wider range that needs to be covered by this concept, together with increased efforts to recalibrate the content.

A utilitarian definition of strategic analysis could be: the identification of those developments with negative impact on the topic of interest (economic field, geographical region, security issue, etc.) having as a starting point a set of values registered by previously validated tools (technical, computational, or even results of human observations) and the interpretation of maps of interdependence networks among quantified factors (building on Cynthia M. Grabo's warning – "facts don't speak for themselves") by resorting to intuitive and imaginative experts' criticism.

A strategic analyst should, at the same time, resist the temptation to excessively appeal to his own imagination or personal convictions, as in the desire to prove something, data is sometimes selected to fit the desired picture.

Of all classical definitions of *strategic warning*, the closest to its current role in the *intelligence* field was forwarded, in our opinion, by Jack Davis: "timely analytic perception and effective communication to policy officials of important changes in the level or character of threats to national security interests that require re-evaluation of country's readiness to deter or limit damage", in order to prevent strategic surprise.

However, the current challenge consists in the increase in potential risks and especially in the proliferation and diversification of factors able to influence the security situation. As stated above, there is a series of new threats or crisis developments that can turn, on the short term, into security threats.

For this reason, the key to success for a strategic analyst lies in his/her ability to determine which of the dangers that seem improbable today deserve to be seriously considered as having the capacity to turn into real threats.

At the same time, there is the tendency to include into this category any prediction, any projection on the future, regardless of its connotation in relation to security, by exacerbating the impact on the social, political and economic stability.

Thus, the areas of interest have been limited today, with the mention that the dynamics is very high, and changes of emphasis and interest – objective or, sometimes, subjective - are and will be permanently made.

There is a quite widespread perception that the *strategic intelligence* addresses issues with low relevance to current operational needs as the strategic analysis is the manager's tool[9].

The strategic dimension of *intelligence* activity does not focus on individual targets/goals, but major trends that can be interpreted by assessing a large volume of target activities. Moreover, in the problem assessment process, analysis focuses on identifying and exposing the structure, goal and nature of topic of interest, not on achieving immediate, opportune reaction.

We list below, as example, trends that can make the subject to strategic analysis, which are of interest in achieving national security: enhancement of disagreements among most international political players over the approach on global issues, maintenance and, in some cases, deepening of some disputes among various subjects of international law in order to get a dominant status at the global, regional or local level, emergence of asymmetrical risks as criminal groups or extremist movements take advantage of globalization, deepening of the gap between available resources and the increasing needs of the contemporary society, maintaining some regional hotspots with a potential to spread, etc..

Briefly, the main functions a strategic review should meet are the following:

- assessing the medium- and long-term potential evolution of the main threats;
- signaling the emergence or amplification of negative effects or potential risks to country's interests;
- providing useful forecasts for state institutions' representatives to adopt political, economic and social lines of conduct as well as to exploit the opportunities opened up by timely information on the consequences of a potential action.

The importance of strategic analysis is also highlighted by its defining features:

- it has an anticipatory component that, starting from the operative diagnosis of the situation, indicates the medium and long term trends and effects, at local, regional and global level, of certain ongoing processes and phenomena that could have an impact on the national security and interests as well as on those of our allies and partners;
- it is a research method which consists in decomposing a phenomenon or process into its primary elements, to identify the factors, causes, and conditions that generated and, respectively, influenced them, their (potential or probable) future development playing a crucial role;
- it cumulates a set of methods, techniques, procedures, and tools that provides comprehensive approach of all available information in order to lay down relevant considerations on the analyzed phenomenon, the identification of factors, causes, and conditions that generated him as well as on the way of addressing/improving it in terms of efficient use of human, material, and financial resources;
- it requires identifying, extracting, corroborating, analyzing, and assessing information obtained from a variety of sources;
- in the case of security information, it focuses on an increase in the role of integrated multi-source information.

The analytical practice highlights the need for a series of conditions that has to be fulfilled in order to be able to build an efficient strategic assessment mechanism:

- establishing the exact needs in relation to capacities;

Striking a balance between the analysis possibilities and the need for security is fundamental. Covering the whole range of potential threats would be ideal, but the reality shows us that an extremely expensive system is needed. Meanwhile, the customer's capacity to manage information is limited by the legal barriers and the interactions with the other actors in the system. Therefore, the support systems of *strategic warning* should be carefully tailored according, as a rule, to types of customers.

- efficiently using the input collection, storage, and classification tools;

In the absence of correct, constant, and systematic signals, any warning is nothing but a "riddle". Experience shows how important is to identify the areas of information collection and, implicitly, the potential risks, to define the correct scanning and assessment indicators, a well-dimensioned scale and, last but not least, to train operators, starting from the idea that an automated system cannot fully catch the relevant nuances.

- providing complex training to analysts;

The emergence of so many new factors in the security equation puts any analyst into difficulty. The previous security crisis showed that a linear interpretation of the numerous available warning data did not allow the coverage of full range of potential risks.

Meanwhile, although the rigor and maintenance of a quantifiable formula of interpretations are the foundations of classical analysis, it is impossible for an analyst to make a strategic forecast without imagination. Stimulating imagination is a *must* in the mechanism of training dedicated analysts.

- fostering wide cooperation.

In order to fulfill his/her role, a *strategic warning* producer should have the capacity to share his/her knowledge and experience with other analysts, so that he/she be able to compare, supplement, and deepen reasoning and conclusions.

The *need to share* paradigm consistently used by the US intelligence community has been enforced in the most relevant environments. The fundamental condition of an efficient system is building trust among *intelligence* producers, which cannot be achieved in the absence of full willingness to share expertise.

Models of Interaction

"To work" on a strategic problem means to predict the events within the political, economic, military, diplomatic and cultural contexts. Most crises have their roots in the past, a generally far more distant past than the moment indicated as a triggering factor by analysts. A *strategic warning* assessment is not a compiled product of potential facts or indications, regardless of how useful they might be. The warning is built on indicators.

According to Cynthia M. Grabo, an indicator is a known or theoretical step taken by the potential risk factor in preparation for the attack/threat. It is something we anticipate may occur, which we usually include in a list of potential developments to be watched, known as the "indicator list".

The analyst's perception of the facts, events, situations, and phenomena of interest to achieve national security requires, equally, knowledge and understanding of them, being determined by the proficiency, professional experience, education level, and cultural values.

The problems frequently encountered in achieving a strategic analysis are the following:

- wrong perception on emerging threats, especially the low-probability ones but with a high potential of danger;

- inadequate collection of data and information on the analyzed threats or risk factors;
- communication gaps among collectors, analysts, and information structures;
- deflecting attention from the minority points of view;
- vulnerability to deception.

Awareness of theoretical and practical stalemate the contemporary analysis is facing mainly due to the negative, devastating effects of forecasting failures (such as the 9/11 attacks or economic crisis) has made the *intelligence* community undertake reform measures.

The US Intelligence Community, which relied, theoretically and practically ("500 Day Plan for Integration and Collaboration"), on a collaborative approach on sharing the information and expertise its various components held, was the first and more advanced in this regard.

It is impossible to hold the necessary expertise at the level of a single structure, especially when the topics of interest focus from nuclear missile technologies to pandemics - ignoring tomorrow's emerging issues. Furthermore, the current analytical challenges are less confined to a specific logic of a relevant domain, often resorting to multiple disciplines and various areas of expertise, developments that make almost impossible for a single analyst to achieve a strategic assessment.

Sharing knowledge and creating favorable conditions for exchanging opinions and shortening to minimum hierarchical chains result in removing gaps arising from the technological advance and diversification and diffusion of the security risks, streamlining the intelligence process and supplementing, through the contribution of available human potential, knowledge in the field of competence, establishing a common language, which is extremely important in the intelligence process, as well as setting customer's feed-back as a norm.

According to William J. Lahneman, the intelligence community needs to remain a hierarchical structure, able to generate or access collaborative networks if interdisciplinary analysis is required. These networks should integrate OSINT and should contain analysts and experts from the private sector[10].

Moreover, in order to correctly answer the "commandments" of the moment, the effort of identifying a solution to those challenges should be accompanied by strengthening knowledge and stimulating adaptability and innovative imagination as support factors in the analytical activity.

The outsourcing activity, still in a hybrid stage within the intelligence communities, may be a response to the unprecedented increase in the amount of information to such an extent that makes it impossible to classically manage data and, implicitly, the intelligence flow.

Objectively, it is impossible for an analyst to address by himself, with high professionalism, all the challenges he is subjected to in the numerous areas that have become of interest in the current security context.

Recently, the solution of striking a partnership between the intelligence structures and academic circles has enjoyed increasing recognition so that, building on sharing the responsibility of achieving the common good, a series of security challenges targeting niche domains or requiring access to basic research could be approached in a convergent manner.

The economic crisis in the recent years can be a landmark for supporting the imperative of rethinking strategic analysis. A review of the analyses elaborated and published by relevant institutions reveals a significant failure of previous estimates and a worrying alternation of approaches from a vivid optimism expressed before August 2008, to an almost generalized pessimism and skepticism towards a rapid recovery in the following year.

In order to highlight the contrasts, we put forward some aspects that could be lessons for the *intelligence* professionals, since the methodology was applied to economy - a field that best regulated the principles of strategic assessment and which, previously, defined the role of strategic analysis and planning.

One of the lessons learned from economists is that according to which they started from the wrong hypothesis that the obtained data were an exact reflection of reality. The New York-based financial organizations have made risk assessment based on an algorithm eliminating exactly the conditions that generated the crisis. According to Barry Ritholtz, many of the actions that hastened the emergence of crisis – the crowd rushing to withdraw the money from banks - were not perceived even by the finest observers. The conclusion is that the panic often passes unobserved, but even the analysts generally manifest an irrational attachment towards reasoning.

In the mutual observation activity between the information providers and customers, the *intelligence* experts do not realize that, in most cases, the decision that has to be made is but an option - not necessarily a very clear one - among other equally valid options which would be immediately amended or outrun by events.

The ability to provide certain signals about a threat or opportunity cannot be improved only by drafting more relevant analyses. More reliable information sources and, perhaps, new revolutionary types of cognitive techniques are needed.

References

[1] John G. Heidenrich, "The State of Strategic Intelligence. The Intelligence Community's Neglect of Strategic Intelligence", *Studies in Intelligence*, Vol. 51, No. 2, 2007, available at https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol51no2/the-state-of-strategic-intelligence.html.
[2] William J. Lahneman, "The Need for a New Intelligence Paradigm", *International Journal of Intelligence and Counterintelligence*, Vol. 23, 2010, p. 212.
[3] *Senior National Security Analyst* at the Science Applications International Corporation/ SAIC, company focused on providing services based on innovative application of science and technology.
[4] Heidenrich, "The State of Strategic Intelligence".
[5] Josh Kerbel and Anthony Olcott, "Synthesizing with Clients, Not Analyzing for Customers", *Studies in Intelligence*, Vol. 54, No. 4, 2010, available at https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-54-no.-4/pdfs/Olcott-Kerbel-Client vs. Customer-Extract-Annonated.pdf (accessed on 5 April 2012).
[6] Jeffrey S. Lantis, "Strategic Culture and National Security Policy", *International Studies Review*, Vol. 4, No. 3, 2002, pp. 87 - 113.
[7] Colin S. Gray, "National Style in Strategy: The American Example", *International Security 6*, No. 2, 1981, p. 35.
[8] Lahneman, "The Need for a New Intelligence Paradigm", p. 203.
[9] Don McDowell, *Strategic Intelligence. A Handbook for Practitioners, Managers, and Users* (Lanham, Toronto, Plymouth: The Scarecrow Press, 2009).
[10] Lahneman, "The Need for a New Intelligence Paradigm", p. 204.

Intelligence Analysis in the Circumstances of New Challenges and Security Threats

Emilija GEORGIEVSKA[*]
Ivona ANASTASOVA[*]

Abstract

The beginning of the third Millennium was marked by globalization, industrialization and fast IT and scientific development that contribute to the connection between states and regions. Aside from the numerous advantages, these processes determined also the division between people and marginalization of "the week ones" and poor ones, which implies manifestation of new ones and strengthening of the existing security challenges and threats. In that sense, the global international politics led to emerging of economic, political and military crisis, so called "system crisis" in the transition societies, new forms of terrorism, increase of organized crime – trafficking/smuggling of weapons, humans and drugs, threats of proliferation of weapons for mass destruction, computer and ecological crime.

With the aim of successfully countering new security challenges and threats, continuous reforms in security/Intelligence Community are necessary, adequate to the level of the criminality in the society. In that framework, it is necessary that the analytical work, as key part of the intelligence cycle, is compatible with the modern trends of the security challenges and threats, which is the basic precondition for successful and timely countering and preventing them. Therefore, it is imperative to have continuous reviews of the basic principles and methods of the process of analysis and carrying out adequate and timely training of the analysts of different disciplines.

Simultaneously, the multilateral cooperation is of great importance, as with other institutions on national level, states and international organizations based on fully integrated national and international approach, which will enable real dimensioning of the phenomenon and tendencies of such phenomenon, complex and timely reaction and improvement of forms and methods of countering.

National Security at the Beginning of the Third Millennium

The processes of globalization, industrialization and the fast IT and scientific development, for several decades, have been producing a new social, economic and political ambience, but also an international security surrounding which is becoming more and more complicated and insecure. On one hand, they have contributed to the connection of states and regions into a whole, but on the other hand,

[*] Intelligence expert, Republic of Macedonia
[*] Intelligence expert, Republic of Macedonia

they have incited the growth of migration processes, change of the demographic structure of states, disproportional economic development and strong polarization between the world population and the ethnic groups.

In such changed circumstances, the wish for economic prosperity, fast gaining wealth and providing a long term life existence in no time, have resulted in the appearance of economic criminal, change of the ideological matrix, inter-culturalism, corruption, urban criminal, murders and mass criminalization of the societies. At the same time, the tendencies for domination of the trans-national capital in the less developed countries have resulted in class division and separation between people and in marginalization of the week and poor ones. All this, eventually, generated a global economic crisis (incited by the most developed societies while mostly felt by the mid-developed and underdeveloped countries and regions)[1], but also political and war crisis and conflicts with ideological, ethnic and religious character in most regions in the world.

All these changes led to the strengthening of the existing, but also emerging of new, global threats[2], the identification of which has become more difficult and more complicated. With the evanescence of the two military – political blocks (so called "bipolar world"), the disintegration of certain states and the appearance of new ones, the traditional threats of war nature (so called "symmetric" threats) did no longer present the main preoccupation for the national security of the states, although they have not entirely disappeared. At the same time, the traditional threats of extremism, terrorism, organized crime, computer and ecological crime outgrew the local and national frames, growing into threats of international dimensions. The international terrorism, the trans-national organized crime, cyber crime, as well as the threats of epidemics, vulnerability in supplying the resources and the price shocks, ecological changes and so on, have more often been pointed out as a new type of the so called **"asymmetric" threats**, whose probability to happen is relatively low, but the possible harm of them would be immensely high[3].

In the scientific and expert public the adjective "asymmetric" is a subject of numerous debates nowadays, but broadly speaking, it could be said that the perpetrators of "asymmetric" attacks, as far more weaker and far less numerous, make use of the vulnerabilities and the weakest points of their opponents, with implicit supposition for including the surprise element, regarding the time of the attack, as well as the methods, means and targets. Actually, it could be said

that this is not the case of a classical war clash, but an activity that is directed towards draining the will of the stronger power, or more precisely, those are "threats that are conceived with the intent to achieve disproportional effect by use of a lot less strength against the vulnerabilities of a far stronger opponent in order to undermine the opponent's will to win[4].

Most of the authors think that, in short term or long term, the prospects of the countries to deal with "asymmetric" threats are not positive. Thomas Quiqqin[5] points out that this comes from the fact that, "regarding the nature of the "asymmetric" threats, those people who try to perpetrate them use the positive weaknesses which are multiplied because of several reasons: *fast technology changes* (e.g. the development of the computer technology means that technological crimes can affect more people in a shorter time); *international cooperation* (as opposed to the successful functioning of intelligence and law enforcement services in certain areas, the flow of intelligence data among institutions at national level, as well as among countries remains limited); *confusion between intelligence and law enforcement* (the competent services do not have equal roles in all the countries, as well as insufficiency of mutual functionality, in the sense of refusal of certain intelligence services to cooperate with the police and the legal bodies); *legal obstacles* (a legal "evidence" in one country might not be an evidence in another one); *sum of skills* (within criminal and terrorist organizations these might sometimes be more developed than within the bureaucracies of the authority. They usually engage highly educated and highly profiled individuals who work under pressure, as opposed to certain bureaucracies that often rotate their employees to different job positions, regardless of their skills, trainings and responsibility for the achieved)."

The "asymmetric" threats develop with great speed; they are easily adaptable and considerably unpredictable, thus presenting a challenge for the Intelligence Community[6] in new ways. Their timely anticipation and the proper reaction of security and intelligence services, inevitably imposes the need for high degree of their flexibility and adaptability to changes. Actually, national security institutions have to continuously be apt to structural and organizational changes that will be compatible with threats, which eventually implies the recreation of the intelligence cycle and the intelligence concept.

The Intelligence Community in Circumstances of New Security Surrounding

Nowadays, in a complex and unsafe international security surrounding, the country is vulnerable at several levels and in terms of a wide range of questions. Those are conditions in which the system threats (at the level of countries or big organizations), come down to an individual level or to a level of smaller groups. At the same time, it is estimated that the vulnerability of small and mid-developed countries is the greatest, although the danger for big and highly developed countries cannot be excluded thoroughly.

The appearance of new challenges and the strengthening of existing security challenges and threats put huge pressure on the Intelligence Communities to constantly define and update their targets and to find new means and methods for following these changes. The needs for reforms became inevitable especially after the events on 09/11, which brutally moved the tendencies of many intelligence services that regarded their security systems as being capable of dealing with the greater part of security threats. This imposed the need of aggressive reforms not only at the level of strategic thinking, but in the intelligence concept and the organizational set up of the lower levels as well. The adequacy of the reforms in the security section with the type of threats and the level of criminality in the society itself is the precondition for security institutions to do their function and to successfully confront the newly appeared forms of crime and other security challenges and threats. Following, are the basic characteristics of some of the current threats upon the national and global security:

- **Terrorism,** which "for a long time was used as a weapon of the weak ones against the strong ones, and was used by the anarchists, nationalists, anti-colonial, political and religious extremists,"[7] in the last two decades made fast development at world level and manifested change in the shapes of appearance (it is directed towards civil targets, and its goal is to cause a greater number of casualties, not only fear among the population). At the same time, "the IT and the world-wide Internet network enabled them to pass through space and time"[8]. With the ease of fast and easy communication it gradually grows into global terrorism, in terms of recruiting individuals, logistics, enabling transit through certain territories, financing paramilitary formations and so on. Actually, global terrorism cannot exist without direct participation and logistics (material and financial) of members from other countries and regions.

- The weakened state polity in certain countries let the **national-separatist and extremist movements** to grow and threaten the established values of the democratic societies, and in certain circumstances to destabilize countries and cause violence through violent criminal acts. New types of extremism have also been manifested – ethnic (national) and religious (so called "green" extremism) and they rapidly outreached the territorial barriers of countries themselves and grew into an international phenomenon.
- New social processes, globalization and transitional changes above all, contributed to the outreach of the local boundaries by organized crime organizations, thus reaching international dimensions and growing into **transnational organized crime**. Criminal networks involved in human, drug and weapon smuggling and illegal trafficking, due to the incomplete and aggravated function of state institutions (in countries with ethnic conflicts and crises and in so called "transiting societies") make use of the possibility for easier illegal movements through the territories, most often territories whose population is of the same or "close" ethnic background, as well as for gaining relatively greater profit. They have the ability to take advantage of the new technology, the weaker border controls, and the new growth of the financial markets, implementing itself into new social and financial flows. Contrary to older networks of organized crime, which were very often led by families, were strictly hierarchical by nature and relatively stable in their fields of interest, new transnational criminal structures show the tendency of greater fluidity, better network connection, functioning beyond greater number of international borders and so on. Many forms of organized crimes are often mutually connected – in direct or indirect cause and effect relation, while the illegally gained profit is often used for financing terrorist organizations. **Weapon trafficking** is an activity which is a direct, real threat for national security and the peace of certain countries in certain regions. Regarding the fact that it is motivated by getting financial, political and military gains, while it is in function of achieving certain goals of geopolitical and geostrategic interests, it enables the militarization of certain regions, the creation and support of aspirations for starting an ethnical conflict, activating new military hotspots or reactivating the old ones, as well as producing terrorism. **Illegal migration, human trafficking and drug trafficking** present an indirect

threat for national and international security which lately manifests new, complex, negative effects and receives organized dimensions. Primary effects are manifested as indirect destabilization of the country due to political and economic pressure, deranging the internal stability and function of the state institutions in the field of health, social care and economy. Secondary effects refer to the increase of the rate of overall criminality in the country, having in mind that very often migrants and people who are victims of human trafficking are included in direct perpetrating of some other types of crime (prostitution, thefts and so on) as well.

- **Computer crime**, as a newly appeared threat in the modern world, manifests consequences at the level of global security and economy, of the world in general, in the field of national security and at the individual level as well. Besides the possible threats to the industrial security and the financial system, to the huge governmental and security systems, this type of criminal affects to a great extent the privacy of citizens as well, through: sabotage, creating and sending so called "viruses and worms", propaganda of any kind through computer systems, illegal shapes of electronic piracy "hacker" realized as an illegal access into the computer system, illegal interception and data forging, up to actions related with children pornography, violation of author's rights and other related rights.
- **Ecological security**, understood not only as climate change and pollution, but also as criminal activities related to dumping radioactive wastes, the possibility to use biological, chemical and nuclear weapons for mass destruction, the exhaustion of natural resources, illegal trafficking of protected animal and floral types, operating of the forestry mafia and so on, is also related to the international, national and individual safety. These problems, especially the development of nuclear potentials and the spread of mass destruction weapons, concern all countries, and from that comes the necessity for solving them at an international level.

In the new security surrounding, the Intelligence Community must provide data for the possible intrastate clashes, but at the same time it needs to have the potential to deal with all untraditional types of threats, to provide timely informing and to be capable of preventive action and fast reaction. Its engagement should be directed towards following the trend of development of security

threats and challenges, timely recognition of the forms and methods of action, the possible dangers and proper setting/layout of the established intensity.

For that purpose, it is necessary to use all the available means and ways to access information, including data that are received by using the most up to date communication, signal, audio and visual means. However, most of high technology intelligence systems, which were compatible to state level threats from the period of the Cold War, function well only against threats of huge proportions. Nowadays, they cannot perceive or react against capabilities or intentions on an individual level, characteristically for the "asymmetric" threats. In such conditions, high technology systems themselves, might not offer advantages, but they can, to a great extent, present vulnerability. From that comes the conclusion that a proper approach towards handling of current threats is to put analysis first.

In addition, starting from an ideal intelligence cycle, in which the users of intelligence announce their requests (directing), the Intelligence Community tries to collect the necessary data (collection), data is processed (analysis) and is sent back to the person who gives the directions (distribution), collecting data in general is not a problem anymore, but the deficiency of capability for their processing. This imposes the need for a greater attention towards analyses, while lesser attention to the technology and the hierarchical organization.

From the abovementioned, as well as from the weaknesses of "asymmetric" threats blows, the need to redirect the attention from technology towards the so called "humanization" of the intelligence process, i. e. towards knowledge management imposes. That implies greater investments in knowledge, analysis above all, as opposed to investments in technology, infrastructure and various support systems where until now the greater part of resources more being invested[9]. In the circumstances of "IT revolution" and "asymmetric" threats, **knowledge** (in the sense of understanding the threat and the ability to prevent it before it is realized), **experience and organization**, enable great advantages over the bearers of threats and probably are the sole functional weapons in the fight against them.

Intelligence Analyses: Condition, Trends and Perspectives

When it comes to intelligence, there are numerous definitions of this term in literature, part of which are too narrow, part of them emphasizing only certain elements or interests from only one point

of view, and others are very arguable in terms of their scientific sustainability. So, for the term "**intelligence**" there are definitions like "secret activity"[10], "espionage", "technical activity where photographing and communicational satellites collect inaccessible information" and so on. Still, regarding the new security surrounding, we would point out the notions that incorporate analysis as an important link in intelligence, as a "processed information", as well as "knowledge and analyses conceived to help the action"[11]. According to Sherman Kent, "intelligence has three main attributes and these are: shape of knowledge, shape of organization and shape of activity"[12], while Roy Godson emphasizes four important elements of intelligence: collection, counterintelligence, analysis and secret action[13].

Although intelligence analysis includes several levels of combining and processing, i.e. analysis and evaluation of the accessible data and information (which can be from one, several or all sources), in certain scientific circles, intelligence is equaled to **strategic intelligence assessment.** If this assessment is understood as a "final intelligence product of all the sources of knowledge which can be acted upon, in order to foretell and reduce the uncertainty in the following or protection of the own international political, economic and security interests", in complex international circumstances, knowledge is of crucial importance. So, if the term **"strategic"** is understood as "important issue that is of interest of the national authority," and these can be issues of historical, current or future interest, knowing the resources, terrain, demography and capability for information technology imposes the need of multidiscipline approach and widely based expertise in great number of areas (politics, law, economy, military stuff, international relations, psychology, sociology, statistics and so on). At the same time, **assessment** as a final step in the analytical process which includes all the sources of intelligence data (open/public and secret), information and knowledge, which is processed to the creators of the politicies from the highest level and is usually followed by an action or implications for policies, the role of the strategic intelligence assessment is to provide **knowledge** which can be acted upon or an anticipated caution to the decision makers. Aside to that, the knowledge which should foresee the risk through an insight into priory complicated situations is of crucial importance.

In the context of new security challenges and threats, intelligence analysis of all levels has a constant need for adaptation to the ongoing flows in the contemporary societies. Thus, it is necessary to **redefine the greater part of their strategies, tactics, skills and methods** that are used in everyday work. That need is of high importance, starting from the fact that intelligence analysis provides information that are of crucial importance not only to creators of the governmental policy and other official users, but to other (operational) sections in intelligence and security services as well. Generally speaking, changes should proceed in the following directions:

- The first important segment into which continuous changes compatible to the new trends of security challenges and threats should be conveyed is the **human potential.** This imperative includes constant revision and improvement of the work in all phases:
  - recruitment, selection, training and motivating the analysts;
  - usage and development of the most suitable analytical methods;
  - organization of the analysts' work (as individuals or as a team);
  - communication with users of their information.

If the basic job of analysts is to connect all data and information that they have, to integrate them and in that way to find the current trends, every analyst should have talents that include: to judge logically, to be open-minded and skeptical at the same time, to be persistent, cautious, precise in the work, creative and innovative, to possess "intellectual honor" – to admit when wrong, to have sufficient time and maybe what is most important to have a solid knowledge of the field that the analyst works in – prior knowledge. These qualities are not only basic criteria for recruitment and selection of the future analysts, but they are the base for every training and methods that are used for motivating the existing analysts as well. Training should also include continuous updates regarding the new "asymmetric" threats, while the analyst should be generative by nature being capable of recognizing a wide range of questions.

If we look at the analysis i.e. the levels of processing (of the available data, starting from information and knowledge up to assessment)[14], basic principles that should be followed are distinction, examination and confirmation, with which, in all the phases knowledge is the key point i.e. knowing the conditions, characteristics of the "asymmetric" attackers, the development trends

and their directions etc. Thus, in the continuum from data to assessment, weaknesses would be avoided i.e. the part "from knowledge to assessment" which is the weakest, as opposed to the part "from data to information" which is the strongest.

In order to find answers to the numerous questions about the capacities of current and future security challenges, the analyst should possess specific knowledge and skills and should have a wide spectrum of methods, techniques and tools, among which adequate analysis software as well. Starting from the imperative for upgrading, improving, equipping and use of means and methods which will result in job success, the knowledge of the analysts should incorporate the latest scientific research too, as well as the use of advanced scientific, computer and technology achievements. At the same time, the process of evaluation of intelligence data should strive towards use of principles, recorded standards and comprehension of exact and social sciences about analytical methods. In that way, the time for processing the extremely huge number of intelligence data would be shortened and the exactness of analytical conclusions, assessments and estimations made would be increased. The use of scientific methods and procedures for interpreting data and information, on the other hand, enables making/conveying clear conclusions and useful recommendations to the final users/decision makers.

Regarding the organization of the work, analysts go through the process of "processing" a huge number of data on everyday bases and they convey information and assessments to final users, working individually or as a team. Irrespectively of the type of threats, team work is an especially important segment within the lower levels of analysis, the so called "tactical" analysis, delivering requests as final products to the operative/terrain workers. The importance of such type of organization of the work comes to the fore in the new "asymmetric" threats, which spreads over the so called "strategic" analysis too. In the newly emerged surrounding, the making of strategic intelligence assessments imposes the need for everyday or occasional team work, depending on the urgency of the request or the nature of the threat. Of course, team work offers numerous advantages and represents an imperative in the analytical work.

When we consider the relation between the analyst and the final users (operatives or decision makers), a question that imposes

and that affects the objectivity of the analysis is: "Does the analyst have to be at a distance or in a constant communication with the users?" On one hand, the close contact presents a danger of analysts being biased or politicized (an impact which might be mutual, so that analysts might inform about something that users already know or something that they want to hear), while on the other hand, there is a possibility that analytical products might not be of use for beneficiaries, because they do not know their interest. It is common that possible weaknesses are avoided by the use of a "control mechanism", the so called "departmental devil's advocate" – experienced independent analyst or analytical team that appreciates the objectivity of the analysts. Despite some weaknesses and limits, related to the so called "secondary subjectivity", it is estimated that in circumstances of complex security surrounding and fast changes of threats, the permanent communication between the analysts and the final users has indeed its advantages for national security.

- When building decisions, estimations and assessments, the analyst must take into consideration the strength of the arguments, as well as the degree of compliance of the intelligence gathered from different sources (Humint, Osint, Imint, Sigint etc.), and which confirm the conclusion ("the more the sources, the stronger the conclusion"). In this way, the so called "intelligence deceits" or disinformation are avoided, which are most often received through technique (audio, video and satellite surveillance) and which sometimes might be delivered on purpose. One of the biggest advantages in the detection and confrontation of "asymmetric" threats nowadays is **Open Source Intelligence (OSINT)**, which uses information that is accessible to the public. Although OSINT is most often related to the Internet and the World Wide Web (www), the OSINT sources are various and include: big commercial data bases (Lexis, Nexis and Dialog which offer considerable advantages over smaller data bases on www), books, newspapers, scientific and academic magazines, phone books, TV and radio shows, governmental data bases, census reports, maps, lists of municipalities, high resolution photographs, business reports, budget reports etc, and they are received through professional and business contacts with physical and juristic persons from other countries, diplomatic- consulate agencies, military and civilian missions,

commercial offices, non-governmental organizations, scientific institutions etc. At the same time, it is important to emphasize that OSINT does not only consist of open source information, but it presents a specific analytical process which integrates the human expertise and open source information, and which results in intelligence that is relevant for the final users. Some theoreticians believe that OSINT can fulfill all the intelligence gaps, right away and for a very low price. From this come the assessments that, only by careful and complete analyses of these sources, 95% of the information that are relevant for intelligence can be found in open sources. Also, it is considered that a good analysis of the data received through OSINT might give about 80% precise image of the phenomenon or the subject of the analysis.

Thomas Quiqqin[15] points out several characteristics of the OSINT, part of which offer *advantages* in the timely detection and prevention from "asymmetric" threats, and that is: cutting intelligence costs, outgrowing time and territorial barriers and getting a complete picture of the subject of interest. This comes out from the fact that today even the financially strong intelligence communities, cannot cover all the countries in the world with technical equipment and human potential, nor can they successfully monitor every potential subject of interest. What goes in their favour is the already drawn information needed and expertise from the private sector, which from the 1990s onwards has already invested in the technology suitable for business interests. Also, contrary to the so far close specialization in a specific subject of interest, at present, the best analysts are those who create links among already accessible expertise and decision makers. Starting from the fact that with the increase of the "asymmetric" threats, the greater the probability that the subject of interest will happen in those territories or geographical areas that are not "covered" with reliable sources or that are time limited. So, having an established OSINT capability to find and convey information from expert sources in as shorter time as possible (which sometimes are measured in hours), sometimes is of an essential importance. In this context are the *conclusions* that secret intelligence reports offer unconnected facts and pieces of information (often from electronic recordings), and not a complete picture or information review that is necessary to the final users. Although this

information by itself is valuable and sometimes of crucial importance too, due to improper training of analysts, it might not be included in the analytical product. From this comes the need that the overall picture is built by including information from OSINT.

Although it is believed that OSINT is less authentic, actually, as in every other type of information there are methods for confirming the *authenticity of the sources and the facts* received in this way. So, the source is estimated by evaluating the way that the individual provided the information and evaluating the organization/firm he works for (in cases of clash, the lower grade is taken). Regarding the facts and their authenticity, what matters is that their consistency and logic is asserted, in order to comprehend their accordance or overlapping with what is already known. The possible inconsistency in the reporting should be assessed whether it is a result of the changed situation or it is a case of bad reporting.

- Starting from the fact that the "asymmetric" threats nowadays develop very rapidly, while the timely manner and the correctness are the basic suppositions in the intelligence cycle, the transmission of information "from where they are to where they are needed and this to be done in timely manner", imposes the need of thorough reforms in the process of **exchange and distribution of intelligence and analytical materials** as well. The institutions from the security section should have potentials to cope with all types of current threats, to provide timely reporting, to be capable of preventive actions and to react fast. Basic measures and activities for their confrontation and prevention of the phenomena that affect the security situation are cooperation, coordinated engagement and exchange of information between state institutions responsible for national security.

Still, the security threats and challenges are complex phenomena, which almost inevitably spread beyond national borders as well, and which create problems that can be solved only with the help of internationally coordinated policies. The process of constant changes of the security threats in world frames asks for the security structures to excel their local needs and start functioning globally. Realizing the international dimension of security challenges and threats of "asymmetric" kind, crucial is the need to build a completely integrated national and international approach, which will be based upon

cooperation with other countries, international organizations and institutions, through timely exchange of relevant data, information and strategic assessments, as well as through realization of joint actions. From this, the possibility to prevent the current and future security threats is possible only with one global access, besides the continuous development of the forms and methods for their confrontation.

Conclusions

Analyzing the present complex international surrounding, numerous indicators point out that non-state factors, small groups, and even individuals have the power and capability to cause great changes in the security and political surrounding at an international level, and in the future they could take over strategic role and affect the policy of the country. The probability that these trends in the future would intensify is huge.

To answer the current and future challenges it is necessary to: strengthen the positions of analysis, as opposed to intelligence data collection; the intelligence analysts should base their work upon knowledge, and it is essential to develop global views, with a multidisciplinary access to many questions; quick and relevant flow of information, which will support the analysis adequately, which implies intelligence from reliable and highly technological sources, but at the same time an increase use of open sources for intelligence goals; as well as a voluntary sharing of information beyond institutional and national borders. Such directions, at the same time, ask for elimination of the so far detected weaknesses in the intelligence units' work and especially in the work of intelligence analysts, and that is: close disciplinary realization of the problems, not recognizing the weak signals/warning information that were not properly assessed, too many bureaucratic procedures as opposed to the time needed to be paid to analysis and assessment of information, untimely distribution/hold of needed information in the frames of the intelligence service, keeping/not sharing the information on a national and international level with the excuse of "secrecy" of data, improper reaction by final users/decision makers, in the sense of unsuccessful policies and/or politicization of the intelligence process in order to serve already made/brought political decisions.

It is assessed that the role of intelligence to protect the national security will become broader and more difficult in future. Thus, for an effective approach towards intelligence/intelligence analysis it is necessary to build global view points, making multiple scenarios and establishing collective frames for handling the new security challenges and "asymmetric" threats. At the same time, changes will have to be made constantly and services will have to reach outside their own organizations in order to gain the knowledge necessary to handle future challenges. Additionally, essential suppositions for reaching the goal of the intelligence – security function are the combining of information from different sources and their processing i.e. conveying the "relevant information to the relevant people in right time".

References

[1] See http://www.peaceoperations.org, accessed on 14.08.2012.

[2] **"Threat"** - a possibility for an individual or a group to perform an activity that takes advantage of certain vulnerability. With that, the key word is *possibility*, which does not automatically imply the existing level of danger. Threat is a term that defers from **"risk"** understood as "probability of harmful consequences that come from an act (action or reaction) undertaken by a certain source in order to take advantage of a certain vulnerability." In this sense, common is the definition that "the risk is equal to the seriousness of the consequences multiplied by the probability of such event taking place." From this, the proper estimation of the risk implies a direction of action or reaction that can be undertaken as an answer to them. Related to the threats and risks is the question of *vulnerability*, in the sense of human, technical and/or natural weaknesses, while in the decision making, for the creators of the politics, it is necessary to connect the vulnerability and the real consequences of the action; See http://www.disastercenter.com/terror/0_risk.htm and Thomas Quiqqin, *Seeing the Invisible, National Security Intelligence in an Uncertain Age*" (Skopje: Magor, 2009), p. 26.

[3] Above all, on a socio-political and economically-material plan, but also with potentials to cause mass collateral, as uniquely characteristic for the transnational terrorism and the epidemics.

[4] Kenet McKenzy Jr., "*The appearance of asymmetric threats*", available at http://www.ndu.edu/inss/press/QDR_2001/sdcasch03.html, accessed on 14.08.2012.

[5] Thomas Quiqqin, *Seeing the Invisible*, pp. 18-19.

[6] This term will be used as a synonym for *National Security Institutions*, i.e. *Security and Intelligence Services*, that is to say *Institutions from the Security Section*.

[7] J. Baylis, J. Wirtz, C. Gray, E. Cohen, *Strategy in the Contemporary World (*Skopje: NAMPRES, 2009), p. 194.

[8] *Ibid*., p. 186.
[9] In some countries it reaches up to 99% of the budget expenditure; Thomas Quiqqin, *Seeing the Invisible*, p 106.
[10] James Der Derian, "Anti-diplomacy, intelligence theory and monitoring practice", *Intelligence and National Security*, Vol. 8, No 3, July 1993, p. 31.
[11] Robert Baui, quoted in Ernest May, *Knowing One's Enemies* (Princeton, New Jersey: Princeton University Press, 1986).
[12] Sherman Kent, *Strategic Intelligence for American World Policy* (Princeton, New Jersey: Princeton University Press, 1949), p. 7.
[13] Roy Godson, *Intelligence Requests for the Eighties: Intelligence Elements* (Washington, DC: National Strategy Information Centre, 1979), pp. 6-9.
[14] **Data –** the lowest form of collection that has not been processed, which is useless for the user without basic level of processing and analysis; **information –** what is received after the primary level of processing; information by itself is not sufficient and the analyst needs further sources of information in order to make judgments; **knowledge –** next level of analysis that enables bringing preliminary judgments, for which further sources of information are needed (prior analyses of photographs, diplomatic reports, signal intelligence, open source reports). By adding new information in the context of the previous ones, the result is knowledge; **assessment –** its goal is to provide the decision makers with knowledge which can be acted upon and which should decrease the surprise and the risk with an insight into complex situations. The strategic intelligence assessment in a huge extent consists of "*what we know and how we know it*", as well as of "*how we change the opinion about what we think we know?*"; Thomas Quiqqin, *Seeing the Invisible*, pp. 50-52.
[15] *Ibid*., pp. 160-171.

Challenges in the Science of Intelligence Analysis

Daniela-Elena MITU[*]

Abstract

If intelligence is knowledge for prevention and countering of threats, analysis is the core instrument to get access to knowledge, enabling us to correlate a series of currently known facts with the less known, imaginary ones.

Science is among the instruments which allow us to get access to knowledge. Unlike other methods (opinions, thinking patterns, rationalism, and empiricism), science is based both on rationalism and empiricism, having, among other things, the ability to identify errors and correct them, which is exactly what analysis should do in order to avoid intelligence failure.

Beside the brief presentation of the main topics of the debates centred upon the intelligence analysis, perceived as a tradecraft or a science, the present paper intends to measure science in intelligence analysis. Therefore, it will highlight the main challenges of the scientific dimension of analysis, residing in the use of structural analysis techniques, statistical data and probabilities as well as in verifying hypotheses and the correct use of arguments, providing at the same time solutions to overcome the above-mentioned difficulties.

Intelligence Analysis – Tradecraft and Science

The science of intelligence analysis has not been much debated in the speciality literature, most of the references covering the respective issue through analogies with scientific methods, considered to be the main pillar of the analytic process.

Theoreticians have focused on the scientific approach of the intelligence analysis since its early conceptualisation, namely in the papers elaborated by its founding fathers, such as George Pettee, Sherman Kent and Washington Platt, in the '40^{s} and '50^{s}.

In the past 20 years, the American intelligence school, comprising Robert Gates, Douglas MacEachin, Jack Davis, Rob Johnston, Robert Folker, Richards Heuer, and many others, has brought its substantial contribution to the development of intelligence analysis, having a great influence on the so-called *analytic tradecraft*, a concept frequently used in the intelligence culture and literature, to the detriment of the science of intelligence analysis.

In general, the basic tradecraft assumption is that analysis is a process which helps us identify the variables or drivers and generate hypotheses. Although emphasis has been placed recently on the

[*] PhD Candidate, "Mihai Viteazul" National Intelligence Academy

development of structural analysis techniques and methods, which support the analytic reasoning, most intelligence theoreticians and practitioners would rather consider intelligence analysis as tradecraft and science, as reflected in the debate on: *analysis – science or tradecraft?*

Some experts, such as Rob Johnston, adopt a clear stance, claiming that the concept of *analytic tradecraft* cannot be applied, since analysis is a part of a scientific process. According to the author, tradecraft purposefully implies a mysterious process learned only by the initiated and acquired only through the elaborate rituals of professional indoctrination. In an oral tradition, individual tradecraft methods are passed on by means of apprenticeship. The consequence for any culture tied to an oral tradition is the loss of important knowledge that occurs with the loss of practitioners.

In organizations, the retirement of experts and innovators leads to the loss of that expertise and innovation, unless there is some formal written and educational system to keep that knowledge alive. Thus, the process of reaching a specific conclusion is explicit and replicable[1].

Knowledge Is the Stake

According to Sun Tzu, in his paper The Art of War, *"if you know the enemy and you know yourself, you need not fear the result of a hundred battles"*.

The scientific approach of intelligence analysis is centered on the role of the process and its outcome in adding value, known as added-value in the intelligence literature. That must be the goal and motivation of any analytical process, especially in the field of intelligence.

According to James B. Bruce[2], the authority, habit of thought, rationalism, empiricism and science are major sources of knowledge, the last enabling us to avoid mistakes.

Acquiring knowledge through authority implies a reliable source, such as a person (HUMINT/*Human Intelligence*) or mass media (OSINT/*Open Source Intelligence*), and so on. The habit of thought refers to styles of practice, thought and action that constitute typical approaches of a community, without knowing the source of information.

One can obtain knowledge through rationalism, applying various systems of thought to process data, such as induction, deduction, and abduction.

Finally, empiricism is knowledge through senses. According to Bacon, Locke, Hume and Galileo, empiricism is based on observation, experience and experimentation.

The fifth source of knowledge, *science*, resorts both to rationalism and empiricism, enabling us to identify and avoid errors. Among other things, its reliability resides in:

- use of hypotheses – after forming hypotheses, they are checked for validity by using standard samples to see if predictions come true;
- objective methods – employ of rigorous procedures to ensure that data are collected and analyzed in the most objective manner;
- transparency – visibility of methods helps to ensure integrity and replicability of the study;
- replicability – all scientific investigations must be reproducible by other researchers, for example in the case of intelligence analysis, the hypothesis is not true if other intelligence analysts do not draw the same conclusion;
- peer review – the results do not attain the status of knowledge until they are consistent with the used methods;
- provisional results – the results are always subject to modification as procedures are refined, when new information emerge.

The Traditional Debate

If intelligence is knowledge for prevention, and analysis is the core of this process, it should enable us to correlate a series of currently known facts with the less known, imaginary ones. To that end, some experts say that one must have creative imagination and intuition to deal with problems, while others support the employ of rigorous methods.

The intuition *versus* structured analytical approach is heavily debated in the intelligence culture, ever since its beginning. Is the intelligence analysis an art based on the practitioner's intuition or is it a science, employing structured methods and techniques? That is the question that is at the core of the controversy I mentioned[3].

In the equation *analysis to be an art*, the main approach is inductive, based on creativity, pattern identification, instinct, training and experience. Its supporters claim that, "*because in many cases the variables are so complex, countless and incomplete, attempting to analyze them using scientific methods is pseudo-science*"[4]. Moreover,

any attempt to make predictions based on such variables is futile. Science could bring minimal improvements. The real improvement of its quality would come from the analyst's increasing intuitive skills and knowledge in the field, by staying connected.

According to those who claim that analysis is an art, using rigorous methods to analyze issues would make the analyst ignore the factors that cannot be measured. In their opinion, the intuitive approach and imagination would lead to the best results.

However, the practitioners that support structured analysis claim that it could lead to rigorous assessments, having also high predictive accuracy[5]. Arguing that *analysis is science,* they claim that, although it is impossible to take into account all variables, science helps us identify the most important ones. Thus, starting from known facts and reasonable assumptions, they have developed a more realistic approach, improving at the same time its transparency.

Die goldene Mitte

The disputes between the supporters of the two different approaches could be settled through mutual consensus, as most experts believe. The settlement of problems which sometimes lack logical consistency could be based on intuition. However, it must be backed by rigorous analysis.

Jan P. Herring supports such an analytical approach, claiming that successful intelligence analysis reflect "*a Holistic approach with a balance between art and science*". Paul Lehner also believes that intuition, experience and expertise are not enough, and that objective tests need to be considered[6].

We think that combining the two dimensions is visible in scenario development for performance predictions. To generate scenarios and forecasts, the analyst resorts to intuition and imagination as well as to scientific methods.

Although unexplained, the respective feature of intelligence analysis was highlighted for the first time in 1957. Referring to the role of social science in intelligence analysis, Washington Platt mentioned that social science did not focus on predictions but rather on facts, or, in his opinion, on "*identifying the critical factors which will bear on the working out of the situation under given circumstances*", namely on "*drawing dependable cause-consequence relationships*" in order to understand the issue better[7].

The creative role played by imagination in intelligence analysis and in the process of implementing scientific methods was

emphasized 30 years later by Isaac Ben – Israel, in 1989, and recently by David Moore and Liza Krizan, in 2003. For them, imagination plays a vital role in hypotheses generation, through abduction.

It is therefore useless to emphasize that the two dimensions are fundamental for any structured method of generating scenarios, such as pattern analysis, two axes analysis or branch analysis.

Analysis and Scientific Methods – Common Elements and Limits

Intelligence analysis is thought to be a collection of tailored and qualitative scientific methods, placing the emphasis on applied social sciences research.

The intelligence analysis uses induction, deduction and abduction, in a complementary manner, in order to check the evidence, generate and test hypotheses.

Deduction and induction are classical forms of reasoning, used in many philosophy departments and mathematical logic, while abduction is a pragmatic form of reasoning, introduced by mathematician Charles S. Peirce. In general, induction generates hypotheses and new research directions (*data - driven analysis*), while deduction is used to check evidence (*conceptually driven analysis*), and abduction helps us generate multiple hypotheses, based on existing evidence. Thus, induction shows probabilities, deduction – possibilities, and abduction – the likelihood of hypotheses.

The intelligence analysis uses the scientific method structure, as follows:

- observing and describing phenomena based on data obtained from multiple sources, and not on experiments, as in social sciences research;
- generating hypotheses to explain phenomena – identifying the main factors of incertitude or key drivers that might have a strong impact;

There are various sources for generating hypotheses, starting from reasoning techniques such as *brainstorming* or comparison, challenging other hypotheses, to the above mentioned logical judgements.

- checking hypotheses to see if they are valid or not, taking into account any clues or signals that might question premises, stressing at the same time the dramatic events that might influence the foreseen developments included in conclusions.

This process is extremely important because it makes the difference between scientific and non-scientific methods, since it helps us decide whether the assumptions are valid and credible.

The fact that analysts should challenge hypotheses is a truism, as *"experience tells us that when analytical judgments turn out to be wrong, it usually was not because the information was wrong. It was because an analyst made one or more faulty assumptions that went unchallenged"*[8].

Regarding the quantitative data, it is relevant to check hypotheses using statistical methods, but such instances are rare in intelligence analysis, where the qualitative dimension prevails. Up to now, social sciences have developed certain techniques to check qualitative hypotheses, such as the *Analysis of Competing Hypothesis*, or those based on counterarguments, for example the *Red Team*, *Team A - Team B* and *Devil's Advocacy*.

Last but not least, intelligence analysis and scientific methods are based on five main discursive pillars, namely explanation, description, presentation, prediction and argumentation, the last having functions as a suprastructure, because analysis in general, and intelligence analysis in particular, have an intrinsic argumentative dimension.

Structured Analysis - Advantages

Structured techniques are probably the best way to reveal the similarities between intelligence analysis and science, from the point of view of the processes applied.

Structured or alternative analysis resorts to *"instruments created in order to help analysts and decision makers to undergo a thorough self-examination, question their judgement and explore alternative scenarios"*[9]. Therefore, structured techniques encourage critical thinking, being created in order to counter cognitive biases.

As a member of CIA's *Board of National Estimates* founded in 1949, Sherman Kent spent most of his career trying to elaborate rigorous academic methods for intelligence practitioners, arguing that intelligence analysis is a social science methodology. According to the well-known expert, applying scientific methods helps us develop adequate conclusions and avoid errors. Collecting evidence, generating hypotheses, applying critical thinking are part of the intelligence analyst's mission, which cannot be accomplished without a set of adequate analytic tools[10].

Eventually, intelligence experts acknowledged the need to distinguish between known facts and ways to obtain knowledge, on the one hand, and analytic judgments and the manner in which they draw conclusions, on the other hand.

Almost 50 years after Sherman Kent's contribution to the development of intelligence, at the CIA level, namely the *Directorate of Intelligence*, a significant progress was recorded in the field of structured analysis through the *Tradecraft 2000* project, in 1995. Subsequently, well-known intelligence experts brought their contributions to the development of the respective type of analysis. *Tradecraft 2000* laid the basis of structured analysis, establishing a set of criteria or best practices, known as *linchpin analysis,* which explains the steps to be followed by analysts in their quest.

A series of techniques appeared, their number ranging between 50 and 200, including *mind mapping, process activity mapping, link analysis, environmental scanning, brainstorming, Delphi technique, key assumptions check, adversarial collaboration, "What If?" analysis, cone of plausibility*.

Being extremely useful at the operational, tactical and strategic levels, the structured techniques provide a two-fold dimension to analysis, namely prognosis and diagnosis, helping practitioners understand and describe the background and imagine future developments as well as to reveal clues.

Structured analysis has the following advantages:

- takes into account alternative hypotheses and identifies potential developments;
- offers the possibility to review stages and correct errors, the analytic process becoming thus transparent and verifiable;
- reduces the risk of cognitive errors by challenging judgements;
- provides the beneficiary the opportunity to better understand the product delivered and establishes guidelines meant to prevent and counter risks and threats;
- offers a deep understanding of certain issues, through methodical study;
- increases the analytic process credibility, through rigorous and almost scientific methods.

Challenges

The use of structured techniques depends on internal drivers, such as the knowledge possessed and the analyst's efforts to improve his or hers abilities as well as on external drivers, most of them of an organizational nature.

A major challenge resides in the fact that one should permanently conduct structured analysis. Therefore, the main limitations are the lack of time, the distribution of tasks, and the planification of requests, along with logistic and financial issues.

This means more time and efforts, whileas the analytic product must be disseminated to beneficiaries as soon as possible. Till this point, however, the analyst needs times to learn and apply the respective techniques correctly. The former intelligence practitioner and manager Arthur Hulnick claims that structured techniques "*are unpopular with analysts because they have no time to absorb these ... in the face of tight deadlines*"[11], most experts preferring to resort to intuition.

In addition, if the analyst elaborates more products on different issues, his or hers judgement ability could be affected as far as the selection of the right method is concerned. The inadequate distribution of requests or tasks by managers may also lead to the implementation of unsuitable analytic techniques.

Most intelligence practitioners refrain themselves from using structured analysis because of the responsibility attached, since mistakes can more easily be explained if the process is non-transparent.

Moreover, this type of analysis is more difficult to conduct because of the lack of adequate IT applications which could facilitate the implementation of useful instruments as well as of the difficulty to co-opt multi task teams, which would imply the strict observance of confidentiality as well as other with logistic and financial issues.

Finally, the use of structured analysis is limited mostly due to the high number of variables[12]. The implementation of quantitative methods, probabilities and statistical instruments is also limited. Therefore, as I have mentioned in the beginning of this chapter, intelligence analysis is rather a tailored, qualitative technique than a scientific method. However, studies on intelligence analysis clearly reveal that intuitive techniques are mostly employed, along with *a priori* probabilities, which need no scientific support, being subjective.

Beyond those limitations and challenges, the implementation of scientific methods is a paradox, which, in time, has led analysts to refrain from using structured techniques.

However, resorting to scientific methods is not enough to provide the analytic process a scientific dimension, since there is no evidence that

structured techniques could help us improve the quality of analytic products. Unfortunately, no studies have been elaborated yet to prove the efficiency of various analytic methods. Therefore, the analytic community is somehow skeptical about the scientific value of many methods and techniques, which is "*claimed rather than demonstrated*"[13].

Conclusions

Although none of the structured analysis techniques offer guarantees that strategic surprises can be avoided, they help us eliminate errors and reduce the risk of cognitive biases.

Structured analysis has many advantages that should not be neglected by practitioners, including the opportunity to connect elements that appear to be independent, identify information lacks and diagnose hypotheses.

From the analyst's point of view, it could be a good opportunity to apply critical thinking. For the intelligence organization, it could be one of the potential methods to anticipate risks and threats, while decision-makers could benefit from comprehensive, insightful, add-value products, which could help them adopt the best decisions.

An institutional framework offering analysts the opportunity to understand the real value of structured techniques and train adequately is needed in order to prove the efficiency of such methods. Thus, the decision-makers could benefit from add-value products. As a result, intelligence analysis can prove its scientific dimension and enhance knowledge.

Eventually, *our perception over intelligence analysis is vital, since it could be considered a scientific method, a tradecraft or a profession.*

The changes that occurred at the level of the intelligence organizations in the past 10 years facilitate the professionalization of intelligence analysis. However, research in the field shows that singular efforts (such as those carried out by the USA, Great Britain, France, Sweden) are not enough, and that a comprehensive approach and a general analytic program aimed at developing an educational system, establishing a doctrine or a theory of analysis as well as of clear standards of efficiency and ethical codes are needed.

References

[1] Rob Johnston, *Analytic Culture in the US Intelligence Community. An Ethnographic Study* (Washington, DC: Center for the Study of Intelligence, 2005), pp. 17 – 21.
[2] James B. Bruce, "Making Analysis More Reliable: Why Epistemology Matters to Intelligence", in Roger Z. George and James B. Bruce (eds.), *Analyzing Intelligence. Origins, Obstacles, and Innovations* (Washington, DC: Georgetown University Press, 2008), pp. 172 – 178.
[3] Stephen Marrin, "Intelligence Analysis: Structured Methods or Intuiton?", *Intelligence Journal*, Summer of 2007, p. 8.
[4] Robert D. Folker Jr., *Intelligence Analysis in Theatre Joint Intelligence Centers: An Experiment in Applying Structured Methods. Occasional Paper*, no. 7 (Washington DC: Center for Strategic Intelligence Research, Joint Military Intelligence College, 2005), p. 8. Available at http://www.fas.org/irp/eprint/folker.pdf.
[5] *Ibid.*, p. 1.
[6] Jan P. Herring, "Measuring Success in Intelligence Analysis", in Russell G. Swenson (ed.), *Bringing Intelligence About, Practitioners Reflect on Best Practices* (Washington, DC: Center for Strategic Intelligence Research, Joint Military Intelligence College, 2003), p. 100; Paul Lehner, *Summary Record of the GFF Community of Interest on the Practice and Organization of Intelligence Ottawa Roundtable. What Can the Cognitive and Behavioural Sciences Contribute to Intelligence Analysis? Towards a Collaborative Agenda for the Future*, 2010, pp. 6 – 7.
[7] Washington Platt, *Strategic Intelligence Production: Basic Principles* (Westport, CT: Praeger, 1957), p. 137.
[8] Richards J. Heuer Jr., *Psychology of Intelligence Analysis* (Washington, DC: Center for the Study of Intelligence, 1999), p. 69. Available at https://www.cia.gov/library/center-for-the-study-of-intelligence/csi publications/books-and-monographs/psychology-of-intelligence analysis/PsychofIntelNew.pdf.
[9] Warren Fishbein, "Making Sense of Transnational Threats", in *The Sherman Kent Center for Intelligence Analysis Occasional Papers*, Vol. 3, No. 1, 2004. Available at https://www.cia.gov/cia/publications/Kent_Papers/vol3no1.htm.
[10] Roger Z. George, "Fixing the Problem of Analytical Mind-Sets: Alternative Analysis", *International Journal of Intelligence and CounterIntelligence*, No. 17, 2004, pp. 387 - 388.
[11] Arhur S. Hulnick, *Fixing the Spy Machine: Preparing American Intelligence for the Twenty-First Century* (Westport, CT: Praeger, 1999), p. 53.
[12] Stephen Marrin, *Improving Intelligence Analysis. Bridging the Gap between Scholarship and Practice* (London, New York: Routledge, 2011), p. 40.
[13] Stephen Marrin, "Intelligence Analysis: Structured Methods or Intuiton?", *Intelligence Journal*, Summer of 2007, p. 10.

The Meaning of "Irrational" in the Intelligence Analysis

Dumitrina Iulia GALANTONU*

Abstract

The beneficiary of intelligence products wants most of all to avoid surprise. What is the most common source of surprise? Human mind and its unique and often incomprehensible settings. We are so much used to be confident in "homo sapiens" capabilities, so we cannot accept the „irrational" in the information processing. The term is usually used pejoratively, but I certainly do not refer to mental deviations. Irrational is not something opposed to rational, it is something that cannot be understood using the classical logic. Processes as emotion, belief, perception, contradiction and even coincidence could be included in the idea of irrationality. This paper will focus especially on the idea of contradiction as a form of irrational. In this regard, demonstration will be based on Ştefan Lupaşcu's principle of dynamic contradiction and Basarab Nicolescu's transdisciplinary research. The final purpose of this study is to underline that intelligence analysis should consider much more what is beyond traditional logic. In the intelligence process, the „irrational" might indicate vulnerabilities, which represent a huge source of surprise.

Motto:

"The one who is the master of contradiction (...) is also the master of the world".

(Ştefan Lupaşcu, *The three matters*)

Introduction

Sun Tzu notices in *The Art of War* that if you know the enemy and know yourself, you don't need to fear a hundred battles. If you know yourself, but not the enemy, for every victory you will suffer a defeat. If you know neither yourself nor the enemy, you are a fool and will face defeat in every battle.

To know yourself and the enemy, but especially knowing yourself interacting with the enemy, a big amount of experience and knowledge is required. That knowledge comes from studying people's psychic, with both parts: consciousness and unconsciousness, rational and irrational.

* PhD Candidate, "Mihai Viteazul" National Intelligence Academy

What makes the difference between ordinary information and intelligence analysis is foreknowledge. In a time when information is almost entirely available for us, as well as for our competitors, what makes the difference? A holistic picture of a situation, that assumes taking into account the irrational part of people's way of thinking.

This is the working hypothesis: the irrational, which means what is beyond traditional logic, must be considered as a part of knowledge integrality. Intelligence analysis as a cognitive approach must also pay attention to the irrational part of an issue. As long as, usually, accepting something as rational means accepting it as making sense, it is understandable why many events are easily considered irrational, even if sometimes it is just the human limit of understanding new things.

Understanding how the human mind works requires studying the consciousness. Unfortunately, any discussion about consciousness has not a clear experimental base. Gerd Sommerhoff writes in *Understanding Consciousness* that you cannot find out how a TV set works by watching the pictures on the screen and at the same time measuring the voltages and the temperatures in different locations of the device:"At some point you have to jump to inspired hypotheses about the functional architecture of the set, about the modular functions being performed on the incoming signals to produce the observed pictures"[1]. It is the same situation with intelligence analysis: sometimes it is necessary to go beyond the evidence and, in this way, to perceive the direction of the action and to succeed in being one step ahead the events.

Anyway the purpose of this paper is not to offer a concrete model of dealing with irrationality, but first of all to open the perspective of seeing and processing information differently. That could easily lead the intelligence analyst from information to knowledge and eventually to wisdom.

Information/Conscience/Significance

Intelligence analysis requires reaching the meaning of things and processes they are involved in. Reaching the sense of one event represents not only information, but information processed by conscience. Information is "knowledge, facts, meanings resulted from the investigation of reality"[2] and conscience is "the dynamic organization of human psychic life manifested in human relations with itself, with the others and with the environment"[3]. How does

information alter consciousness? By creating meanings. A significance contains a compaction, a synthesis of information. Jeana Morărescu claims, in "Universul informaţiei şi fenomenologia conştiinţei" that the significance contains the "hologram information of the entire universe, with possible meanings and relations"[4]. In other words, if we understand the holistic nature of meaning, we can pass from ontology to axiology, from simple existence to value and sense.

In this respect, information could be defined as the entrance of energy of every creature in its shape. For Jeana Morărescu information is coding the energy and it could be expressed in four ways: a) virtual b) intentional, c) integrative and d) integrated. The goal of any cognitive approach is to obtain integrated information, which means the significance that has the effect of "guaranteeing axiological" the information structure[5].

Also, Basarab Nicolescu writes in "Noi, particula şi lumea" that the energy appears as a unifying concept of the substance (as related to energy), the space-time (geometrical form of energy) and the information (encoded form of energy). The matter is in this case a complex of energy-substance and space-time-information[6].

We know so far that information is the encoded form of the energy. The purpose of the intelligence analysis is to find out the code and also to find out what is behind the information. That means finding out the direction of the encoded energy. Passing through the consciousness, a simple information receives a significance. So, behind data and information, the analyst has to discover the energy that gives direction and long term significance to any phenomenon.

The Dynamic Logic of Contradiction - Ştefan Lupaşcu

The Romanian philosopher Ştefan Lupaşcu proposed in his 1940 book "Experienţa microfizică şi gândirea umană"[7], a new method to understand the microphysics level of human thinking. This new method is called the logic of contradiction and consists in accepting contradiction as part of knowledge. Lupaşcu begins with the question: What happens if we deny the absolute character of the non-contradiction principle of classical logic? How will things look like if we accept contradiction as being part of the world? According to the classical principle of non-contradiction, contradictory statements cannot both be true in the same sense at the same time.

Instead of the classical principle, Ştefan Lupaşcu brings into question a principle of contradictory complementarity to replace the

noncontradiction principle as a foundation of logic. He considers that we should look better to what contradicts a phenomenon, in other words, what is its complementary contradictory part. When you look at just one of a couple of contradictory terms, you see only a part of its reality. Thus, the principle of contradiction more than the one of noncontradiction should become the rule.

In this way, Lupaşcu founded a new logic, questioning the excluded third principle (tertium non datur), from the classical logic. Besides the two terms of classical logic (A and non-A), he introduced a third state, going beyond the duality principle, the T-state. The T-state is neither "actual", nor "potential" (categories perceived in Lupaşcu's system as the "true" or "false" values of standard bivalent logic), but a resolution of the two contradictory elements at a higher level of reality.

Contradiction is not something static. It is a dual process which starts with the notion of possible, that in his opinion means a state that for now is nor actual, nor potential. Actual is possible, which is realized and potential is possible, which cannot be achieved because it is kept in the pure state by its opposite, which is made actually in contradiction with it.

Our experience about systems is that they have a tendency to organize themselves in critical states, which are sensitive to variation, so that the smallest change can produce new effects across the system. Such phenomena are unpredictable and cannot be analyzed in detail. It is as the mathematician John Barrow said: "Be it the grains of sand or the thoughts that are being organized, their next move is always a surprise"[8]. And yet, even if it seems impossible, managing the unknown and preventing the surprise is the main task of intelligence analysis.

The Trandisciplinary Approach – Basarab Nicolescu

Basarab Nicolescu, a Romanian theoretical physicist, enunciated in 1982 the transdisciplinary theory of the levels of Reality. He believed this theory was a good starting point in erasing the fragmentation of knowledge and the fragmentation of the human being. This approach permits us to transform knowledge into understanding: "Understanding means fusion of knowledge and being"[9].

In the article "Transdisciplinarity and Complexity: Levels of Reality as Source of Indeterminacy", he explains the meaning of the main terms. By "transdisciplinarity" he means that which crosses all

disciplines and finds itself between and beyond all disciplines. Even more important for the purpose of this paper is the definition of transdisciplinarity as transgression of duality opposing binary pairs: subject/object, subjectivity/objectivity, matter/consciousness. By reality, Nicolescu designates that which resists our experiences, representations, descriptions, images or mathematical formalizations. By level of Reality, he designates an ensemble of systems which are invariant under the action of certain general laws. Quantum entities, for example are subordinated to quantum laws, which are very different from the laws of the macrophysical world[10].

If one remains on a single level of Reality, all manifestation appears as a struggle between two contradictory elements. The third dynamic, that of T-state (Ştefan Lupaşcu's principle of dynamic contradiction), is exercised on another level of reality, where that what appears to be contradictory is perceived as non-contradictory.

The logic of the third part included does not mean that we can affirm a thing and its opposite in the same time. In such a situation we would have a mutual annihilation and we could predict nothing. No, we have contradiction, but for understanding it, we must go to a higher level of knowledge.

The Romanian theoretical physicist notices that every level is characterized by its incompleteness: the laws governing this level are just a part of the totality of laws governing all levels, which means that knowledge is forever open. And if knowledge is forever open, that means intelligence analysis has to be at a higher level, to have a transdisciplinary vision, for succeeding in making good forecasts about the direction of events.

The Manifestation of Irrational in the Process of Intelligence Analysis

It is clear, so far, that the intelligence analyst must keep his mind open to the methods of different sciences and to alternative interpretations. Intelligence refers to the process of defining needs, collecting, analyzing information and providing information needed by decision makers to determine the right decisions about a state's policies[11] . Stan A. Taylor wrote in *The Role of Intelligence in National Security* (included in the tome Contemporary Security Studies, 2007) that a general theory of intelligence can be drawn from cybernetics - a complex science about how information can maintain or alter any biological, social or artificial system. Cybernetics, as a science

of feed-back, is a metaphor for the role of intelligence applied to statecraft. Decision makers must use skill, intuition and a constant flow of information to get most security at the least cost for the state. In the same way, cybernetics is about" goal-oriented behaviour at all levels of living systems" that allows systems to reach defined goals based on information flows. Intelligence defined as process involves collecting and analyzing billions of stimuli (information) from the national or international environment.

The intelligence process begins with the need to know of the national security and foreign policy officials. Next is the collection stage, followed by analysis that is considered the most difficult stage in the intelligence process, because it is essential to make the right correlations and to have the right conclusion. That's why, most intelligence failures arise in this stage. Information sent to the analyst is called raw or unfinished intelligence and it is often" conflicting, ambiguous, contradictory, or even occasionally accurate"[12]. Production follows analysis and the final stage in the intelligence process involves the delivery of the information to those who requested it.

Abram Shulsky and Gary J. Schmitt argue in *Silent Warfare* that: to be useful in evaluating the determinants factors of a context, the analysis of information must underline those elements that can be influenced, because usually the beneficiary of intelligence product is interested eventually to change, and not only to know. Sherman Kent considers also that intelligence is not knowledge for knowledge's sake alone, but that intelligence is knowledge for the practical matter of taking action.

How could intelligence analysis that is a practical approach be influenced by the irrational from the human mind? More precisely, how could the logical contradiction be integrated into an analysis that in the end has to be „actionable information"?

The irrational is defined as a view which releases the deliverance of some faculty, such as belief, or intuition from the critical scrutiny of reason[13]. As it was said in the introduction, the hypothesis is: accepting contradiction might help us to avoid some cognitive traps of the intelligence analysis. In other words, admitting the existence of contradiction is better than avoiding it. Analysts construct a reality based on objective information, filtered through complex mental processes that determine which information is attended to, how it is organized, and the meaning attributed to it.

Four basic types of reasoning apply to intelligence analysis: induction, deduction, abduction and the scientific method.

When talking about the irrational – be it emotion, perception or contradiction - we refer also to the mind of the analyst and to the mind of those who are the ”target” of analysis. Richards Heuer Jr. wrote in *Psychology of Intelligence Analysis* that intelligence analysts must understand themselves before they can understand others.

Mirror-imaging is one of Heuer's favorite example of a cognitive trap, which the analyst substitutes his own mindset for that of the target.”The intelligence analyst's own perceptions are likely to exert a greater impact on the analytical product then in other fields where an analyst is working with less ambiguous and less discordant information”[14]. In the NATO Open Source Intelligence Handbook are also mentioned some categories of misperception and bias, such as the rational-actor hypothesis: assumption that others will act in a “rational” manner based on one's own rational reference and the denial of rationality, which consists in the attribution of irrationality[15] .

The point I am trying to get across is that: Lupaşcu's and Nicolescu's ideas, applied to intelligence analysis could complete the existing ways of looking at familiar data from a different perspective. Richard Heuer Jr. presents some techniques such as: thinking backwards, crystal ball, role playing or devil's advocate. To these four methods could be added the third included principle, initiated by Ştefan Lupaşcu and the transdisciplinary approach, developed by Basarab Nicolescu.

The Emotional Component in the Process of Analysis

In the human psychic lots of emotions, passions, ambitions and resentments of a great subtlety are acting. The intellect and conscience convert this multitude of impressions in a surprising manner that is very difficult to control. As Lev Tolstoi said in *War and Peace*, even historical events are converted by the individual or collective psychic. In this way the psychic seeks for justifications, trying to escape the moral responsibility of those who triggered the events.

Harold J. Leavitt wrote in *Managerial Psychology* that our biggest mistake in our efforts to understand and to change others was “to treat the human being as though he were only a rational, reasoning critter”[16]. He also underlined that feelings and facts got intertwined and almost inseparable in many of our problems. “It is the whole person who makes the decisions, not just the logical part of him”[17].

Why should the irrational - that acts in the individual conscience - be not omitted when analyzing national or global issues? Because individual anxieties can become national anxieties and eventually, can be designed internationally. Do not forget that in the Information Age, when due to technology, information started to be transmitted very quickly, what is hiding behind every decision, after all, is a human will and a consciousness. Hans Morgenthau claims in *Politics Among Nations* that information and ideas that are to be transmitted represent the reflection of the experiences emerged by the philosophies, ethics and political views of different people. That is why an idea that captures the consciousness of the individuals, whether false or true, it must establish a special connection between the information it contains and the conscience that seeks to influence. This connection is given by the life experiences and the interests of people, who receive the message[18].

Where the contrast between the ideas and life experiences of people is high, failure is guaranteed, says Hans Morgenthau. He gives as an example the rejection of Western ideas in China or the success of Communism among those who wanted the most the eradication of inequalities. Morgenthau notices that trying to understand the world rationally, when it is not rational, is a problematical issue. If all men were rational, all conflicts between them would disappear and harmony, wealth and happiness would reign in the world. But the reality is far from that. In each situation there is a mix of contradictory trends. A good analyst can only observe various trends that have the potential to become actual in a given time.

Conclusions

Only by the means of their analytical thinking, people face with difficulty a world increasingly incomprehensible. Associative mechanism of the mind simply does not provide knowledge. More than that, knowledge itself doesn't represent real power, but a potential one. Human experience and conscience must be taken into account. Even so, between experience and conscience many manifestations of irrationality can occur. Any information obtained by rational means, in contact with the conscience, can lead to irrational and unpredictable reactions. The main message of this article is that: though we may wish for a rational world, we are not

likely to understand it by exclusively rational means. That does not suppose to abandon the battle of reasoning, but just to change the weapons used in the battle.

Lupaşcu's philosophical system, focused on the dynamic logic of contradiction, is a new way of treating with the unknown, that can't be revealed because we use an inappropriate method. We call irrational the rational, analyzed with the wrong method. Ştefan Lupaşcu aimed even an essential change of the human capacity to understand the reality. Lupaşcu generalized his logic to physics and epistemology and, above all, to a new theory of consciousness.

What an intelligence analyst should compulsory consider is that: everything is a process, in which we have more than two elements. So, when analyzing a fact or a situation, we must look for the opposite, in order to have the whole picture of the situation. Contradiction, or the irrational as it was named in the title, is part of the world. That will help us to understand how things really work like and not how we would like them to function (as it sometimes happens when looking at just one part of a situation that could be seriously affected by the analyst's mind sets).

That is why it is important to detect the irrational from the human mind and to recognize its power. The dynamic logic of contradiction, the third included principle and the transdisciplinary theory of levels of Reality could be useful tools for intelligence analysis. The dynamic logic of contradiction, for example, entitles us to say "Nothing is what it seems", because nothing is completely actualized, nor completely virtualized, nothing is absolute. That means even the intelligence analyst can say nothing for sure, until one thing becomes a fact. The suggestion is to keep the mind open to alternative interpretations, in a rapidly changing world. And most important: Look for dynamics, not for statistics!

References

[1] Sommerhoff Gerd, *Understanding Conciousness* (London: Sage Publications, 2000), p.7.
[2] Cătălin Zamfir and Lazăr Vlăsceanu (eds.), *Dicţionar de sociologie* (Bucharest: Babel, 1998), p. 296.
[3] *Ibid.*, p. 132.
[4] Morărescu Jeana, *Universul informaţiei şi fenomenologia cunoaşterii* (Bucharest: Floare Albastră, 2006), p. 151.
[5] *Ibid.*, p. 150

[6] Basarab Nicolescu, *Noi, particula şi lumea* (Iaşi: Polirom, 2002), p. 99.
[7] Ştefan Lupaşcu, *Experienţa microfizică şi gândirea umană* (Bucharest: Editura Ştiinţifică, 1992).
[8] John Barrow, *Impossibility: Limits of Science and the Science of Limits*, 1998
[9] Basarab Nicolescu, *The concept of levels of reality and its relevance for non-reduction and personhood*, 2011, p. 127, available at http://bdigital.ufp.pt/bitstream/10284/2392/3/119-130.pdf, last accessed January 2013.
[10] Basarab Nicolescu, *Transdisciplinarity and Complexity: Levels of Reality as Source of Indeterminacy*, 2000, available at http://ciret-transdisciplinarity.org/bulletin/b15c4.php, last accessed January 2013.
[11] Stan Taylor, "The Role of Intelligence in National Security", in Alan Collins (ed.), *Contemporary Security Studies* (New York: Oxford University Press Inc., 2007), p.250.
[12] *Ibid.*, p. 256
[13] Blackburn Simon, *The Oxford Dictionary of Philosophy* (New York: Oxford University Press Inc., 2005), p. 191.
[14] Richards Heuer Jr., *Psychology of Intelligence Analysis* (Washington, DC: Center for the Study of Intelligence, Central Intelligence Agency, 1999), p. 15, available at https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis/PsychofIntelNew.pdf, last accessed January 2013.
[15] *Nato Open Source Intelligence Handbook*, p. 46, available at http://www.oss.net/dynamaster/file_archive/030201/ca5fb66734f540fbb4f8f6ef759b258c/NATO%20OSINT%20Handbook%20v1.2%20%20Jan%202002.pdf, last accesed January 2013.
[16] Harold J. Leavitt, *Managerial Psychology* (Chicago: University of Chicago Press, 1978), p. 87.
[17] *Ibid.*, p. 54.
[18] Hans Morgenthau, *Politica între naţiuni* (Iaşi: Polirom, 2007), p. 291.

The Revolution in Intelligence Affairs (1989-2005)

Eric DENECE[*]

Abstract

It is widely known that a "Revolution in Military Affairs" (RMA) took place in the early 1990s. The concept was born of technological, political, social and economic changes that were to fundamentally alter the future of warfare, introducing a completely new type of military and organisational structure for the effective projection of force.

Though most experts accepted the reality of a fundamental transformation in the practice of warfare, few saw that a parallel revolution was occurring in the intelligence world, even though this specific field of national security was undergoing similar challenges and change.

The present paper will attempt to ascertain whether there actually was a "Revolution in Intelligence Affairs" in the 1990s and early 2000s and, if so, what its effects were.

This "intelligence revolution" resulted from a combination of changes in international politics, information technologies and socio-political context.

- Geopolitical Upheaval. In the early 1990s, the intelligence community was hit hard by geopolitical upheaval and the collapse of the former international paradigm. The Cold War was a war involving covert operations that lasted nearly half a century. East-West rivalry drove the activity of intelligence agencies in NATO and Warsaw Pact countries over that period. The sudden loss of an opponent, which had up until then justified their very existence, first disoriented agencies, and then made them question their future.

- Information Technologies Revolution. Since the late 1980s, the world has undergone a far-reaching technological revolution with innovations in data communications, electronics and telecommunications. The combined effect of these innovations has radically altered the world we live in. Digital technologies led to a convergence of sound, image and data, allowing instant transmission, automatic processing and increased computing capacity and storage. This technological revolution has had a major impact on intelligence practice.

- New Socio-Political Context. The rise of new democratic demands and political requirements (better governance, ethics, pressure groups, etc.) has also impacted intelligence agencies.

The combination of these three factors transformed the context in which agencies operate, their areas of focus, and their tradecraft. They have led to major changes in the rules governing intelligence activities.

[*] Director, Centre Français de Recherche sur le Renseignement

Consequences of Geopolitical Upheaval

New Threats and New Enemies

From one major threat emanating from a single opponent (the former USSR), agencies now face and must track six dangerous phenomena involving new players with highly unpredictable patterns of behavior.

- *Radical Islamic terrorism*

Since 9/11, Islamic jihad has been the main threat to international security. Al-Qaeda is a new kind of terrorist organization in that it does not depend on any one state and no one has direct control over it. No other terrorist group enjoys such a degree of independence. Jihadist networks operate in more than 60 countries, but without a hierarchical structure.

It is strange to think that bin Laden himself did not exert any direct control over terrorist groups. The organization he founded operates more like a "holding company", defining strategy and targets and offering volunteers money, training or logistical support. This is – and was - primarily a technical assistance center for Islamic terrorists. Al-Qaeda taught other radical groups how to use the Internet to communicate and disseminate bomb-making techniques. It provided them with skills to increase their operational capabilities.

- *Transnational Criminal Organizations*

They constitute the major threat of the twenty-first century. These organizations have turned the IT revolution and economic globalization to their advantage to develop the illegal economy. They are continually expanding and diversifying their activities: drugs, weapons and human trafficking, smuggling and counterfeiting.

Specialists say that criminal money represents more than 7% of the global economy. At the beginning of the 90^{s}, criminal activity represented 2% of global gross domestic product (or Gross World Product). The illegal economy grew threefold in a decade.

The financial power wielded by criminal organizations is awesome. Whole regions of Latin America, Africa and the Caucasus are now in the hands of criminal organizations. Their development is a serious threat to the national security of some states. They do not seek to control territory, rather they wish to control institutions and commercial companies and banks that allow them to launder money.

- Proliferation of Weapons of Mass Destruction

Most former USSR nuclear weapons have remained under the control of Russia. But some Soviet nuclear scientists provided expertise to spread nuclear technology and materials to ideologically radical states (Iran, Pakistan, North Korea, etc.). The unpredictable behavior of these states and their relations with terrorist groups are a major cause for concern.

- Increased economic competition between developed countries

The main consequence of the end of East-West rivalry has been increased competition between developed nations. States and companies are engaged across all sectors in a veritable war for access to markets or global natural resources. There is fierce competition with some analysts talking of a new economic war, and saying that the rules of this new 'game' are far from fair.

Some countries – for instance the United States - have redirected part of the activities of their intelligence services to support exports and to destabilize foreign competitors. More and more people with backgrounds working in state intelligence agencies are now employed in the private sector.

- Rise of new violent activists

The victory of the liberal model over communist totalitarianism has paradoxically led to a proliferation of anti-capitalist groups, seeking to challenge or fight the evolution of modern societies for a range of reasons (communist nostalgia, anarchy, far-right and far-left ideologies, etc.)

Post-industrial societies have also given rise to a myriad of protest groups on almost every issue: anti-globalization, opposition to vivisection, environmental protection, anti-consumerism, anti-advertising.

Most of these movements are willing to take violent action or even carry out terrorist attacks to promote their ideas (eco-terrorists, animal rights groups). Such groups specialize in sabotage, kidnapping or bomb attacks. They see themselves at war and adopt a covert organization approach like that used by terrorist groups.

For example, in the UK, the Animal Liberation Front (ALF) has destroyed medical laboratories and sent letter bombs to scientists working in the pharmaceutical industry. In USA, the Earth Liberation Front (ELF) has been even more violent in the name of protecting the Earth. As a result, these movements have been blacklisted as terrorist groups like Al-Qaeda.

- New unpredictable events or 'disrupters'

The fragmentation of the New World Order (Balkans, Central Asia, etc.) means that there are more regions where crises are likely to break out. Some states will try to take advantage of the new world situation (cf. Iraq 1991). Other new phenomena, for example the Arab Spring, erupt without warning. A myriad of threats, a diversification of crises and growing unpredictibility are the hallmarks of this new situation.

Most new threats stem from the *development of non-state actors*. Today, many organizations have taken full advantage of new technologies, world decompartmentalization and globalization. NGOs as well as transnational terrorists, international criminal organizations, cyber hacktivists or protest groups are all Internet-savvy and globally operational. They have developed strategies beyond the control and scope of nation states with new kinds of organizations: networks, Starfish system, etc.

But though new actors are now taking part in "The Great Game", previous threats (secessionism, political violence and extremism, civil war and the threat of military action) still remain.

Changes to Tradecraft and Agency Organization

Traditional intelligence methods no longer worked against Al-Qaeda, criminal organizations and newly emerged activists. Indeed, nothing is more difficult than fighting a virtual organization, with no land or physical headquarters to protect and operating without a central command. This has led intelligence agencies to change their operational practices inherited from the Cold War. Intelligence practice has gone through five major transformations.

- From Macrointelligence to Microintelligence

During the Cold War, intelligence agencies where looking to acquire knowledge on large targets: garrisons holding several thousand men, air or naval bases, missile sites, weapons production plants, etc. The information sought was necessarily housed in several different places, due to the high number of staff or forces involved, the importance of telecommunications, the large number of subcontractors, etc. Those numerous resources offered many targets for the recruitment of agents and intercepts. Moreover, though the services were working tirelessly to better understand enemy capabilities, the intentions of the enemy were well-known.

After 1991, the situation changed dramatically.

Al-Qaeda does not have a centralized command. This specificity makes the identification of decision centers more complicated and increases the number of potential targets. It is extremely difficult to gather data that will prevent a terrorist act. Agencies are looking for information of a microscopic nature, specifically protected within 'closed societies'. The critical data is often only housed in the brain of the terrorist, in an off-line, off-grid computer or in a message lost among the plethora of phone calls made each day, in a suitcase, or a hotel room where three Salafi terrorists meet together, etc. Secrets are shared among a small number of people, who live in a state of constant paranoia, and who implement stringent security measures.

Such target data is called microscopic intelligence: it differs greatly from intelligence acquisition during the Cold War, where the objective was to acquire information on macroscopic targets.

- New challenges for HUMINT and the running of agents

Information gathering through illegal means remains an essential part of the intelligence work but it is difficult because of the nature of the objectives.

On the one hand, the penetration of a terrorist network or a criminal organization is an extremely difficult operation. Jihadist groups are what we call 'closed societies'. In each cell, men often come from the same village, have usually known each other for a long time and may speak a dialect unknown to Westerners. It is easy for them to immediately detect and eliminate an intruder.

On the other hand, it is almost impossible to recruit within terrorist movements. Their very strongly-held, radical Islamic beliefs make them resistant to conventional methods of recruitment as double agents. So, Western agencies have to recruit men from outside the movement in order to infiltrate them. But that process often involves working with individuals whose loyalty remains fragile.

Moreover, when the West succeeds in infiltrating an agent into a jihadist group, ensuring secure and constant communication with the agent is a huge challenge as terrorist cells apply drastic security measures. The members live closely together, monitor each individual member and prohibit any contact with the outside world. And, obviously, information about a future attack has no value if it comes too late.

Finally, infiltrating a terrorist organization poses a moral problem: the agent usually has a very short lifespan (a few weeks to a few months) as the objective of the cell is to carry out a suicide bomb attack. Few men and services agree to risk such an outcome.

Consequently, gathering secret intelligence via human assets has become increasingly difficult and dangerous: recruitment and penetration are still possible but increasingly complex.

- *Limits of Technical Intelligence*

As it is very difficult to penetrate such groups, agencies must seek out information on the periphery, in areas where technology is key. Although, during the Cold War, it was possible to understand the Soviet mindset from the outside, it is impossible today to counter terrorist strategy without penetrating their organizations.

- *Growing interdependence between agencies*

Today, an increasing part of the intelligence work is done as part of international cooperation programs. To investigate and monitor a jihadist group or a criminal organization it is necessary to have an overview of its global activities. No country can do it alone.

But some cooperation is sensitive and can generate problems for democratic countries. Cooperation with Middle East intelligence agencies in particular is difficult due to the widespread use of torture in most of these countries. Western public opinion is increasing vocal in its criticism of these kinds of partnerships, even if it is in the interests of their own security.

- *New Economic rivalries and Coopetition*

But though intelligence agencies around the world are working together more and more, there is still rivalry between them, mostly for political or economic reasons. This results in what we call 'Coopetition'.

A good exemple is the French/US relationship in 2003. The US and France were strong adversaries on the Iraqi invasion, but very close allies in the fight against Al-Qaeda.

Consequences of the Information Technologies Revolution

Limits of Signals Intelligence

One of the biggest paradoxes of modern intelligence is SIGINT. In Western countries, intelligence by technical means grew substantially during the Cold War, mostly because human research provided only limited results against the Communist security system. 80% of the information collected on the USSR was of a technical origin.

These tools are now clearly limited. Technical intelligence (also comprising IMINT, and the other INTs) is increasingly effective, but cannot provide all the answers, for several reasons:

- Exponential growth of world telecommunications

The incredible growth of modern communications - telephone, GSM, Internet, etc. - is a major challenge for SIGINT agencies. It should be remembered that 40 years ago there were only 5000 computers in the world. These computers were not linked to each other nor were they connected to a fax or phone.

Today, there are 400 million computers worldwide, which are all interconnected, as well as nearly 20 million fax machines, and hundreds of millions of mobile phones, etc. In 2000, the US provider AOL transmitted 225 million emails per day. Today, traffic on the electronic networks is more than twelve times greater.

Of course, the development of SIGINT satellites, combined with the rise of new supercomputer capacity, has made significant progress and data storage is also improving rapidly. However, the reality is that agency technological capacity has failed to match the growth of telecommunications. Even the USA cannot monitor the hundreds of millions of emails, phone calls and electronic money transfers made every day worldwide. And among the huge amount of communications surveiled every day by the U.S., only about 10% is seriously processed and analyzed on time.

- Development of private cryptology

There has also been a rapid development in cryptography. Encryption by companies or private individuals is growing everyday, posing a major challenge to SIGINT agencies. The fight between the cryptologists and those seeking secure communications has turned to the advantage of the latter. Of course, it will always be technically possible to break a code with adequate computing capability. But such a process can take weeks, and most terrorist or criminal organizations just need to protect their secret talks for a few days, as they plan their operation.

Above all, there are many means of communications available now to an individual, terrorist or criminal, allowing them to bypass the issue of encryption altogether, meaning that most of them can send high-value messages by simply using non-monitored devices and means.

For example Al-Qaeda uses both modern means of communication (Internet, encrypted cell and satellite phones, radio, etc.) and human operators who carry messages. With several mobile phones, a jihadist can thwart wiretaps set by intelligence agencies. Wiretaps are sometimes of no use at all because terrorists often communicate among themselves using direct human contact.

- *Translation problems*

Another challenge for SIGINT is translation. The National Security Agency (NSA) says that there are some 6,500 languages spoken around the world. It is extremely difficult for intelligence agencies to find enough translators in rare languages used by mafia or terrorist organizations.

In 2000, the FBI linguistic department had 900 translators and a budget of 21 million dollars. By 2004, the figures had climbed to 1,200 translators with a 70 million dollar budget. However, that same year, 30% of intercepted communications were stored without being translated. After a three-year period, due to data storage problems, a large proportion had been deleted without being processed.

New Challenges of Data Processing

Today there is more information available to us than ever before. One of the major challenges facing modern intelligence is not information gathering, but data processing. There are three areas where this is particularly important:

- *Open Source and Social Media*

The IT Revolution has generated an explosion in information resources. Information is found everywhere, in all forms (books, journals, videos, CD-ROMs, Internet, social media, etc.). The volume of online resources is growing incredibly fast. About 10 million web pages are created every day and the total volume doubles every four years. Specialized commercial databases are created and updated everyday, creating new sources of information. Commercial imagery is also a new resource available to anyone and has put an end to the monopoly of State intelligence from space. More recently, the growth of social media - Twitter, Facebook, etc. – has provided another channel of access to individuals and their private life.

Opportunities to acquire knowledge on any subject have changed. When we consider the huge amount of data collected every day, the great challenge facing modern intelligence is to separate «the wheat from the chaff» and «to connect the dots».

- PROPINT and Personal Data Protection

PROPINT (Proprietary Intelligence) is the term for data-protected personal information to be found in digital databases that are either in public or private sector hands. It concerns our communications, movements, air travel, our financial transactions, immigration status, national insurance records. We all leave tracks behind us as we go about our lives in a high-tech society.

PROPINT is very useful for counterterrorism or counter-intelligence, and much more so than OSINT (Open Source Intelligence). These databases are (or not as the case may be) legally accessible to intelligence and security agencies, depending on applicable personal data protection legislation. Every country has a different approach to and legislation on data protection, but the price to pay is often the end of people's privacy.

For 20 years, the amount of data and product to process has grown at a rapid pace. Intelligence agencies have seen their work change as they expand their spheres of activity. They have had to develop new skills in new directions (technology, finance, economics, market research, technology, climate change, international crime.)

Consequently, what are the Benefits and Risks of I.T.?

The information revolution has provided new tools: data mining and automated analysis software, increased computer and data storage capacity, etc. But enemies or disrupters are also using these tools to criminal ends. This gives them unmatched power for covert activities and even small organizations can take advantage of low-cost technologies to develop highly effective intelligence systems.

Privatization and diversification of intelligence operators and suppliers

The information revolution has also led to the development of private intelligence companies, creating new partners as well as new competitors for state agencies.

New partners…

- Companies: new customers of Intelligence. Over the last decade, economic competition has become much more intense. This has led many companies to develop their own business intelligence capabilities to meet their information needs and to protect themselves from acts of destabilization.

- Consultants: new providers of intelligence. Many consultants - mainly former members of state agencies – have taken advantage of this new market to develop their business. They are given missions that were previously part of the tasks of state agencies. Some of them also perform intelligence, training or security missions on behalf of governmental agencies.

In 2010, the newly appointed US Director of National Intelligence (DNI) found that 70% of the intelligence budget was allocated to private contractors and 50% of employees working for the Defense Intelligence Agency were private contractors.

- Industrial sector also offers a wide range of intelligence products, from databases to software.

… And new competitors

Privatization of intelligence challenges the traditional position of state agencies, which have long been the only ones "to feed" policymakers. They are, for the first time in their history, in competition with new actors coming from the private sector, who are often able to provide high-quality intelligence, and sometimes more quickly and accurately than the agencies themselves. As a result, state intelligence agencies must accept some form of comparison with private players.

Consequences of the New Socio-Political Context

The third major evolution for agencies is the new demands made by modern democratic societies (ethics, governance and transparency) and new demands on politicians who face the threat of terrorist attack.

New Demands of Democratic Societies

- Ethics: the rejection of torture and demands for protection of personal data

Law enforcement, security and intelligence agencies should accept that ethics do matter to democratic public opinion: there are 'red lines' that must not be crossed.

Indeed, the non-respect of international law and the development of coercive methods (as seen in Guantanamo and Abu Ghraib) – and which are considered counter-productive by specialists - deeply shocked our democratic societies and was a source of embarrassment to the authorities.

Ethical principles should also be applied to govern the use of PROPINT and intrusive investigative methods.

- *Governance: Generalization of parliamentary oversight and performance auditing leading to the proper use of I & S agencies*

Historically, agencies have long enjoyed freedom of action justified by "la Raison d'Etat". However, it is no longer acceptable to democratic societies that organizations working in the shadows are unaccountable for their actions.

Moreover, citizens and their elected representatives need to be sure that authorities are using agencies properly and that they are delivering "the best result for the money spent".

- *Transparency: Publicized intelligence – Communication vs. secrecy*

To the modern citizen, transparency is ineffective without proper communications. Intelligence agencies should develop their public relations because, since 9/11, they have been under the spotlight. They are, as never before, a subject of public interest and debate.

Agencies should explain what their job is, mobilize public opinion and attract the best people in the country. Communicating to the public is also useful to explain how taxpayer money is being used and what the effectiveness of the intelligence agencies actually is. However, the public and media must accept the secrecy involved in intelligence work, as it is a key component for the success of intelligence operations and consequently the security of the general public.

New Behavior of Policy Makers

- *New political pressure*

A terrorist attack always has a profound effect on public opinion. When such an event happens, it often looks like a government and security services have failed. So policymakers are aware that such attacks must not occur on their own soil, both to protect their citizens, and also to ensure reelection. Therefore, there is increasing political pressure on agencies. Political leaders are more and more demanding of intelligence and securities agencies. They apply pressure on intelligence and security agencies to avoid any surprises that could destabilize their government.

- *Manipulated intelligence*

Unfortunately, most of the time in our democracies governments refuse to bear their responsibilities and blame agencies for their own mistakes when attacks occur. This is easy for them, as an intelligence agency is unlikely to protest. An example of this approach was given on 9/11 in the US.

Moreover, some government behavior - for exemple the US and UK in 2003 - has led to a politicization of intelligence. Some political leaders, like Bush and Blair, manipulated intelligence to promote their own agenda and interests. The White House requested intelligence, not to have a clear assessment of the situation in Iraq but to find information that would support its decision to invade Iraq. This led to disinformation such as the alleged and spurious links between Saddam Hussein and Al-Qaeda or the question of Iraqi weapons of mass destruction.

The result is that some agencies have lost their independence.

- *Terrorism: a narrow focus for I & S agencies*

Simply focusing on terrorism and hostages (to the detriment of everything else) is dangerous. This is not the only threat agencies have to deal with. For example, on February 2013, in the USA, a secret report highlighted intelligence blind spots because the intelligence community was so focused on Al-Qaeda. A panel of White House advisers warned President Obama that U.S. spy agencies were paying inadequate attention to China, the Middle East and other national security flash points because they had become too focused on Islamic terrorism.

- *Persistent misunderstandings with policymakers.*

Intelligence is not a magic tool, able to do everything, at all times. Intelligence works only under specific conditions. But in most countries policymakers ignore the real role of intelligence agencies and what can be asked of them.

*

When we look back at the history of modern intelligence, three different stages emerge, three major “evolutions”:

- *World War 1.* The early years of the XXth century saw the birth of modern telecommunications (telegraphy), and with it the development of cryptology and intercepts, which grew significantly during WW1. In this first case, the main driving force was technology, seconded by global geopolitical conflict.

- *World War 2*. In the early 1940s, intelligence agencies operated on an unprecedented scale, all over the world, and there was a major evolution in the use of HUMINT, Counterintelligence, SIGINT and Special Operations. In this second case, the main reason was geopolitics, seconded by technological/military innovations introduced during the war. At the end of the war I & S agencies became permanent bodies of national state administrations. The Cold War brought nothing really new, just a global spread of the innovations that had emerged during WWII.

- *1989-2005: «The Third Wave»*. This "Revolution" took place over a fifteen-year period, from the fall of the Berlin Wall to the London 7/7 bombings. It resulted both from geopolitical and technological upheavals, but also from socio-political changes.

It is a real revolution: context, matters of interest, opponents, methods, technologies, time of response, have all changed and the new situation has nothing in common with the intelligence landscape of the Cold War. Something huge has happened which has transformed "The Great Game". It could be called a "Copernican Revolution".

Today, *I & S agencies cover a smaller part of policymaker information needs*. Though modern services are increasingly effective, they paradoxically cover a smaller proportion of the information needs of decision-makers on world issues and challenges. This is a normal evolution. Open source intelligence has reduced the focus of intelligence agencies down to their core business: gathering the secrets of others. Studying climate-change is not part of the intelligence agency remit.

Intelligence and security agencies are not forecast institutes or prospective bodies. Forecasting is another profession entirely. This is not the direction for agencies to take. Prospective reports do not constitute intelligence. We should not try to and are not able to predict the future.

I&S agencies should do what others do not. They are government 'Secrets Finding and Problem Solving' organizations. They are not "global intelligence" agencies! Intelligence agencies are not the ones who provide a total picture, but rather deliver the missing parts of the puzzle.

What Next? Looking Forward

Because of the urgency of and narrow focus on Islamic terrorism there are question marks over whether the next intelligence threats have actually been scoped out. Unfortunately, in most countries, the answer is a negative one.

Intelligence agencies should develop prospective analysis for their own purposes:

- Threat dynamics and evolution;
- Threat convergence (terrorism + crime / Islamism + far-left extremism);
- Identification of new threats.

Though the intelligence work cannot be reduced to mere foresight, services should try to detect the rise of future opponents. They should track particular states or organizations who, given their financial or technological clout, could become the disruptive actors of tomorrow.

But if we try to predict the future in all directions, on every subject, we will surely commit more mistakes in the future than we did in the past.

Intelligence is an Art. Not a science.

Effective Organisation for Effective Intelligence Organisations

Philip H. J. DAVIES[*]

Abstract

The following paper argues that there are substantial lessons to be learned from the literature on contingency theory of organizations regarding the optimal organizational structure for intelligence agencies. Particular attention is paid to the differences in structure required for large-scale routine processes in stable environments and traditional models of state administrative practice as opposed to the smaller scale, more agile needs of intelligence agencies. This distinction is even more pronounced in the current global and technological environment. The paper concludes that the modern intelligence service needs to be organizationally more similar to a small, high-tech firm and its 'campus' than a traditional state or industrial bureaucracy.

Introduction

By and large, the scholarly study of intelligence has typically emphasized the operational activities of intelligence services, individually or in concert, on the one hand or the finished intelligence appreciations they produce. Given the grounding interests of the study of intelligence services, that is, what they do and its impact, this is an entirely reasonable point of departure. But it is and must be no more than a point of departure. Slightly less developed has been discussion of what intelligence institutions should do, that is, normative theorizing as opposed to descriptive accounts. One of the least developed areas is the study of how intelligence institutions are organized, that is, the systematic characterization of structure and process to underpin a general rather than case specific understanding of how intelligence agencies actually do operate and have to operate, and also in contrast with normative pronouncements of how some commentators imagine they ought to operate. That such analysis is so thinly developed is a troubling one. How can one assess how well an agency or community performed in a historical circumstance without understanding the architectures and dynamics that constrain and enable action within sizeable, formally

[*] Director, Brunel Centre for Intelligence and Security Studies

constituted organizations? How can one pass judgement on how agencies and communities ought to operate without having a grounding understanding of how they have to operate and why?

The problem of organization becomes especially pronounced when concerned with intelligence reform, either as a consequence of democratization and political transformation or in order to try and keep pace with the challenges of today's globalised world, its discontents[1] and associated 'wicked problems'[2]. Reform advocates in both cases tend to issue shopping lists of requirements for a reformed organization should look like with comparatively little reference to what intelligence needs to look like. The results tend to fall into the realm of that category of informal logical fallacy broadly termed a presuppositional fallacy. Built on one or other inaccurate premises about how intelligence can operate, the real world inevitably falls short of advocates' standards. By much the same token, retrospective accounts of intelligence operations and assessments for their part tend to lapse into hindsight bias and fallacies of the *post hoc ergo propter hoc* variety. In short, absent rigorous organizational analysis discussion of the past and future of intelligence, as well as its present, leads all too easily to unrealistic judgements and expectations. While this might serve well where advocates or scholars wish to use intelligence institutions as scapegoats or bogey-men it is of little value when one needs to go forward with realistic reform measures.

Part of the problem is, of course, that the organizational analysis of government institutions in general is weakly developed. Consequently, if one is to examine intelligence agency organization there is very little precedent within 'mainstream' political studies upon which to draw. To a very real degree, the study of intelligence agencies ends up having to strike out on its own. The upshot of this, however, is that the resulting scholarship may well find it has something more general to offer the 'mainstream' beyond providing an understanding of a generally poorly understood sphere of governmental activity.

Precedent and its Problems

This is not to say, however, that there has been no work done on the organization of intelligence organizations. Some of the earliest work done in the field of intelligence studies, especially in the United States, was concerned with the study of organization[3] or the application of organizational analysis to intelligence processes[4]. From the early 1970s[5], however, concern with expose and intelligence

scandal largely supplanted more understated analysis, even though the archetypal expose by Senator Frank Church's committee deliberated at some length on the organization challenges of the US intelligence community[5]. In the UK, however, absent the scandals in the USA or Canada, the massive official history of British intelligence during World War 2[6] was so concerned with machinery of government issues that one reviewer dismissed the work as 'written by a committee, about a committee, for a committee'. But the machinery of government approach has always been limited in its conceptual reach and interests, concentrating chiefly on narrative discussions of structure, process and their development.

It was not until the 1990s that one began to see theoretically-informed discussions of intelligence organization. It is in this context that one sees a key aspect of such analysis that serves as both essential strength and critical weakness. The early form of this work built largely on variation on the organizational politics approach and the later derivations from that approach subsumed under the unwieldy notion of 'neoinstitutionalism'[7]. The double-edged aspect of this work was the effort the then-prevalent view of intelligence as being some mysterious, free-wheeling 'parapolitical' (as some British left wing critics termed it) realm beyond and behind the overt processes. To the contrary, intelligence services were and are part and parcel with the routine workings of modern government and characterized by the same kinds of dynamics that institutional process scholars had demonstrated at work in government since the end of the 1960s[8]. This strategy of what might be termed 'normalising' intelligence institutions and our understanding of them fitted well not only with the growing open-government trends in at work chiefly in the English-speaking world but also with the processes of lustration and liberalization at work in the emerging democracies of the former Soviet bloc and the fast-growing 'newly industrialized countries' in Asia, Africa and South America.

The normalization strategy has, however, a limitation which few discussion intelligence institutions have explicitly addressed let alone resolved. That problem is that by integrating intelligence into the routine understanding of routine government one runs the risk importing analytical weaknesses endemic to that routine understanding of routine government. That one of those endemic weaknesses has contributed centrally to the lack of systematic organizational analysis within mainstream studies of government.

Two Approaches to Organisation

Political scientists have been struggling to understand the British Cabinet Office for decades. Even the dynamic and otherwise innovative exponents of 'core executive' theory in British government have run into shallow shoals of confusion and incomprehension reckoning with the Cabinet Office[9]. It is a division of government that has, historically, had a leading Permanent Secretary but (until New Labour) no dedicated departmental minister to lend it political authority from Cabinet. It holds sway across the entirely machinery of British government and yet has no enforceable powers to impose compliance. It is absolutely central to facilitating the negotiation and collaboration that underpin interdepartmental relations and individual departmental work in the Westminster and Whitehall system and yet has no resources to trade other than its own centrality and role as intermediary. To the eyes of political scientists and, indeed, to a generation of first-rank politicians steeped in the understandings and conventional wisdoms of recent political scholarship the Cabinet Office simply makes no sense. It should not work, indeed, it almost should not exist. And yet it is resilient, robust and has existed since the early years of the last century. It is also vital to the workings of the UK's intelligence community.

This incomprehension appears to arise in a large part because of a certain conceptual premise in political studies that amounts to a variety of cognitive bias, specifically selection bias. Politics is, of course, about power. And so politics scholars look upon government organization as ultimately being about power as well. The administrative machinery is seen in the first instance in terms of being an *armature of control*, applying political power in support of political policy. The first premise for any political approach is where, how or why an entity has power.

The problem here is that organization is also about other things as well, chief amongst these is *getting things done*. At a certain level, deploying power in the political arena, and being seen to do so, can be a political end in itself. But it is also all to easy to forget that government is about getting things done, in principle on behalf of the citizenry (even tyrants legitimize themselves as representing and acting on behalf of 'the people' or 'the nation'). Roads need to get built for traffic and trade to flow; treaties need to be signed off and put into practice for that trade to cross borders or be properly protected from challenges or threats within or without. Weights and

measures standards need to be articulated and enforced for much of anything to get done. In this sense, one looks at organization not as an armature of control but an *apparatus for implementation*.

If political scholarship has developed with its eye towards power and authority it is economics and the study of business that have been concerned with organization as practical instrumentality. The business firm above all else about getting things done, and it is not surprising that study of organization as effective (and often ineffective or counterproductive) means of implementation has been the paradigmatic orientation of economic and business scholarship. When Richard Cyert and James March first articulated their 'behavioral theory of the firm'[10], their question was why firms made commercial decisions one way or another, and for better or worse in terms of the quality of that decision. While the transaction cost theory of Oliver Williamson[11] might have clashed with the 'inseparability' hypothesis developed by Armen Alchian and Harold Demsetz[12], both sides were asking why it was easier to get things done by employing people in the long term rather than relying on successive short-term contracts secured through the open market-place. When contingency theories on both sides of the Atlantic examined the differing organizational templates required for high-tech manufacturing, mass-mass production or continuous-flow production processes[13] their question was kind of organizational structures were best suited for performing different kinds of production tasks.

This is not to say that there has not been business scholarship on organizations as power structures because a substantial amount of such work began to appear as 'critical' social science scholars with intellectual roots in one branch or another of the Marxist tradition cast their gaze on commercial processes and institutions[14]. Nor either that there has not been political scholarship on how the state machine might be best suited to 'getting things done'. As we shall see in more detail shortly, much public administration and even the troubled core executive school are extensively concerned with the ability of governmental apparatus to effectively deliver goods and services. But much as critical organization scholarship had contributed little to the real-world conduct of the business firm so political approaches to state organization still try to work within the axiomatic framework of power and control. While there have been isolated attempts to apply organizational theory to state organizations they are few and far between[15], and have had relatively little impact on the discipline.

The problem with this intellectual balkanization between political and sociological scholars approaching state organizations mainly as armatures of control and economic and business thinkers concerning themselves with effective instrumental apparatus is that if one is that intelligence reform debate ultimately needs to be about getting things done and not articulating control. But government and politics create a climate more concerned with the latter than the former, and this is especially the case for comparatively recent democracies trying to cope with legacies of authoritarianism and totalitarianism. In such regimes, expression of power typically takes precedent over, and at the cost of, effective delivery of goods and services. Such legacies make developing an instrumentally effective intelligence system a difficult proposition, geometrically more so if one is trying to democratize, modernize and adapt to the 21st century's information space all at the same time.

Contingency versus Institutionalism

The distinction between armature of control and apparatus for getting things done encapsulates another, conceptually more profound problem in the understanding of organization. That intellectually profound problem is the degree to which one can, in fact, make instrumentally rational decisions in an organizational context at all. After all, if organizations are intrinsically incapable of making substantively rational decisions as opposed to formally compliant ones then reform and transformation in intelligence or any aspect of life is a forlorn hope.

In the late 1980s, the emergence of 'neoinstitutional theory' essentially took as its point of departure the idea that decision-making in organizations – public or private – is structured in terms of compliance with formal process rather than judgements made on any objective evidence. This development is often credited to John W. Meyer[16] but made absolutely explicit by Walter Powell and Paul DiMaggio[17]. Ironically, the point of entry for this almost defeatist approach was with a micro-economist and one of the founders of economics' theory of the firm. Originally in collaboration with Richard Cyert in their 1963 volume, James March took the organizational choice paradigm developed therein to an extreme form in collaboration with Johan P. Olsen resulting in what they termed the 'garbage can' model of organizational decision-making[18].

In the original behavioral theory of the firm, members of an organization made rationally self-interested strategic decisions in seeking to get their preferred policy adopted by the firm at large or its CEO. They would log-roll by trading votes on multiple issues, horse-trade other resources as side incentives to convince others to vote their way. Advocates of common or similar positions would form a voting bloc called a 'dominating coalition' that could run the table in decision-making even if they were actually in a minority. They simply had to persuade few people to vote their way than smaller factions or single individuals – regardless of the substantive merits of who was right or wrong about a specific matter. During the 1970s March and Olsen concluded that this effectively decoupled any and all organizational choice from the merits of any case at hand. Individually rational action resulted in collectively irrational decision-making. Later Powell and DiMaggio further argued that strategic compliance was confined not just to individual organizations but collectivities of organizations engaged in common activities defined as an 'organisational field'. The neoinstitutional approach, therefore, sees organizational life as intrinsically about power, control and compliance and, bluntly, little else.

This stands in a sharp contrast the approach developed by contingency theories in the UK and USA. Work here emphasized in particular how large-scale, highly uniform research, development and manufacturing needed to be organized compared with highly variable processes in industries characterized by complexity and rapid technological and market change. Almost as if in lockstep, teams in the UK and USA found that high-tech firms needed to rely on highly collegial, collaborative management structures, very flat hierarchies and weakly articulated authority relationships in which command and control would defer on matters of substantive judgment to the views of subject matter experts and teams of those experts[19]. Still in close order a decade later concerns were raised about the scalability of such collegial or 'organic' management resulting in hybrid combinations of bureaucratic hierarchy and flexible, task-specific project teams and sub-enterprises that became known as 'matrix' management'[20]. Interestingly enough, one of the chief case studies in matrix management was the US firm TRW, at the time the principal contractor producing satellites for the US overhead reconnaissance programme. This is an example that will shortly prove significant. Contingency theorists collectively argued for two key conclusions. The first was that different industries and production processes required different management models to get things done effectively and efficiently. The second was that if a firm

understood what kind production process they were engaged in they could make a rationally constituted decision about what kind of management model – bureaucratic, organic, matrix or other – they should employ to best effect.

In truth, these insights had already been presaged by Max Weber who noted that bureaucracy was better suited to large-scale routine tasks that required 'quick and consistent solutions' while more unpredictable settings that favoured 'greater thoroughness in weighing administrative decisions' were better handled through collegial arrangements[21].

In other words, contingency theory argues that rational organizational choice is appears to be possible because successful firms in common industries had adopted similar management structures.

There are both empirical and theoretical caveats to the contingency case. During the 1970s Hannah and Freeman looked at the presence of similar models in organizations engaged in similar fields[22]. Their evidence suggested that the correlation between successful firms and common models in various industries was less because there was a method for making the right choice than because those which made the wrong choice disappeared from the sample set because they went out of business. This conclusion, of course, conforms nicely to the neoinstitutional approach. By the same token, although John Child's work on organizational design has always conformed closely to the design-for-environment approach of the contingency school[23], he has always noted that the design process depended on collective, organizational choice processes articulated through some version of Cyert and March's original 1963 formula[24].

That being said, the contemporary information technology industry also shows a history of firms strategically choosing collegial, organic 'campus' model of corporate headquarters precisely because of their sense of how the IT industry operates. Of course, government organizations cannot rise, fall and disappear in the same way as private firms in the market place. They are not subject to quite the same commercial counterpart to natural selection in the biological ecosystem. Government departments can last decades and even centuries, whether they get the job done or not – not least because while being instrumental failures they are likely still comparatively 'successful' as expressions of political power and authority. The tension between the control and instrumental aspects of organization is, therefore, particularly fraught in government. This can only be more acutely the case where that organization is concerned chiefly

with questions of policy, power-projection or national security, all of which are themselves profoundly internally divided between the priorities of ensuring control and getting things done.

A Contingency Theory of Intelligence[25]

A minority interest amongst minority interests, the application of contingency theory has been a growing sphere of activity in intelligence studies although to day most of the specific studies have been confined to British agencies. Intelligence is, of course, a complicated and nuanced field. Operational agencies work with complex, highly technical sources of information that change in technology in the technical systems and cultural and linguistic competence for human intelligence. And that change has been continuous and rapid since the Secret Service Bureau was set up in 1909, and still more so since the Government Code and Cipher School was established in 1919. The analytical task has similar pressures, and of course scientific and technical intelligence assessments must cope with both sources of change and complexity. It is not surprising, therefore, that pooling the technical challenges and understanding of analytical needs and interests would require TRW to adopt the matrix approach for which Lorsch and Allen took it as an exemplar.

By the same token, I have argued at length elsewhere[26] that many intelligence activities require collegial, organic and matrix management structures. That conclusion has been echoed with reference to cryptography by Chris Grey and Andrew Sturdy[27], with the caveat that while cryptanalysis is served best by a flat, collaborative organic model *interception* is mainly a large-scale, highly routine enterprise best served by a mechanistic bureaucracy. Former GCHQ director Sir Davied Pepper has argued that, for his agency, even matrix management was too rigid and top-heavy[28] and so a range of initiatives to make Britain's SIGINT agency fluid and adaptable despite its size (roughly three times the size of the highly organic Secret Intelligence Service) such as an open-plan workspace and a highly flexible team-based process were adopted in the 1990s.

Thus is can be argued that, especially for smaller agencies and higher echelons of the interagency environment, intelligence needs to look more like a high-tech firm than a government department or the kind of factory floor envisioned by one US Director of Central Intelligence as 'an assembly plant for information produced by

collaborating organizations of government'[29]. Like Burns and Stalker's electronics firms, Lawrence and Lorsch's plastics firm or today's silicon valley start-ups, the modern intelligence agency needs to pool expert collection techniques and analytical understandings from a wide variety of disciplines, professional backgrounds and even diverse institutions – and it needs to do so in an environment subject to both complexity and rapid change where the 'state of the art' is competitive and fast-moving. Intelligence history in the modern era is fundamentally about a continuous and accelerating race between denial and deception techniques on the one hand and collection methods on the other. This is as true of human intelligence as of SIGINT or of hiding in plain sight amidst the background noise of the internet as of overhead reconnaissance. The 21st century intelligence service needs to be flat and flexible, collegial and collaborative, building fused syntheses through the informed consensus of properly indoctrinated peers and partner (rather than cobbling together syncretic aggregates from divergent, detached and competitive interests). Practitioners need to think of themselves less as political or governmental animals than technical specialists playing active and constructive roles in collective products and achievements.

Much the same argument can be made about the higher interagency management of intelligence. Observers often forget that although the US intelligence community employs more ten times as many personnel as the UK's, their top-level interagency bodies – the National Intelligence Board and Joint Intelligence Committee for example, or National Intelligence Council and Assessment Starr – are nearly identical in size and have always been so[30]. This is because they are not so much organizations as such as what has recently come to be known as 'meta-organizations' – organizations of organizations[31]. While the wider implications of a concept of meta-organization are still being articulated by academics, from the intelligence point of view there are two principle consequences. The first is that, the various member agencies of any intelligence community are specialist contributors to a collective intelligence enterprise in which they each play key contributive roles much like individual subject matter experts inside a single organization. The second is that at the senior working, executive and sub-Cabinet levels of government interagency metaorganization is intrinsically restricted in scale. This means that regardless of the overall size of a community, at the upper levels intelligence is unlikely to fall afoul of the size constraints on collegial and organic management identified by contingency theorists.

That being said, the chronic problems experienced by many intelligence communities in achieving the level of integrated collaborative effort across multiple intelligence agencies speaks to a caveat originally noted by Burns and Stalker. The formal, structurally collegial arrangements of organic management were not enough to achieve effective organic management. Effective implementation also depended on *informal* organizational considerations, on normative questions of ethos and culture. This consideration has also been applied to understanding how and why collegial and organic arrangements in intelligence have a history of working reasonably well in the UK and not the USA, even in organizational contexts where there is only a minimal difference in actual scale[32]. It is not, therefore, enough to adopt the outer shell of collegial, organic or matrix administrative architectures; a reinforcing culture trust as well as reciprocity needs to be encouraged and cultivated. Unfortunately, steering culture is radically more difficult and prone to unintended consequences than rearranging culture.

Closing Thoughts

The idea that intelligence institutions have more in common with agile and innovative high technology firms than with agencies concerned with taxation, law-enforcement, public works or the environment presents challenges for many countries. As I have pointed out in a number of pieces, the wider US government is ill-disposed in terms of management culture to coping with the kinds of flat, collegial management practices that organic and matrix formulae require. Indeed, the UK's central government has a long history of employing organic arrangements, indeed decades earlier than management scholars even coined the term 'organic management'. This, then, is the clue to understanding the Cabinet Office because facilitator, mediator and interlocutor it is fundamentally about getting things done and *not* articulating or pursuing control. Its nearest counterpart is the organic management team in a large technology firm or a joint military command staff, not a department or ministry of government. SIS and GC&CS were improvising organic arrangements as early and the Second World War, almost unconsciously however. But the administrative ethos of Whitehall is very much the exception rather than rule in such matters.

Herein also lies the challenge for new and recent democracies. They are coming from models of state bureaucracy that developed on

the one hand to express and impose power in preference to getting things done, and the principal goal of the regimes they served was precisely stability, continuity and the absence of change. On at least two counts the acculturated model of state organization in such nations in mechanist, bureaucratic and profoundly ill-suited to the needs of effective intelligence and its support to policy. To add the need to adopt flexible, collegial, network-oriented management structures in order to cope with the 21st century information space and the operational and analytical environments it entails on makes the task more challenging despite its urgency.

In some respects, democratization itself provides some basis for the necessary shift. Maintaining continuous effective government and policy-delivery in the face of regular, even frequent changes of incumbents at the top level of political authority makes on-going effectiveness in getting things done an absolute necessity. The development of a permanent, politically independent civil service also favors continuous instrumental effectiveness. While such a civil service might appear detached from political accountability, frequent changes of personnel at multiple echelons (such as those endured in the US system every election or two) push senior administrators towards acting as an armature of control entrenching new leaderships' authority. Ultimately, however, effective organization transformation in intelligence as elsewhere depends on upon effective organizational choices about the shape such transformation must entail. And on the possibility of such choice, as I have argued, the jury is still out. But if the neoinstitutionalists have a more accurate view of collective decision-making and organizational design than the contingency theorists, then perhaps for would-be reformers and transformers to be forewarned of the pitfalls of organizational choice will to be to some degree forearmed.

References

[1] G. Stiglitz, *Globalization and its Discontents* (New York: W. W. Norton, 2002).

[2] Development, Concepts and Doctrine Centre (DCDC), *JDP 04 Understanding* (Shrivenham, UK: DCDC, 2010); K. Grint, "Wicked Problems and Clumsy Solutions", *Clinical Leader* 1, 2 December 2008.

[3] E.g. R. Wohlstetter, *Pearl Harbor: Warning and Decision* (Stanford, CA: Stanford University Press, 1962).

[4] H. Wilsenky, *Organizational Intelligence: Knowledge and Policy in Government and Industry* (New York: Basic Books, 1967).

[5] US Congress, House of Representatives, 94th Congress, 2nd Session, Select Committee to Study Governmental Operations with respect to Intelligence Activities, *Foreign and Military Intelligence, Final Report (The "Church Committee Report"),* 26 April 1976.
[6] F.H. Hinsley, *et al.*, *British Intelligence in the Second World War* (London: HMSO, 1979, 1981, 1984, 1988, 1990, 1990), 5 volumes.
[7] P.H.J. Davies, "Organisational Politics and Britain's Intelligence Producer-Consumer Interface", *Intelligence and National Security,* Vol. 10, No. 4, 1995; A. Zegart, F*lawed by Design: The Evolution of the CIA, JCS, and NSC* (Stanford, CA: Stanford University Press, 1999).
[8] E.g. G. Allison, *Essence of Decision: Exploring the Cuban Missile Crisis* (New York: HarperCollins, 1971).
[9] See, e.g. R. Rhodes and P. Dunleavy (eds.), *Prime Minister, Cabinet and Core Executive* (London: Macmillan, 1997); M. Smith, *The Core Executive in Britain* (London: Palgrave Macmillan, 1995).
[10] Richard Cyert and James March, *A Behavioral Theory of the Firm* (Oxford: Blackwell, 1963).
[11] Oliver Williamson, *Markets and Hierarchies: Analysis and Antitrust Implications* (New York: The Free Press, 1975).
[12] H. Demsetz, "The Theory of the Firm Revisited", in O. E. Williamson and S. G. Winter (eds.) *The Nature of the Firm: Origins, Evolution and Development* (Oxford: Oxford University Press, 1993), pp. 159–178; H. Demsetz, and A. Alchian, "Production, Information Costs and Economic Organisation", in Harold Demsetz (ed.) *Ownership, Control and the Firm: The Organisation of Economic Activity*, Vol. 1 (Oxford: Basil Blackwell, 1988), pp. 1–30.
[13] T. Burns and G.M. Stalker, *The Management of Innovation* (London: Tavistock, 1961); P. Lawrence, and J.W. Lorsch, *Organization and Environment: Managing Differentiation and Integration* (Cambridge, MA: Division of Research, Graduate School of Business Administration, Harvard University, 1967); J.W. Lorsch and S. Allen, *Managing Diversity and Interdependence: An Organisational Study of Multidivisional Businesses* (Boston: Harvard University, Graduate School of Business Administration, 1973).
[14] E.g. S. Clegg and D. Dunkerly, *Organization, Class and Control* (London: Routlege and Keegan Paul, 1980); D.L. Morgan, *Focus groups as qualitative research* (London: Sage, 1988), pp. 141-198, 273-320.
[15] See, e.g. D.C. Pitt and B.C. Smith, *Government Departments: an Organizational Perspective* (London: Routlege, 1981).
[16] J.W. Meyer, "The Effects of Education as an Institution", *American Journal of Sociology*, No. 83, 1977; J.W. Meyer and B. Rowan "Institutionalized Organizations: Formal Structure as Myth and Ceremony", *American Journal of Sociology,* No. 83, 1977.
[17] W. Powell and P. DiMaggio, *New Institutionalism in Organizational Analysis* (Chicago: University of Chicago Press, 1991), p. 11.

[18] J.G. March and J.P. Olsen, *Ambiguity and Choice in Organisations (*Oslo: Universitetforlaget, 1976); J.G. March and J.P. Olsen, *Rediscovering Institutions* (New York: The Free Press, 1989).
[19] Burns and Stalker, *The Management of Innovation;* Lawrence and Lorsch, *Organization and Environment*.
[20] Kenneth Knight, "Introduction: The Compromise Organisation", in Kenneth Knight (ed.), *Matrix Management* (New York: Pbi, 1977); Lorsch and Allen, *Managing Diversity and Interdependence*.
[21] M. Weber, *Economy and Society* (London: University of California Press, 1978), translated by Guenther Ross and Claus Wittich, pp. 277-278; for a detailed discussion of this duality see P.H.J. Davies, *MI6 and the Machinery of Spying* (London: Frank Cass, 2004b), pp. 321-325; P.H.J. Davies, *Intelligence and Government in Britain and the United States* (Santa Barbara, CA: Praeger Security International, 2012), pp.75-97.
[22] M.T. Hannah and J.H. Freeman, "The Population Ecology of Organizations", *American Journal of Sociology* Vol. 82, No. 5, March 1977.
[23] See, e.g. John Child, *Organization: A Guide to Problems and Practice* (London: Paul Chapman, 1988).
[24] Child, *Organization: A Guide to Problems*.
[25] I am indebted to my former Reading colleague Dr. Bill Poole for this notion.
[26] P.H.J. Davies, "Intelligence Culture and Intelligence Failure in Britain and the United States", *Cambridge Review of International Affairs*, Vol. 17, No.3, October 2004a); P.H.J. Davies, *MI6 and the Machinery of Spying;* P.H.J. Davies, *Intelligence and Government*.
[27] Chris Grey and Andrew Sturdy, "A Chaos That Worked: Organizing Bletchley Park", *Public Policy and Administration,* Vol. 25, No. 1, January 2010.
[28] Sir David Pepper, "The Business of Sigint: The Role of Modern Management in the Transformation of GCHQ", *Public Policy and Administration,* Vol. 25, No. 1, January 2010.
[29] W. Bedell Smith , "Report by the Director of Central Intelligence," TS #63459, April 23, 1952, reproduced in Michael Warner (ed.), *CIA Cold War Records: The CIA under Harry Truman* (Washington, DC: Center for the Study of Intelligence, 1994), p.462.
[30] Davies, *Intelligence and Government,* Vol.1, 2012, p. 9.
[31] See, for example, G. Ahrne and N. Brunsson, "Organizations and Meta-Organizations", *Scandinavian Journal of Management,* No. 21, 2005.
[32] Davies, "Intelligence Culture and Intelligence Failure"; Davies, *Intelligence and Government*.

Adaptation of Intelligence and Security Services to Contemporary Challenges

Rada LESIDRENSKA[*]
Vessela BANCHEVA[*]

Abstract

Dynamism and unpredictability mark the security threats and challenges we face today. Information technologies rapidly develop, being disseminated even faster, often falling into "the wrong hands" – those of terrorists and cyber criminals. Taking advantage of the innumerable opportunities of the global information infrastructure, they communicate freely, sharing information on tactical issues and targets. Under the circumstances, the intelligence and security agencies are compelled to operate even faster – not in reaction, but rather in pre-emption. Therefore, more than ever they need to reinforce the cooperative attitude among agencies, and to analyze information, originating from all possible sources – clandestine or publicly accessible. Opening of intelligence and security services to the civic sector, as well as OSINT become increasingly important, though not to the detriment of HUMINT and the specific means and resources of the intelligence job. A thorough enhancement of national intelligence capabilities and of strategic analysis is needed to meet today's security requirements.

Instead of a Foreword. An Overview of the Security Challenges. Implications for the Special Services

Unpredictability of today's security challenges and the constant emergence of new threats put to the test the capacity of intelligence and security services to accommodate to the incessantly changing security environment. The dynamism of the insecurity generating processes is a challenge by itself. "Fluidity" and "uneasiness" of the security environment derive from the information revolution and globalization, for the latter feeds the emergence of new sources of conflict and fosters transnational character of threats (e.g. the Arab Spring, the global economic crisis, etc.). The emergence of new threats adds constantly to the existence of traditional ones (proliferation of WMD, terrorism, interstate conflicts, etc.). Cyber threat, which is among the most topical threats, is a direct

[*] Intelligence expert, Republic of Bulgaria
[*] Intelligence expert, Republic of Bulgaria

consequence of the development of the global information infrastructure, as well as of the enhanced cyber capabilities of the state and non-state NATO and EU adversaries.

Therefore, intelligence and security services experience certain implications, with their tasks growing in number and difficulty, on the backdrop of an increasingly limited time for reaction or prevention. Early identification and analysis of problems, even before their actual manifestation, is crucial in combating today's security threats. That is one of the major challenges in the work of the special agencies, whose analyses and assessments attract on increasing number of customers – both domestic and foreign. The growing demand of intelligence expertise is illustrative for the mounting importance of intelligence and security services in the decision making process. At the same time, collection of intelligence, necessary to draft assessments and analyses for the needs of state leadership, is becoming an increasingly more arduous and risky enterprise. The protection of information security is another challenge of growing concern. Global information infrastructure, the boom of social media and the cheap and easy access to information technologies reduce the capacity of decision making bodies to rein and control information, thus giving state and non-state adversary factors huge advantages.

How Do Intelligence and Security Services Adapt to Today's Challenges?

- **Opening of the Services to the Civic Sector**

In the aftermath of 9/11, intelligence and security agencies initiated a process of opening to civic sector. Renouncing traditional isolation is imperative, on the background of the increased number, kinds and intensity of security challenges.

The opening process is **two-faceted**. On the first place, intelligence begins to **demystify before society,** unveiling its "human face". Why is that necessary? The challenges and threats have reached such a magnitude and intensity, that agencies are increasingly aware that they could not handle them without the back-up of society. What is indispensable, is to win the credibility of the populace (tax payers), by way of a higher degree of transparency and

accountability in the agencies' work. Ensuring transparency departs from legislation, which is to explicitly regulate the role and responsibilities of a given agency, as well as the ways to exercise democratic public oversight on its activities. Society is to be convinced that clandestine activity, inherent to all intelligence and security agencies, is not misused for the purpose of concealing publicly important information or for achieving goals contrary to morality or law. The more informed society is, the better it is expected to perceive the particularity of the intelligence profession, including its natural secrecy drive, based on its sensitive activities.

In democratic societies the agencies' departure from the previous "capsule" by way of a dialogue with the civic sector, is a relatively new philosophy, giving way to the comprehension of both sides that combat against security challenges is a common one – it is not reserved to intelligence and security services alone.

Here, we touch upon the second aspect of opening. The services' demythologization and demystification in front of society through achieving unprecedented transparency in their work, creates prerequisites for initiation and maintenance of reinforced **cooperation of the services with the non-governmental and private sectors** in the common battle against contemporary challenges. Seeking to enhance their capabilities, the agencies increasingly open to the assistance of external experts from the academic community, the non-governmental and the private sectors – experts on information technologies and cyber security, mathematicians, chemists, biotechnologists, energy specialists, etc. In turn, civic sector demonstrates positive attitude towards the opening of the services, indicative of which is its readiness to join different initiatives as conferences, workshops and other projects, organized jointly with the security sector. The purpose is to achieve maximum efficiency in the combat against contemporary challenges, applying comprehensive interdisciplinary approach, stepping both on national and international expertise. Gathering on the same venue experts of different nationalities and diverse scientific and corporate experience for the accomplishment of short or long term projects on particular national security topics, is becoming increasingly common practice in the work of intelligence agencies. The benefits of the

synergic approach in the combat against contemporary and emerging security challenges are beyond discussion. Participation in such events usually preserves the interest in further continuing the professional dialogue. Thus, unclassified multinational and multidisciplinary communities and even networks (including blogs) are created under the organizational auspices of the respective agencies. It is this reason, for example, why in Bulgaria the so called Sofia Security Forum was established. Opening to civic sector, which in substance means reinforced use of open sources of information, allows the collection of a maximum number of viewpoints and reduces the possibilities of omissions in "assembling together the intelligence puzzle". It also enables the use of a common professional terminology, reflecting the common understanding of concepts and ideas. The more we experiment with partners beyond the intelligence community, the easier we arrive to the ways of adapting to security challenges. It is important to intelligence agencies to draw on the experience of civic sector and to adopt its best practices. Moreover, non-intelligence experts readily procure their expertise, attracted by the opportunity of an equal performance shoulder-to-shoulder with the intelligence experts, representing the government[1]. The idea is to create a culture of cooperation, in order to provide decision makers with the best possible analysis.

The formation of joint expert teams at national or international level for the purpose of resolving a particular problem is a flexible formula to face emerging challenges without reallocation of resources within the intelligence community. Virtually, that is a financially effective way to reinforce expertise. In that manner under the conditions of a global economic downturn the intelligence costs are optimized, rather than cut down.

- **The Importance of OSINT**

All of the above is indicative of the growing significance **of open sources intelligence (OSINT)**. Such a category of sources are not just the news media and the specialized periodicals and books, but also the experts working outside the intelligence community with their "tacit knowledge"[2]. Nowadays intelligence agencies have better opportunities to obtain valuable expertise from

the academia, the private and the non-governmental sector, as compared to the time prior to the information revolution. Free access to all kinds of data has brought about a quantitative and qualitative reinforcement of the analytic potential outside the intelligence community. Practically, information revolution has led to a "privatization" of expertise – many companies offer high quality analyses (e.g. risk analyses), which sometimes overrides the intelligence assessments of state agencies[3]. For that reason the informal/non-state analytic/think-tank centers cope to successfully compete for the attention of decision makers. A number of academic institutes and companies dispose of a valuable expertise, based on processing open and generally accessible sources. That has made intelligence and security services place greater emphasis on open sources, with the role of the latter being irrefutable in the course of elaboration of quality strategic analyses. Non-clandestine sources of information are crucial in studying the politics, economy, culture, demography and history of a society, state or region. Some of the newest sources of open information are social networks, though their reliability is far from always uncontestable, based on the possibilities for anonymous expression.

Today the role of open sources in elaborating strategic all-sources analyses is beyond doubt. The bulk of intelligence assessments is based on OSINT, without downplaying the information collected through the specific clandestine methods and means of intelligence agencies. At the same time analysis, based entirely on open sources, acquires its own importance along with the analysis, based on all types of sources, including open.

- **The Significance of Services' Own Strategic and Operational Analysis – Need to Enhance the National Intelligence Capacity**

An important aspect of adaptation of intelligence agencies towards today's challenges is the need to reinforce not only their connections with non-intelligence expertise but also their **own operational and analytic potential**.

Mastering rare languages like Arabic, Persian, Urdu, etc, as well as having deep knowledge on local (tribal) cultures in the regions

of intelligence interest is becoming increasingly important. Successful operational (terrain) work on countries like Afghanistan, Pakistan, Iran and Iraq is hardly possible without having a personnel mastering of the respective rare languages. Relying on local interpreters and translators is a precarious and virtually inefficient enterprise. Contacts with the local population have become indispensable for collecting intelligence in the "flash points". In other words on the backdrop of today's security challenges the so called **HUMINT** retains its significance. Collecting intelligence from human sources in crisis regions is a challenge by itself, requiring high level of staff preparation, and therefore considerable investment on the part of agencies. Infiltrating or approaching terrorist and organized criminal groups is impossible without taking into account the role of human factor.

The creation and maintenance of a strong analytic core with comprehensive knowledge on the respective intelligence topics (which does not preclude the specialization in particular areas) is another priority of modern agencies. The activities in the **Headquarters (Center),** especially the processing of open sources (e. g. Islamist sites) also requires high levels of language, cultural and other knowledge. **Strategic intelligence analysis,** based on in-depth and comprehensive knowledge of the respective countries, regions, movements, non-state and other subjects, challenging the security of the international democratic community, is becoming more and more important. The formation of a strong expert and analytic potential is to be accompanied by the application of the latest IT novelties, of modern analytic technologies, including mathematic models and simulations, allowing early grasp of emerging negative trends. On the background of the dynamic and increasing challenges it is necessary that we are well aware of the capacities of our adversaries not just in quantitative terms. It is important that we dispose of information on subjective factors[4] as well, predetermining hostile behavior.

Tactical/operative intelligence analysis is to step backward to the benefit of the strategic one, which allows "scanning the future" for new threats. The idea is to avoid unpleasant surprises by way of permanent adaptation of the intelligence capabilities towards the dynamically changing security environment.

- **Reinforced Interagency Collaboration at National and International Level. "The Need to Know" vs. "The Need to Share" Philosophy**

  - *At national level*

Common security challenges and the need of a common response to them suppose close cooperation among security services themselves both at national and international level.

After 9/11 the "need to know" principle has gradually been displaced by the "need to share" concept. Nowadays, the latter is gearing up, leaving behind the inherent rivalries among the representatives of the intelligence communities of all countries. The major purpose is to improve the capabilities, necessary to preempt and surmount new challenges, by way of transforming the national intelligence community in a **single integrated mechanism**. This is the way that decision making bodies receive valued and comprehensive intelligence product, instead of separate and often overlapping fragments of the general picture of the state of security. It is important that a common platform for routine exchange of expertise and knowledge among analysts and intelligence officials be set up. Within the dynamic insecurity environment the representatives of the intelligence community are to exchange timely and accurate information. Certainly, information sharing is to be done under rules and regulations, allowing the protection of the following: **1.** the sources and sensitive information against unauthorized access; **2.** the information infrastructure against its compromising, damage or destruction as a result of a cyber attack, omission or negligence; and **3.** the right to personal life and civic liberties[5]. A balance should be established between the need to share information and the risk of its unauthorized dissemination. Reinforced cooperation is based on mutual trust, which in turn depends on due management of the risk, posed by unauthorized access. Active interaction implies good knowledge of the protection of information practices of the respective partner, as well as availability of uniform standards in the area of protection of information.

As far as **coordination** is concerned – it could be carried out in different ways. In some countries a **standing central body** is responsible for the efficient interaction among services. In this way each body or institution belonging to the intelligence community is well aware of its exact place in the system, the latter not allowing non-coordination, randomness or rivalry among its composite elements. It is that logic on which the new NATO intelligence architecture is based on, with its NATO Steering Board being the major coordination entity. The Board assigns the tasks, drafts the summaries of the results and makes sure that overlapping in the process of elaboration of the final product be avoided.

The work on ***ad hoc* intelligence assessments or in the framework of standing joint units** allows unification of efforts and their orientation in one and the same direction. This is the way to have better quality of tasks accomplishment, by way of avoiding chaotic and indiscriminate "flooding" with overlapping or colliding intelligence assessments, worked out by different agencies. It is essential to decision makers to be provided with analyses agreed upon in advance, with all points of view presented. It is to note also that such coordination allows better quality of the final output, based on a more efficient utilization of the financial and personnel resources. In the Bulgarian context the draft Law on the National Security provides for the establishment of a Coordination and Analysis Center, as well as of a Crisis Center.

Another coordination mechanism is ensured through an **exchange of liaison officers or through special units**, in charge of the cooperation with partners. Maintaining regular, even **daily work contacts at an expert or higher level** is another prerequisite for the smooth functioning of the national intelligence community.

In most democratic countries intelligence and security agencies are not entitled to work on the territory of their own country. Therefore, they are to cooperate with other security and law enforcement agencies – police, military staff, gendarmerie, border control and customs services. The domestic manifestations of transnational challenges, like international terrorism and organized crime, make such an interaction an absolute must[6].

In many countries **joint analytic centers and data bases** are established for the purpose of reinforced cooperation and coordination at national level – e.g. for combating terrorism or cyber crime, facilitating information sharing among the numerable security services.

- *At international level*

Nowadays' insecurity environment places the emphasis on the need of enhanced cooperation at international level as well – **both within bilateral and multilateral format**.

Like in cooperation at national level, here the main objective is to facilitate the elaboration of all-sources analyses. Another advantage is the opportunity to obtain information on a region or country in which the respective agency does not dispose of intelligence coverage, in exchange of its expertise on alternative issues. The mutual complementarity of intelligence expertise is a way to provide state leadership with the necessary information, while saving at the same time considerable resources. The main problem here is that big intelligence agencies are not always willing to share intelligence with their smaller counterparts, as the former obtain much less information in the course. Nonetheless, information sharing at bilateral and multilateral level is an irrefutable necessity, as the agencies having more limited capabilities aspire to compensate for that liability with assets in alternative areas – e.g. with expertise on regions to which big agencies lack access or with knowledge in rare languages and cultures, etc. Interagency collaboration may prove to be of key importance not only because of the opportunities for exchange of assessments and data, but also for exchange of valuable experience in other activities.

Consolidating all-sources information, including intelligence, obtained in the framework of international cooperation, has certain setbacks as well. There is a risk of information over-saturation of the analytic units and thus of omission of vital information for forthcoming terror attacks[7].

Beneficial cooperation, whose main purpose is to create mutually complementary intelligence capabilities, implies the edification of a respective interoperability among partners. The existing asymmetry in the technical and technological standards between the bigger and the smaller intelligence agencies is normally overcome through rendering assistance to the services, disposing of less resources.

Conclusions

The complex character of the security challenges requires a complex approach in the combat against them. The requirements for the quality of intelligence capacities are increasingly higher. That implies *inter alia* the combined usage of the information obtained by way of HUMINT, SIGINT, IMINT and OSINT, as well as the application of contemporary analytic methodologies.

The edification of a well integrated intelligence community at national and, why not, at international level is the main leitmotif of the effort to counteract contemporary challenges. The key words are: single intelligence architecture, guaranteeing high level of coordination and facilitated capacities for information sharing.

References

[1] Roger Z. George, "Meeting 21st Century Transnational Challenges: Building Global Intelligence Paradigm", *Studies in Intelligence*, Vol. 51, No. 3, 2007, p. 10.
[2] *Ibid.*, p. 4.
[3] Geneva Centre for the Democratic Control of Armed Forces (DCAF), Security Sector Reform Working Group, *Contemporary Challenges for the Intelligence Community* (Geneva: DCAF, 2006), p. 3.
[4] AFCEA Intelligence Committee, *The Intelligence Community New Challenges, Sources and Methods*, White Paper, Oct. 2009.
[5] US Intelligence Community, *Information Sharing Strategy*, 22 Feb. 2008, p.7.
[6] DCAF, *Contemporary Challenges*, p. 4.
[7] Center for Security Studies, "Intelligence Agencies: Adapting to New Threats", *CSS Analysis in Security Policy*, No 82, Oct. 2010, p. 2.

Resilience – The X Factor of the Organizational Endurance

Cristina IVAN*

Abstract

The current paper aims to outline a potential model for building and enforcing collective resilience in organizations such as intelligence services creating a balance between the necessity to obey orders and the necessity to flexibly adapt to change and efficiently address adversity creates the need for forward thinking and collective empowering. It is the reason why, suggested interventions are designed to function in a continuous practice of resilience development, within the framework of a sociological – ecological system, as advanced by theoreticians of resilience such as Michael Ungar, Ann Masten or Hellen J. Boon.

Motto:
"The positive social science of the 21st century will have as a useful side effect the possibility of prevention of the serious mental illnesses... But it will have as its direct effect a scientific understanding of the practice of civic virtue and of the pursuit of the best things in life" (my emphasis).
Martin E. P. Seligman, President, American Psychological Association

Introduction

As early as the 1960's, the open systems theories applied to organizational behavior broadened the framework in which **employee satisfaction and development** were tackled with. As these two factors gained in importance, so did the idea that any organization is in fact an open system, – that is, to quote two reputed theorists like Wagner and Hollenbeck, "*a unified structure of interrelated subsystems, subject to the influence of the surrounding environment*"[1]. This central tenet of the open systems approach focused on the issues of **interaction** and **adaptive resistance** (later on resilience) and their role in creating the formula for successful organizations. Almost fifty years later now, we can add that it was then that a new perspective occurred. **One in which survival and growth of an organization was intrinsically made dependent on the capacity of its subsystems to adapt to the outer environment change**. Adaptation meant that a system was no longer seen as self-sufficient and autonomous.

* Researcher, National Institute for Intelligence Studies, "Mihai Viteazul", National Intelligence Academy

But that was not the only change emerged with the new concept of open systems. Adaptation also meant that time efficient procedures and their implementation within a system/organisation had to be complemented by actions meant to consolidate group members capacity to respond to adversity and transgress procedures whenever the outer environment change required it. It therefore also meant finding ways to encourage the individual and group welcoming of a more volatile, and swiftly changing epistemological paradigm. In other words, of a narrative in which changing, performing multiple roles and tasks, taking risks and stepping into the unknown had to be accommodated as positive triggers.

It was only natural then, in the 1980's and 90's, when psychologists began to focus less on the negative and pathological and more on human strengths and potential, that **survival** and **resilience** of **collective systems** came once again into the spotlight, this time as a corollary of individual/community positive psychology. It was then that an interesting cross-fertilization occurred and findings of positive psychology began to be used as a pool from which solutions could be phished out and tailored to produce **increasing incidence and prevalence of agency, positive thinking and endurance at collective level within an organization.**

In Seligman and Csikzentmihalyi's words[2], positive psychological results – that is the results of the mental and emotional processes studied by positive psychology - could be described at three distinct levels:

- **the intrapsychic level**, as well being, contentment, and satisfaction; hope and optimism; flow and happiness;
- **the individual level,** as the capacity for love and vocation, courage, intrapersonal skill, aesthetic sensibility, perseverance, forgiveness, originality, future-mindedness, spirituality, high talent and wisdom;
- **the interpersonal (group) level** *as civic virtues and the institutions that move individuals towards better citizenship* – **responsibility, nurturance, altruism, civility, moderation, tolerance and work ethic (my emphasis)**.

Of all features cited in the three levels under discussion, when dealing with **organizational behavior we must obviously focus on the interpersonal group level**, the one in which **interactions between groups at large and individual group**

members in particular create those models and patterns of behavior that account for multiplication and replication of civic virtues, better citizenship and work ethic. That is not to say of course that intra-psychic or individual level operations are not relevant. Their role is fundamental as they lay the foundation for resilient behavior and successful negotiation of adversity at individual level. Yet, for the purpose of the current paper, which is not the individual but the group, or, to be more exact, organizational membership to intelligence services, **focus shall be placed on those factors, processes and patterns that lead to collective resilience and their importance in building an adaptive model of collective successful endurance**.

Can a Human Development Model Designed in the Open System Paradigm Be Fit for Intelligence Services?

To this question we will answer by first taking a short loop. Let us remember that growth, mastery, insight, drive and positive self-perception developed out of painful events and adverse circumstances have also been the focus of human developmentalists and positive psychology advocates for more than three decades now. And that while most research focused on individual traits and temperament that make such desirable results of adversity possible, some thinkers, increasingly many, under the influence of the open system theories mentioned before, have chosen a more contextualized understanding. Without contesting the utmost importance of individual traits as assets which increase chances of individuals to successfully negotiate stressful situations and perform, they have gone further. That is to say they chose to change perspective and focus by contrast on the effects of **interactions and relations created between individual features and the environment**. **By taking this approach, environmentalist and later on ecologist thinkers managed to integrate social, physical, climate and economic triggers and factors into the framework of resilience construction**.

A breakthrough analysis of resilience as the result of a not only individual assets and traits at work, but rather as that of a complex navigation of the individual through chances provided by society is offered by Michael Ungar[3]. This researcher and thinker has placed the finger on the **adequacy, meaningfulness and quality of the opportunities and resources** offered by the environment to individuals at risk as **the most influential factor** in predicting

and encouraging resilience and positive development. He defines this new understanding of resilience as **interactional and ecological**, stating that "*resilience results from a cluster of ecological factors that predict positive human development (more than individual traits), and that the effect of an individual's capacity to cope and the resources he or she has is influenced by the nature of the challenges the individual faces*"[4]. To put it more bluntly, that is to say that resilience cannot emerge in the absence of **quality, tailored resources and opportunities**, made available to individuals before, during and after their confrontation with a specific challenge. What Ungar does in fact is to enlarge the overall picture to include opportunities offered by social ecology and their impact on triggering positive development processes. These positive processes in their turn are shown to lead to the formation and manifestation of behaviours, cognitions and their narratives, all generating resilience.

But why and how would that be relevant to the formation of successful and resilient individuals functioning well in organizations subjected to high levels of stress, as an intelligence service inherently is?

First of all, let's look at the why's! Why is social ecology generating resilience relevant to the current contextual transformations within intelligence services?

It is a fact that intelligence services today, so much more than their predecessors, must respond to a growing demand for fast responses to global interacting patterns of risk. Fundamental activities such as collecting intelligence, processing data and building knowledge by connecting the dots and narrowing blank spaces on rapidly changing operational contexts have become increasingly challenging. And so is the task of disseminating information to relevant bodies on time and without risking jeopardizing operational interests. But this reality may sometimes contrast severely with the type of behavioral patterns generated by the classical, military type, strictly hierarchical organization, which tends to generate and encourage conformity, discipline and a procedural modus operandi directed from superior hierarchical level. And while these may be traits successfully insuring military performance, they are at the same time likely to block creative, adaptive and outside the box responses to unforeseen stress factors and undrilled crisis situations. They are also likely to discourage individual assertiveness and role-model generation at informal level. Therefore, one could argue, there might by appropriate to promote, at least in specific areas of activity where stress and crisis are most likely to emerge with high frequency, an adaptive model of (collective) successful endurance fit for the well functioning of an open system.

General Laws for a Socio-ecological Framework Generating Resilience

In order to attempt creating an ecological framework generating and enforcing resilience, let us first remember what resilience is today generally perceived to be: the capacity of the individual or group to recover or come up whole and functional, perhaps more spiritually, mentally and emotionally enriched, after having been exposed to chronic or acute stress or trauma. Creating a so called invulnerability or high resistance to later trauma is also a goal shared by all resilience thinkers designing models of intervention[5].

Coming to the idea of **intervention**, it must be stated first that focusing on the persons exposed and addressing their individual needs has been reported as a highly successful preventive and/or reparatory method across the world. Then, the open systems theory created room for alternative and complementary approaches. Interventions at collective level were shown to strengthen community/group resistance and, we would add, by implication, organizational endurance. Then, ecological approaches introduced a new type of intervention: that aimed to increase and support the high capacity of the individual **to navigate** through opportunities made available, **negotiate for them** and finally **acquire the most likely to offer benefit** in increasing resilience.

But how can that be done? Is it something depending on the individual or rather on the solutions provided by the system? These are the main question this chapter aims to address. In approaching them, we would like to take as illustrative example cited by Ungar in his work[6]. It refers to a research documented by members of the Conduct Problems Prevention Research Group. Research was based on a survey of 10,000 kindergarten children from four high-risk neighborhoods in Canada. In the survey, 891 children were identified as being at risk for future conduct problems and were therefore randomly assigned to interventions in control groups across a ten years span. Interventions included parent behaviour management training, child social cognitive skills training, reading support, home visiting, mentoring etc. Results have shown most relevant positive results (1) in children with the highest level of risk (2) to whom services were provided most constantly and with high intensity.

There are four main conclusions of interest to the current topic we can extract from Ungar's detailed analysis:

- First, that individuals **at highest risk level benefit the most** from interventions, their path in life being the one most impacted in terms of positive development.
- Secondly, that **the wider the choice of interventions, the better the result**.
- Thirdly, that **intensity and repetition** with which interventions are applied also **maters greatly**.
- Fourthly, that what such interventions do is **not** to annihilate the potential for failure and disorder but rather **to offer alternative channels of development and manifestation which greatly lowers the likelihood negative traits get to be expressed**.

As a side note, we can add that convergent findings of field studies carried out in Canada or Australia have been highlighted by Masten Ann S.[7] or Boon Helen J.[8].

The obvious next question is: Can we translate findings of studies applied on children and youth into organizational practices fit for employed adults? Is it necessary and possibly to do so? First of all let's take a look at necessity. Studies in resilient behavior in middle aged adults and old people show that the level of resilience varies not only across various people but also in the life span of the same individual[9]. Drawing on conclusions of Laub and Sampson, 2003, Schoon, 2006, Werner and Smith, 1992, Ungar states: "*as longitudinal studies of resilience show, these patterns of behaviour are temporal, changing over time as new horizontal stressors (normative developmental challenges that occur over the lifespan) and vertical stressors (acute or chronic challenges that transect the developmental life course and negatively skew growth) influence the individual's capacity to cope and the resources available*".

Therefore, we can infer, as a logical consequence, **continuity** in providing and encouraging access to interventions consolidating resilience is likely to increase the level of positive and continuous adaptation when confronting with adverse situations (stress, trauma, etc.). It has to be noted though that for a model of continuous consolidation of resilience to be successful, **it must act on multiple levels, be carried out across a long time span and yet avoid generating routinized perceptions and irrelevance.**

Argument for a Continuous Practice of Resilience Development

In order to be able to draw a model of continuous practice of resilience development, let us first dwell on the conditions that make resilience emergence and consolidation possible, as outlined by Ungar. These conditions can be resumed as a synergic fusion of **opportunity** and **meaning**.

- First of all, opportunities for resilience building must be available and accessible to individuals at risk.
- Secondly, they must be built so as to attract interest from individuals at risk, who must perceive them at the same time as relevant and accessible or attainable.
- Last but not least, in order to generate positive proactive behavior, these models should accommodate the right meaning. Because meaning is the element that determines individuals value opportunities as desirable and effective.

From studies of narratology, we learn that **meaning** is culturally created and embedded, through narratives, in their turn used to legitimize normative behavior. Baker for example, drawing on the social theory work of Sommer and Gibson[10], defines **narratives as the principal and inescapable mode by which we experience the world.** Narratives, in Baker's view, "*are public and personal 'stories' that we subscribe to and that guide our behaviour. They are the stories we tell ourselves, not just those we explicitly tell other people, about the world(s) we live in. It also follows from this that a narrative, in the social theory sense, is not necessarily traceable to one specific stretch of text but is more likely to underpin a whole range of texts an discourses without necessarily being fully or explicitly articulated in any one of them*"[11].

Going back to the construction of resilience building strategies, let us reiterate that their efficiency depends not only on how opportunity is successfully structured as available and attainable but also – and that is going to be our next topic of discussion – on meaning systems.

Meaning systems greatly depend on narratives, be them, in Baker's categorization[12], **ontological** (personal stories we tell ourselves about our place in the world), **public** (stories elaborated by and circulating among social and institutional formations larger than

the individual, such as the family, religious or educational institution, the media, and the nation etc.) and **conceptual** (narratives developed by scholars to define the framework of a discipline).

Relevant for our topic of discussion will therefore be to identify and employ ontological and public narratives in the making and continuous enforcement of resilience patterns at organizational level. And in order to be able to create a framework in which efficient strategies could be developed and implemented, let us first acknowledge that, as the current paper has already illustrated, **the concept of resilience transcends the boundaries of distinct academic disciplines, such as sociology, positive psychology, narratology etc. and requires an approach based on interdisciplinary inquiry.** As a direct consequence, **solutions and programmes designed to create and consolidate resilience must, in their turn, have an interdisciplinary character**. They must be able to accommodate multiple level interventions into a coherent pattern. Because resilience is in its turn a multidimensional concept, integrating **cognitive** aspects (how we understand and attribute value), **transactional** aspects (how we negotiate our position in the face of adversity), **behavioural** (how much we persist in positive behavior when confronted with adversity), **motivational** (how clear and persistent is our sense of purpose and our focus on attaining it), **existential** or **spiritual** (how we answer the big questions of life), **relational** (how much we draw strength from the support of other) and last but not least **emotional** (how we anchor when we feel devastated and lost) - according to the taxonomy of resilience outlined by Wong Paul, T. P. & Wong Lilian C. J.[13].

With these criteria of necessity in mind let us then attempt to illustrate how such a model of resilience building for intelligence services could be imagined, mapped and implemented....

Towards a Practical Model of Collective Resilience Consolidation for Intelligence Services' Use

A potential resilience building model for intelligence services employees should be built, according to findings detailed in the previous chapter, **on a holistic and integrative approach**. Moreover, given the fact that adults create resilience mostly through cognitive processes, behavior training and existential/spiritual

mapping of the self, it is our belief that a successful intervention model could and should be based on a meaning centered approach developed via narrative techniques and cognitive skills development.

Another idea that must be taken into account is that of the predictable mindframe of an intelligence service employee. Diversity cannot and should not be resumed to schematic oversimplification. Nevertheless, there is one element we can predict, based on the same approach developed by Wong[14], who makes the distinction between a meaning mindset and a happiness mindset. In Wong's view, "*for those individuals with a happiness mindset, the primary objective in life is to pursue whatever gives them optimal happiness, which may be money, power, fame, or pleasures. Thus, the happiness mindset may also be referred to as the success mindset. In contrast, for those individuals with a meaning mindset, the ultimate concern is to devote their lives* ***to pursue something meaningful and virtuous for the common good. Thus, the meaning mindset can also be referred to as virtue mindset*** *(our emphasis). The happiness mindset asks, "What can I get from life? How can I be happier?" whereas the meaning mindset asks, "What does life demand of me? How can I do more to make life better for others?*"

We find this distinction to be extremely relevant in building resilience interventions targeting intelligence services employees. Given the type of adversity they position themselves in and negotiate with, cognitive and narrative skills conferring essential meaning elements such as strength and moral virtue play an important role. That is not to say that happiness bearing significators are not important. We do **not** believe that the two mindsets described by Wong should be seen as completely apart from each other, but rather as interacting within the complexity of any individual. The distinction between them should be, in our opinion, understood as coming from the percentage of significance the individual attributes to one or the other. **But we believe authentic and enduring resilience to come from a synergic fusion of the two, balanced to form the frame of a whole being functioning in integration rather than separation. In other words, according to the laws of an open system.**

To resume, we propose a model of resilience building focused on generating (1) **cognitive competence** (learning how to think positively and resist negativity), (2) **transactional competence**

(learning coping and problem solving skills, ways to access ecological resources), and last but not least (3) **relational/emotional competence** (learning how to create and preserve secure attachment, bonds based on the same core of values with peer workers and collective group, creating means of anchoring the self in times when joined navigation through adversity is necessary).

And here intervenes the agency of the organization, which must in its role of core social environment and frame designer, insure the right instruments for the creation, consolidation and reinforcement of above-mentioned competences. **And again we arrive at the need for a multidimensional, long time span model encompassing interventions able to create and enforce individual cognitive skills, a set of core values shared by the group, cohesion, bonding and anchoring etc.**

Therefore, in our view, recommended levels of intervention should include:

- **The organizational level**. Here we should reflect on the importance of building, enforcing and adapting organizational culture and set of values to the type of challenges faced by employees. It is a given fact that culture prescribes both values and expectations. Therefore, **creating a PR strategy focused on the internal public demands for empowering and positive thinking might be part of the solution**. As already shown, a personal and public narrative promoting self-agency and proactive behavior is a powerful instrument.

Keeping track of master narratives (large social systems of meaning about the role of the state, national security, and role of law enforcement agencies) and negotiating institutional positioning within them is another important element in such a PR strategy.

- **The educational level**. Interventions on this level should also be conceptualized to work on multiple levels, being integrated not only in university and MA programmes but also in later vocational and managerial education.

Social cognitive skills and problem solving skills could be as a result made an integral part of training and coaching at university level. Later training programmes, be they devoted to vocational

or advanced professional practice, should include mentoring, optimal peer relationship development practices, strategies for work climate improvement, conflict resolution etc.

- Last but not least, we suggest inclusion in the model of an applied **workgroup module focused on group narrative creation sessions.** Such sessions could provide a useful **follow-up to skills learned during training, facilitating their contextualization to the challenges of each specific workplace and team.** It could foster development of peer bonds and facilitate work climate improvement.

- Last but not least, we assess involvement of employees in the creation of a e.g. virtual discursive space in which shared narratives facilitating agency (navigation, negotiation and acquisition of resilience) could also be a useful tool in the making of both group and individual strategies.

Instead of Conclusions

The above reflections on a potential model for building and enforcing collective resilience in organizations such as intelligence services should be regarded merely as a starting point to further work. The model as such could benefit greatly from sociological and psychological field research as well as educational input. Nevertheless, its utility stands in timing. As previously stated, it is a fact that intelligence services today, so much more than their predecessors, must respond to a growing demand for fast responses to global interacting patterns of risk. But fast responses to complex interacting problems do not come from fixed, strictly hierarchical built organizations. Organizational culture studies have proven this all to well. Military organizations in general promote strict subordination, learned behaviour, procedures and conformity. Therefore, more often than not, their employees lack the skills necessary in adapting and finding solutions to fast emerging threats and unforeseen patterns of adversity. It is then perhaps now the time to include in their development elements such as: partial autonomy, mobility in thinking, as well as resilience to unpredicted adversity. Creating a balance between the necessity to obey orders and the necessity to flexibly adapt to change and efficiently address adversity creates the need for forward thinking and collective empowering. The result remains to be seen...

References

[1] John A. Wagner and John R. Hollenbeck, *Organisational Behaviour, Securing Competitive Advantage* (New York: Routledge, 2010), p. 32.
[2] M.E.P. Seligman and M. Csikszentmihalyi, "Positive Psychology: An Introduction", *American Psychologist*, Vol. 55, 2000, pp. 5-14.
[3] Michael Ungar, "Social Ecologies and Their Contribution to Resilience", in Michael Ungar (ed.), *The Social Ecology of Resilience: A Handbook of Theory and Practice* (Springer Science and Business Media, LLC, 2012), p. 13.
[4] *Ibid.*, p. 14.
[5] Adapted after N. Garmezy, "The study of children at risk: New perspectives for develop- mental psychopathology", paper presented at the annual meeting of the American Psychological Association, New Orleans, Louisiana (1974, August); N. Garmezy, "Stress-resistant children: The search for protective factors", in J. E. Stevenson (ed.), *Recent research in developmental psychopathology: Journal of Child Psychology and Psychiatry Book Supplement 4 (*Oxford, England: Pergamon Press, 1985), pp. 213–233; E.E.Werner, "Research in Review", *Young Children*, Vol. 39, No. 9, 1984, pp. 15-26.
[6] Ungar, "Social Ecologies", pp. 15-16.
[7] Masten Ann S., "Ordinary Magic: Lessons for Research on Resilience in Human Development", *Education Canada*, Vol. 49, No. 3, available at www.cea-ace.ca, last accessed October 5th, 2012.
[8] Helen J. Boon, "Risk or Resilience? What makes a difference?", *The Australian Educational Researcher*, Vol. 35, No.1, April 2008, available on James Cook University official site http://eprints.jcu.edu.au/1958/
[9] M. Cantalbiano and N. Cantalbiano, "Resilience and Health Outcomes in the Elderly", in Linda Ryan and Marie L. Caltabiano, "Development of a New Resilience Scale: The Resilience in Midlife Scale (RIM Scale)", *CCSE Asian Social Science Journal*, Vol. 5, No.11, November 2009, p. 42. Available at www.ccsenet.org/journal.html. G. Wagnild and H. Young, "Development and Psychometric Evaluation of the Resilience Scale", in "Development of a New Resilience Scale: The Resilience in Midlife Scale (RIM Scale)", *CCSE Asian Social Science Journal*, Vol. 5, No.11, November 2009, available at www.ccsenet.org/journal.html, p. 40.
[10] Margaret R. Somers and Gloria D. Gibson, "Reclaiming the epistemological "Other", Constitution of Identity", in Craig Calhoun (ed.), *From Persons to Nations, The Social Constitution of Identities* (London: Basil Blackwell), pp. 37-99.
[11] Mona Baker, "Narratives in and of Translation", available at www.scribd.com, last accessed September 9th, 2012.
[12] *Ibid.*, pp. 5-6.
[13] Paul T.P. Wong and Lilian C.J. Wong, "Chapter 27 - A Meaning-Centered Approach to Building Youth Resilience", in Paul Wong (ed.), *The Human Quest for Meaning, Theories, Research and Aplications*, second edition (Routledge, 2012), pp. 592-593, available at http://www.DrPaulWong.com/documents/HQM2-chapter27.pdf, last accessed October 11th, 2012.
[14] *Ibid.*, p. 599.

The Five Architectures of Intelligence: Implications for a New Intelligence Curriculum

Chris PALLARIS*

Abstract

Intelligence work takes place across five architectures or domains: informational, organisational, operational, technological and cognitive. To be effective, intelligence services must educate their staff in the many disciplines that inform these architectures. Doing so requires a rethink of the education given to intelligence staff. As well as specialists and generalists, the intelligence community should look to cultivate holists, individuals who are as comfortable maintaining a database as they are generating an intelligence product or motivating their staff. Some tentative ideas are presented in support of this.

Introduction

Over the past three years, a number of EU funded projects have sought to improve the practice of intelligence analysis in Europe[1]. The first, VIRTUOSO, is intended to improve the technological state of the art by providing a platform for the seamless integration of different intelligence tools and technologies. The second, RECOBIA, is intended to examine the negative impacts of cognitive bias on intelligence professionals and propose possible solutions[2].

Both projects have brought the author in direct proximity with European intelligence professionals. While the methods used to gather their inputs (surveys, workshops, roundtable discussions, etc.) are far from scientific, the evidence collected suggests that some of the thorniest challenges confronting today's intelligence services have little to do with the business of collection or analysis[3]. Rather, they involve those dimensions of organisational life that are common to professionals everywhere.

A case in point: the management of intelligence professionals. For all the scorn that is heaped on it, management is the primary driver of operational effectiveness. It follows that improving the quality of middle and upper management should be the foremost priority of senior government officials. And yet, the number of programs or electives dedicated to the management of the intelligence enterprise remains worryingly limited. Not surprisingly, many analysts lament the lack of leadership, mentoring and feedback they believe necessary to their work.

* Director and Principal Consultant, I-intelligence

On the issue of policy and process, the evidence suggests that "best practices" in intelligence work are rarely or inconsistently applied. The RECOBIA project has identified approximately 1,200 separate activities that the "average" desk officer is likely to undertake in the course of their work. Practitioner inputs suggest that many of these processes are undertaken without adequate training or guidance (or are avoided completely)[4]. A decade on from the intelligence failures of Iraq and 9/11, a large number of analysts are ignorant of, or indifferent to the value of structured analytic techniques to improve analysis. The lack of time is frequently cited as a factor here, but the lack of training more so.

The development and maintenance of IT systems is a further headache. By most accounts, intelligence agencies continue to spend vast sums of money on media monitoring systems that fail to meet their requirements. And yet, far too many analysts remain ignorant of how a handful of tools – e.g. Google Reader, Google Alerts, RSS/XML and the right browser – can be used to generate situational intelligence from all four corners of the globe.

A further challenge is that of data quality and data management. As well as purchase access to commercial information services, intelligence services frequently develop databases of their own to archive information from both sensitive and open sources. The use of databases is something all intelligence professionals are familiar with; their management and maintenance less so. Consequently, analysts are obliged to work with data that is poorly structured, missing or incomplete. A shoddy database is no more conducive to effective intelligence than a library where half the books have been put back on the wrong shelf. The lack of training here has resulted in information services that are of little value to analysts or collectors. The inevitable consequence of poor data is poor analysis and poor policy.

The challenges listed here are not exclusive to European services. They have been echoed by the many novices and professionals the author has interacted with over the past decade. Nevertheless, they prompt some awkward questions:

- If poor management is an impediment to effective intelligence work, why is this discipline excluded from most intelligence curricula (particularly those dedicated to graduate students)?

- If poor policies and processes undermine individual and organisational effectiveness, why is no training given on such disciplines as process planning, operations management, etc.?
- If technology is such an important enabler of intelligence work, how might we enhance and sustain the information literacies of all intelligence staff?
- If information (or data) is our basic tool of work, why don't we train people in data management, data quality, data processing, etc.? Moreover, why do we continue to behave as if such tasks are best delegated to algorithms?
- Drawing from the above, if intelligence involves much more than the collection, processing, analysis and communication of information, why does the teaching of intelligence professionals remain unchanged?

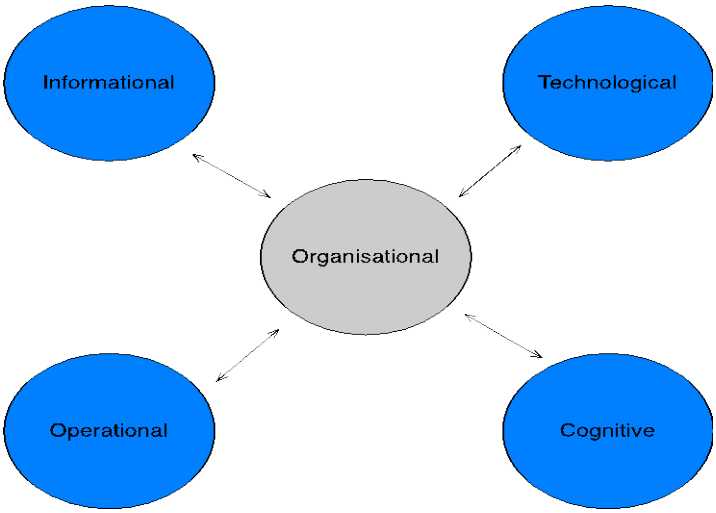
Addressing these questions (as opposed to merely answering them) obliges us to re-imagine the intelligence curriculum, and to significantly expand our notion of what constitutes valid intelligence work. The Five Architectures framework is one possible step in this direction.

The Five Architectures Framework

The Five Architectures framework was developed by the author to support his teaching and consulting practice. The framework, together with its accompanying maturity models, was originally developed to support enterprise planning and development. More recently, it has been used to inform the development of training curricula for researchers and analysts in both the public and private sector[5].

The framework posits that intelligence is a multifaceted activity occurring across five separate domains: organisational, operational, information, technological and cognitive. Each domain requires a separate body of knowledge. This knowledge has to be *constructed* to allow for a holistic understanding of intelligence work. This, in turn, requires the patient labours of an *architect*. In other words, for the intelligence enterprise to function effectively it must be designed, built and engineered by architects schooled in the many subjects that inform the Five Architectures. Let us examine the architectures in turn so that we can understand their significance.

Figure 1: *The Five Architectures Framework*



The *organisational architecture* informs the agency's mission, vision, strategy, structure and so on. Put simply, this is the architecture of control, one that shapes how an intelligence agency is governed and directed. Those shaping this architecture must be well versed in management, leadership and the many schools of strategy. More importantly, they must have the discipline and wherewithal to implement the ideas they advocate to their staff.

The *operational architecture* determines how an intelligence agency gets things done. It is manifested in the policies, processes, workflows, habits and practices of its staff. Effective workflows require competent project, process and operations managers, as well as staff experienced in the difficulties of capability development.

The *informational architecture* determines the extent to which an agency's information assets - its databases, file servers and the like – are managed and used. This architecture is reflected in the organisation's approach to information and knowledge management, its naming and metadata conventions, its approach to data quality, etc. Implementing this architecture requires a solid grounding in information science, data quality, and so on.

The agency's *technological architecture* enables the flow of data, knowledge and ideas. It is realised through its choice of tools and technologies, as well as its attitudes to technological progress and innovation. A robust technological architecture requires a solid grounding in IT security, computer science, technology management, programming, and so on.

Finally, the agency's *cognitive architecture* determines its capacity for learning, flexibility and adaptation. It is manifested in its intelligence curiosity, and capacity for perception, decision-making, foresight and judgement. It can be strengthened by providing staff with sufficient opportunities to learn and grow, and to exercise their capacity for critical, creative and conceptual thinking. It also requires a sold grounding in such disciplines as individual and organisational psychology, cognitive science and so on.

All five architectures are a perpetual work in progress. All are relevant to the success of the intelligence enterprise and must be developed in parallel. No architecture is more important than the other. But all are composed of different schools of thought that must be synthesised to enable the agency's work.

Working with First Principles

In recent years, a number of authors have argued that intelligence practitioners should look beyond the immediate horizons of their profession for guidance and inspiration[6]. Their advice is well taken; even the lowliest of professions have something to teach the analyst on the processing of information in conditions of uncertainty.

So what does architecture have to teach the intelligence professional? One of the first attempts to codify the discipline is Vitruvius' *De Architectura* (*On Architecture*)[7]. Herein, Vitruvius argues that all structures must exhibit three qualities[8]. To begin, they must demonstrate *firmitas* or strength. They have to be durable and resistant to shock. From an intelligence perspective, they must also have the capacity to withstand ignorance and failure.

Second, the structure must demonstrate *utilitas*, or usefulness. In other words, they must function well for those who inhabit and use them. An intelligence service that doesn't serve the interests of its customers as well as those of its staff is unlikely to be of any long-term value. Moreover, its uses should multiply with time. Thus, just as a house can become a home and an office, so too should an intelligence agency adapt to meet the changing requirements of its constituents.

And third, the structure should demonstrate *venustas*, or beauty. From the perspective of the intelligence service, it should "delight" through the provision of insight, foresight and knowledge. Indeed, if truth (or at least the approximation of it) is an analytical imperative, then Keats dictum that beauty is truth and truth beauty is almost certainly true[9].

To the principles of Vitruvius we can add those of space, form, function and light. Louis Khan referred to architecture as the "thoughtful making of space"[10]. Architecture's renewal, he argued drew from our perpetually changing notions of space.

Today's intelligence professional is required to traverse an ever-broader array of knowledge spaces. The average desk officer should be knowledgeable of the history, culture, society, economics, politics and language of the countries or regions they are assigned to monitor. To this should be added knowledge of their profession, and the policies and processes that inform it. Further, they require knowledge of the tools and technologies that enable their work, as well as of the sources and methods that support collection and analysis. Analysts are also required to apply this knowledge so as to secure the physical and digital spaces that government's need to operate effectively.

With regard to form, it is sufficient to say that the size, shape and configuration of the agency should reflect its mandate or raison d'être. Thus, an agency dedicated to navigating risks, threats, challenges and opportunities should be as flexible and adaptable as possible.

On the issue of function, the agency must determine *what* it does and *how*. Again, the organisation is required to think laterally. Intelligence services exist not just to marshal data, but also to identify talent, to educate stakeholders, to enable decision making, to drive technological innovation and so on. Such functions rarely feature in the organisational mission statement. Others are so banal (e.g. to provide a comfortable work environment), that they are routinely ignored until the lack of attention prompts crisis or dysfunction.

Finally, architects spend a considerable amount of time working with light. The same is true for intelligence professionals whose efforts are dedicated to illuminating the corners of ignorance and uncertainty. We can be more specific here. Architects work with task light, the light needed to do our work (the tools, technologies, ideas, etc.). They also work with ambient light (the subject to regional knowledge that provides context and meaning. Architects (like intelligence professionals) use highlights and spotlights to draw attention to those features of significance or prominence; they also use contrast to evaluate and draw out differences. Not for nothing does Francis Bacon refer to clandestine operators as “merchants of light” in the New Atlantis[11].

Intelligence Professionals as Holists

We can go on but the point should be clear: architecture, like business or medicine, has much to teach the intelligence professional. Its most valuable lesson, perhaps, is in the value of holism and holistic thinking.

Holists (from the Greek *ὅλος* or *holos*) see systems and their properties as wholes and not just a collection of separate parts. Like

the architect, the intelligence holist understands that the intelligence enterprise cannot be understood in terms of its constituent parts (or the specific phases of the intelligence cycle). Rather, it must be seen and understood in its entirety. Only then will he have the depth and breadth of knowledge needed to steer the intelligence enterprise toward its many objectives.

The holist differs from the specialist whose focus is invariably subject or region specific. He also differs from the generalist, whose interests might cover many issues or regions but rarely embrace the minutiae of process management, organisational theory, information processing and so on.

I posit that the intelligence enterprise of tomorrow must add to its roster of generalists and specialists a cadre of holists whose knowledge of intelligence work spans the five architectures, and whose knowledge and experience here is as broad as it is deep.

Building the New Intelligence Curriculum

Acquiring such staff obliges us to re-imagine the intelligence curriculum so that it includes those disciplines that inform the Five Architectures including, *inter alia*, leadership, management, organisational theory, operations management, information science, cognitive science, human psychology, technology strategy, IT security, and so on.

The knowledge needed here is distributed across academia, the Internet and the working world. However, it has yet to be synthesised or codified for the intelligence professional. To the best of my knowledge, there are no courses on data quality or database management for intelligence professionals. Nor are there any seminars dedicated to IT standards and how these can be used to generate intelligence from open sources, including social media. These may not seem like serious omissions to the standard curriculum, but the intractable grievances of intelligence professionals and their customers suggest they are.

Indeed, I would counsel greater boldness still. The Five Architectures framework suggests that the intelligence practitioners of tomorrow require the equivalent of an MBA – a Masters in Intelligence Administration (MIA) if you will – an applied, multi-year program that provides a solid grounding in the disciplines summarised above. Such a program could be administered by a single institution or, borrowing from the more successful MBA programs, by a consortium of partners focusing on a different part of the Five Architectures model.

This is not to criticise existing training programs. Quite the contrary; they play a critical role in preparing intelligence professionals to enter the workforce. By all means, let us continue instructing practitioners in the rigours of collection, analysis and critical thinking. The necessity of doing so is grounded in hard won experience and is evident from the challenges listed at the start of this paper. But it is high time we acknowledged that an intelligence education that offers little more than a heavy dose of theory with case studies of success and failure will not resolve the functional challenges we have spent the past decade reliving.

References

[1] These remarks were prepared for the 18th International Conference "Intelligence in the Knowledge Society" held in Bucharest on 19 October 2012. I am grateful to staff at the National Intelligence Academy of the Romanian Intelligence Service for giving me the opportunity to present at this event.

[2] For more on the VIRTUOSO and RECOBIA projects see www.virtuoso.eu and www.recobia.eu respectively. The author's work on both projects has been undertaken as an analyst with the UK-based consultancy Hawk (www.hawk-ism.co.uk).

[3] The proceedings of the various RECOBIA workshops, together with the project's research on the intelligence cycle are summarised in the various reports published here: http://www.recobia.eu/publications.

[4] The proceedings of the various RECOBIA workshops, together with the project's research on the intelligence cycle are available on www.recobia.eu/publications

[5] This is part of an ongoing research project at the Zurich University of Applied Sciences, the results of which will be published later in 2013.

[6] See, for example, Stephen Marrin and Jonathan D. Clemente, "Improving Intelligence Analysis by Looking to the Medical Profession", *International Journal of Intelligence and Counter Intelligence*, Vol. 18, No. 4, 2005, pp. 707 — 729.

[7] Vitruvius, *On Architecture* (London: Penguin Classics, 2009; originally 40 BC).

[8] The term "structure" is here understood not just as a physical entity. It can just as easily embrace macro and micro concepts, from the national security infrastructure, to the database structure used to manage information.

[9] See John Keats, "Ode on a Grecian Urn" in *Selected Poems* (London: Penguin Classics, 2007).

[10] See Louis Kahn, *On the Thoughtful Making of Spaces: The Dominican Motherhouse and a Modern Culture of Space* (Lars Muller Publishers, 2010).

[11] Francis Bacon, *The New Atlantis* (1627). The quote reads: "For the several employments and offices of our fellows, we have twelve that sail into foreign countries under the names of other nations (for our own we conceal), who bring us the books and abstracts, and patterns of experiments of all other parts. These we call merchants of light." See http://www.gutenberg.org/ebooks/2434

Re-shaping Intelligence for the Prevention and Countering of Terrorism after 9/11. A Cultural Approach to the "Need to Share" Paradigm

Cristian BARNA[*]

Abstract

After 9/11 Al Qaeda had been transformed, in the eyes of most terrorism experts and intelligence analysts, from a criminal network into a global hydra with linked cells embedded in dozens of countries, being misunderstood both inside and outside the intelligence community. The preeminent threat had been less an Osama bin Laden-driven terror network than a global Islamist insurgency.

In this context, the limits of purely military methods to defeat armed Islamist insurgency had been painfully evident in Iraq. But how exactly can intelligence defeat terrorism? Intelligence actors fear being asked to play the predictive game, connecting the proverbial dots right and fast 100 percent of the time. They must learn how to use the information and how to use that greater degree of information to analyze the Jihad puzzle.

This paper analyzes the way that a cultural approach of "need to share" paradigm has been successfully in rethinking intelligence in countering terrorism after 9/11 terrorist attacks.

Introductory remarks

The 9/11 terrorist attacks have been the object of many analyses, especially in what concerns the tactical and strategic errors of intelligence analysis, while less significant attention was given to the strategic errors of the decision makers. A logical explanation for this phenomenon is that if the intelligence analysis proven inaccurate than the decision makers will not possess the accurate intelligence and the necessary estimates to generate efficient strategies[1].

The Report of the American Senate Committee which has investigated the causes of these terrorist attacks has underlined that, because intelligence agencies have not produced any intelligence on this subject, the experts who believed that Al Qaida might represent a serious threat had no means of gaining support for their beliefs. As a consequence, they were not able to convince decision makers to implement a more flexible strategy against the terrorist threat[2].

[*] Associate Professor, "Mihai Viteazul" National Intelligence Academy

In other words, a strategic error in intelligence analysis was the main cause of the failure to prevent the 9/11 terrorist attacks. This hypothesis can only be validated if there was a significant deficit in knowing the enemy. However, if intelligence agencies have provided analyses, which could have represented a basis for strategies aimed at preventing these attacks, but the decision-makers did not take them into consideration, then the performance of the latter should be subject to criticism.

Moreover, reports from the American Intelligence Community have circulated in 2001, including a number of intelligence analyses dealing with the ideology promoted by Osama bin Laden, intelligence gathered from terrorists captured in Jordan in December 1999, the operational mechanism of the Al Qaida etc.[3].

Furthermore, the Report of the American Senate Committee showed that several intelligence analyses dealing with the terrorist threat posed by Al Qaida: "Bin Ladin Threatening to Attack US Aircraft [with antiaircraft missiles]" (June 1998), "Strains Surface Between Taliban and Bin Ladin" (January 1999), "Terrorist Threat to US Interests in Caucasus" (June 1999), "Bin Ladin to Exploit Looser Security During Holidays" (December 1999), "Bin Ladin Evading Sanctions" (March 2000) or "Bin Ladin Preparing to Hijack US Aircraft and Other Attacks", had been disseminated by intelligence agencies to the highest decision-makers inside the government[4].

9/11: the Need to Re-shape the Intelligence Cycle for the Prevention and Countering of Terrorism

When rethinking the role of intelligence in the fight against terrorism we must take into consideration the performance of intelligence agencies, especially after the 9/11 terrorist attacks, as this moment has brought to the limelight the organizational dysfunctions of the US Intelligence Community. One of the conclusions of the analysis on the causes for the "failure" of the US Intelligence Community in preventing these terrorist attacks is that it did not focus enough on the aspects related to the qualities of the intelligence analyst, his knowledge and culture. Moreover, after 9/11 we deal with a new type of threat from the part of Islamic fundamentalist groups, which we are not prepared to confront.

At a first glance, the solution identified by the intelligence agencies in order to fill their need for knowledge in this field was to open up to the academic environment. But, it became clear that these institutions were not prepared to provide a solution, as the Muslim world is very diverse. Arabic speakers proved insufficient, and most of these researchers were linguists and in the best cases they could also speak Persian and Turkish, in addition to Arabic. Western research centres and universities focused on the study of the Islamic world should be able to offer intelligence agencies researchers well versed in this field, with a good knowledge of the history of the region. Not understanding that history has a real impact on current trends, can lead to errors of judgement, which intelligence agencies cannot afford[5].

But the representatives of the Academia were not able to ask the right questions at the right time with regard to the resurgence of Islamic fundamentalism in the Middle East, underestimating its impact in the 80s, erroneously interpreting its role in the early 90s and failing to notice its ideological potential in legitimizing terrorist attacks against the US in the end of the 90s. This is only one of the reasons why intelligence organizations should be aware of the importance of having a good knowledge of Islamic history and culture, in addition to just having a good knowledge on the evolution of the Arab political system in modern times.

Because, despite all efforts made to identify and prevent terrorist attacks, the sad events of 9/11, the attack on the USS Cole and the suicide attacks in Iraq and Afghanistan triggered an alarm signal in what concerns the need to enhance both the collection and analysis of intelligence in the field of counterterrorism.

From an institutional point of view, intelligence agencies have implemented counterterrorist strategies, which aim to train special intervention units and optimize the methods for gathering intelligence from within terrorist groups' chain of command of.

Furthermore, intelligence exchange on terrorist groups has known an upward trend, based mostly on bi-lateral cooperation among intelligence services with a strict respect of norms aimed at preserving the secret of these types of activities[6].

An important dimension of intelligence gathering on terrorist threats was the elaboration of strategies for obtaining the necessary intelligence to prevent, counter or at least mitigate the impact of

terrorist actions. Firstly, intelligence agencies have been forced to identify solutions to infiltrate human sources inside terrorist groups!

Another important requirement was the need to gather intelligence from the so-called "failed states" (Yemen, Sudan, Somalia) where, in the absence of police control or because of the inefficient activity of local intelligence agencies, terrorist groups had developed logistical bases as well as training camps.

Lastly, according to Janet Napolitano, US Secretary of Domestic Affairs, the death of Osama bin Laden "does not, unfortunately mark the end of terrorism!". The American official drew attention to the fact that currently Al Qaida and other Islamic fundamentalist movements focus on recruiting individuals with strong ties to the West, but with comparatively weak ones to terrorist groups, because this could alert intelligence agencies[7].

On Multiculturalism and the Role of Intelligence in Preventing European Radicalization

In the contemporary age the Islamic factor has determined and continues to determine demographic and geographical mutations on the European continent. The co-inhabiting of the native Europeans with Muslim immigrants has generated negative social phenomena: the appearance of a new type of anti-Semitism, an ideological movement of some of the European political parties towards the far right, a re-consideration of national political equations in European states, complications in consolidating the European institutions and a re-conceptualization, if not a complete reformulation of European foreign policy[8].

Institutionalizing Islam is a phenomenon underway in Europe and Muslims living here identify themselves more easily with the Islamic world than with the European nations amidst which they currently live[9].

Muslims in Europe want to integrate and respect the values and institutions of the states in which they live, but at the same time, they want to preserve their Islamic identity. They fear that their assimilation in the European society would make them loose their own identity[10].

Marginalizing Muslim minorities, which are not allowed to shape their own social behavior, is an effect of Western multiculturalism which creates a diffuse basis of needs and services,

not taken into consideration by institutional actors. This status quo generates opaque subcultures, where Islamic fundamentalist groups can act without fearing identification. In reality, Europe is a closed society when it comes to immigrants. Tom Hundley observes that "Europe, with an ever raising population of Muslim immigrants and offering them relatively limited opportunities for social and economic integration, becomes a factory for transforming frustrated individuals in fundamentalists and even terrorists"[11].

Francis Fukuyama believes that Europe should have considered the need for social integration of Muslim minorities decades ago, before "the wings of Islamic fundamentalism opened"[12].

But although Europe is blamed for the deficiencies in absorbing immigrants, people often forget there is also despotism of minorities, too stubborn to be assimilated, even though assimilation is not accompanied by a status of extra-territoriality. Because, intentionally or not, under the cover of respect for cultural or religious differences (the main creed of multiculturalism), individuals are locked in an ethnic or racial definition[13].

It is important to mention that all European states must face different problems connected to the Muslim community. An important percentage of the Muslim population living in Great Britain comes from Southern Asia, while in Germany, the majority of Muslims are of Kurdish or Bosnian origin. French Muslims originate from the French-speaking Africa, especially Algeria and Morocco, while in Spain and Italy, Muslim immigrants, who have entered these countries illegally, come from Northern Africa or the Middle East[14].

According to official statistics, France has around 5 million Muslims, half of which have French citizenship. In Germany, there are four million Muslims, three of which have Turkish nationality, while Belgium and the Netherlands each have around one million Muslims. In UK, figures show that there are around 2 million Muslims, coming from Pakistan, India, Bangladesh and the Near East, with only 65% of them having British citizenship. In 1999, Spain had around 250 000 Muslims, and Italy 522 000 Muslim immigrants. In South-Eastern Europe, states such as Romania, Bulgaria, Hungary and the former Yugoslavia had on their territory Muslim communities, ever since they were under the occupation of the Ottoman Empire[15].

In the case of Great Britain, in a report made by the Royal Unites Services Institute (RUSI) it is stated that the vulnerability against the threat of Islamic fundamentalist terrorism could be reduced by preventing the "*ghetto*" effect on the Muslim community.

Gwyn Prins, one of the authors of the aforementioned report, stated that decision-makers in the UK are wrong if they believe that through the development of these isolated communities, a fertile ground for the promoters of Islamic fundamentalism, they are in fact promoting humanism and multiculturalism: "the British society must respect and allow the practicing of religious faiths by the immigrants, in accordance with legal provisions, but must not permit them to live in isolated communities, in which they are united rather by the cultural values of their country of origin then by those of Great Britain"[16].

Aware of the peril of Muslims radicalization in the UK, David Cameron pleaded for and managed to impose a strengthening of the counterterrorist strategy, as well as an institutional response to the Islamic traditions which do not reflect "British values". The governmental strategy for combating terrorism, made public in June 2011 by Theresa May, the British Minister of Interior, redefines extremists as those individuals, who share "not-British" principles, the primary targets being British colleges, as it is believed these have become a fertile ground for the education of youngsters attracted to the Islamic fundamentalist ideology.

Theresa May, the British Minister of Interior has stated that British universities do not take the problem of radicalization seriously and Muslim extremists find it all too easy to put together jihadist cells in campuses "without anyone knowing about it"[17].

During the German Interior Ministers Conference in 2011, the federal and land ministries debated the issue of the increasing terrorist threat posed by the Salafist ideology in Germany. Joachim Hermann, the Bavarian Minister of Interior used this opportunity to launch a warning against the fact that Salafi movement may bring to lide terrorist, which have been raised in Germany[18].

Similarly, Boris Rhein, the Minister of Interior from Hessen draws the attention to the fact that by organizing seminars dealing with the subject of Islam, the Salafi movement creates a fertile ground for Islamic terrorism in Germany[19].

According to the 2010 report of the Office for the Protection of the Constitution (BfV), the number of Islamists is raising continuously in Germany. At the end of 2010 there were 29 Islamist organizations active with approximately 37.500 members. This means an increase with 2.700 persons in comparison with the last two years. According to Heinz Fromm, the director of the BfV, up until now, almost all Islamic terrorists in Germany have been Salafists or have had connections with this movement[20].

If up until a few years ago there were only two or three Salafi preachers, nowadays they are a few dozens, a worrisome fact taking into consideration that all the Muslims which have joined Al Qaida or other jihadist groups in Pakistan have frequented the Salafi mosques Al-Nur from Berlin or Al-Quds in Hamburg[21].

In France, the periphery of cities such as Paris or Marseille is full of discontented Muslims, who consider themselves discriminated by the education system, the public sector and social services. In addition, as a result of the increase in radicalization in the 90s, these peripheries are now under the actual control of Islamic fundamentalist groups[22].

As a result of the 9/11 terrorist groups, France has adopted a dual strategy to solve the problem of Muslim inhabitants. On one hand, it had supported the creation of the "French Council for the Muslim cult" which acts as an official representative of this community in its dialogue with state authorities. On the other hand it has introduced stricter rules regarding the display of Islamic symbols in schools and has intensified its measures of monitoring the mosques. More than half of the 1500 Muslim preachers do not even speak French, which is why preaching Islam in French mosques is conditioned by the graduation of a course accredited by the authorities in order that they "have a good knowledge of the French language and culture"[23].

In this context, it is not surprising that an important potential terrorist threat in France is considered to be generated by auto-radicalization of "discontented people in their homes", Muslims who live in France, very hard to control. Such individuals, as was the case of Mohamed Merah, can decide one day to act in order to bring their contribution to what they call the global jihad[24].

Italian secret services consider that the threat to this state comes both from the part of terrorist groups active abroad, but also from the part of radicalized Muslims, present on Italian territory, the so-called "self starters", which represent a very "dangerous unknown". This concerns those individuals who radicalize "in an unpredictable manner at the end of a solitary and invisible journey". The places most exposed to the dissemination of jihadist ideology are the meeting centres, especially those from Northern Italy, such as prisons where older jihadists can recruit younger Muslims arrested for petty crimes[25].

The same opinion is shared by Franco Frattini, according to whom: "Italy continues to be a privileged area for creating logistical bases by Islamist extremist" and "behind the mosques operate hate preachers and even terrorist instructors. That is why a detailed strategy of monitoring the mosques is needed"[26].

Bulgaria has a large autochthonous Muslim community subjected both to the influences of the Turkish fundamentalist sects such as Nurcular, Suleymancilar and Mili Goruş but also to Wahabi Islamic fundamentalists, represented by the Saudi non-governmental organization Al Waqf al Islami.

Al Waqf al Islami, with the main headquarters in the Netherlands has been forbidden in Bulgaria even since 1994, a year after its registration as a non-governmental organization and its leaders have been expelled from the country on chargers of threatening Bulgarian national security. It is important to mention that Al Waqf al Islami has also been forbidden in the US, after suspicions were raised that its members had ties with members of the terrorist cell, which has organized the 9/11 terrorist attacks[27].

The land border between Bulgaria and Turkey is an "Achilles's heel", as this area is inhabited by a poor Muslim community, vulnerable to proselyte activities conducted by the Wahabi group Al Waqf al Islami, thus generating insecurity and increasing the risk of terrorist activities. We should not dismiss, in this respect the Burgas attack which took place this summer and which has enhanced the vulnerability of Bulgaria's national security.

In the case of Romania, while the Turks and Tartars from Dobrogea have a common history with native Romanians, sharing the same socio-political values and having to face the same

economic problems, the Muslim immigrants from the Middle East, North Africa or Central Asia form heterogeneous communities, which do not promote an Islamic religion based on the principles of ethnicity, but have a more diffuse and globalizing basis.

With regard to the radicalization of Muslim immigrants or of the members of the local Muslim community we must mention that there is the risk that elements from the Muslim immigrants may act towards promoting an Islamic fundamentalist religious trend within the Turkish and Tatar communities from Romania, having significant material resources as well as ideological support from their countries of origin[28].

But this phenomenon of radicalization must be perceived as a two-way road, the activism manifested by the Muslim minority appearing capable of overcoming Europe's ability to draw in a rational, consistent and persuasive manner the limits of tolerance. It appears that Europeans see Muslims as a direct threat to the identity and traditional values of the "old continent", as proven by the heated debates surrounding the wearing of the traditional Muslim veil in schools, building mosques, teaching Islam in schools, Muslim burial habits, Muslims being the social group which Europeans least wish to have as neighbours[29].

Indeed, the number of anti-Islamic incidents has increased in most European countries, becoming more visible after the 9/11 terrorist attacks. For example, the "Muslim Commission for the monitoring of Islamophobia" from the UK has warned against the fact that more and more Muslims feel excluded from society and inter-ethnic tensions in British cities are about to burst.

In France hundreds of Muslims prayed on September 16th 2011, on the streets of Paris, despite the fact that only a day earlier a law was adopted which prohibited such a manifestation. Claude Guéant, the French Minister of Interior at that time, warned that the police will use force if Muslims will break the law designed to preserve the secularity of public spaces in the French capital: "praying in the street are not respectful for religious practices and violate the principles of secularism". Forbidding street prayers is the most recent action of the French government meant to eliminate Islam from the public arena. In April 2011, a law was adopted which prevented women from wearing in public the traditional Muslim veil[30].

The worst alarm signal was represented by the terrorist attacks made by Anders Behring Breivik in 2011, with the declared purpose of combating the "colonization" of Norway by the Muslims, in the context of "the betrayal" by which the victims of the attacks were guilty in promoting multiculturalism[31].

Following the Breivik terrorist attacks, some of the mosques in the UK have enhanced their security measures, as a result of the fact that Anders Breivik declared that he fears that the Muslims are targeting Europe, a good example of the failure in eradicating the Islamophobia which has extended on the "Old Continent"[32].

In this respect we must mention the message posted on Facebook, which called for the "stabbing of Muslims in place of sheep", with the occasion of the *Eid El-Adha* celebration, on November 6th 2011. The French Council for the Muslim Cult has expressed its concern that the proliferation of such an Islamophobic discourse "may lead to a massacre such as the one from Oslo"[33].

In Germany, a country known for the activism of its extreme rights groups, authorities are afraid that the author of the Norway attacks may become an example for the enemies of Islam. Alexander Eisvogel, the Vicepresident of the Office for the Protection of the Constitution stated that Breivik may become a model for imitators: "we are currently very concerned especially because of the combination between the attacks and the planning which took place beforehand, as both events are described in detail and all the information is available to the public". According to Eisvogel, we are dealing with "a new type of xenophobia, which is no longer argumented from a racist point of view, but from a cultural or ideological perspective"[34].

Instead of Conclusions: a Cultural Approach to Intelligence for the Prevention and Countering of Terrorism

We consider that in preventing and combating terrorism intelligence agencies need both analysts and field officers with an unconventional mind, who can become integrated parts of a strategic concept which can provide solutions on how to use intelligence in order to defeat Islamic fundamentalist terrorism. The limits of the

purely military methods employed against this type of terrorism have become painfully obvious in Iraq, and in what concerns the diplomatic and financial efforts against the global jihadist insurgency we consider many years are yet to pass until they will give actual results [35].

The first step in combating the terrorist threat must be the identification of the threat, from a strategic point of view. In order to do this, intelligence agencies must have trained personnel capable of understanding the nature of the threat, much better educated, trained and euristical analysts in comparison with those from the tactical or operational level.

First, analysts from the strategic level involved in combating terrorism have to understand the manner in which the enemy thinks and reacts, "his vision of the world", history, culture and last but not least language. If the enemy is represented by Islamic fundamentalist groups, intelligence agencies need analysts, who have a good knowledge of the manner in which violence is portrayed in Islam, the way jihad is conducted, for jihad is a global phenomenon.

Secondly, providing solutions to prevent Muslims radicalization via a more proactive use of intelligence.

That is why we plead for a cultural approach on Islamic fundamentalism as well as enhancing the role of intelligence in the fight against terrorism.

Because of this, intelligence agencies must create a flexible training programme for the education of future analysts. The key to success for intelligence services can be insuring "all-source" expertise, operatives who can gather intelligence from multiple sources, working in a collaborative manner with analysts, and "absorbing" knowledge, relatively refined from their various fields of expertise.

Also, we should not restrict to intelligence collection and analysis, but rather work in partnership with decision makers, Academia and civil society, in order to identify why Muslims from Europe radicalize.

Because a failure in understanding the enemy will lead to serious errors in an era marked by the global jihadist insurgency and its secondary effects, by Islamophobia and the resurgence of right-wing extremism, intelligence agencies can afford few mistakes.

That is why, we consider that intelligence should not be exclusively contained within intelligence agencies and disseminated to decision makers. As a threat impacting society as a whole, all of its members should be made aware of each and everyone's role in countering it!

References

[1] Stephen Marrin, "Intelligence Analysis and Decisionmaking: Methodological Challenges", in P. Gill, S. Marrin and M. Phythian (eds.), *Intelligence Theory: Key Questions and Debates* (London and New York: Routledge, 2008).

[2] National Comission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States- Authorized Edition* (New York: W.W. Norton & Company, 2004).

[3] Stephen Marrin, "The 9/11 Terrorist Attacks: A Failure of Policy Not Strategic Intelligence Analysis", *Intelligence and National Security*, Vol. 26, Nos. 2–3, April–June 2011.

[4] National Comission on Terrorist Attacks Upon the United States, *9/11 Commission Staff Statement No. 11: The Performance of the Intelligence Community*, 2004, available at http://govinfo.library.unt.edu/911/staff_statements/staff_statement_11.pdf.

[5] Joint Military Intelligence College, *The US Intelligence Community Response to Jihad in Global War on Terrorism: Analyzing the Strategic Threat*, Discussion Paper Number Thirteen, November 2004, available at http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA476563.

[6] Eric Herren, "Counter-Terrorism Dilemmas", 5 April 2002, available at http://212.150.54.123/articles/articledet.cfm?articleid=432.

[7] "Janet Napolitano: US terror threat highest since 9/11", 9 February 2011, available at http://www.bbc.co.uk/news/world-us-canada-12407859.

[8] Timothy Savage, "Europe and Islam: Crescent Waxing, Cultures Clashing", *The Washington Quarterly*, Summer 2004.

[9] *Ibid.*

[10] Zachory Shore, "Uncommon Threats: Germany's Muslims, Transatlantic Relations, and the War on Terror", *AICGS Policy Report*, No. 5, 2003, available at http://www.aicg.org/site/wp-content/uploads/2011/10/shore.pdf.

[11] Tom Hundley, "Anti-semitism Debate Swirls Across Europe: Muslim Alienation Sees as a "New" Worry", *The Chicago Tribune*, January 4, 2004.

[12] Francis Fukuyama, "Europe vs. Radical Islam. Alarmist Americans have mostly bad advice for Europeans", *Slate Magazine*, 27 February 2006, available at http://www.slate.com/articles/arts/books/2006/02/europe_vs_radical_islam.html.

[13] Pascal Bruckner, *Tirania penitenţei* (Bucharest : Editura Trei, 2006).

[14] Geoffrey Kemp, "Europe's Middle East Challenges", *The Washington Quarterly*, Winter 2003 – 2004.
[15] Abduljalil Sajid, "Islam and Muslims in Europe: Integration or Assimilation/ Alienation: Clash vs. Peaceful-Coexistence", available at http://www.mcb.org.uk/downloads/Islam-Muslims.pdf.
[16] "Marea Britanie, vulnerabilă în faţa islamiştilor", *Lumea*, Vol. 6, No. 183, 2008.
[17] Polly Curtis, "David Cameron to target Islamists who hold 'un-British' beliefs", *The Guardian*, 5 June 2011, available at http://www.guardian.co.uk/politics/2011/jun/05/david-cameron-islamists-counter-terrorism.
[18] Roland Preuß, "Deutscher Sicherheitsbericht zu Salafisten Stopp für Missionare der Intoleranz", *Suddeutsche Zeitung*, 20 June 2011, available at http://www.sueddeutsche.de/politik/deutscher-sicherheitsbericht-zu-salafisten-stopp-fuer-missionare-der-intoleranz-1.1110213.
[19] "Rhein: Salafisten gefährlichste Verfassungsfeinde", *Frankfurter Allgemeine Zeitung*, 01 June 2011, available at http://www.faz.net/aktuell/rhein-main/hessen/verfassungsschutzbericht-rhein-salafisten-gefaehrlichste-verfassungsfeinde-13327.html.
[20] Florian Flade, "Wie deutsche Frauen für al-Qaida kämpfen", *Die Welt*, 05 July 2011, available at http://www.welt.de/politik/ausland/article13466009/Wie-deutsche-Frauen-fuer-al-Qaida-kaempfen.html.
[21] Raffaello Pantucci, "Terror-in-Germany: An Interview with Guido Steinberg", 16 March 2011, available at http://icsr.info/2011/03/terror-in-germany-an-interview-with-guido-steinberg/.
[22] Soner Cagaptay, "Muslims in France: A Ticking Time Bomb?", FrontPageMagazine.com symposium, 4 July 2005, available at http://www.washingtoninstitute.org/html/pdf/cagaptay070405.pdf.
[23] John Rossant, "France's Crackdown On Islamic Radicals", *BloombergBusinessweek Magazine*, 7 June 2004, available at http://www.businessweek.com/stories/2004-06-06/frances-crackdown-on-islamic-radicals.
[24] Yves Bordenave and Remy Ourdan, Interview with Bernard Squarcini : "La France est la cible n° 2 d'Al-Qaida", *Le Monde*, 12 May 2011, avilable at http://lemondewatch.blogspot.ro/2011/05/bernard-squarcini-la-france-est-la.html.
[25] "Allarme degli 007: rischio terrorismo", *La Stampa*, 24 February 2011, available at http : www.lastampa.it/2011/02/24/esteri/allarme-degli-rischio-terrorismo-B4S3OsSFh3sMjxva7egGKN/pagina.html.
[26] "Frattini: "A ottobre mappa moschee", *TGCOM Mondo*, 22 July 2007, available at http://www.tgcom24.mediaset.it/mondo/articoli/articolo371921.shtml.
[27] Clive Leviev-Sawyer, "Raid on radical group was not 'anti-Islam', Bulgarian prosecutors say", *The Sofia Echo*, 7 October 2010, available at http://sofiaecho.com/2010/10/07/972924_raid-on-radical-group-was-not-anti-islam-bulgarian-prosecutors-say.

[28] Gyula Kozák, "Muslims in Romania: Integration Models, Categorization and Social Distance", *Working Papers in Romanian Minority Studies*, No. 18, 2009.
[29] "Forget Asylum-Seekers: It's the People Inside Who Count", *The Economist*, 8 May 2003.
[30] "Sute de musulmani s-au rugat pe strazile din Paris in ciuda legii care interzice acest lucru", 17 September 2011, available at http://www.hotnews.ro/stiri-international-10156391-sute-musulmani-rugat-strazile-paris-ciuda-legii-care-interzice-acest-lucru.htm.
[31] "Norway terror suspect claims to have worked with two other cells", *The CNN Wire*, 25 July 2011, available at http://edition.cnn.com/2011/WORLD/europe/07/25/norway.terror.attacks/index.html.
[32] Paisley Doods, "APNewsBreak: Extra security at UK mosques", *The Guardian*, 25 July 2011, available at http://www.guardian.co.uk/world/feedarticle/9762136.
[33] Mihai Drăghici: "Consiliul francez al Cultului Musulman denunţă un apel care îndeamnă la uciderea musulmanilor", Mediafax, 15 September 2011, available at http://www.mediafax.ro.
[34] "Der Terrorist und die Brandstifter", *Der Spiegel*, 01 August 2011, available at http://www.spiegel.de/spiegel/print/d-79723321.html.
[35] John Schindler, "Defeating the Sixth Column: Intelligence and Strategy in the War on Islamist Terrorism in the War on Islamist Terrorism", *Orbis*, Vol. 49, Issue 4, Autumn 2005, http://dx.doi.org/10.1016/j.orbis.2005.07.009.

Reforms in the Greek Intelligence Service (NIS-EYP) and the Need for an Academy in the 21st Century

John M. NOMIKOS*

Abstract

Nowadays, Greece faces complicated and dangerous challenges (Illegal Migration, Transnational Organized Crime, Human Trafficking, Islamic Fundamentalism) as it tries to navigate muddy and unpredictable intelligence waters. The article will focus on the reason(s) why Greece needs an Intelligence Academy in order to train and educate intelligence officers. Unfortunately, Greek intelligence performance even during better times left much to be desired. Intelligence capabilities and manpower did not escape the debilitating effects of bureaucratization, political patronage and political squabbling. Greece does not possess the luxury of wasting more time.

Introduction

Human beings have always needed information to secure their livelihood and their safety - the location of the best fishing stream, the site where firewood might be gathered, when deer herds were likely to appear. In classical Greece, covert action and clandestine operations were among the most common and yet most vilified methods of statecraft. All states used them (Athens and Sparta), no state wanted to admit the fact, and if the operations became public the world severely disapproved. The Greeks used local citizens as proxenos[1]. A proxenos had to be a citizen of the state he served, not of the state he represented. These men were the equivalent of modern spies or agents as conduits for information and clandestine activities in the course of normal duties during the Peloponnesian Wars[2].

The historical record suggests that very few societies (especially not empires) could pass up the opportunity of using such useful and flexible human tools when overt military operations were either impractical or impossible. Nowhere is this clearer than in the case of the Ancient Romans[3]. In their public propaganda they prided

* Professor, Director of the Research Institute for European and American Studies

themselves on being open, aboveboard, and honest. In reality, they were experts at political manipulation, spying, and dirty tricks. For five centuries they ruled over the Mediterranean world with an iron fist, yet much of that control was not the direct result of using military force.

As the Intelligence Community inexorably works its way into the twenty-first century, it faces an unprecedented array of challenges. The chaotic world environment of the post-Cold War era offers a wide range of different issues to be understood, and a variety of new threats to be anticipated. The rapidly developing information age presents advanced and complex information technology and methodologies to be mastered and integrated into the intelligence process[4].

During the first decade of the 21st century, as long as national and international security is concerned, terrorism remains a major issue. The events of September 11th 2001 in the USA, March 11th 2004 in Madrid, July 7th 2005 in London and most recently July 18th 2012 in Burgas, Bulgaria, indicate, or actually prove, that the distribution and analysis of information by those who are competent to eliminate international terrorism is inefficient.

The article is divided in three parts. First, it describes the history of the Greek Intelligence Service (NIS-EYP). Second, it points out the reforms of the Greek Intelligence Service (NIS-EYP) between 1986 and 2008, and finally it elaborates on the concept why Greece needs an Intelligence Academy in order to promote training and education among its members.

History of the Greek Intelligence Service (NIS-EYP)

In the Hellenic Republic, the first attempt to construct and Intelligence Unit started in January 1926. A new special intelligence branch was formed with the name State Security Branch (Geniki Asphalia). This intelligence unit, which lasted only a year and a half, was supervised by the nation's President. Ten years later (1936), a new intelligence branch was formed, under the name Defence Intelligence Branch (Ypiresia Aminis), which reported directly to the Minister of Defence. In November 1936, the Defence Intelligence Branch was renamed General Directorate of Foreign Citizens, and supervised by the Minister of Public Order. Its tasks included espionage and counterintelligence. Despite limited sources, the General Directorate of Foreign Citizens functioned effectively in the espionage arena during World War II. In 1946, a new military intelligence unit was

established, the Military Protection Department (Ypiresia Prostasias Stratevmatos). After three years (1949), General Alexander Papagos renamed it the General Directorate of Information (Geniki Ypiresia Pliroforion), and it was put under his supervision.

In 1952, when General Papagos became Prime Mimister, he renamed it once again, as the Central Intelligence Service and Research (Kentriki Ypiresia Pliroforion and Erevnas, KYPE). The new intelligence agency now reported directly to the Prime Minister. KYPE became the foundation for today's National Intelligence Service (NIS-EYP).

A new intelligence branch, the Central Intelligence Service (Kentriki Ypiresia Pliroforion, CIS or KYP), was established along Western standards as a self-standing agency, subject to the Prime Minister, with the country's national security as its mission[5]. From 1969 until 1974, the Central Intelligence Service functioned as an independent public service and reported to the Prime Minister[6].

But under statutes enacted afterwards, the CIS/KYP was successively subject to the Prime Minister, the President of the Republic, back to the Prime Minister, then the Minister of the Prime Minister's Office, and again to the Prime Minister.

After the end of the World War II, the NIS-EY's (then known as CIS/KYP) main tasks were to track down Communists and antimonarchists. During the dictatorship era, under Colonel George Papadopoulos (1967-1974), terrorist attacks began in Greece. Most of NIS-EYP's work was against the anti-dictatorial resistance organizations that, for the most part, concentrated their attacks against the police, public officials, institutions, and those foreign states which were believed to support the colonels[7].

After the fall of the dictators, CIS/KYP, then being held in check by legitimate political forces, did not make the necessary progress toward reform, resulting in the failure of the Greek Intelligence Service to solve some longstanding problems. These days, however, the NIS-EYP seems to follow more professional ways in safeguarding national interests[8].

Bureaucracy versus Reforms: New Challenges for Intelligence Services

Furthermore, intelligence cooperation is still an obstacle for information analysis due to the combination of a net centric world which facilitates terrorist groups with ethnocentric perceptions.

Moreover, the fact that intelligence services are integrated into the state apparatus, and as a result suffer from relative bureaucratic weaknesses, has been disregarded. This fact cannot be easily studied due to the covert nature of these particular services.

The writer had the chance to speak with Michael Herman, an academic analyst of the intelligence services (Oxford University), who underlined that «the dramatic increase of workforce in the intelligence area and the fact that most of the employees have obtained a public-employee mentality is the biggest change since 1945. Intelligence services have adopted the features of "Weberian bureaucracy", which has changed because of the computer technology but it is ubiquitous as a structure»[9]. Like the Greek National Intelligence Services (NIS-EYP), intelligence agencies in other countries services suffer similarly and undergo the comparable changes within the bureaucratic environment of each country.

During the last decades most intelligence services of European countries and the USA have conducted sweeping changes concerning their way of function and action, but also their way of recruiting new executives – highly merit and with constant training-, while they make sure that their workforce is always adjusted to the new environment[10].

All the changes mentioned have brought the managing practices of these services closer to the existing techniques of private organizations and moreover in many cases there is modernization of the logistical infrastructure as well as establishment of new building substructure. It is important to mention that these changes took place during the transition to the post-Cold War era, when the new facts imposed strict supervision and more effective management of these services by their societies (Parliamentary Oversight).

Reforms and New Tasks in the Last Two Decades: 1986-2008

The restructuring of the Greek Intelligence Service (NIS-EYP) started in 1986 with a new Presidential Decree, N.D. 1645/1986, which put the steps to transform the "Central Intelligence Service (CIS or KYP)" towards its new name – "National Intelligence Service (NIS-EYP)." NIS-EYP constituted a self-standing civil public agency and its political head was then the Minister of Public Order. The mission of the National Intelligence Service (NIS-EYP), as defined in Article 2, of the Presidential Decree 1645/1986, includes the following:[11]

- The collection, processing and dissemination, to the component Authorities, of information pertaining to the Country's National Security.
- Counterintelligence activities focusing on foreign intelligence officers acting against the country.
- The security of national communications.
- In time of war or mobilizations the NIS-EYP, in parallel with its above-mentioned powers, also becomes the country's intelligence staff.

The Greek Parliament debated a significant new law covering intelligence reform and modernization. In February 2008, the Greek Government passed a new law in order to modernize the Greek Intelligence Service (NIS-EYP). Several innovations were introduced into the NIS-EYP[12].

A District Attorney is appointed to decide on a purely legal basis whether privacy laws can be lifted in order to support an investigation by the Greek intelligence service;

Establishment of a Joint Ministerial Committee including officials from eight most important ministries;

Computer Emergency Response Team (CERT) – responsible of protecting the security of critical networks;

Emphasis is placed on training with the creation of a "Training Directorate", aiming for modern education, training and specialization of personnel;

The Sub-Directorate for International Terrorism and Organized Crime has been upgraded in order to reply to the needs of the new era;

A New Operation Center together with an Open Sources Intelligence Center (OSINT).

The Greek Intelligence Community under Change in the 21st Century

The current economic crisis that plagues Greece, with the uncontrollable illegal immigration –which constitutes a national threat for the consistency of Greek society- and the Turkish threat, calls for the establishment of a Greek Intelligence Community, which will be able to cope with the contemporary challenges with high-level skills, efficiency and human resources management.

The Greek Intelligence Community has to face the need for adjustment to a constantly changing environment in order to serve the interests of Greek foreign policy and support cultural, economic and military choices of the executive authority.

However, the writer has repeatedly referred to the need for modernization of the Greek Intelligence Service (NIS-EYP) in articles published in academic journals[13] that included some of the following suggestions:

- establishment of an Intelligence Academy which will provide academic education giving the corresponding diploma in studying intelligence services and creating a new generation of talented operational analysts
- establishment of a department –within the Academy- for the communication strategy of the National Intelligence Services with Greek and foreign media and
- smoother cooperation with the Parliament and various other agencies.

Concluding Remarks

Greece needs a modern and efficient intelligence service that can collect and process information that is able to plan and carry out secret operations for the protection of the national interest. It needs a new generation of highly skilled officers and modern technological equipment[14].

The NIS-EYP needs to follow the rest of the western intelligence agencies, which have undergone massive internal changes in recent decades that could be said to constitute reforms. NIS-EYP has to change the nature and extent of its recruitment policies; it has to ensure that its staff is more representative of the population it serves; and its management practices to begin to match those in the private sector more closely. However, much of the internal modernization has occurred in the Greek Intelligence Service (NIS-EYP), but it also has to adapt to a new external policy context because of the post Cold War era[15].

Overall, intelligence is in an exquisite awkward position in adapting to a changed world. It is a service industry once designed to serve Greek foreign policy. It has to embody the qualities of high national security and professional intelligence competence as well

as the undoubted integrity that leaders of the Greek Intelligence Community have always had. But they will also have to have the vision so that they can foresee an Intelligence Community of the 21st century that portrays a realistic, credible, and attractive future, but that at the same time is different and better in important ways than that now existing. Today, more than ever, the Greek Intelligence Service has to deal with a variety of different missions. However, the Greek government should seek to keep the more threatening intelligence operations within reasonable limits, particularly those linked with diplomacy[16].

References

[1] Andre Gerolymatos, *Espionage and Treason: A Study of the "Proxenia" in Political and Military Intelligence Gathering in Classical Greece* (Amsterdam: J.C. Gieben, 1986).

[2] The Greek historian Thucydides documented the war between Sparta and Athens, which lasted for twenty-seven years between 431 and 404 BC. The war, the largest the Greek world had known of up to this date, encompassed almost the entire Greek world, and came with a very high price, for Athens, once the mightiest power in Greece, lost her supremacy due to the war.

[3] Rose Mary Sheldon, "The Ancient Imperative: Clandestine Operations and Covert Action," *International Journal of Intelligence and Counterintelligence*, Vol. 10, No. 3, Fall 1997, pp. 299-300.

[4] William H. J. Monthorpe Jr., "Leading Intelligence in the 21st Century," *Defense Intelligence Journal*, Vol. 7, Spring 1998, pp. 1-3.

[5] Presidential Decree, N.D. 2421/9/5/1953, from the Greek Government for the development of the Greek Intelligence Service.

[6] Presidential Decree, N.D. 380/69, from the Greek Government in order to readjust the tasks of the Greek Intelligence Service.

[7] Kaminaris Spyros, *Terrorism in Greece and Governmental Responses (1974-1998)*, unpublished doctoral thesis at the Center for Byzantine Ottoman, and Modern Greek Studies, University of Birmingham, UK, July, 1999, p. 49.

[8] Dimitrios Agrafiotis, "17 November Caught at Last," *Intelligence Net*, No. 1, March 2003, pp. 30-31.

[9] John M. Nomikos, "Intelligence and National Security – The Case of Greece," August 2012, available at http://www.rieas.gr/research-areas/editorial/1837-intelligence-and-national-security-the-case-of-greece.htm,.

[10] *Ibid*.

[11] John M. Nomikos, "The Internal Modernization of the Greek Intelligence Service (NIS-EYP)," *International Journal of Intelligence and Counterintelligence*, Vol. 17, No. 3, 2004, pp. 435-448.

[12] John M. Nomikos, "Looking Back to See Forward: The Greek Intelligence Service in the 21st Century," March 2008, available at http://rieas.gr/index.php?option=com_content&task=view&id=582&Itemid=41.

[13] John M. Nomikos, "Intelligence and National Security"; J. Nomikos , "Reforming the Greek Intelligence-Security Community: New Challenges", *Journal of Romanian Intelligence Studies*, No. 5, June 2011; J. Nomikos and A. Liaropoulos, "Truly Reforming or Just Responding to Failures? Lessons Learned from the Modernisation of the Greek National Intelligence Service", *Journal of Policing, Intelligence and Counterterrorism*, Vol. 5, No. 1, 2010; J. Nomikos, "Greek Intelligence Service", in Stuart Farson, Peter Gill, Mark Phythian and Shlomo Shpiro (eds.), *Global Security and Intelligence*, (USA: Praeger Security International, 2008); J. Nomikos, "Greek Intelligence Service: Past, Present and the Future", *National Security and the Future*, Vol. 9, No.1-2, 2008; J. Nomikos, "Greek Intelligence Service: A Brief Description", *European Journal of Intelligence Studies*, Vol. 2, 2008; J. Nomikos, "Greek Intelligence Service and Post 9/11 Challenges", *The Journal of Intelligence History*, Vol. 4, No.2, Winter 2004; J. Nomikos, "The Internal Modernization of the Greek Intelligence Service", *International Journal of Intelligence and Counterintelligence,* Vol. 17, No. 3, Fall 2004.

[14] John M. Nomikos, "Greek Intelligence Service (NIS-EYP): Past, Present and Future".

[15] *Ibid.*, p. 86.

[16] *Ibid.*, p. 87.

Why Real Ethics and True Wisdom Are Keys to Keeping Intelligence Agencies Guardians of the People, Instead of Persecutors of the People

Michael ANDREGG[*]

Abstract

The quintessential missions of a Special Agent are to protect the people, and innocence as a concept.

Protecting the state is also important, of course. If you do not, you won't be employed as an intelligence professional. But it is vital to remember which comes first, and that governments can change from protectors of the people to persecutors of them quickly. Eastern Europe had such vivid experiences with this problem during the last century that its current guardians should be models to the world. Protecting innocents is our eternal mission, and when governments go bad they often lose sight of this distinction.

To be a truly Special Agent one must always remember that people come first and be loyal to them first, while also serving the state that employs and empowers you. States are your paycheck and pension, so serve them well, but … keep priorities as indicated. That could be the end of a philosophic discussion, but this issue comes up practically in careers because decay is eternal. Graft grows. Corruption appears spontaneously. There is a little dictator in every politician's heart, and truly Special Agents never forget these problems. Thus an important question for the career professional is, "What missions would I refuse to do, and why?" Then, how does one refuse effectively? We will ask other hard questions here.

Intelligence professionals serve missions assigned by states in daily work, whether collectors, analysts, operators or support staff. They are expected <u>not</u> to ask big questions unless they really 'need to know.' But today we face civilization level crises, so the world needs Special Agents with global vision. How can "global vision" coexist with the secrecy so essential to many intelligence operations?

An important check on state hubris is a strong professional ethos rooted in the security services, but known more broadly. This should be supremely idealistic, deeply courageous, and grounded in WHY the people must always come first. You are their guardians – do not let <u>any</u> state oppress them! The rest of this paper will try to show how "real" ethics and "true" wisdom, or aspirations to such ideals, can help with cultivating an intelligence community ethos for the Third Millennium of the Common Era.

[*] PhD, Adjunct Instructor, Justice and Peace Studies, University of St. Thomas

Introduction

What are "Real Ethics?" What is "True Wisdom?" If the answers to questions like these were easy, the world would have less problems. But analysts must often assess difficult problems so I will do my duty. "Real" ethics to me are the codes one carries in one's heart. Why? Because these prevail at moments of truth, when agents in the field must make decisions of life and death, sometimes in seconds with limited recourse for consultation. All the rule books in the world cannot cover every contingency. And no set of laws or regulations can decide in the blink of an eye who is innocent or evil in the chaotic fog of combat. Yet sometimes soldiers must decide, and fast. Intelligence professionals are much like soldiers, devoted to protecting their people and state from all enemies foreign and domestic, and willing to sacrifice their lives if necessary for the good of greater communities. Most **Special** Agents are loyal to humanity.

Intelligence professionals in the Third Millennium should be more than ordinary soldiers, because the threats to civilization today are complex, and often armored by elaborate deceptions. "Terrorism" and "Weapons of Mass Destruction" are obvious challenges, each cloaked with the best deceptions their creators can devise. Organized crime afflicts every nation, deeply, grievously, under complex covers and often protected by officials whose duty is the opposite of their deeds. Yet even these problems are simple compared with several others.

How can one protect a nation against the masters of international finance when bad bankers can bankrupt a country overnight with false securities? How does one attack climate change, a very non-traditional threat, when energy transnationals spend millions on propaganda declaring global warming a myth? How does one defeat corruption of governance, which cripples so many efforts to solve so many other problems, when bad leaders use their powers to keep the people in the dark? How does one protect "whistle blowers" who try to reveal such corruptions, when bad leaders prosecute the whistle blowers instead? How can Special Agents reveal and neutralize the false prophets of "religion" who urge their followers to violence while wrapped in religious clothing and quoting scriptures all the time? How can one defeat such problems without making enemies of whole religions, governments and the many good banks and businesses that exist next to the greedier, corrupt ones? These are very difficult questions to answer. But it is a duty of Special Agents to try, because bad bankers, industrialists, politicians and preachers can do far more damage to the people than ordinary criminals.

True Wisdom helps, but what is that? Wisdom is a quality of intelligence fused with ethics and deep understandings of both human nature and of the behavior of organizations such that 'the wise' can tell how things once set in motion will turn out. That is not easy. Unintended consequences are a perennial problem of governments, and are especially pernicious in the murky, deceptive world of intelligence affairs. But wisdom, like beauty, is very much in the eyes of beholders, and opinions vary enormously. I say, avoid trying to define 'wisdom' and cultivate it instead. This is introduction; now for some details.

How Wisdom Differs from Knowledge in National Security Intelligence Systems

The spectrum from data to information to knowledge to understanding to wisdom is important for intelligence professionals anywhere because their most common job is to distill vast volumes of data into very concise forms of much higher quality for the policy makers they advise. Therefore I commend this topic to anyone who would be an intelligence officer of any kind. But in this short paper I will focus on the quality called "wisdom" and how ethics, real ethics, is essential to that.

It is customary to start with definitions, but there can be no consensus on that for words like "wisdom." In fact, just defining the meaning of "intelligence" consumes whole papers in journals like the CIA's "Studies in Intelligence"[1]. In intelligence affairs where propaganda is abundant, he who controls a definition often controls an argument, and definitions can be very fickle.

Observe how the US government recently "changed" the meaning of the word "torture" in order to violate solemn treaties and conventions. As though any government or attorney can really change the meaning of things known for millennia. That decision was extremely unwise because it sacrificed many long term strategic strengths, like cooperation with allies, information sharing, and a modest reputation of respect for rule of law and human rights that took generations to create. All were sacrificed for scraps of intelligence of trivial and transient value. So I will discuss wisdom a bit without definition.

In the modern world of rapidly changing, interdisciplinary threats, even basic concepts like the meanings of "national security" have been reexamined. Traditional models of national security have been almost 100% military, but modern threats are not. The UN has promoted

a concept called "human security" that tries to go beyond that start, to notice things like "food insecurity", presence or lack of affordable health care, education, energy, "environmental security" and such[2].

George Cristian Maior, former Ambassador and current Director of the Romanian Intelligence Services wrote about these challenges for the Kennedy School at Harvard in 2011[3]:

> "Nowadays new risks such as the financial crisis, natural disasters, nuclear dangers as the ones now present in Japan, growing food insecurity, environment pollution or dangers to energy supplies are affecting national security and citizens' life as much as traditional threats if not even more. How should intelligence communities be prepared to deal with such threats that are difficult, if not impossible, to predict and to prevent? **In this respect, strategic knowledge relies on the ability to respond to the question of where national security starts and where it ends in the 21st century.**"

When struggling with such issues in 2003, I wrote a 'think piece' for the intelligence studies section of the International Studies Association[4] where I concluded:

> "Wisdom has a longer time horizon than either intelligence or knowledge. It spans a greater scope of concern, and reflects a set of values infused into knowledge that include compassion as a core component. It requires a deep understanding of human nature, because it is mainly called upon during crises of human affairs. All the rest is details that can distract from these cardinal truths."

So, longer time horizon, greater scope, values infused especially **compassion** and for guardians, **courage**, and some undefined, mystic like "understanding of human nature." How do such concepts fit with most bureaucracies? Not very well. In fact, intelligence bureaucracies can be among the most difficult, because of their traditional obsession with secrecy and focus on worst case scenarios[5]. You need look no further for evidence of dysfunction than to observe how intelligence bureaucracies treat whistle blowers even when those are exposing serious problems in the most judicious ways they can.

This is why I claimed in the beginning that a critical question every intelligence professional should answer for themselves is "What missions would I question or even refuse to do, and why?" This gets to the essence of who you are, why you exist, things that are at risk at moments of truth, in addition to whatever the state is concerned about. Unfortunately, bureaucracies often ask people to do immoral or stupid things and intelligence bureaucracies are no exception. In fact, some aspects of "intelligence" are necessarily 'dirty business' chosen usually as a less evil option than enduring some worst case scenario.

Professionals must discuss worst case scenarios seriously; military history is full of them coming true and people being exterminated. So someone must watch out for them (you) and be prepared to cope with them (you) even to die confronting them if necessary (you, and me). But balance on such topics is essential, lest you drive yourself into varieties of paranoid paralysis or worse, paranoid action.

This is where the 'longer time horizon' and 'greater scope' that wisdom surveys is helpful. Broader views generate better options. This is where the **courage** mentioned earlier is essential, because you must be prepared to face the 'worst case' in the blink of an eye with action, sometimes deadly action. But **compassion** is also essential, because you must remember that the field of battle is often littered with innocents, and that your information is always incomplete and sometimes is completely wrong. So rash action is exceedingly unwise unless the enemy is unambiguously in your eyes.

Remember that intelligence, even genius, are not the same things as wisdom. Nazi scientists were often brilliant but evil, precisely because they followed and served an evil national command. Nazi generals were, with some exceptions, dedicated and competent men. Many died trying to preserve their country when the national command became insane. Discerning the difference between good and evil is among the hardest tasks that wisdom faces. What to do when leaders go nuts is another. That difficulty is compounded by the secrecy and deception in military operations and especially in intelligence affairs.

If you are on the analytic side instead of operations, a particular evil may come to you that you must be aware of from the beginning to the end of your career. That is "politicization" of intelligence products by overbearing or irredeemably ignorant policy makers. Remember as I mention this, that you are NOT the policy maker unless you have been elected or appointed to such a position. You are an ADVISOR to policy makers who make those ultimate decisions. But all too often, ambitious politicians have taken advantage of this power imbalance to insist on "intelligence" that confirms their biases or career goals.

Well that is a delicate situation for the serious analyst, because he or she must be extremely devoted to truth and courageous enough to "speak truth to power" even when power is very unhappy about that. At the least, this advisor can be ignored thereafter, which is

considered a fate near death for those with career ambition. But it can get worse, as the fate of professionals who told Ceauşescu truth during his decline exemplify. A truly **Special** Agent must find ways to educate his sovereign even about very difficult things, or to survive blowing whistles if the boss is not educable.

Politicians tend to operate on very short timelines. Their scope of responsibility may be vast, but their scope of interest is usually focused on preserving power against domestic contenders, (~ 75 %+) or they won't be the commander who needs to be educated about some extremely difficult situation. So they tend to want to get things done quickly, visibly or secretly, and they want intelligence systems to help them. Wisdom wants to get the right things done, properly. These are not identical frames of reference, but it is the business of advisors to help the commander make the best decisions for the people and the state. The great Chinese educator General Sun Tzu had much to say about that in about 500 BCE[6].

> "Secret operations are essential in war; upon them the army relies to make its every move"[7].

> "Generally, in war the best policy is to take a state intact; to ruin it is inferior to this. To capture an enemy's army is better than to destroy it; to take intact a battalion, a company or a five-man squad is better than to destroy them. For to win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without fighting is the acme of skill"[8].

> "If not in the interests of the state, do not act. If you cannot succeed, do not use troops. If you are not in danger, do not fight. A sovereign cannot raise an army because he is enraged, nor can a general fight because he is resentful. For while an angered man may again be happy, and a resentful man again be pleased, a state that has perished cannot be restored, nor can the dead be brought back to life. Therefore the enlightened ruler is prudent and the good general is warned against rash action. Thus the state is kept secure and the army preserved"[9].

There is a reason Sun Tzu is still published and read millennia after most of the generals and emperors who hired him have been forgotten. Sun Tzu was wise; the others were merely intelligent or powerful. We should all aspire to that virtue during these difficult times for responsible nations.

Finally, a few words about "collecting" intelligence or wisdom. Obviously a large part of official intelligence involves gathering information about potential enemies and threats, then analyzing that mass of information into useful distillates that can help policy

makers. The policy people may then make better speeches, better laws, or task operators to act upon the world in some way, from propaganda to bribery to assistance to prosecution, or any of the thousand other options in their bags of tradecraft.

Well you can collect data easily, but it is very difficult to collect intelligence, and gathering wisdom is a truly Sisyphean task. It is more productive to try to grow such things slowly. You can gather tin cans or videos, and you can sort them in a thousand ways. But you cannot "collect" real wisdom, only data. REAL intelligence and genuine wisdom have to be cultivated, and they both involve refined abilities to throw out noise and to integrate meaning at least as much as to gather all the information that you can.

Aristotle thought that wisdom was a virtue. To Aristotle "intelligence" was an innate human capacity to acquire knowledge. Knowledge, however, was an acquired grasp of reality "the way it is" not just the way we wish it to be. And "wisdom" was an intellectual virtue, an acquired habit of reflection that perfects raw intelligence into something more useful and far more broadly based. Finally, both the Greeks and the ancient Hebrews had a healthy fear of hubris, which is an occupational hazard of both high political leaders and very smart people. Presumably those would include you. Be warned: hubris is extremely corrosive to intelligence, to wisdom, and to all the other virtues.

How "Real Ethics" Can be Cultivated: Core Values, Codes and "God"

The shortest path to "real" ethics is a good relationship with God, but what "God" is, what "God" wants and whether "God" is even a meaningful concept are topics of eternal dispute. Some think they know for sure, but none persuades consensus. And almost all evidence is testimonial. So I will spend some words on conventional ideas, like rule-based versus utilitarian ethics, and how to create a professional "ethos" in the hearts of individuals. Then I will return to the paradox of religious evils, like "holy" war, the ultimate oxymoron. But I repeat that when chaos prevails and danger is everywhere, rules written on paper carry very little weight. Whether you think you have a soul that actually endures beyond death and will be judged by something that animates the universe matters more. Those who do are prudent.

Western philosophers tend to divide "ethics" into three forms, rule-based (or deontological), utilitarian (where consequences matter more) and "virtue ethics" like Aristotle wrote about. Professionals of intelligence should be familiar with all three because they will certainly encounter each. Even the most daring Special Agent is supposed to obey some rules, if not those of their target country. Bureaucracies grow rules spontaneously, like bread grows mold. You won't be deployed unless the bureaucracy thinks it has SOME control over you. But bureaucracies do not have either souls or consciences.

So in addition to ordinary laws, and extraordinary exemptions from law that are often written for spies and intelligence organizations, some will try to create codes of ethics specific to their craft or "Core Values" cherished by their groups. For examples, the US Air Force core values are "Integrity, Service and Excellence" and US Army core values are "Loyalty, Duty, Respect, Selfless Service, Honor, Integrity, and Personal Courage." We will set aside for now all questions about dropping bombs on targets thousands of kilometers away from the person pushing the button, or beating someone to death in a prison in Afghanistan trying to get information they may or may not have. Core values must be very short, a list of words, almost always of universally positive and generally admired virtues.

Codes of Ethics tend to be longer, but still concise. For example, American doctors often swear to obey some version of the Hippocratic Oath during training. And if they want to belong to large professional groups like the American Medical Association they must also agree to uphold the AMA's "Principles of Medical Ethics." US Attorneys have a similar set of mid-level codes called the "Rules of Professional Conduct." Such codes often include some reference to "obey all laws" bowing to those far more detailed rule books that governments create.

The US intelligence community has been struggling to professionalize off and on since it was created, for which some code of ethics is required. But it has also been bedeviled by an unending torrent of tasks considered more important, and by other stresses of dealing with corrupt politicians and real worst cases daily. Jan Goldman, formerly with the National Military Intelligence College, now director of the FBI's graduate programs has been a pioneer in that Sisyphean task[10]. Dr. Goldman has been replaced at what is now called our National Intelligence University by retired Army Colonel J. D. Christopher Bailey who is doing the best he can to keep the ethics ball rolling in the heart of our declining global hegemon.

This has been and remains a very difficult birthing process for reasons already noted, but also because different Presidents often have extremely different ideas about what is moral to begin with. What Presidents want they tend to get, and they are the prime customer of our entire intelligence community. Every employee quickly learns that there are boundaries one can press, and others that just vaporize your career. Elder Romanians can no doubt tell you vivid stories about Romanian examples from the past.

Having watched this process from intimate positions for a long time I offer these observations:

- Codes are good, but take much longer to create than most suppose. It took our doctors and our lawyers over a century each, and it may take our spies longer due to the extreme conditions they work under and unusual problems they work on. We hope they succeed before someone blows up the planet.
- For a code to work well, it must be grown organically, not totally imposed from above. More than half of the value of these codes is the effort expended on discussing what they should be. So whatever code you might create, this is something mid-career people should strive to improve on, or at least to dissect as a normal part of professional development.
- Be wary of the lawyers even though you want some present. There should be real correlations between "law" and "ethics codes." But when governments go "bad" the law decays also. And attorneys often like to make the simplest things horribly complicated, which guts a key point. To work well codes should be clear, concise and emotionally compelling. Philosophers have the same vice. No one can argue the meaning of a single word for millennia like philosophers.
- A sage from Latin America told me that "ethics begin where laws end." Concise, and true as far as five words can be. Latin America has experienced a vast transition much like Eastern Europe, when military governments were replaced by more democratic forms. Therefore many Latins have thought hard about how to create intelligence organizations that truly serve their peoples instead of serving mainly a thin ruling class by surveilling and oppressing political opponents. That is the #1 question for intelligence communities today, far more important in the long run than "terrorists," a demon *du jour*. A review of the process of democratization of intelligence organizations, most Latin but a few European, is being edited now by Peter Gill of the UK[11].

- All the wise words of a million sages, a thousand presidents, and your personal boss may be less instructive at critical moments than memory of your mother or grandmothers. Remember them when contemplating words about morality, and you may find more durable answers.

Back to "God" for a moment. It is difficult for me to imagine growing up in a country where religion was suppressed, and it may be difficult for you to imagine a country like mine where religious enthusiasts are everywhere and come in 1000+ varieties, roughly half crazy. The most zealous from many traditions truly believe that "God" wants their personal children to occupy the entire earth. Put too many of those folks in the same place and something like war or genocide is much too likely.

You may read 100 books on "intelligence" and never see the word "God." So I must write about that as one human to another, with only a tiny focus on the special needs of **Special** Agents. There probably is a God, poorly understood by the organized churches. The churches are sincere, but hobbled by idolatry of words written by tribal men long dead, who could only write in the terms and languages of their time. After them came many editors, not all pure of heart. **Special** Agents observe that religious conflicts are a big cause of wars and violence on this earth, even though all the prophets spoke about peace as a prime objective. So this paradox is important to war forecasters and similar specialists.

What should matter to any human who deals with life and death issues are the questions of afterlife and judgment. There are rumors these occur. There is even some evidence of the scientific sort that can be contemplated, like systematic study of Near Death Experiences by physicians, or reports from remote viewers trained and deployed by the US Army, DIA and CIA over 20 years. Set aside the misguided "war" between science and religion – that is a distraction. One example is alleged contradiction between evolution and religion, fought over generations but solvable with nine words provided by my Ukrainian genetics professor Theodosius Dobzhansky. "Evolution is God's way of creating life on earth."

There probably is a God, and what you do in this life **MATTERS**, whatever you believe or not. If you intend to be a Special Agent for any country on earth today you have duties that transcend the commands of your superior officers. Our planet is in trouble; our civilizations endure incredible stress. Yet any moron with the "best" of special weapons could kill billions if he knew how to deploy one precisely.

So. In addition to your duties to your people and your state, I say that you have some duty to care about human survival as well, even if you don't work on that every day like me. We all do simple things each day, but we also all have higher responsibilities. If you have no faith in any God, then promote human survival for your children. God has plenty of work to do without dealing with you. Protect all children, because they are all precious. Protect the concept of innocence, because without it the noblest warriors can become mere mercenary killers. But if you are working on laws or codes or regulations related to intelligence operations, do not forget God. **IT** is the short path to ethics in challenging circumstances.

The Really Hard Cases in One Page: Torture, Murder and Worse

Philosophers and attorneys are fond of arguing extremely hypothetical cases until the sun grows cold. But **Special** Agents must be prepared to make life or death decisions in the blink of an eye with serious consequences for many people. So I will try to illustrate here interaction between rule based, utilitarian and virtue ethics with one of those bizarre, hypothetical cases.

Assume some "terrorist" or criminal genius has acquired a weapon that could blow up the entire planet, and for reasons comprehensible only to her has hidden it and set it to detonate within one day. This is an extreme version of classic 'ticking time-bomb' scenarios. The terrorist is in your custody, but will not talk except to babble rationalizations. She is an 80 year old grandmother of ten with an otherwise lovely record of compassionate, productive life. Remember, time is short and certainty scarce.

Relevant questions are:

- Should you torture her to try to find out where her weapon is?
- Might you torture or kill her grandchildren, one by one before her eyes, to get that information?
- Might you order a nuclear detonation over your main city, in hopes of destroying the weapon before it kills the entire earth?
- Should you offer her the bribe of anything she wants forever if she will tell you what you need to know? What if she says yes, but lies?
- Other options? Generating options for hard hypothetical cases can help in training for real cases.

Well rule based behavior says that you must follow due process of law no matter what, in which case the world might blow up

while the bureaucracy spends time and money in its normal sluggish ways. No torturing Grandma much less murdering her utterly innocent grandchildren. But kiss the earth goodbye.

Utilitarian ethics calls for the greatest good for the largest number (of people). Grandma's needs are tiny compared with the whole planet. So by that philosophy you might do anything to terrorist Grandma or even to her children if you think that will save the planet. Some practical problems. Torture seldom provides accurate answers quickly if at all. Do you know for sure that Grandma really is your terrorist or that such a weapon even exists? And who are you to label innocent children mere "collateral damage?"

Faced with dilemmas like these, the truly **Special** Agent will think hard about creative, 'out of box' solutions. In the end, he or she will choose the least evil option capable of protecting the people, or as many people as possible. Agents will need moral courage, more rare than physical courage, because they should be prepared to face a judge and jury to explain why they broke laws of God and Man in order to save the world. Agents should not be asking governments to break laws themselves, or to make special laws giving police immunity from accountability. If they do this they will enable the very police-state they are supposed to protect their people from. If you do so, believe me, corrupt states will find reasons to torture mere political opponents by calling such opponents "terrorists," and democracy may die.

Finally, never forget that in daily work on normal problems you are supposed to obey the law and your superiors at all times. This was an extreme, hypothetical case for teaching. There is no Grandma terrorist threatening to blow the whole world up. Whatever you do in whatever bizarre crisis that comes, you are accountable to our Creator who has heard every rationalization there is for human misbehaviors.

Conclusions

Teaching ethics is a teacher's nightmare. Even if you have a nice, tight, right sized code that is only a couple of pages long, try to get modern students to memorize that! Having failed once, try to get them to care. Remember, they must care deeply so ethics will be expressed when fear is sharp and chaos great. With ethics, knowing the rules is trivial compared with having the courage and insight to go in the right direction at the right moment in the excruciating circumstances of time urgent, life and death decisions.

Teaching wisdom; what is that? One can pile up quotes from sages and make your students read them (I recommend including some female sages from the modern era). For example, Cristiana Matei observed that in the great transition from communism, reform of Romanian security institutions was critically dependent on a newly independent and fiercely engaged public media[12]. We hope those critical independents endure, because evil powers have always tried to buy or bully publishers. The decline of independence among America's "major" media is a big reason for our failure to solve many other problems of governmental decay today. And "God" may bless the Internet, but our intelligence groups and operators were there first. Wisdom helps us to separate truth from fiction, and good from evil.

Is there a line you will not cross? This is the line you must know intimately, because in the heat and chaos of combat it distinguishes heroes from terrorists and madmen, not decisions by bureaucracies.

38 more pages of commentary on Ethics for Intelligence Professionals can be found in Chapter 44 of the Oxford Handbook of National Security Intelligence[13]. There one can find reference to the classic Just War Theory and clinical opinions on thorny issues like torture, targeted killings, when to switch from rule-based behavior to utilitarian calculations, and when choosing the lesser of evils among a set of ugly options is the best that one can do. But that chapter can be summarized much more concisely.

The primary duty of all intelligence professionals during these difficult times is to protect their peoples and their state (in that order) from a vast and metastasizing set of threats to innocent life and public order, in the worst cases even to human survival itself. The 20th century of the Common Era brought us many examples of intelligence systems that turned on their own peoples to serve corrupted governments. Therefore a quintessential challenge for modern intelligence professionals is how to keep your own government from becoming so corrupted that it becomes a danger to your own people. Good luck!

Among all these complex challenges, the easiest to understand is protecting the children who are our common future and as innocent as the dawn.

Be professionals, and protect them! Learn what you can about ethics and wisdom along the way.

References

[1] Michael Warner, "Wanted: A Definition of 'Intelligence'", *Studies in Intelligence*, Vol. 46, No. 3, Summer 2002, available at http://www.cia.gov/csi/studies/vol46no3/article02.html.
[2] Neil S. Macfarlane and Yuen Foong Khong, *Human Security and the UN: A Critical History* (Bloomington, IN: Indiana University Press, 2011).
[3] George Cristian Maior and Sergei Konoplyov (eds.), *Strategic Knowledge in the Wider Black Sea Area* (Bucharest: Editura RAO, 2011), p. 26.
[4] Michael Andregg, "How Wisdom Differs from Intelligence and Knowledge in the Context of National Intelligence Systems", paper presented at the Meeting of the International Studies Association in Portland, Oregon, USA, 28 February 2003. This paper has not been published, but is available at http://www.gzmn.org/pdfonline/ISApaper2003-Wisdomdiffersfromintel.pdf
[5] Michael Andregg,"Do Intelligence Bureaucracies Fear Ethics and if so Why?", *International Journal of Intelligence Ethics*, Vol. 3, No. 2, Fall 2012.
[6] Sun Tzu, *The Art of War*, translated by Samuel B. Griffith (Oxford University Press, 1963).
[7] *Ibid.*, p. 23.
[8] *Ibid.*, pp. 1-3.
[9] *Ibid., pp. 17-19.*
[10] Jan Goldman, *Ethics of Spying: a Reader for Intelligence Professionals*, 2nd edition (Lanham, MD: Scarecrow Press, 2010).
[11] Peter Gill and Michael Andregg (eds.), "Democratization of Intelligence Organizations", *Intelligence and National Security*, forthcoming 2013.
[12] Florina Cristiana Matei, "Romania's Intelligence Community: From an Instrument of Dictatorship to Serving Democracy", *International Journal of Intelligence and Counterintelligence*, Vol. 20, No. 4; Florina Cristiana Matei,"Romania's Transition to Democracy and the Role of the Press in Intelligence Reform," in T. Bruneau and S. Boraz (eds.), *Reforming Intelligence: Obstacles to Democratic Control and Effectiveness* (Austin, TX: University of Texas Press, 2007), pp. 629 – 660, 2007.
[13] Michael Andregg, "Ethics for Intelligence Professionals," *The Oxford Handbook for National Security Intelligence* (Oxford, UK: Oxford University Press, 2010), pp. 735-773.

The Activity of the Special Services of the Republic of Azerbaijan on the Counteraction to the Youth Recruitment into the Religious Extremist Organizations

Sultan MALIKOV[*]

Abstract

Globalization processes of a modern world, in particular, the deepening of the international interaction and cooperation, the ongoing development of information technologies and the growing transparency render various influences on the general security system of the country. The probability of a renewal of the armed confrontation, the occurrences of international terrorism, organized crime, and various sorts of economic risks define the main threats to the security of Azerbaijan. Undoubtedly, all of this influences the tasks put before the Foreign Intelligence Service by the government of the country.

In its turn, the Foreign Intelligence Service of Azerbaijan tries to become an effective tool in the decision-making process of the problems vital for the security of the state and in the process of neutralization of the threats stated above, aspires to faithfully serve its nation, as well as to thoroughly fulfill its assignment.

One of the main challenges of the present day consists of the display posed by the religious extremism with which many countries of the world had already come to face. Modern day conditions are allowing us to observe the expansion of the activities of religious extremist organizations representing threat to the safety of many states. This problem has ceased to be a problem of a single country and has acquired a much more global character.

As the experience of the special services of the Republic of Azerbaijan shows that just with the joint efforts on the channel of international cooperation, by coordinating our activities, exchanging the experience and the information in counteracting various displays of religious extremism and terrorism, it is possible to achieve desirable results in maintaining the stability and security of our states.

The main goal of the Foreign Intelligence Service of the Republic of Azerbaijan alongside with other state agencies of Azerbaijan is to detect and expose the arising threats, track the tendencies of their development, make an analysis and relate it to the country's leadership for the acceptance of a proper political decision. In general, the work of the Foreign Intelligence Service is directed towards the maintenance of national security of the country, as well as the protection of the national interests.

[*] Intelligence expert, Republic of Azerbaijan

Nowadays the Foreign Intelligence Service is engaged in a wide and diverse range of threats to the security of the state. It includes international terrorism, religious and political extremism, separatism, organized crime and narcotics trafficking.

The greatest threats to the security of our state are caused by the unresolved conflict with Armenia over the Mountainous Garabakh region of the Republic of Azerbaijan, the stalemate in peace negotiations and the 20 % of the Azerbaijani territories that have been occupied by Armenia. At present time, the situation when the Azerbaijani authorities do not control those territories creates favorable conditions for the separatists to implement smuggling operations, as well as illegal drugs and arms trafficking and trade, to create illegal armed formations, as well as international terrorist cells and to carry out other types of illegal actions. Tracking the developments in the specified problems is one of the most important duties of the Foreign Intelligence Service.

It is necessary to mention, that terrorism at the present stage became one of the most serious sociopolitical problems, which in its process of evolution affects not only the security of a single country, but the international stability as a whole. Nowadays, terrorism has stepped out of the boundaries of a single nation's borders, has acquired the form of a global threat to mankind, has affected different sides of the social, political and economical life of a society. Year after year manifestations of international terrorism acquire all new features and dangerous aspects. The forms and methods used by terrorists are getting improved every day. Leaders and ideologists of terrorist organizations are using the newest technologies and advanced weapons in their subversive activities. There is a real threat of an absolutely new type of technological terrorism. The variety of attacks conducted by terrorist organizations, as well as the constant danger to the public proves the necessity of conducting the war on terror not only at an interstate, but at an international level. State of affairs dictates that the work of the Foreign Intelligence Service and its interaction and cooperation with the special services of other countries begets even greater significance. The experience acquired from such a cooperation by the special services of the Republic of Azerbaijan have proven that joint efforts in the struggle against terrorism had been essential in the process of achieving the desired results.

At the same time, it should be mentioned that there is a growing necessity for international cooperation between special services in a struggle against illegal drug trafficking, money-laundering, illegal migration and other forms of organized crime.

Globalization processes of a modern world, in particular, the deepening of international interaction and cooperation, the ongoing development of information technologies and the growing transparency render various influences on the general security system of the country. The probability of a renewal of armed confrontation, the occurrences of international terrorism, organized crime, and various sorts of economic risks define the main threats to the security of Azerbaijan. Undoubtedly, all of this influences the tasks put before the Foreign Intelligence Service by the government of the country.

In its turn, the Foreign Intelligence Service of Azerbaijan tries to become an effective tool in the decision-making process of the problems vital for the security of the state and in the process of neutralization of the threats stated above, and aspires to faithfully serve its nation, as well as to thoroughly fulfill its assignment.

One of the main challenges of the present day consists of the display posed by the religious extremism with which many countries of the world had already come to face. Modern day conditions are allowing us to observe the expansion of activities of religious extremist organizations representing a threat to the safety of many states. This problem has ceased to be the problem of a single country and has acquired a much more global character.

The main goals of religious extremism can be defined as the usage of violent and illegal means directed to the task of kindling of many inter-ethnic and inter-confessional conflicts, as well as overthrowing the government and changing the political system. Most of the religious extremist organizations masking behind the cover of the appurtenance to the worlds' religions in reality propagandize their own political goals. The ideology of those religious extremists concentrates not only on the struggle with the infidels, but also with the citizens adhering to the secular way of life.

Nondependent of the doctrines on which religious extremist and terrorist organizations form their outlook (vahhabism, fundamentalism, salafism, radical Shiism and so on) the main feature uniting all of them is the continuous expansion of their ideology in order to increase the numbers of their supporters.

The operational experience acquired by the special services of RA on the channel of counteraction to religious extremism has shown that preachers of religious extremism who are in the business of recruiting new members for the organizations are, as a rule,

concentrating their attention on the so-called marginal layers of the young generation which are, for some reason or another, appearing not to be in demand by the society. Overestimated expectations from life and the inability to realize their own needs leads to self-alienation of some young citizens within the structure of any given society, as well as, to illusions concerning their ability to make changes to the existing order. Such category of youth is the most vulnerable and pliable to the influence of propaganda dispersed by religious extremist organizations, which in reality are aspiring to use it for their own political goals.

The most common form of recruiting youth for religious extremist organizations is the invitation to study at religious educational centers, many of which are controlled by extremists disguising themselves under the banner of radical Islam.

Extremist religious organizations are trying to invite youngsters to enroll in religious educational institutions illegally, at first recruiting and then taking young citizens to the territories under their own control, utilizing many informal channels. The complexity of the situation consists of the difficulties involved in conducting statistical follow-up not only on the citizens who have illegally left for study, but also on the religious educational centers themselves. Thus, alongside with a number of foreign religious centers new ones periodically appear. These centers, as a rule, function only for a short period of time and frequently are not even known to the related state structures of the country in which they operate. This results in complications for the task of inventorying those religious educational centers.

Special services of RA among others is engaged in solving the problems above mentioned and leading in purposeful work on acquisition of anticipatory information on the channel of an illegal enrollment of young citizens in religious educational centers controlled by various religious extremist organizations. As a result of continuous intelligence gathering operations the special services of RA were able to reveal and identify several similar educational centers functioning in some Central and Eastern Asia countries, where citizens of RA were studying.

It is known that many of these educational institutions are used by extremists for recruitment of their listeners, especially foreign citizens. Recruited students are then being sent to various camps and ideological centers. At these camps youngsters are being

taught the trade of terror and acquire necessary skills for a future deployment in the country of their residence. Thus, these people in due course become the initiators and the heads of underground network structures connected with international religious extremist and terrorist organizations.

Recently, due to timely and forestalling intelligence information acquired by the Foreign Intelligence Service, as well as, efficient and precise interaction of all special and law-enforcement bodies, the activities of a number of terrorist and extremist organizations in Azerbaijan were possible to be stopped. During operational and investigatory activities it was established that some young members of the extremist groupings mentioned above had illegally traveled abroad and received combat training in various terrorist centers and camps under the pretext of religious education.

For the purposes of preventing and suppressing possible and probable acts of extremism conducted by the youngsters studying in a various religious educational institutions abroad, the special services of RA, alongside with the continuous intelligence and counterintelligence activities, closely interacts with such state and public structures of the country, as the State Committee on the Work with the Religious Organizations, the Ministry for Foreign Affairs, the State Committee on Work with Diaspora, the Ministry of Education, the Ministry of Youth and Sports, the Moslems' Spiritual Administration of Caucasus and numerous other nongovernmental organizations. This interaction assists in the task of accumulating the necessary statistical follow-up on the citizens studying abroad and conducting the explanatory and prophylactic work amongst them, as well as the task of detecting and identifying the persons influenced by extremist religious organizations.

Huge help in the organizational part of the struggle against international religious-extremist groupings is rendered by the daily work done by the Foreign Intelligence Service on the acquisition, systematization and analysis of intelligence information concerning the persons and the educational centers involved in religious-extremist activity, as well as the creation of an operational database for their statistical account. The above mentioned work lays the ground stone for the effective operational and search activities, for the detection of negative tendencies and potential threats arising from the religious-extremist activity, as well as the prevention of possible and probable illegal actions of an extremist orientation.

It would be necessary to mention, that the intelligence materials gathered by the Foreign Intelligence Service of RA, after corresponding analysis and processing are used in propaganda activities aimed to discredit the activities of the religious-extremist and terrorist organizations and their leaders. These materials are being placed in mass-media and used in the explanatory and prophylactic work conducted with youngsters and representatives of educational establishments.

The use of the Internet by various extremist organizations has become one of the recent ways of recruiting the youth for extremist activities. The opportunities provided by the world-wide network are used by extremists in searching for supporters, applying psychological influence on them, enrolling youngsters into religious-educational centers controlled by them, teaching those supporters the trade of conducting an act of terror, under various slogans attracting the youngsters to their criminal activity, conspiring their own goals and plans, as well as safely exchanging the necessary information. For this purpose, on various Internet sites, extremist type materials appealing to conduct an illegal action are placed and discussions on religious-extremist themes are held.

For the purposes of preventing and suppressing the possible and probable crimes of a terrorist and extremist orientation, the special services of RA conducts search, analysis and apprehension activities in the global information network aimed at the detection of the local citizens involved in extremist activities.

The investigations conducted by the special services of RA revealed that some extremist groups have placed numerous materials on the site controlled by them appealing to overthrow the secular government and to establish a Shariah state in Azerbaijan. During the investigations it became known, that the authors of the well-known internet-portal “Caucasus Center” were actively involved in the process of creating that site. By the verdict of the Grave Crimes Court of RA all members of the group have been condemned and the activity of the site controlled by them has been stopped. At the same time, for the purposes of preventing a similar sort of crime, especially amongst the young generation, special attention has been given to the wide coverage, with the concentration on the specifics of the caused harm, of the given process in mass-media.

It is necessary to mention, that for the purposes of radicalizing the actions of their supporters, religious-extremist organizations use a variety of slogans, leaflets and other literature of the extremist sense, calling upon their supporters to fight for "Islamic order", to conduct acts of violence, to create illegal armed formations, to kindle inter-ethnic and inter-confessional enmity. For this purposes religious extremism frequently began to resort to terror, hoping, as a rule, to achieve a psychological effect from their actions.

For example, in 2008 as a result of the timely acquired intelligence information during the continuous investigation regarding the persons involved in the illegal armed formations, the activities of the religious-extremist and terrorist grouping called "Forest brothers" headed by the emir of the "Dagestan front" Ilgar Mollachiyev had been uncovered and stopped. That grouping was involved in many crimes on the territory of the republic, including the terror act of August 17th, 2008 that took place at the "Abu Bakr" mosque in Baku. During the investigation, it had been established that members of the grouping prepared numerous terror acts in Baku and several regional centers of Azerbaijan with the purposes of destabilizing the political situation, creating an atmosphere of fear and intimidation, as well as initiating panic moods amongst the population. Certain concerns were caused by the attempts of the extremist groupings' members using the religious factor to kindle religious intolerance among the population of the border areas, initiation of separatist moods and creation of preconditions for an encroachment on the sovereignty of the country.

Recent developments proved that religious extremism in Azerbaijan must be approached from the regional perspectives, as the aims of the terrorists are not limited only to damaging the Azerbaijani state, but also forwarded towards Western interests in the country. At the same time, all terrorist attempts in Azerbaijan have had international dimension and have somehow been affiliated with broader terrorist cells operating either in the neighboring countries or in the Middle East. For example, just before the Eurovision song contest in Baku, the MNS of Azerbaijan neutralized an armed group headed by Azerbaijani national Vugar Padarov and prevented a series of terror actions in Azerbaijan.

It would be prudent to mention, that the Foreign Intelligence Service of RA constantly traces and analyzes the activities of religious-extremist groupings in the world and their possible relations within Azerbaijan. The analysis of the gathered intelligence

on this channel shows the tendency towards amplification in recruiting young citizens and radicalization of the specified groupings' illegal operations.

Taking into consideration the global character of the threat caused by the spread of the religious extremism, it is necessary to acknowledge, that a single national intelligence agency would not be able to solve this problem. In this regard, there is a necessity for a closer cooperation between intelligence and other law-enforcement services of the countries involved in the fight against this international form of evil.

The special services of the Republic of Azerbaijan emphasize international cooperation in fighting against religious extremism and terrorism. Due to the coordinated and united work with a lot of partner special services, experience and information exchange the activity of a number of cells of international religious extremist and terrorist organizations have been exposed, as well as possible, unlawful operations have been prevented on the territory of Azerbaijan lately. At the same time, the information provided by the special services of the Republic of Azerbaijan has been favorable to some of our partners for preventing possible destructive actions on their territory in proper time.

It should be mentioned that along with the information exchange on matters being of mutual interest international cooperation promotes to gain necessary professional experience in fighting against religious extremism and terrorism, as well as to create an operational data bank on the activity of international organizations and groups with extremist and terrorist orientations and persons involved.

Therefore as the experience of the special services of the Republic of Azerbaijan shows, only by the joint efforts on the channel of international cooperation, by coordinating our activities, exchanging experience and information in counteracting various displays of religious extremism and terrorism, it is possible to achieve desirable results in maintaining the stability and security of our states.

Security Structures Approaches on Critical Infrastructure Protection Issues in the Context of an Increasing Globalization Process

Ana Ligia LEAUA[*]
Dragoş ARDELEANU[*]

Abstract

The trends and perspectives of the globalization process require new directives for the integrated approach of critical infrastructure protection in the security strategies.

Implications of threats to critical infrastructures and the need to protect them were consistently reflected in the elevated concerns of state governments and international organizations in order to improve, on the one hand, the security strategies subsumed to the identification and protection measures for these types of infrastructure and, on the other hand, the institutional and organizational security systems, in order to allow the identification and early warning of risks, while adopting and initiating timely decisions/preventive intervention approaches and countermeasures.

This research analyses the approaches of the security structures on critical infrastructure protection issues, taking into account cross-border interconnections of critical infrastructures and the field of occurrence risks that borrowed representation and evolution elements set by the globalization process. This phenomenon is characterized by higher chances for an increased intensity and amplitude of the aggression's effects aimed at a component or the whole system on the national territory of other states.

Introduction

Dynamics, dimension and concentration of the activities related to the globalization process, to maintain the independence or to rally to new architectural configurations of the micro and macro regional sphere, induced new vulnerabilities and threats to global security. The globalization process is in close relationship with the interference of great powers on emergent markets aimed primarily at strengthening political and economic position globally, but also with the opposition of targeted countries by traditionalist means, especially religious ones.

An important issue concerning the new security challenges are the threats generated by the global warming phenomenon (causing

[*] Assistant Lecturer, "Mihai Viteazul" National Intelligence Academy
[*] Lecturer, "Mihai Viteazul" National Intelligence Academy

extreme weather events) and also the vulnerability of technological systems as a result of unauthorized intrusions (with a high degree of permissiveness due to the interdependence with computer systems) and its inappropriate exploitation. The destructive effects are evident for the viability and stability of infrastructure networks.

Rapid and sometimes high unpredictable developments, coupled with the size and complexity of vulnerabilities and risks, generate a key challenge for critical infrastructure protection systems.

Risks and threats to vital objectives related to the good functioning of the society and to citizens' security have acquired new meanings, with high dynamics and high degree of intensity, which led to the need for an integrated approach of the "critical infrastructure" concept.

The concept of "critical infrastructure" and "protection of critical infrastructure" have seen, over time, several forms of approach, given the technical and economic specificity, the research and risk coordinates, and the strategies adopted by different states or organizational types.

Although approaches vary, based on the common elements regarding the importance of safe functioning and the induced effects, the "critical infrastructure" concept can be assimilated with any functional economic entity that provides products, goods and public services vital for the entire society and whose destruction or degradation has a major impact at socio-economic level, at micro and macro regional level[1].

Taking into consideration the basic characteristics of critical infrastructure, the critical element of its stability, including the transboundary context, has acquired new connotations in terms of national/transnational strategies.

The complexity of critical infrastructure protection (CIP) and its importance to social stability, or citizen and state security generated a concrete correlation of the strategies initiated by states and organizations.

The US Critical Infrastructure Protection Approach

The critical infrastructure issue has been configured more significantly as a topic of interest, especially toward the end of the 20th century and the beginning of the current one, mostly as a result of escalated risks and asymmetrical danger (determined, mainly, by traditionalist religious threats, subsumed to acts of terrorism but also by extreme weather phenomena). The strengthening of these risks

has generated consistent premises for the appearance of vector threats toward infrastructures, mostly those with an elevated risk of being critical to stability and social and economic security.

The concept of critical infrastructure had its genesis and was developed in the US, being initially a research product determined by analysis made during the 1980s regarding the infrastructure's conditions - improper technical conditions, technological adequacy and the need of developing it according to increasing economic and social requests of that country.

The 90's accelerated the process of defining the concept of critical infrastructure, as a direct result of the attempts to define and implement a new world order which would respond more adequately to the new manifestation forms of dangers and threats, specific for the post-Cold War period. The concept of critical infrastructure was promoted during those years, especially in federal countries (United States, Canada, Australia) determined by the need for a holistic approach of safety in systems regulated by federal laws but also by local authorities.

Officially, the term "federal infrastructure" - defined as "part of the national infrastructure so vital, that its destruction or incapacitation can severely diminish the defense or the economy of the USA" - was first used in June 1996, in the Executive Order no. 13010 for Critical Infrastructure protection[2]. On February 27, 1998, during the Conference for Critical Infrastructure Protection, which was held at Lawrence Livermore Laboratories, in Livermore, California, Attorney General Janet Reno announced the founding of the National Infrastructure Protection Center - NIPC at the FBI headquarters, Washington DC. On May 22, 1998, President Bill Clinton announced the launch of two new directives designed to strengthen US defence against terrorism and other nonconventional threats: Presidential Decision Directives (PDD) 62 and 63. PDD-63, entitled Critical Infrastructure Policy[3], which defined seven sectors as components of critical infrastructure - energy, telecommunications, emergency services, financial, transportation, oil and government services, is focused mainly on protecting critical infrastructure from physical and cybernetic threats.

As a result of the 2001 September events, the USA Patriot Act was emitted, containing a section dedicated exclusively to the protection of critical infrastructure, also known as the Critical Infrastructure Protection Act. This defines critical infrastructures as systems and assets, physical and virtual, vital for the US, whose

incapacitation or destruction would have a destabilizing effect on the security, economic, healthcare or public safety sectors, in any possible combination. Also, the contents of this act highlights the interdependency between the private sector, government and security structures on one hand and the interconnected physical and informational infrastructures, including communications, energy, financial services, water supply systems and transportation grids, on the other hand - the National Infrastructure Simulation and Analysis Center (NISAC) being founded. This institution represents, at national level, a source of competence on critical infrastructure protection through activities linked with the fight against terrorism, threat evaluation and risk management.

In 2002, through the USA Patriot Act, the Department for Homeland Security was established in which the Director of Information Analysis and Infrastructure Protection functions, having responsibilities in the area of critical infrastructure security, including the virtual one.

Homeland Security Presidential Directive 7 (HSPD-7) (December 17, 2003) defined the policy of the US for a better protection of Critical Infrastructures and Key Assets - CIKR, by establishing a framework for National Infrastructure Protection Plan (NIPP) partners, in order to identify, prioritize and protect critical national infrastructures from terrorist attacks. This framework provides the unification structure into a single national program for the integration of existing and future efforts to protect infrastructures and "key assets" (CIKR).

The directive has identified 17 sectors of critical infrastructure and has designated a federal one (Sector-Specific Agency – SSA) to lead the protection efforts in every sector, allowing the Department of Internal Security to identify the gaps in existing sectors and establish new ones for filling these gaps. Under this authority, in March 2008, the Department established the 18th sector "Critical Manufacturing Sector"[4].

The Policy Framework in European Union and Romania

At European level, in the general context of increased terrorist threats as well as that of a more pragmatic response in case of natural disasters, the European Commission adopted in 2004 a Communication on critical infrastructure protection in the fight against terrorism, which presents the preventive measures in the case of a terrorist attack and the response actions to these attacks.

In 2004 the European Network and Information Security Agency (ENISA) was established through the Regulation of the European Parliament and the Council of Ministers no. 460/10.03.2004. ENISA is specialised in security issues, and its site serves as a "hub" for the exchange of information, best practices and knowledge in the field of information security related to critical infrastructure[5].

Subsequently, EU Council conclusions on "Prevention, preparedness and response to terrorist attacks" and "EU Solidarity Programme on the Consequences of Terrorist Threats and Attacks" were developed, which gave rise to the Commission's initiative to elaborate the European Programme for Critical Infrastructure Protection (EPCIP)[6] and initiate the Critical Infrastructure Warning Information Network - (CIWIN)[7].

The "Green Paper" on an European Programme for Critical Infrastructure Protection (2005) sets out the principles for developing EPCIP and the designation by Member States of relevant areas of critical infrastructure: subsidiarity, complementarity, confidentiality, cooperation, sectoral approach and proportionality.

Separately, the "Green Paper"[8] states that the definition of what constitutes European Critical Infrastructures (ECI) is determined primarily by the transnational effects that an incident occurred on the territory of a Member State might have on the other EU states. ECI could include those physical resources, services, information technology elements, networks and infrastructure assets whose disruption would have a serious impact on the health, safety, security and socio-economic welfare:

- of two or more Member States interconnected on certain segments of critical infrastructure;
- of three or more countries – in this case addressing the problem involves the extended format of inter-state and inter-institutional cooperation.

After the adoption of the "Green Paper", the European Commission has designated as critical infrastructure those segments where "errors, incidents or attacks would affect both the state where they were produced, and at least another European Union member state". Also, ECI were divided into two broad categories:

- "general critical infrastructure" (CI) - such as power grids and financial services etc.;
- "critical information infrastructure" (CII) – including all IT&C systems, vital by themselves and essential for the good functioning of other critical infrastructures - telecommunications, Internet, satellites, etc.

The main document that outlines specific tasks and provides the procedures and parameters to be respected by Member States when designating critical infrastructure is Directive no. 114/2008 of the European Union Council on the identification of European Critical Infrastructures and the assessment of the need to improve their protection.

According to the Directive no. 114/2008, National Critical Infrastructure is "a system or a part thereof located in Member States, which is essential for the maintaining of vital functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions" and European Critical Infrastructure is a "critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States". The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure".

Congruent to the Directive no. 114/2008/CE, European Critical Infrastructures are defined only from two economic sectors: energy and transport[9]. The major objective of the document is to accelerate the development by Member States of their own unitary protection systems for critical infrastructure, so that after completing this step, these systems will allow the creation of a central European authority.

In the future, the expansion of new major infrastructure segments - Telecommunications and Information Technology - outlines the need to complete the ECI portfolio, taking into account:

- their role in ensuring interdependence and coordinated functioning of all other components;
- the degree of risk of cyber attacks, resulting in the ratio between the costs for organizing and committing it and the damages generated to the segments on which it is directed.

The Telecommunications and Information Technology sector was regulated at EU level through the Commission Communication no. 149 from March 30, 2009 "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience"[10].

One of the major objectives of the European Union is represented by the necessity to reduce the transnational nature of critical infrastructures issues and to speed the implementation process regarding the unitary measures, following the American model (where, unlike the EU, the issue has mainly a national character).

The similar spectrum of threats and risks to the security of critical infrastructure in the US and EU requires a transatlantic approach including dialogue on delimitation and regulation of the critical infrastructure domain. In this regard, an argument could be the example of public-private partnerships in the US with expert groups operating within them.

At European level the implementation process acquires new dimensions due to the following aspects:

- different criteria on infrastructure designated as CI;
- national goals versus community goals;
- unequal levels of infrastructure development;
- uneven exposure to threats;
- reluctant communication;
- constant need to adapt legislation and implementation.

Although, as the European society is developing in an interconnected way the dependence on the state of functionality of the critical infrastructure inevitably increased, a significant part of the organizations and people seem to underestimate the risks the sectors of vital importance are exposed to. This situation was reported by the Centre for European Policy Studies, who stressed the imperative of establishing, through public - private partnership (PPP), a well-balanced cooperation formula between European and national institutions, on the one hand, and private owners/operators on the other hand[11].

In the current context, nationally, by adopting GEO no. 98/2010 on the identification, designation and protection of critical infrastructure (approved with amendments by Law no. 18/2011) the following National Critical Infrastructure (NCI) sectors have been established: energy, water supply, food, healthcare, administration, transportation, chemical and nuclear industry, research and space, as well as the responsible public authorities.

The legal requirements of GEO no. 98/2010 (that established 10 sectors/31 sub sectors of NCI) comprise:

- design of security plans by operators (OSP): conducting a risk analysis, identification of important assets, identification, selection and prioritization of counter-measures and procedures;
- classified information protection;
- exercises, reports, re-evaluations and updates of documents.

The Institutional Working Group for Critical Infrastructure Protection was established in order to implement the legal framework regarding this domain, by Government Decision no. 1.110/2010.

The Coordinating Centre for Critical Infrastructure Protection within the Ministry of Administration and Interior (MAI) has the responsibility of organizing and developing the necessary activities for implementing the legislative framework and achieving cooperation between public authorities and non-governmental structures. This entity ensures a national contact point in relation to other Member States, the European Commission, the North Atlantic Treaty Organization (figure 1) and other international bodies, as well as the national CIWIN network management. Through the CIP Coordination Center, MAI:

- every two years delivers to the European Commission a summary report containing general information on the types of risks, threats and vulnerabilities identified in each of the sectors where ECI has been designated;
- supports competent public authorities and owners/ operators/managers of designated NCI/ECI, giving them access to information on best practices and methods available and facilitating participation in training and exchange of information sessions on new technical developments in the field of CIP, coordinated by the European Commission[12].

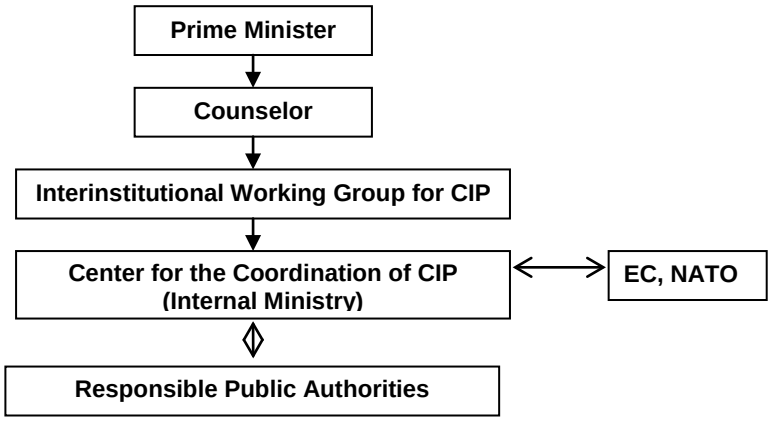


Fig. 1: *The decisional flow (critical infrastructure protection)*

The responsible public authorities have developed the procedure for identifying National Critical Infrastructures/European Critical Infrastructures by applying criteria, critical sectoral/intersectoral thresholds and security plan requirements for their operators.

The legal framework was completed by the National Strategy for Critical Infrastructure Protection, approved through GEO no. 718/2011, realized in accordance with the programmatic documents

in the area of national security and defense, thus establishing policies and courses of action in the field, necessary to develop and to complete the national normative framework[13].

Community-wide recommendations on European critical infrastructure protection and joint actions taken at the national level stress the irreversibility of the direct connection between the domestic objectives/strategies and the ones targeted by the EU bodies and simultaneously accelerate their inclusion on the path of uniformity and harmonization, a necessary aspect and of mutual interest.

The implementation of the legal requirements regarding the protection of critical infrastructure is hampered by a number of disturbing factors:

☑ the emergence of new CI sectors;

☑ the implementation of strategies: sharing information, segments interdependencies, associated to CI backup plans;

☑ terrorism;

☑ setting an equilibrium between budgets and priorities;

☑ global issues: cyber attacks warning and alert, harmonization of legislation.

The National Security Structures Measures to Protect Critical Infrastructure

Usually, critical infrastructures are vulnerable to a range of internal/external factors, facing the risk of being destroyed or disabled[14]. Especially damaging those interdependent systems ("systems of systems") that ensure the connection between regions and continents can have a wide scale impact at regional, continental or intercontinental level (financial and banking systems, customs and transport control systems, etc.).

Given the increased vulnerabilities of infrastructures and the multiple causes of malfunction - human, natural or technological causes - governments and institutions are increasingly concerned about their security.

This is the reason for the overall protection of public (governmental, military), as well as private networks and systems, by physical, judicial and informational measures against the actions or the inactions that affect their operation and security.

The need to secure the critical infrastructure is supported by:

- the growing frequency and intensity of extreme natural phenomenon, induced by climate change and global warming;

- the intense exploitation and operation of some infrastructures at their maximum limits, which can deteriorate their stability due to inappropriate use, climate change or introduction of new technologies;
- local/regional events causing accidents that disturb or disable regional and sometimes global networks of critical infrastructures;
- totally secure functioning of the basic utilities or IT systems impaired due to ongoing extensions of related equipments, which require complex measures that often exceed the capabilities of the management structures.

Infrastructures are or become critical primarily due to their vulnerability to those threats that target them directly or are directed against systems, actions and processes which they belong to. Threats to critical infrastructures are conditioned and favoured by at least three very important factors[15]:

- lack of flexibility, given the fixed nature and relatively precise location of infrastructure, including the critical ones;
- the flexibility and fluidity of dangers and threats to critical infrastructure and the very broad spectrum of their manifestations;
- the unpredictable and surprising nature of threats to critical infrastructure.

After September 11, 2001 the main threat on which the efforts of states are being concentrated in order to acquire and maintain their protection and security is represented by international terrorism. With the increasing dependence of society on its basic structures and the use of modern technology by terrorist organizations the need to protect critical infrastructure against terrorist attacks has increased. The level of this type of threat in Romania remains low. In our country, so far, critical infrastructures in various sectors have been particularly affected by extreme weather phenomenon. It is expected that, in the future, climate changes will add further pressure on critical infrastructures, even in temperate climates.

Another major category of risks is arising from equipment damage, due to insufficient/inefficient maintenance, rehabilitation and upgrading and the cyber dimension (hardware and software). Effects consist of potential interruptions in the operation of critical infrastructure information systems as a result of criminal acts, errors or technical/human malfunctions, natural disasters or managerial deficiencies.

Each critical infrastructure poses a degree of risk, estimated and even assumed by users/beneficiaries. Risks in this area are systemic[16] and characterized by complexity, uncertainty/insecurity and ambiguity.

Therefore, a constant concern nationally and internationally is the assessment and management of risks related to critical infrastructure protection, as it is necessary to cover more extensive areas, from traditional (accident, malfunction, human error, etc.) to emerging ones (terrorist attacks, excessive computerization of systems and critical infrastructures and effects induced by natural disasters and climate changes). Risk assessment is based on its complexity, context of occurrence and the consequences it generates.

Risk management requires a systematic and integrative approach and is based on: transparency, openness, communication, accountability, efficiency and conflicts of interest mediation, requiring a thorough knowledge of the operational situation of the critical infrastructure, firm application of the procedures provided by the law and initiation of appropriate action for:

- preventing the occurrence of dysfunctions and vulnerabilities;
- removing threats and threatening situations and reducing/eliminating the consequences in case of their materialization;
- countering aggressions;
- restoring their functionality.

The main actions taken by the security structures for the protection of National Critical Infrastructure are related to:

- intelligence action – constantly and timely inform the state's decision-makers on threats, vulnerabilities, dangerous and risks affecting CI;
- physical protection – intervention in case of an imminent materialization of any kind of threats (terrorist attack);
- cyber-intelligence protection – prevent and counter attacks on computer systems.

The measures taken must be proactive, following the steps of an effective risk management process, namely:

- detection (knowledge/forecasting/prediction);
- monitoring (analysis/evaluation, strategies for prevention/ response adapted on a case by case basis);
- communication (awareness/warning public opinion and also practice/control/operationalize the intervention for the actors with responsibilities in this area).

Risk management must be made on the basis of operational strategies, with the objective of developing, maintaining and protecting critical infrastructure including[17]:

- development policy: the decision-maker awareness (political/economic, leadership of institutions/companies) on the need for critical infrastructure design and construction based on a project

that drastically reduce the possibilities of occurrence from the very beginning of special events (disorder, accident/failure, disaster, human actions, especially terrorist attacks, sabotage or incidental error);

✓ maintenance: solutions that ensure an optimal relationship between costs/benefits, taking into account the functioning of the systems in situations other than the normal ones;

✓ protection: timely identifying the vulnerabilities and dysfunction and operationalizing the intervention algorithm for emergency situations.

Critical infrastructure can be affected simultaneously on the physical level and symbolic structure so that, according to the amplitude of dysfunctions, vulnerabilities or risks, the whole national security system can be affected[18].

The complexity and diversity of critical infrastructure, domestic and international security environment influences, often marked by challenges and unpredictable events related to national, regional and international security, require deep and comprehensive information activities of a preventive anticipatory nature.

Anticipating existing or predictable risks to the critical infrastructure and the disturbing factors determine the legally qualified intelligence services to conduct mainly preventive activities, in order to reduce, eliminate and counter the actions of risk generating sources, create structures and train specialized personal for this purpose.

In knowing the dysfunctions, vulnerabilities, risk factors, threats and threatening situations related to critical infrastructure and, consequently, the national security, a fundamental role is being played by the searching and obtaining of relevant information activities and the process of transmitting/communicating this information to the factors legally entitled to take preventive and counteracting decisions. This objective can be achieved if there is a permanent communication, based on an appropriate legal support, a specific responsibility reported to the legal competence between information structures legally established, state institutions, public authorities, NGOs, communities and citizens.

Conclusions

An analysis of the potential risks to critical infrastructures requires an integrated approach to the description and implementation processes of all strategies and the procedures and programs for prevention, preparedness, response to disasters and emergencies.

The success and effectiveness of these common actions will depend primarily on the efficiency of the process in which EU Member States will comply with EU legislation and programs and the extent to which they manage to mobilize, through public-private partnership (vital taking into consideration the fact that many of the organizations/operators/managers of critical infrastructures were privatized), active operators on the infrastructure segments of critical importance for safe operation in the economic and social environment at EU level.

Constant security strategies updates (here we are referring to both the current expansion of infrastructure – transport and computer networks - as well as future major projects that our country will be involved in) and the permanent changes in the spectrum of threats posed increasing problems regarding the delimitation of segments designated as critical infrastructure.

In order to reduce vulnerabilities and increase responsiveness, the security structures responsible for the protection of critical infrastructure should grant special attention to the following aspects:

- developing the perception capacity and referenced expertise;
- involvement in all legislative and implementation efforts related to critical infrastructure protection;
- strengthening of institutional cooperation at national, European and macro-regional level due to growing interdependences between similar components of security structure;
- improving the communication of warnings, risk assessments and security reports to appropriate government structures.

References

[1] *International Journal of Critical Infrastructures*, Vol. 1, No. 1, 2004.
[2] Executive Order Critical Infrastructure Protection available at http://www.fas.org/irp/offdocs/eo1301htm.
[3] Presidential Decision Directive 63, available at http://www. fas.org/irp/offdocs/paper598.htm.
[4] Available at http://www.dhs.gov/files/programs/gc_1189168948944.shtm, http://www.dhs.Gov/xabout/laws/gc_12145 97989952.
[5] Available at http://europa.eu/agencies/community_agencies.
[6] European Programme for Critical Infrastructure Protection – EPCIP, available at http://europa.eu/legislation_summaries/justice_freedom_security/fight_agains_terrorism/l33260_en.htm
[7] "Critical infrastructure protection", available at http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_ terrorism/l33259_en.htm.
[8] European Comission, Green Paper on a European Programme for Critical Infrastructure Protection - Com(2005) 576 final, Brussels, 17.11.2005.

[9] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection.
[10] "Protecting Europe from large scale cyber attacks and disruptions", available at http://europa.eu/legislation_summaries/information_society/internet/si0010_en.htm
[11] http://www.ceps.eu/taskforce/critical-infrastructure-protection-eu.
[12] GEO no. 98/2010 on the identification, designation and protection of critical infrastructure, Official Gazette no. 757 of November 12, 2010.
[13] GEO no. 718 of July 13, 2011 approving the National Strategy for Critical Infrastructure Protection, Official Gazette no. 555 of August 4, 2011.
[14] Edward Balkowich and Robert Andrerson, "Critical infrastructures remain vulnerable and communities must be able to protect themselves", *International Journal of Critical Infrastructures*, Vol. 1, No. 1, 2004.
[15] Grigore Alexandrescu and Gheorghe Văduva, *Critical infrastructures. Dangers, threats against them. Protection Systems* (Bucharest: "Carol I" National Defense University Press, 2006).
[16] Systemic risks lies at the intersection between natural events (with the human factor influence, positively, decreasing their effect, or, conversely, negative - i.e. emission of pollutants into the atmosphere), socio-economic and technological developments and actions resulting from policies both locally and at regional or global/international level. Identifying, analyzing and assessing systemic risks require a new form of analysis of risk factors that highlights all existing interdependencies within different phenomena. The effects most commonly encountered are economic repercussions. Hence, results the need for a more balanced management of systemic risks.
[17] Adrian Gheorghe and Lamine Mili, "Risk management: integrating social, economic and technical aspects in the situation of some chain accidents occurred on the infrastructure networks", *International Journal of Critical Infrastructures*, Vol. 1, No. 1, 2004.
[18] Mihai Ţăpârlea, "Crisis Management in Romania - a new concept", *Romanian Military Thinking*, No. 6, 2000.

The Impact of New Technologies on Intelligence Processes: Computational Instruments and Collaborative Environments

Iulian BODOLAN[*]

Abstract

The evolution of the human race was always based on the ability to invent and use tools and technologies that allowed the improvement of physical strength.

Although some of them proved to be amazing, recent technological evolutions seem to be less beneficial (as they led, for example, to global warming or nuclear threats or, in some cases, even to social disruptions).

Nevertheless, technological progress may be considered rather an advantage than a threat.

Technological innovation is a fundamental part of social development, technology playing the essential role of infrastructure-support and main resource in the constant process of resizing the evolutionary potential of humanity.

Important steps in speeding up technological developments in space exploration, accessing/sharing knowledge, radically transforming medicine, have been significant for the second half of the 20th century and early 21st century.

Therefore, similar to most representative activity segments, intelligence is characterized by a development trajectory mostly related to the technological discoveries in the latest decades, the analytical component benefiting of specialized solutions, coordinated and applied to increase the product's efficiency and quality for each associated sub-domain.

Defining Technology

The linguistic roots of the word "technology" come from the Greek word *tekne or techne*, which can be translated as "art", "craft" or "skill"[1]. In the early 18th century, the word was closely used with the current meaning, an English dictionary defining it as "a description of the arts, especially the mechanical ones". In 1831, Jacob Bigelow

[*] PhD Candidate, "Mihai Viteazul" National Intelligence Academy

published "Elements of Technology", the first book in English that contains the word "technology" in its title. According to his definition, *technology* consists of "principles, processes and names of more special arts, especially of those involving science applications"[2].

As humanity progressed, understanding and using technology became a group effort, making it difficult for one individual to ensure the activities necessary to produce a car (designing, material purchasing, component manufacturing, assembling, testing and selling). Therefore, technology can be seen as a combination of devices, skills and organizational structures and users, too.

Every technological advance brings changes of mentality, as well as social and sometimes even political adjustments. Technological change is not always a smooth process. According to William Ogburn[3], technology is a main driving force in the social and cultural change. The same author notes that change is uneven in the elements of the non-material culture. Ogburn coined the term "cultural lag" referring to the material culture is tendency to change faster than the non-material culture.

Rudi Volti[4] proposed a schematic definition of "technology": "A system based on the application of knowledge, manifested in physical objects and organization forms, for the attainment of specific goals", pointing out that it is not a comprehensive definition.

Collection/Processing/Analysis – Dissemination Software Products. Automatic Filtration and Collection/Processing of Information in Thematic Documentary Highlights

Capture

Automation of Data Collection from Various Sources

In the intelligence process, analysts need easily accessible data. In the current context of sources development and diversification, mainly in cyberspace, the automation of the collecting process is a priority for the integrators of OSINT solutions.

The hectic pace of IT processing technology's development imposes the alignment of intelligence agencies to these standards for further being competitive. The data collection process involves capturing almost in real time new data that can occur at any time in various media (printed or audio-video).

Besides data collected from cyberspace, audio-video data plays a special role. Recording shows of interest and analysts' "real time" information access are subject to a permanent competition on the

technology market aimed at satisfying that demand. The process involves hardware with high processing capacity required to conduct both recordings and transcripts in different languages, with an increasing accuracy.

Once integrated into the system, data is passed through a filter of "primary analysis" consisting of: summarization (automatic extraction of the article contents), categorizing (creating categories/areas of interest), and clustering (grouping information with similar topics).

Autonomy Company has developed a module for capturing and indexing virtual data (IDOL) and of audio-video data (Virage). Data indexing module provides multiple functionalities, such as: summarization, deduplication, creation of categories, alert based on keywords, search agents, extraction of entities (person names, locations etc.). The module of audio-video data capture provides the recording of the programs of interest, the automatically execution of transcripts (with the possibility of involvement), tape conversion, *face recognition* etc.

BBN Broadcast Monitoring System is an application that creates a continuous searchable archive of international television broadcasts and automatically transcribes the real-time audio stream and translates it into English. Both transcript and translation are searchable and synchronized to the video.

ZyLab offers a solution for collecting, indexing and processing data from various sources. Besides indexing, creating categories, bidirectional OCR, it also provides functionality in the field of *text mining* and *data visualization*, such as: extraction of entities (people's names, locations, addresses, companies etc.), automatic translation of text, *link analysis* (hidden connections between entities).

Processing

Automatic Translation

Regarding the "real time" automatic translation, the applications for *smart* devices could become generally available in the coming years, as researchers are close to finalize the technology and apply it through *smart phones*, an optical software for character recognition and Google Translate technology being used in the process. A one-way communication device has been used for several years in the military field: *P2 Phraselator*, created by Voxtec Company, can translate thousands of pre-defined English phrases.

LanguageWeaver and *Systran* technology can handle translation in several languages almost in real time. Each of the automatic translation tools on the market is built using either statistical (*LanguageWeaver*) or linguistic (*Systran*) models or even a hybrid model that combines the other two models (Google Translate).

During the *Mobile World Congress* in Barcelona, Spain, Google CEO Eric Schmidt presented a feature of a smart phone that allows the user to take a picture of a text in German and translate it quickly into English, using optical character recognition software and Google Translate technology.

Speech-to-text (STT)

Retrieving relevant information in audio-video files is another challenge. In the absence of soundtrack transcripts and synchronization with the audio-video file, the retrieve is limited to listening to the clip. The manual transcription is a costly operation in terms of human resources involved and time needed to accomplish it. Therefore, the emphasis is increasingly on getting more the automatic transcription (*speech-to-text*/STT) of audio-video files, with specialized applications.

STT function requires the configuration of specific modules for each language, besides granting high processing hardware resources. These modules can be trained using different methods (with audio files, text files etc.), to increase the accuracy of transcripts, which is influenced by several factors, such as: the quality of the input signal, the presence of background noise, a speaker who is untrained or has difficulties in pronunciation etc. The main utility of STT is to find an audio/video file based on keywords. The transcript synchronized with the audio/video file allows the instant tracing of the moment when the keyword of the search was generated/pronounced. Therefore, STT can be integrated with the alert module – when a pre-defined keyword appears, the system can send a message (email) to alert a user group.

Alerts

One of the stringent requirements of any intelligence organization is that each user, depending on the goal, should be informed of the updated information from various Internet sources. Each department is interested in updating their professional profiles. Instead of reviewing manually and periodically the news on the favorite sites for retrieving the needed information, the user will be informed on the news by the alert mechanism provided through technical solutions.

These solutions enable the professionals to create alerts on certain monitored profiles. Data is continually updated from thousands of Internet sources, interesting blogs and forums in different languages, websites for analysts, organizational websites, personal sites and many other websites available to crawlers for data identification on a topic defined within the profile. When news/a document that fits the profile is found, an alert is issued.

The method of operation of such a mechanism is as follows: relevant Web sources defined by the same analyst and sources within the organization are provided to the collection module. The automatic review schedule for these crawlers' sources determines the automatic identification and retrieval of the relevant documents, according to the analyst profile. The users can be alerted by email through a message in the application, regarding the profile updates, or by SMS. SMS alert requires dedicated application integration and the connection with the GSM operator. Producers included such mechanisms in the solutions provided on the market (MindCite, Autonomy or Expert System).

Analysis

The New Generation of Interactive Analytical Products

Currently, the amount of received data and their speed of updating, corroborated with a decrease in the processing time have transformed the intelligence process. In order to obtain and draw reliable conclusions we need to create an OSINT-type workspace and define the interactive process for exploring and analyzing structured and unstructured information, data and knowledge in order to discern the trends or patterns. It is very important to develop a powerful data integration technology that enables analysts to quickly connect data from multiple sources and explore unified data through extended graphics, maps, timelines.

Collaborative Work

As organizations increasingly extend (by regional, national or multinational spreading), collaboration among dispersed employee groups can be a problem. Therefore, in order to allow them to efficiently use knowledge and skills held by the decentralized entities, it is necessary to implement technologies and strategies that enable communication and collaboration beyond geographic boundaries.

Development of communication technologies, such as e-mail, videoconference and Internet, led to designing software products that facilitate sharing information and knowledge within geographically dispersed groups and allow them to cooperate in order to achieve the common goal.

Since the users work simultaneously with the same data, it is important to centralize data storage. The users can access the latest data each time they connect to the application, being required to save changes when the application disconnects. The centralized data storage and the version control minimize the risk that more users will make the same changes.

The communication within this type of applications can be achieved in various ways: from the *instant messaging* services, to the Web conference facilities, group calendars for tasks scheduling and workflows that enable automatic routing of information to the committed users. One of the great advantages of the collaborative *software* is providing the same data to all members, allowing the development of the group's problem-solving skills. The collaborative *software* proves also to be very useful in creating knowledge bases, such as *wiki* platforms. The facility to access and modify a knowledge base by more users allows collecting expertise held by each contributor.

Social Network Analysis

Social Media comprises Web and mobile technologies used to turn communication into interactive dialogue among users.

Andreas Kaplan and Michael Haenlein[5] have defined *social media* as "a group of Internet-based applications that build on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of user-generated content".

The social networks are social structures composed of individuals (or organizations), called "nodes" and connected through one or more types of interdependencies, such as relations of friendship, kinship or common interests. They are very popular and can be accessed with various purposes, from knowledge and networking to promoting some business, liaising with stakeholders and even ideas, ideologies or groups supporting an idea, a concept. The large number of social networks has led to a continuous competition among their developers, statistics being periodically conducted to determine which network is more appreciated, more used.

Data Fusion & Analysis (Relational Database)

The organization's internal databases store many records on a certain customer, partner, product or competitor. Reference to a particular entity is possible when a fusion is made in order to show/display data to the same entity from different sources.

Data fusion is the process of gathering/acquiring data from multiple sensors/sources from multiple platforms in a single composite picture of the environment. In this case, the sensors are used to connect the existing databases in different disintegrated organizations on various operational platforms.

Mapping/Geographic Information System (GIS)

It is a useful application to display geographic data using appropriate dots or forms similar to specific locations or areas on a map to help mapping and drawing diagrams of strategic intelligence.

Data Mining and Link Analysis

Together with data collection and fusion, the relationships among different samples/users and the association analysis are particularly interesting.

The link analysis process enables the identification of useful data required by analysts, ranging from data fusion by creating relationship graphics, with powerful visualization techniques, to alerts based on rules and inferences that would allow the process automation in finding the wanted objects/users.

Setting the patterns and links from a very large volume of information (either statistical or in the text) is difficult to manage by the human factor.

Data mining tools can help in the complex management cases where there are several targets, victims and information about the case, also in making connections among different entities. Dedicated software applications are able to identify the negative, neutral or positive way of an article.

Data Visualization

The recent researches have shown how graphical data visualization simplifies the process of understanding and increases their analysis efficiency.

The ability to display data stored in tables and databases - an object (a person, organization, event, property etc.) that links the other - accelerates and streamlines the process of understanding.

"A picture is said to worth more than a thousand words". Data Visualization is useful for learning data patterns and meaning. The ability to graphically navigate through the stored data without affecting their integrity, offers the analyst an efficient way to simplify the understanding of raw data during the analysis process in order to make decisions.

The process of visualization facilitates, in fact, the analysis of the displayed data links. A good tool for data visual representation includes:

- best practices of visual design;
- real time analysis;
- data interactive exploration;
- quick configuration, with little or no IT support.

Interactive data visualization enables the analyst to process massive amounts of data in different visual representations and, thus, isolate important facts and models. But it is more than an image.

It gives the *investigator* the freedom to ask questions through direct interaction with the visualization. As the investigator reveals new insights, he/she can easily navigate and develop active/alive profiles.

He/She can link together individuals, suspicious events, past events, current and historical alerts and accounts, knowledge, background checks and transactional behavior. The ability to detect and quickly confirm conclusions is an important interactive feature of data visualization and analysis.

The next generation of tools for data visualization allows employees within an organization to ask and get the answer to their own question. With drag-and-drop interface and views with one click, data visualization tools allow users even less familiar with the technique to obtain access in a few seconds[6]. There are viewing tools for search, music, networks, online communities, but also special ones offered by on the market suppliers that allow the visualization of all types of data[7]. Steps to be followed:

- to complete information (data identification, filling gaps, corroboration and synthesizing);
- to identify entities (proper names and words extraction/ key phrases);
- to construct and complete clustering matrix;
- to identify clusters (using visual bookmarks for the relations among entities);
- to draw network preliminary diagrams;
- to refine diagrams;
- to develop hypotheses.

Impact of Social Media

Variety of Dissemination Platforms

The information dissemination method should be based on the wanted/required target, its specific content and the customer profile.

The dissemination methods vary from the usual printed material to the facilities offered by the current technology: SMS, RSS feeds, email, post in the categories/dedicated sections.

Concerning intelligence agencies, the need to operatively inform the policymakers imposes choosing a method for rapid dissemination, so that the user makes a minimum number of operations.

In a permanent collaborative process with data collectors, analysts must be able to select and validate the sources, to establish and manage complex features and pictures, to understand the studied problems, to have initiative, intuition, curiosity, and perseverance, legal and ethical sense and to show loyalty and sincerity.

Competition, strategic orientation, capability to act under uncertain circumstances, creative intelligence, a sense of reality and responsibility are other qualities and skills that an analyst should have.

To cover the OSINT process (from data accessing to data dissemination) three important stages must be taken into account:

- training and performance management;
- planning and disseminating requirements;
- communication and collaboration to meet requirements.

Real-time access to important information has always been a major point in the success of intelligence. Its importance further increased with the boosting of the Internet and the increased number of the information sources.

As a result, both companies and intelligence services have collected huge amounts of data in an effort to understand the evolution of their activities, to improve their performance and create an enhanced relationship with employees, beneficiaries and partners.

It is difficult to efficiently exploit such data, starting from giving them a meaning to integrating them in an institution. In an organization, data is usually dispersed in a variety of systems, and many institutions have difficulties in organizing and interpreting their meaning. They face fragmented data and tools, resulting in an incomplete view of the system.

Technically, an OSINT platform must:

- access or, when necessary, collect and store a significant amount of information from open sources (regardless of the capture mode), which subsequently should be easy to use;
- be scalable in order to allow the addition of new modules that work with the system and to adapt to the needs of the users;
- embed hardware and software in order to allow fast and efficient query and retrieval of archived data as well as their timely analysis and correlation;
- quickly translate *text-to-text*, *audio-to-text* from several languages into the native language;
- have a unique user-friendly interface that can be customized in order to reach the analytical priorities;
- enable implementation of some tools needed for the analysis of trend, corroborating sources, social network analysis etc.;
- have tools enabling the specialists to collaborate with the entire intelligence community in order to accurately use open sources;
- provide necessary tools for incorporating text documents, graphics or audio-video materials;
- develop a transfer procedure between the unclassified and classified information area and implement a security architecture on several levels;
- provide necessary tools to the intelligence community in order not to disclose the activity (query, analysis etc.) for external collaborators;
- enable the automatic dissemination of concerned analysis from open sources to customers;
- monitor information sharing within the national community to enhance the technological and collaborative performance while promoting the exchange of information, but also identify and implement new changes in the security levels and work procedures.

Collaboration

It is necessary that the organization owns and develops technical resources in order to facilitate cooperation within the intelligence community. These resources must include the social networking tools and virtual spaces to allow information sharing among the specialists in a particular field.

There are impediments in terms of establishing the collaborative principle at the level of the community. However, with the policymakers' support, those impediments will be surpassed, the ultimate goal of this action being to promote collaborative work, while meeting the necessary security requirements.

Performance Evaluation

The organization must develop clear procedures on performance evaluation. To that end, we should consider the following:

- *customers*' feedback;
- easiness in accessing and using open sources and tools available to intelligence analysts;
- response speed;
- accuracy of tactical and strategic analysis;
- level of cooperation in achieving them.

Dissemination

Analytical outputs will be distributed to customers depending on the information they contain. Thus, they must contain:

- full summary of the analyzed topic;
- corroboration of information from all available sources;
- results of using analytical tools;
- assessments of the situation in the concerned region/area;
- new data on the subject of interest (in case of a state or region data from the social, political, military, infrastructure and technological field are taken into consideration).

Conclusions

Integrating current technological solutions and adjusting them to specific requirements of intelligence analysis in the context of today's technological effervescence are imperative in order to increase efficiency and relevance of intelligence activity to national security.

Therefore, the strategic approach on technological innovations ensures stable coordinates aimed at boosting competitiveness, facilitating the decision-making process, and developing inter- and intra-organizational cooperation in terms of providing quality intelligence.

References

[1] See http://www.webdex.ro/online/dictionar/tehnologie, http://www.etymonline.com/index.php?term=techno-&allowed_in_frame=0

[2] Rudi Volti, *Society and Technological Change*, 6th edition (New York: Worth Publishers, 2010), p. 4.

[3] William F. Ogburn, "Technology and Governmental Change", *On Culture and Social Change: Selected Papers* (Chicago: Otis Dudley Duncan Publishing House, 1936), pp. 132-133.

[4] Volti, *Society and Technological Change.*

[5] Andreas Kaplan and Michael Haenlein, "Users of the World, Unite! The Challenges and Opportunities of Social Media", *Business Horizons*, No. 53, 2010, pp. 59-68, available at http://openmediart.com/log/pics/article.pdf (accessed on 29 March 2012).

[6] See http://www.tableausoftware.com.

[7] See http://www.kdnuggets.com/software/visualization.html#software - Advisor Analyst, Antaeus, bi-drillet, Centrifuge Systems, CViz Cluster Visualization, Daisy, Data Desk, DataMontage, Davisor Chart, Drillet, Eaagle visual text mining software, Grapheur, Gsharp, High Tower TowerView, i2 Analyst's Workstation, IBM ILOG Visualization, IDL, InetSoft Style Intelligence, InetSoft Style Scope, InFlow Network Mapping Software, InfoZoom, Insightful S-PLUS, InstantAtlas™, IRIS Explorer, K.wiz, LeadScope, Mercury Visualization Sciences Group, Miner3D, NETMAP, NovoSpark Visualizer, Oculus, OpenViz, Parallax: Multi-Dimensional GraphsPartek, PV-WAVE, RapAnalyst, SAP BusinessObjects Xcelsius Enterprise, SAP Business Objects Tools For Advanced Visualization: Startree, Tablelens, Timewall, and Vizserver, ScienceGL, Sentinel Visualizer, Spatial Key, Starlight Visual Information System (VIS), Tableau, TIBCO Spotfire, Viscovery, Visipoint,Visokio Omniscope, Visual Insights Visual i|o, VisuaLinks(r), VisuMap, WITNESS Miner, Xanalys Link Explorer.

The Impact of Social and Technological Developments on the Information Flow

Cristian IANCU[*]
Tudor RAŢ[*]

Abstract
One cannot talk about social change without connecting this subject to the phenomena included under the conceptual umbrella of "globalization" that relies mainly on technological evolution. The progress made in this field leads to a radical reshaping of the information flows (as far as quantity, quality, and velocity are concerned) and social interaction (either among individuals or groups), that is shifting, more and more, to the online environment. The implications of these interconnected dynamics have a systemic dimension, especially to the activity of the intelligence organizations, which are considered actors operating in an economy of knowledge. Analysis could play an important role in this increasingly complex environment and help orient the efforts of social adjustment to the realities of knowledge society.

Based on an unprecedented development of the homonymous technologies and thus of the quantity, quality, and, most important, velocity of information flows, the **Information Revolution** is, undoubtedly, the third qualitative leap (the first two were the Agrarian and Industrial Revolutions) mankind has ever known in terms of the human community structure. The intelligence services' specific activity goes also through changes of paradigm in a world increasingly defined by "the need to share". In order to maintain its relevance in the current strategic context, intelligence, seen as social function, has to become more than a data and information supplier, namely a knowledge *provider* in an increasingly complex security environment, as, undoubtedly, inserting the "information" factor into the old production relationship between "matter and energy"[1] will significantly revolutionize, reshape, and transform at least four areas of social life[2]:

- community structure and dynamics;
- identity;

[*] PhD Candidate, "Mihai Viteazul" National Intelligence Academy
[*] PhD Candidate, University of Bucharest

- collective action;
- social order and control.

The changes experienced by these 4 segments converge towards the shaping of two paradigms specific to the knowledge-based society: a paradigm of **networks**[3] (marked out by changes in the social structure and dynamics, identity, and collective action) and a paradigm of **surveillance** (characterized by the new type of social order and control).

Network Society	The network paradigm development represents a transformation of communities' **social dynamics and structure** in terms of multiplying the "reference frames" the individual uses.	In the past, the impersonal structures defining the individual's affiliation to the group(s) were concentrically disposed (for example, family-clan/tribe – people) and, on many occasions, they did not entail the individual's volitional factor. Today, in the globalization era, any individual can belong to different groups, independent from one another, without space or time constraints.
	Today, more than ever, **the individual's identity** loses its monolithic valences, being constantly built, reshaped, and nuanced according to characteristics of each community the individual is part of.	In the agrarian and industrialized societies, a person was usually born and died in a relatively narrow social universe (friends, coworkers and relatives were, more or less, part of the same social category), but, in the postmodern world, each individual activates in networks (based on friendship, kinship, work, interests, hobbies etc.) that can coexist independently, each network requiring another "social mask", namely an identity version adapted to the respective micro-universe.
	Electronic communication environments enhance the social capital[4], namely the human potential for **collective**[5] action, increasing groups' capacity to mobilize, organize, and ensure the information flow.	A *smart mob*[6] is a large, heterogeneous, and unstructured group of people who act intelligently and efficiently thanks to a premise (group intelligence) and a technological catalyst (modern communication means facilitating the *one-to-many* and *many-to-many* information exchange). Many heterogeneous groups hide under the *smart mob* name*:* the Egyptian and Tunisian protesters who used Facebook and Twitter during the 2011 riots in the MENA countries to coordinate their street actions or flash-mobs commemorating pop singer Michael Jackson through synchronized dancing.
Surveillance Society	The development of technologically mediated communication means facilitated not only the enhancement of human networks' ability to act but also the means of ensuring social order and control through side-monitoring mechanisms.	The increasingly accelerated transposition of individual and group life in the online environment has created a denser information environment that can be accessed by any third interested party. Though anonymity is the basic feature of the activity in the virtual environment, the use of real identity elements on different platforms (Facebook or Google services, for instance) makes a new reality increasingly important, namely that of a transparent social universe.

For those in charge of protecting the country against security vulnerabilities, risks and threats (we are, obviously, making reference here to the intelligence officers working within government *intelligence* organizations), the development of the two complementary paradigms has important effects in the professional activity area:

- On one hand, the vectors exploiting vulnerabilities, increasing risks or threatening system operation are grouping and acting in the increasingly dynamic, heterogeneous, volatile networks lacking space and time constraints.
- On the other hand, under the pressure of information avalanche and the increasingly complex security environment, the "traditional" means of the *intelligence* activity (management/ elimination of vulnerabilities, risks and threats) show their limitations. One of the areas feeling a strong pressure to change is the analytical one: in the case of difficult problems, which are difficult to manage mentally, individual analysis (unaided expert judgment) does not produce sufficiently robust results, new types of structured, collaborative, and auditable analysis being required[7].

Information Flow Redesign and Online Interaction

> *"I define 'community' as networks of interpersonal ties that provide sociability, support, information, a sense of belonging, and social identity. I do not limit my thinking about community to neighbourhoods and villages. This is good advice for any epoch and especially pertinent for the twenty-first century"[8].*

The "metaverse", namely the virtual universe, is a very small and crowded place where nearly all individuals are interconnected in overlapping communities and interaction possibilities are unlimited.

Why Do We Live in an Increasingly Smaller World?

However, the world has become smaller for quite a long time. Psycho-sociologist Stanley Milgram conducted an experiment designed to test the hypothesis of Hungarian writer Frigyes Karinty who claims that an individual can be connected to any person on the planet in five steps (through friends, friends of friends etc.). Thus, in 1967, several subjects from Omaha, State of Nebraska, and Wichita, State of Kansas (USA) (cities geographically located far away

from one another) were asked to send a letter to an individual chosen randomly by the researchers (from a completely different part of the country). If the sender did not know the recipient personally, he was asked to send the letter, with instructions, to a friend about whom the initial sender "believed he might know the recipient". The cycle kept repeating until the letter got to the individual designated as recipient of the letter. The 64 (out of 296) letters that reached the pre-determined target were sent through approximately 5.5 steps (*average path length*), a result that led to the promotion of the phrase *6 degrees of separation*.

Lars Backstrom[9] estimated that, on Facebook (721 million users and 69 billion friendship connections at the moment of the research), there are on average 3.74 degrees of separation between users. In other words, on average, a user from Romania can reach another user from Benin in less than four "friends of friends of friends".

This dense environment of overlapping relationships is the most powerful premise for generating added value within overlinear (exponential) parameters in terms of information flow.

Why Do Crowds Produce More than the Sum of Parts?

Undertaking a huge research effort, two physicists analyzed a "strange" phenomenon (collecting an overwhelming volume of raw, heterogeneous data): whenever a city doubles its population, an entire range of phenomena and apparently unrelated parameters grow by 115%: from economic productivity and costs of housing to the spread rate of disease, pollution, and crime[10]. Unlike the animal world, where larger size implies a slower biological process (see the metabolic differences between mouse and elephant), urban areas generate overlinear scaling due to a "positive loop feedback" mechanism: for example, a developing city is a productive city, which attracts more people, fueling thus the cycle.

Small communities are peaceful, nothing new happens because new information cannot enter cohesive and homogenous groups – the information generator cannot contact the abovementioned community members. In a mass of people, whether real or virtual, new information travels fast and is easily collected, creating a dissemination spiral with accelerated increase and decrease.

Information is faster and more perishable, useful only here and now, today and not tomorrow.

This reshaping of information streams is closely connected, both ways, to community configuration and online interaction specificity: within large groups, most relationships between individuals are weak/*weak-ties*[11], namely of the type "my neighbor's sister", "my work colleague's friend", being more useful in terms of information input. The individuals acting as brokers between different subgroups ("connecting" two groups) are the favorite information transmission channel from a clustered region to another. In virtual communities, these resource individuals are more commonly seen within a group, ensuring communication redundancy[12].

The "metaverse" is a genuine melting pot of ideas, information, and initiatives of collective action. Therefore, it is a favorable framework to a more dynamic information stream, a phenomenon that is both an opportunity and a threat to analysts focusing on human action in the virtual environment:

- acting as a resonance and amplification box, cyberspace is the "land" of information avalanches: data and information emerge at a high rate, "travel" fast, quasi-chaotically and often unpredictably, and this makes them difficult to monitor, collect, store, validate, process, and integrate in analytic products;
- facilitating easy interaction, the online environment is favorable to *intelligence* communities' activity: technologically mediated communication tools, especially collaborative platforms (*wiki* applications, forums, *message boards* etc.), provide fast dissemination of the *intelligence* obtained/produced by the analyst to other fellow workers (for review, completion etc.) or customers (for capitalization), encouraging thus intra- and inter-organizational cooperation, wise use of system resources, *feedback* and *feedforward*, etc.

Social Change

"Everything changes and nothing stays the same... and... you cannot step into the same river twice", Heraclitus said. Just as water flows, so the individual changes, in different ways, from one moment to another. But, as Professor Anthony Giddens said, "we usually tend

to believe that it's about the same person and the same river. There is enough continuity in the shape of the river, as happens in the case of physical appearance or personality of the respective individual, to entitle us to say that everyone stays 'the same' despite the changes that occur"[13].

Moreover, according to the sociologist, the analysis of the societal transformation's nature and scale in the Information Revolution Age should begin with the diagnosis of the change undergone by the *basic institutions* of the studied community, which becomes obvious in the light of **cultural, economic**, and **political** influences[14].

Cultural Influences

As secularization of thinking, development of science and rise of modern ideals (liberty, equality, democratic political participation etc.) mark profoundly the present social life, the next period will stay under the sign of technological development, information flow reshaping (in terms of quantity, quality, and velocity), and increased social participation in cyberspace.

Permeability, "osmotic" transfer capacity, heterogeneity, removal of temporal and spatial constraints and democratic character are the main features that will further influence the development of noosphere, of the human knowledge field.

Why Do We Have Access to Increasingly Diverse Information?

In the *offline* world, a mathematical recurring *pattern* called "Pareto Effect/Principle" can be observed in surprisingly many areas of life: 80% of effects are the result of only 20% of reasons. This observation was made by the Italian sociologist and economist Vilfredo Pareto who concluded, in 1906, that 80% of Italy's land was owned by 20% of population. Joseph Juran, *business* consultant, has developed an entire system based on this unusual observation, after noticing that 20% of the bean pods in his garden contain 80% of the bean harvest[15]. Juran is certain that, in its natural form, the entire human system tends to apply this "law of power", according to the *United Nations Development Program Report* (1992)[16], 20% of world population control 82.7% of world wealth; Microsoft considers

that solving 20% of software problems (*bugs*) trigger the disappearance of 80% of errors[17]; in the US, 20% of patients consume daily 80% of resources[18]; 20% of criminals commit 80% of crimes[19] and examples could continue.

The cyberspace changed the way the power is distributed in a certain space, the most influenced area being the culture (in a wide sense of the word). Chris Anderson[20] analyzed the sales patterns of the Amazon, Netflix and Rhapsody platforms and discovered a "long tail" distribution type: if, in the *offline* environment, 80% of sales are generated by 20% of headlines (books, music albums, movies etc.), on these e-commerce sites "the superstars" sell less than 50%. The remaining percentage represents less known or obscure authors/ artists/etc.

On the iTunes website, quasi-anonymous artists sold more albums than Madonna or U2. In other words, most revenue was made by songs that, probably, had not even been broadcasted on the radio. In the virtual environment, all requests find an offer and are not limited by storage space or perishability.

Economic Influence

The production model based on knowledge, namely the "weightless economy"[21], implies anchoring the main traded products and services (*software* solutions, multimedia content, Internet-based services etc.) in the information area. Economy, similar to many other fields, operates through transnational, flexible and quasi-unstructured networks[22].

Certain organizations fully reflect the following reality: there are companies with no physical headquarters, whose employees work from their own homes using the Internet, being likely to never physically meet their colleagues living in remote regions of the world. These companies have concluded partnerships with other similar companies.

Why Do Trade Flows Connect Us?

The Barbie doll is the first "truly global citizen"[23], an expression of the trade and information chain system linking world's economies. The first step in manufacturing the doll is made

in Saudi Arabia, the country where the oil is extracted and then ethylene is refined, the raw material for the doll's body. The Taiwan-based Petroleum Corporation buys ethylene and sells it to Taiwanese PVC producer Formosa Plastic, which transforms raw material into polyvinyl chloride granules. The granules are then sent to one of the four Asian factories (China, Indonesia or Malaysia), where the doll's body is manufactured through injection. Hair is added only after the doll reaches Japan, and Barbie is dressed in clothes made of Chinese cotton. Hong Kong is the port through which these flows are sent throughout the world. The headquarters of the Matell Company (owner of the brand) is in the US, where design as well as marketing and sales strategies are drawn up. The dolls are also packed in the US, several accessories manufactured by third parties being added.

Political Influences

The fall of Communism in Eastern Europe (1989) and the 2011 social movements in the MENA region represent key moments in the process of international spread of the democratic system of government. The collapse of Communism in Europe and the disappearance of a significant number of autocracies in North Africa and Middle East represent simultaneously and equally not only the catalyst, but also the result of globalization itself, thus facilitating the international dialogue and interaction between a growing number of states.

This reality represents a *sine qua non* prerequisite for the proliferation of international governmental organizations/"IGOs" (UN, EU, OSCE, WTO, ASEAN etc.) and international nongovernmental organizations/"INGOs" (International Olympic Committee, Red Cross, Doctors Without Borders etc.), supra-state institutions that can operate beyond the nation-state's borders.

Why Do We Need Supra-State Organizations?

The Universal Declaration of Human Rights, a document ratified on 10 December 1948 by the UN member states, remains one of the greatest achievements of a supra-state body in history:

the noble aspiration of the document, namely universal respect for freedom, dignity, and equality, regardless of nationality, race, religion or political affiliation is one of humankind's ideals and a philosophy that marked the political, military, and social actions of a large number of states for over half a century.

Today's *intelligence* analyst, regardless of the organization, private or non-governmental organization, he/she works in, undertakes his/her activity in a far more complex environment than several decades ago: he/she must identify, anticipate and provide solutions for managing, stopping, or developing more complex, deeply multi-layered phenomena, having deeper and less predictable impact on the activity of the organization/entity he/she has been tasked to protect.

The external environment of the organization is socially, culturally, economically, and politically influenced by the developments in a globalized world: what happens *there* has impacts *here*. The consequences of this situation on the intelligence organizations, particularly on the analytical work, focus on the need to overcome the traditional organizational model (intelligence structures provide knowledge to the customers within the system) and to engage national and international actors performing similar tasks in solving the systemic dysfunctions of the global paradigm - from economic and food crises to pandemics, terrorism, and cross-border crime.

Analysis Role in an Increasingly Complex World

The distribution of knowledge, information and expertise in the interconnected and technologically advanced twenty-first century world makes **analytical intelligence** (namely the cognitive effort aimed at producing actionable knowledge) extremely useful (even essential) to the entire society and its members, not only for intelligence services and consulting companies, but also for individuals, groups and organizations from all sectors of life, as turbulences and volatility are inherent features of any transition period.

Although a relatively small state in terms of population (9.5 million citizens, according to Befolkningsstatistik[24]), representing only 0.13% of the world population), Sweden produces

one percent of the global wealth. According to Stevan Dedijer[25], Sweden is ranked on top positions in the world in any sector of economic and social development. The Gini coefficient (inequality between income and wealth distribution in a society) hits its lowest level in Sweden (0.23), and the country ranks first in terms of education system and scientific research, fifth for economic competitiveness, fourth for "the standard of living", being also the **most developed analytic *intelligence* national community**.

Dedijer[26] identifies 15 features of the Swedish nation that encourage *intelligence* activities at all levels of society:

- urge to bring human rational behavior to its highest level;
- "Ording och Reda" - everything has to be done in a logical and natural order;
- effective (sober and emotionless) communication at work;
- "Yenta lagen" - Swedish society is an egalitarian one, discouraging people willing to stand out;
- respect for individuality and uniqueness of each person, regardless of gender, origin, income or social status;
- society is responsible for producing criminals, there is no "innate evil" (malum in se);
- curiosity is a desirable feature, but it should not be exhibited;
- conflicts must be settled without using violence;
- creativity and innovation must be socially rewarded;
- people must know the world they live in, consequently it is essential to travel;
- the importance of Ombudsman's role, the official to whom citizens can turn to when they are abused by state power bodies;
- love for nature and environment;
- "Allemans Ratt" - respect for private property rights.

Swedish intelligence is defined by a tripartite cooperation of the relevant institutions in the academic, national (intelligence services) and business sectors. In other words, Sweden has a specific manner of conceptually developping all social systems, being, according to Stevan Dedijer, a driving force in humankind evolution toward an omega point of intelligence: year 2053 (50 years after the cited paper has been written). The author predicts that in less than

half a century, humankind will eradicate war "as it eradicated smallpox". The analytical intelligence's role will be to globally solve in a collaborative manner, the major problems of humankind, not to ensure the lowest degree of suffering for the people of a nation.

Such a view requires to operate essential changes in the institutional modus operandi, currently focused on interstate competitiveness, "Dedijer's architecture" being similar to what John Henry Holland called complex adaptive systems: entities which involve "a large number of components, often called «agents», that interact, learn and adapt", namely intelligent groups/smart mobs whose actional capacity is significantly increased by technological facilities. Namely, intelligence structures must perform systemic/organizational changes in response to these new trends, in order to ensure a more organic integration in network society and growing information flow.

Currently, intelligence organizations are mechanically conceived, resembling the industrial production model that characterized the past period: there are clear hierarchical relations, defined by high grading structures (that include several hierarchical levels), work is still divided (according to the principle "need to know"), and the information flow has a repetitive trajectory.

We believe that an intelligence service which operates in a supervisory network society must adopt a "mirror-like" institutional structure. Therefore we propose a further reflection on "knowledge worker" scheme, as it was defined by Reinhardt, Schmidt, Sloep, and Drachsler[27].

Position	Position Summary	Responsibilities
Controller	Monitors the organizational performance, taking into account basic information (statistics).	Analyzing, disseminating, organizing the information flow, monitoring.
Helper	Ensures knowledge/information transfer to other individuals, after they have solved a a certain problem.	Validating, analyzing, disseminating, offering feedback and feedforward, information searching, learning, establishing interhuman connections (*networking*);
Learner	Uses information and "best practices" in order to improve its own abilities and professional skills.	Collecting, analysing, searching for (information, services and experts/helpers), learning;

Linker	Connects and combines data and information collected from different sources in order to create new intelligence products.	Analyzing, disseminating, information searching, organizing the information flow, *networking;*
Networker	Creates and manages connections with people working in the same sector, organizes working projects aimed at sharing information and getting help for critical moments.	Analyzing, disseminating, searching for experts and services, monitoring, *networking;*
Organizer	Involved in planning and organizing activities.	Analyzing, organizing the information flow, *networking*;
Retriever	Searches for and stores up information on a certain topic.	Collecting information, searching for experts and information, organizing the information flow, monitoring;
Sharer	Disseminates information in communities.	Validating, disseminating, *networking*;
Solver	Identifies solutions to problems.	Collecting information, analyzing, disseminating, searching for information and services, learning;
Tracker	Monitors and manages weak signals of future problems.	Analyzing, information searching, monitoring, *networking*.

References

[1] Norbert Wiener, *Cybernetics or the Control and Communication in the Animal and the Machine* (Cambridge: The Technology Press, 1948), partially available at http://tinyurl.com/7khd4on (accessed on 31 January 2012), p. 155; Yannis Veneris, "Modeling the Transition from the Industrial to the Informational Revolution", *Environment and Planning*, Vol. 22, No. 3, 1990, pp. 399-416, available at http://www.envplan.com/abstract.cgi?id=a220399 (accessed on 31 January 2012).

[2] Peter Kollock and Mark Smith, *Communities in Cyberspace* (London: Routledge, 1999).

[3] What Manuel Castells (1996) called *the network society*, namely "the society where structures and key activities are organized around the electronic information processing networks".

[4] Networks' characteristic to provide information and help, respectively individuals' ability to benefit from it; individual and collectivities' ability to benefit from them; the capacity of communities and individuals to produce common goods.

[5] Anabel Quan-Haase and Barry Wellman, "How Does the Internet Affect Social Capital?", in Marleen Huysman and Wulf Volker (eds.), *Social Capital and Information Technology* (Cambridge: MIT Press, 2004), pp. 113-132.

[6] Howard Rheingold, *Smart Mobs: The Next Social Revolution* (New York: Basic Books, 2002).
[7] Richards Heuer and Randolph Pherson, *Structured Analytic Techniques for Intelligence Analysis* (Washington DC: SAGE Press, 2011).
[8] Barry Wellman, "Physical Space and Cyberplace: the Rise of Personalized Networking", *International Journal of Urban and Regional Research*, Vol. 25, No. 2, 2001.
[9] Lars Backstrom, Paolo Boldi, Marco Rosa, Johan Ugander and Sebastiano Vigna, "Four Degrees of Separation" (Cornell University Library, 2012), available at http://arxiv.org/abs/1111.4570 (accessed on 31 January 2012).
[10] Geoffrey West and Louis Bettencourt, "A Unified Theory of Urban Living", *Nature Journal*, No. 467, 2010, available at http://www.nature.com/nature/journal/v467/n7318/full/467912a.html (accessed on 31 January 2012).
[11] Mark Granovetter, "The Strength of Weak Ties", *American Journal of Sociology*, Vol. 76, No. 6, 1973, pp. 1360-1380, available at http://www.stanford.edu/dept/soc/people/mgranovetter/documents/granstrengthweakties.pdf (accessed on 31 January 2012).
[12] The existence of a single individual connecting two subgroups that are otherwise disjunct implies also a significant risk: being aware of his information filtering capacity, he/she can block or manipulate information flow to his/her own benefit. The existence of several such individuals ensures a "lateral surveillance" from the others. The phenomenon's main effect is the elimination of distortions such as the "wireless phone" – there is always a reference point for the assessment of information accuracy and of its degree of alteration through peddling.
[13] Anthony Giddens, *Sociology* (5th edition) (Bucharest: ALL Publishing House, 2010), p 42.
[14] *Ibid.*, pp. 46-58.
[15] See http://www.80-20presentationrule.com/whatisrule.html
[16] This global inequity applies to all levels, even to the rich. In "world's top 10 richest people", the fortune of the people holding the first three places (Warren Buffett, Carlos Slim Helu, and Bill Gates) is equal to the fortune of the next 7 richest people in the world: http://www.thisismoney.co.uk/money/news/article-1607938/The-Forbes-100-billionaire-rich-list.html
[17] See http://www.crn.com/news/security/18821726/microsofts-ceo-80-20-rule-applies-to-bugs-not-just-features.htm
[18] See http://www.projo.com/opinion/contributors/content/CT_weinberg27_07-27-09_HQF0P1E_v15.3f89889.html
[19]See http://howdoigetoffdrugs.com/2010/01/career-criminals-who-are-they-and-what-should-society-do-about-them/
[20] Chris Anderson, *The Long Tail: Radical New Shape of Culture and Commerce* (New York: Hyperion, 2006).

[21] Danny Quah, "The Weightless Economy in Growth", *The Business Economist*, Vol. 30, No. 1, 1999, pp. 40-53, available at http://econ.lse.ac.uk/~dquah/p/9903tbe.pdf (accessed on 31 January 2012).
[22] Manuel Castells, *The Rise of The Network Society, The Information Age: Economy, Society and Culture*, vol. I (Oxford: Blackwell Publishing Ltd., 1996), *passim*.
[23] John Tempest, "Barbie and The World Economy", *The Los Angeles Times*, 22 September 1996, available (31 January 2012) at: http://articles.latimes.com/1996-09-22/news/mn-46610_1_hong-kong.
[24]See http://www.scb.se/Pages/Product____25799.aspx
[25] Stevan Dedijer, "Development & Intelligence 2003-2053", *National Security and The Future Journal*, no. 10, 2002, available at http://swoba.hhs.se/lufewp/abs/lufewp2003_010.htm (accessed on 31 January 2012).
[26] Dedijer, "Development & Intelligence 2003-2053".
[27] Wolfgang Rheinhardt, Benedikt Schmidt, Peter Sloep, and Hendrick Drachsler, "Knowledge Worker Roles and Actions – Results of two empirical studies", *Knowledge and Process Management*, Vol. 18, No. 3, 2011, pp. 150-174, available at http://onlinelibrary.wiley.com/doi/10.1002/kpm.378/abstract.

Cyberculture in Cyberspace

Cristian LAZĂR[*]
Raluca GALAON[*]

Abstract

The Internet has become our symbol for the future, being, in fact, a qualitatively new way of living. We use this technology icon to imagine what will result from our current period of rapid social change. Guidance and insight are the directions approached in this paper, using some of the world's most important and well-respected theorists of digital culture who offered an accessible description of cyberspace – from infrastructure to practice – along with an inspired, far-reaching exploration of its ramifications. We tried to open a window into the digital world, in order to offer a vision of the social realities and possibilities of cyberspace for the experts and beginners alike, arguing that instead of forming a perfect market, the Internet opens the space for knowledge.

Postmodernism – Provider of Cultural Changes

Ubiquity of information in the current social spheres, guaranteed by the technological revolution, is the main landmark of the contemporary world development. Postmodern revolution, driven by the microchip invention, has sustained the information processing and manipulation, which led to changes in form and substance of the communication model, with an impact on the current cultural and social patterns.

The new types of audience and public, specific to the postmodern paradigm, must be connected to the impact of both computer technologies and globalized capitalism, which generated real communication networks, information becoming the main merchandise of the present and future, because the integrity of systems requires it, on the one hand, and because the technology allows it, on the other hand.

If one of the components does not function properly, the systemic and interdependent nature of today's society involves, inevitably, negative effects on all of its other parts.

[*] PhD Candidate, "Alexandru Ioan Cuza" University of Iaşi
[*] Intelligence expert, Romania

The system's optimal function implies communication and information sharing, so that everyone could adapt to the changes of one's environment.

However, since there is no unitary postmodern theory, but rather a set of principles, postmodern theories that coexist, determined by the existence of a large community of postmodern theorists, which, in most cases, have different, even divergent opinions, we can say that Postmodernism is not the exhaustive key to the contemporary universe.

Pierre Levy was considered to be representative for the modern vision on the technology-culture binomial, due to the specific presentation of the digital communication revolution, with an optimistic outlook regarding the potential of cyberspace.

His works, *Cyberculture* (1997) and *Collective Intelligence. Mankind's Emerging World in Cyberspace* (1999) have highlighted the technology's defining role on the global society transformation, as well as the unlimited exchange of ideas in cyberspace, which will free the society from the political and social hierarchies which stood at the basis of its development.

To that end, apart from diversification of the audience, it is noted that the new information and communication technologies (NTIC) generated, within the new society, the emergence of a symbolic space, where declassification and demonopolization occur and legitimatizations of "cultural enclaves" at different intra- and inter- society levels come up.

> *"The new information (virtual worlds, information flows) and communication (many to many) systems are responsible for the contemporary cultural changes".*
>
> *(Pierre Levy, 1997)*

"Computerization of Society"

The dominant logic in receiving the society - technology binomial must be understood by replacing the "postindustrial society" paradigm with "information society" and, most recently, with "knowledge society".

The effect and also the feature of the new information and communication forms are the development of the network type matrix, which is nothing but a product of the contemporary society, of the technique as a whole and of the current discoveries in the field.

The message typology associated with the networks contains hypertexts and hyperdocuments, interactive simulations and virtual worlds, a trend which practically led to the digitization of information and to the development of the virtual dimension of communication, to the detriment of the eye/physical contact. According to Levy[1], the virtual becomes, in fact, one of the most important vectors of creating reality, as the appearance of concepts like "virtual subject", "virtual reality", "Avatar" proves it[2].

The immediate effect was individuals' tendency to customize their computers, a phenomenon the researchers at the Palo Alto Research Center called "ubiquitous computing". Inevitably, the patterns of life and contemporary social architecture have changed, as William J. Mitchell noted[3].

The interaction with and within the virtual world involves many and simultaneously activities: ranging from exploring the data to their updating in real time. When these types of interactions can upgrade a communication model, the virtual becomes a vector of collective brightness and, implicitly, of creation. As a result, the computers and the networks change into infrastructures of the new virtual information universe.

In an attempt to narrow down the information society theory, Jan van Dijk and Manuel Castells proposed a definition of the network society: a society in which the key social structures and activities are organized around electronically processed information networks.

However, Castells argued in his work entitled *Rise of Network Society* (1996) that not only did technology define modern societies but also the cultural, economic and political factors that made up the society network. In fact, the networks are the modern society's basic units.

There is also strong criticism on technology's impact on daily life, an opinion specific to the radical post-humanism (promoted

by Friedrich Kittler), argued through "technologies' apriorism upon humanism", where technologies are classified as "processors of information".

In fact, the reunion between the control theory and the information theory signaled the emergence of three important actors: information, control and communication, actors simultaneously operating together to produce a unique synthesis between organic and mechanical.

Virtuality and Culture

The symbiosis between society and technology takes shape mainly through the transformation of media technologies into culture agents in cyberspace. According to Ileana Rotaru[4], cyberspace is simply a result of the young's desire, internationally expressed, to experience new forms of collective communication, other than those found in the traditional media.

The accessible nature of cyberspace has favored its development as each individual decides on the means to exploit the positive potential at the economic, political, cultural and human level. Therefore, the new medium of communication is created through the global interconnection of computers.

Pierre Levy[5] enunciated Cyberspace's characteristics by introducing two original information systems, namely the virtual world and the information flows, into the postmodern theoretical framework.

> "*The virtual world arranges information into a continuous space, based on the position of the user or his or her representative in this world*".
>
> "*The information stream is a sequence of continuously changing data, dispersed among interconnected storage spaces and channels that can be traversed, filtered and presented to the cybernaut based on his or her instructions by means of programs and navigation systems.*"

Cyberspace's goal is to interconnect all people and encourage them to participate in the collective intelligence within a ubiquitous environment. The immediate effect was the rapid multiplication of both available data and links between different sources of information, within databases, hypertexts and networks.

Furthermore, we can talk about a proliferation of non-hierarchical contacts between individuals, generating an influx of data and information, entering the communication flows, but sustaining the creation and development of skills and competencies (technical and media) in order to foster relations within Cyberspace.

Thus, cultural contexts were used to reshape traditional media, embedded in similar or identical contexts, into digital media. The result was the cyberculture, which can be defined as a set of technologies (material and intellectual), practices, attitudes, ways of thinking, values that have developed along with Cyberspace.

This space – framework of knowledge, characterized by a continuous dynamic and learning, was entitled cosmopedia[6] by Pierre Levy. According to the French theorist, cosmopedia, defined as the knowledge area around the collective intelligence, goes beyond image and text, as communication forms specific to a certain period and combining "still images with videos, sounds, interactive simulation, interactive maps, virtual reality, artificial life, etc...". Through this phenomenon we practically witness the "Pinocchio effect", according to which computers come to life.

Virtual Communities

The new media which generated reconsiderations of the virtual cultural space led to the proliferation of virtual communities, of e-communities. Thus, the cultural communication supported the communities' role in the virtual space, allowing them to develop their own original cultural content and to use it in the form of blogs, journals, electronic encyclopedias or any virtual medium.

Karen Moustafa Leonard[7] concluded that the development of the technological communication contributed to reducing social and cultural distances, although the way people perceive the cultural effects of media faces some barriers.

The major differences identified between virtual and traditional communities by Kumiko Aoki[8] are: freedom from geographical limitation; the accessibility at one's own convenience; the retrievability of information/messages; the limitation of communicative acts to textual messages.

In the literature, a new concept was attached to the virtual communication - *Computer Mediated Communication* (CMC). Most of the CMC is made through textual communication (with pictorial significations of web pages).

In this type of communication, the social status is not an attribute to be considered, since it is mainly based on the text, which cannot contain information about the tone of voice or the facial expressions. The "phatic" aspects of face to face conversation are minimal in CMC and sometimes they are characterized by a certain exacerbated anxiety of the sender when receiving no answer[9].

The features of the new contemporary social structures (in the network), as perceived and expressed by Andreas Wittel[10], are:

- individualization – Cyberspace is populated with experience and biographies of some subjects with a variety of educational and geographical backgrounds. They are practically "extracted" from their own backgrounds, contexts and integrated into a disorganized mass of social relationships to which they must contribute;
- intense and ephemeral relationships – are specific to the knowledge society;
- translation from narration to information – the information represents a compressed section of time and space, event or signal in space and does not claim the right to universality, only to present;
- assimilation of ludic to work – in the social networking, games are encouraged in professional relations, design and distribution of information in order to encourage creativity;
- technology – its purpose is to ensure operation of the whole as social relationship.

Despite the specificity determined by convergence of telecommunication technologies and use of computer, virtual communities represent, in fact, the return to one of the primary, etymological meanings of communication – *communis*.

From this perspective, Cristophe Hebrad[11], identified among the specific elements of virtual communities:

- Common interests and affinities due to sharing the same value system, generating preferential relations, independent of geographical space.

- Interaction, by completely overlapping the transmitter and the receiver, in order to support the intense communication.
- Synchronicity of communication, which makes the individuals develop spontaneous relationships in real time.
- Diversity of participants, where the virtual community means the existence of at least two members from different interacting areas and cultures.
- A certain level of membership and participation.
- Managing a common symbolic space, alongside the technological skills of its members in order to maximize the communication process.
- Cognitive competence to debate, approach or initiate certain topics, themes etc., flexibility and permanent re-composition of the membership.

Based on the above typologies, Ileana Rotaru[12] analyzed two general categories of virtual communities.

The first category refers to those communities including individuals who previously met face to face. In this case, the virtual communication is used only to maintain the routine dialogue in order to discuss some topics considered of interest to its members or to collaborate on certain projects. The main form of manifestation of this type of communication is electronic mail or *e-mail*.

As for the second category, the individuals do not necessarily know each other, but share the same common interests, value systems and objectives. Therefore, the communication is made, mostly, through forums or electronic conferences in order to exchange information and ideas.

One of the direct consequences of increasing media convergence, within virtual communities, is the unlimited perspective of people being present in such different communities, regardless of geographical and temporal differences.

This has started to be evident since 1968, as ARPANET, the first extensive computer network, came into existence, exponentially increasing along with the Internet. In the first stage, most of them belonged to universities, government agencies and companies.

Social networking has transformed social relations into information relations, where the core and common element was not individuals' past, marked by life experiences, but the intense and continuous exchange of data, which is constantly updated.

The development of social networking is due to information and communication technologies, to the globalization and individualization process, to the new media with cultural roots.

Moreover, the interactive media generated, according to the results of an analysis made by Kiyoshi Abe[13], a change of perception over surveillance, developed in the information society.

Traditionally, this activity was regarded as highly repressive, but now the ubiquitous surveillance is perceived rather as a game, an activity voluntarily accepted by those who use interactive media.

The forerunner of the "social networking" phrase is considered Manuel Castells, who also introduced the concept of *network society*[14]. Its aim was to highlight the social relationships and characteristics in the information era, from a macro perspective.

According to the theorist, on the one hand, the networks, considered topics and technologies, are analyzed, and, on the other hand, the relationships among them are pursued. These are open structures, able to expand almost limitlessly and with a high degree of dynamism. Thus, the networks are "tools at hand for the capitalist economy based on innovation, globalization and decentralization, and part of the culture involved in a constant process of construction and deconstruction"[15].

New media – Impact of '*Always On*' Technology

The transition from the industrial, modern technologies to the postmodern technologies is characterized not only by splitting, but by continuity. The virtual communication, as the new form of human experience, is the product of the new technologies of contemporary communication in the electronic and information world.

The '*always on*' technology can be considered both a necessary instrument and an impediment, in some cases, for the analysis of

open sources information. This technology represents a new form of culture that characterizes certain social strata, certain people from different geographical areas, who share the possibility to access and use the new communication technologies.

Ileana Rotaru considered relevant the synthetic model developed by Lister *et al.* in 2007[16] in order to understand the meaning of "new" in "new media":

- new textual experiences – a special typology within the new media consumption for the escape in ludic (electronic games, special movie effects, etc.)
- new forms of world representation – such as the interactive multimedia;
- new relations between users and consumers and media technologies – the changes in the image use and reception in the media communication and at the level of understanding the investment in media technologies;
- new experiences of the identity-community relationship – changes in the personal perception of space, time and place, with implications over the self-perception;
- new understandings of the biological body-media technology relationship – challenges to make distinctions between human and artificial, nature and technology, real and virtual;
- new models of organization and production - large realignments and media integration into culture, industry, economy, access, ownership, control and regulation.

In an interview entitled "The Information Bomb" with German media theorist Friedrich Kittler, in 1999, Paul Virilio pointed out that the fallout from "The Information Bomb" would be as lethal as the nuclear bomb, destroying collective memory, relations, traditions and community with an instantaneous bombardment, overloaded with information.

Preserving the definition of virtual communication, the most important vector of expressing virtuality remains the Internet. Pierre Levy[17] made a distinction between two processes that occur while browsing the Internet, making the virtual communication.

Most often it is a mix of the two. The first is called "*hunting*" and designate a method applied when seeking certain information in a relatively short time. The second process is "*gathering*" and it represents a random browsing of the Internet, completed by gathering information after browsing several websites.

Based on the main ways of virtual interaction and communication, the same Levy[18] identified the major differences brought by the technological innovations and the digital media between traditional (TV, radio, telephone) and virtual communication systems.

- Remote access and file transfer – represent one of the main functions of virtual space by accessing different databases and information regardless of spatial and temporal coordinates. It also promotes interaction within communities, managing to maintain contact between their members.
- E-mail – reasserts the leading role that transmission and exchange of messages play in Cyberspace. This function changes not only traditional relationships as in the written correspondence, but the whole process by: simultaneously accessing multiple lists of recipients, deleting, keeping, or changing the message without using paper, sending a significant amount of information (by attaching documents or hypertext).
- *News* groups and mailing lists - is a more complex function than e-mails, as it allows a group to discuss certain topics, by using a sophisticated program. The group members are connected at the same time and the messages are not usually saved. Through these forms new ways of writing and interaction have developed. It is a form of communication specific to chats. Cyberspace becomes a way of relating with others regardless of the geographical location or name, only based on interests, needs and discussions.
- Group Awareness - is a deeper form of communication than news-groups. This takes the form of relations established, for example, in the cooperative learning based on computer or within the Internet (as a form of organizational communication) and involves

collaboration, providing documents, information, creation of joint hyper-documents. Transparency is the fundamental feature of this type of communication.

The sense of novelty of the *new media* concept contains a certain substrate of abstraction, grounded by the need to use the syntagma in the plural due to its variety.

Our effort should take into account the entire variety of changes caused by the "new", not particularly made meaning the technology developments. Thus, the fluctuations between the new and the old should be taken into consideration as clear aspects of differences.

The main differences specific to new media are: Digitality, Interactivity, Hypertextuality, Dispersion and Virtuality.

The huge number of *corporate* or personal websites, blogs, public forums, the unprecedented popularity of social networks (hundreds of millions of accounts), but also the soar of the user-generated content and the diversity of languages and packages in which the information is delivered are the main characteristics of *new media*.

Conclusions

Billions of Internet users actively participate in the process of innovation, value creation, and social development in a form labeled as utopia several years ago. The deep changes, in terms of demography, in the technology field, economy and world in general, are unambiguously indicative of a new era in which people have a real-time participation in the global processes, its impact being undoubted. They use virtual media as a tool to contribute to the development of competitiveness and innovation in different fields.

Harnessing human skills, ingenuity and intelligence, in a much faster and more efficient way, regardless of the proposed target, should become the defining capacity of any organizational structure.

One should understand that we entered a new era, based on new principles, life philosophies, new models, new standards, where the game has changed and keeps changing with each presence in Cyberspace.

References

[1] Pierre Levy, *Cyberculture. Rapport au Conseil de l'Europe dans le cadre du projet 'Nouvelles technologie cooperation culturelle et communication'* (Paris: Odile Jacob, 1997).
[2] A virtual reality, interface of the human in the virtual space.
[3] William J. Mitchell, *City of Bits: Space, Place of InfoBahn* (MIT, 1995-1997) available at http://www.kejvmen.sk/cob.pdf (accessed on 15 April 2012).
[4] Ileana Rotaru, *Comunicarea virtuală* (Bucharest: Tritonic Publishing House, 2010).
[5] Pierre Levy, *apud* Ileana Rotaru, *Comunicarea virtuală.*
[6] Pierre Levy, *Collective Intelligence. Mankind's Emerging World in Cyberspace* (Cambridge: Perseus Books, 1999).
[7] Karen Moustafa Leonard, "Examining Media Effectiveness Across Cultures and National Borders: A review and Multilevel Framework", *International Journal of Cross Cultural Management*, April 2011, available at http://ccm.sagepub.com/content/11/1/83/.full.pdf (accessed on 20 April 2012).
[8] Kumiko Aoki, "Virtual Communities in Japan", 1994, available at http://www.uni-koeln.de/themen/cmc/text/aoki94.txt (accessed on 11 April 2012).
[9] Kumiko Aoki and Edward J. Downes, "An Analysis of Young People's Use of and Attitudes Toward Cell Phones", 2003, available at http://www.angelfire.com/ego2/lostboyrahul/work/cellphoneuse.pdf (accessed on 10 April 2012).
[10] *Apud* Ileana Rotaru, *Comunicarea virtuală.*
[11] *Apud* Constantin Cucoş, *Informatizarea în educaţie* (Iaşi: Polirom Publishing House, 2006).
[12] Ileana Rotaru, *Comunicarea virtuală.*
[13] Kiyoshi Abe, "The Myth of Media Interactivity. Technology, Communications and Surveillance in Japan", 2009, available at http://www.sfu.ca/~roman/page176/assets/Media Interactivity.pdf (accessed on 15 April 2012).
[14] Manuel Castells, *The Rise of the Network Society* (Wiley Blackwell, 2000, 2nd edition).
[15] *Ibid*.
[16] *Apud* Ileana Rotaru, *Comunicarea virtuală.*
[17] In the revised 2001 edition of *Cyberculture*.
[18] *Ibid*.

Projection, Foresight and Prevention – Elements of Modern Intelligence Systems

Iuliana UDROIU[*]

Abstract

The following paper approaches the debates on the early warning meaning and benefits, as compared to other concepts in the field of threat and risk forecasting and prevention, identifying at the same time the vulnerabilities and dysfunctions that could impact national security.

Moreover, it is useful to underline the conceptual distinction from other instruments aimed at increasing anticipatory capabilities of government intelligence agencies, as there is no clear boundary between prediction and warning mechanisms.

Introduction

Specialized information structures are fundamentally dedicated to risk management, reducing uncertainty, anticipating and preventing any situations that can impact security. At the same time, sources of insecurity are as diverse as complex and can be defined only after analyzing the threats, vulnerabilities, risks and dysfunctions as well as after identifying the interests and opportunities to capitalize on the available operational, tactical and strategic advantages. Analysts working within these systems, together with the intelligence operatives, regardless of their particular focus and the provider-customer relationship, are committed to anticipating threats, warning about and, increasingly more, predicting the course of events and identifying those issues and developments that require decision.

These tasks are performed by bringing together a mix of facts, inferences, value judgments and knowledge based on evidence on the focused topic[1], so that to create a clear projection on the security environment and the potential directions to which factors influencing it could evolve and to anticipate risks, threats, vulnerabilities and dysfunctions, if possible.

[*] PhD Candidate, "Mihai Viteazul" National Intelligence Academy

Forecast is strongly interlinked with prevention and preparation for contingencies or situations deemed possible, including surveillance/ warning activities, prediction, prognosis, multidisciplinary teams, networks, conceptual, technological, intelligence approaches.

Prevention – Basic Function of the Process of Achieving Security

Some recent theories make a difference between *operational prevention*, considered as short-term effort, using military or political means to prevent the conflict or stop it before violence escalates, *structural prevention*, defined as effort to manage the root causes of the conflict through economic means or development, aimed at reducing risk and demanding better regulatory frameworks, and *systemic prevention*, which reduces the conflict on a global basis and exceeds the mechanisms focused on particular states[2].

Structural and systemic prevention focus generally on the complex causes that produce an unexpected event, such as the medium and long term conflict, but they may be inadequate in the case of a crisis which is about to occur or of an acute crisis requiring preventive action[3], such as reducing environmental degradation, preventing epidemics, countering conventional and unconventional weapons proliferation, cracking down on trafficking, fighting corruption etc.

In all these cases, intelligence services play a key role, which implies actional/operational, or analytical support, and communication capabilities, which should efficiently act or be used in order to achieve performance in carrying out basic functions - documentation, forecast, and assessment of events that will or might occur.

Developing anticipative analysis capacity, able to help organizations curb uncertainty, increase resilience and flexibility and enable decision makers/customers to better manage strategic change, depends, according to Kenneth Knight, on five critical elements.

The first is the ability to reliably identify existing challenges and opportunities and anticipate emerging ones. This demands an integrated set of structured analytic approaches, based on both evidence and possibilities, to systematically track global developments, detect existing trends and patterns and faint signals and start the process of ordered analytic triage of sorting, initial prioritization, and early treatment.

The second is the capacity to evaluate and prioritize among challenges and opportunities, which implies: assessing the likelihood that a positive or negative event will materialize, potential strategic impact on the enterprise, confidence in likelihood/impact judgments; identifying potential points of leverage to affect outcomes; recognizing key uncertainties and information gaps.

The third is the ability to have open communication channels to decision makers and hierarchical superiors, necessary to engage them in a continuing dialogue aimed at co-opting them as partners in the process of strategic planning and risk and opportunity management.

The fourth element refers to the ability to reliably monitor enduring issues in order to distinguish between "normal" and "unusual" developments, to evaluate important changes and identify and articulate periods of increasing and decreasing risk.

Finally, the fifth element is the system's ability to assist decision makers in identifying plausible options for mitigating risks and seizing opportunities as well as assessing implications and consequences of potential courses of action[4].

Methods of Ensuring the Preventive Function

Dedicated to the **early warning** concept, M. H. Glantz[5] noted that embedded systems include all aspects of emergency management, including risk analysis, which is one of the main requirements of the system, monitoring and predicting the location and intensity of the natural disaster that is about to occur, communicating the warning to the authorities and target people and responding to the disaster. Warning failures are attributed to poor functioning of one of the system elements, often the communication system and appropriate response plans[6].

According to M. H. Glantz[7], it is essential to note that predictions are not useful unless they are turned into warnings and action plans that the public understands and only if the information reaches the target people in a timely manner.

In its classical sense, early warning is considered "an activity, done formally or informally, that occurs before the conflict has a chance to sharply escalate and before preventive action is taken"[8] and it is aimed at issuing a warning about an event as far in advance as possible.

In this sense, early warning is "fundamental" for preventive work, saying that "where prevention fails, early warning serves a purpose"[9].

According to Cynthia Grabo, expert with over 30 years experience in the analytical division of the CIA, warning is a skill unto itself, requiring an understanding of the attitudes and disciplines of potential adversaries as well as their capabilities, their history, their culture and their biases. Cynthia Grabo conducted an extensive radiography of early warning, in terms of intelligence, imposing the concept of *warning intelligence* in the specialized literature.

As discipline, *warning intelligence* differs significantly from *current intelligence* and long-range estimates, because it is not merely a compilation of facts, but, in the process of elaborating the warning proper on a particular case, it actually accepts the presumption of surprise and incomplete intelligence, relying inclusively on conflicting reports, fragmentary evidence or even their absence.

Early warning is considered by most theorists in the field as a process, not an event occurring at a certain point in time or as part of an operational plan, a part of a continuum that begins with detecting the change in scanned environment, goes through assessment and warning to end (or not) in a decision and response[10]. The response is still an open problem when putting the purpose of the warning process and, moreover, the efficiency of dedicated systems to the issue.

Beat Habegger subsumed it, alongside horizon scanning, the STEEP technique, trend and scenario analysis - to the methodological complex used to monitor the environment in a manner as complete as possible in the first phase of strategic foresight, that of obtaining information (topics, developments, events) that may be relevant to a state or organization, in order to avoid the strategic surprise and provide sufficient time to the decision makers for adopting effective counteraction measures[11].

Early warning can neither detect nor solve all potential conflicts. Moreover, it has no capacity to combat the present causes of future or escalating crisis. It only contributes to finding remedies for crisis situations so that they could be managed in a less expensive manner. From this perspective, the EW should be considered an element of a broader strategy, its basic principle being long-term development.

As an essential tool for strategic management, whether talking about the governmental, nongovernmental or private field, early warning's role is to highlight the political, economic, financial, social, environmental developments and assess their potential impact on the security interests. In essence, they have the mission "to bring the future into today".

The special importance of early warning becomes even more obvious if we mention the fact that, in real terms, the EW process is similar in many respects to the *intelligence* process: information gathering, processing and analysis (detection), interpreting and reporting (forecast). This might seem a negative element, but the competition between the civil and *intelligence* sectors in terms of raising awareness on potential threats is beneficial as long as it is objective, fair, and constructive. Moreover, sharing the two parties' expertise as well as methodology and achievement of early warning brings added value in the area of national security interests, while the *intelligence* sector provides an objective perspective, focused on security interests enjoying the professionalism of those engaged in ensuring and creating social, economic, and political stability.

Forecast is commonly preferred in the economic and financial fields, yet it has become increasingly popular in the political circles, especially when referring to elections, and it is also used in the area of international relations (one of the theorists being Philip Schrodt[12]) or security, as it provides the decision makers with a theory on the possible structure of the future and with an original research methodology, streamlining thus the process of solving complex problems in which uncertainty prevails.

Since the 1960s, forecast has been scientifically documented, being delimited from other prediction tools, and has been mostly underpinned by the research work of Scott Armstrong, who established the Forecasting Principles Project[13], so that to codify and summarize all knowledge about forecasting. Forty international experts and 123 reviewers have contributed to this four-year collective effort and 140 principles have been identified so far, referred to as lessons learned[14].

In practice, forecast is sometimes associated to *strategic foresight*, defined as a systematic and organized process to reduce uncertainty regarding the future[15], and has as starting point "the belief that there are many possible futures"[16].

Committed to this forecasting tool, the authors of the "Handbook for Knowledge Society Foresight" defined foresight as a "systematic, participatory process, which is based on gathering intelligence about the future and substantiates a medium and long-term vision", therefore aiming at "informing present-day decisions and mobilizing joint actions"[17].

Foresight is also defined as a mental model, a result of an organizational process that draws inferences from the present in order to gain insights into appropriate actions for the future. Its role is "to shape actions and events reflected in a chaotic future", and its efficacy depends upon the accuracy of the mental models and the consistency of the subsequent actions[18].

Richard Slaughter dismissed the idea that foresight is a mere "ability to predict the future", instead he described it as a basic human attribute, which all people have and use, associating it to a "deliberate process of expanding awareness and knowledge through futures scanning and clarification of emerging situations, an extension of the innate brain/environment perceptions"[19]. Very important for its conceptual delimitation, he mentioned that foresight is "a sort of early warning system which indicates, as effects, the place where one does not want to reach"[20].

The director of the Futures Studies Centre (Australia) associated four main application areas to the concept of foresight: assessing the possible consequences of actions and decisions, anticipating problems before they occur, considering the present implications of possible future events and envisioning desired aspects of future societies. What Richard Slaughter thought of foresight became the landmark of what we call today "strategic foresight".

Michael Keenan, representative of the British school of *foresight* at the School of Business Management (PREST, Manchester), points out that "there are five important features that

should be considered for a process to be included into the *foresight* category: the scan of future has to be done systematically; the time horizon has to vary between 5 and 30 years; the ratio between the support and funding of science and technology and the capacity of the market (economy, society) to absorb the results must be constantly balanced; the main purpose of the *foresight* process is to create appropriate government support so that research should get the adequate technologies in order to absorb these results into industry or society; equal attention should be paid to the social impact and the process of producing welfare within the society".

Highly interested in promoting innovation and research, the European Union has created numerous bodies dedicated to developing anticipation, forecast, predictive analysis and foresight capabilities at the European level. They are generally included in the European Commission's directorates. By means of its funding programs, the EU puts also particular emphasis on enhancing the anticipatory and projective abilities as well as on the creation of an expert authority in the field, relevant examples of good practice being FOR-LEARN, the European Foresight Knowledge Sharing Platform and the European Foresight Monitoring Network.

The Joint Research Centre (JRC) is one of the best known institutions of this kind, encompassing seven specialized institutes. Among these, one could mention the Institute for Prospective Technological Studies (IPTS), founded in 1994 and located in Seville, Spain, specialized in studying technology, economy and social phenomena. Its work program, based on "Actions" (macro-projects), covers the following fields: *research policy and techno-economic foresight, sustainable development, industrial and clean technologies, energy, transport, agriculture and rural development, and the information society*.

The Institute's activities contribute to elaborating and developing EU policies, but also provide materials to support the monitoring and implementation of the policy cycle stages. Research focuses on challenges of strategic importance to the European Union. The analyses are underpinned by specialized scientific research tools, both quantitative (modeling) and qualitative (foresight).

Instead of Conclusion

Despite its numerous benefits, early warning does not guarantee the success of preventive actions unless it also generates a fundamental shift in the attitude of those required to shape the security environment. Because it is a human-led activity and the relationship between an early warning launched by experts and a preventive measure taken at a high decision-making level goes beyond the "input – output" model, even when the warnings are clear and actionable, the organizational and systemic obstacles can lead to the emergence of diffuse responsibilities or to an increase in costs and risks, so that the unfolding of planned actions could be hindered.

The requirements are equally high for the experts engaged in such projects, who must be able to break bureaucratic barriers and cognitive patterns, to constantly improve their skills and level of knowledge, to collaborate with the best correspondent bodies in their field of activity (regardless of their affiliation to intelligence services or civil society) and to defend their opinions in front of the conservative elements still present in some academic, institutional, or political circles.

In order to answer the most unconventional questions, to make themselves understood and to understand, in their turn, the current political goals and guidelines, experts should permanently interact with decision makers, particularly because effective and timely early warnings, able to guide security decisions and strategies, imply launching even the most whimsical hypotheses and drafting long-term scenarios.

Both the individuals required to ensure the optimal climate for social, economic, and political development and those able to guide these activities must understand and take responsibility for their failures, achievements and their impact on present situations as well as for the detailed assessment of their performance in the field, since no one will ever invest money without being informed on the previous accomplishments.

Early warning is not intended and cannot represent a universal tool for anticipating political, social, and economic crises. Still, as the theoretical basis is being crystallized and the end products intended for political decision makers are getting their own distinctive features, it may become a key factor in preventing and reducing the threats looming over global security.

References

[1] Bowman H. Miller, "Improving All-Source Intelligence Analysis: Elevate Knowledge in the Equation", *International Journal of Intelligence and Counter Intelligence*, Vol. 21, No. 2, 2008, pp. 337 – 354.

[2] Barnett R. Rubin and Bruce D. Jones, "Prevention of Violent Conflict: Tasks and Challenges for the United Nations", *Global Governance*, Vol. 13, No. 3, 2007, pp. 319-408.

[3] Susanna Campbell and Patrick Meier, "Deciding to Prevent Violent Conflict: Early Warning and Decision-making within United Nations", Chicago Conference, 28 February - 3 March 2007, available at http://irevolution.files.wordpress.com/2011/07/campbell-meier-isa-2007.pdf.

[4] Kenneth Knight, "Warning in an Era of Extreme Global Dynamism", *Resilience and National Security in an Uncertain World* (Singapore: Centre of Excellence for National Security, S. Rajaratnam School of International Studies, 2011), pp. 48-49, available at http://www.rsis.edu.sg/cens/PDF/RSIS_GFF_300311.pdf.

[5] M.H. Glantz, "Usable Science: Early Warning Systems: Do's and Don'ts", *Early Warning Systems Workshop*, Shanghai, China, 20-23 October 2003.

[6] Veronica F. Grasso, "Early Warning Systems: State-of-Art Analysis and Future Directions", draft report, *United Nations Environment Programme*, available at http://na.unep.net.

[7] Glantz, "Usable Science".

[8] Walter A. Dorn, "Early Warning of Armed Conflict. An Introduction", course material at the Pearson Peacekeeping Centre, available at http://walterdorn.org/pub/25.

[9] Dorn, "Early Warning of Armed Conflict".

[10] Richard Betts, *Surprise Despite Warning. Why Sudden Attacks Succeed* (Washington: Brookings, 1981).

[11] Beat Habegger, "Strategic Foresight: Anticipation and Capacity to Act", *CSS Analysis in Security Policy*, No. 52, April 2009, p. 1.

[12] Philip A. Schrodt, "Forecasts and Contingencies: From Methodology to Policy", paper presented at the *American Political Science Association Meetings*, Boston, 29 August - 1 September 2002, available at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.15.978&rep=rep1&type=pdf

[13] See http://www.forecastingprinciples.com.

[14] J. S. Armstrong, "Findings from evidence-based forecasting: Methods for reducing forecast error", *International Journal of Forecasting*, No. 22, 2006, pp. 583-598.

[15] Thomas Fingar, "Anticipating Opportunities: Using Intelligence to Shape the Future, and Myths, Fears, and Expectations", Payne Distinguished Lecture Series 2009 *Reducing Uncertainty: Intelligence and National Security*, FSI Stanford, CISAC Lecture Series, 21 October 2009, 11 March 2009, available at http://iis-db.stanford.edu/evnts/5859/lecture_text.pdf, accessed on 25 January 2012.

[16] Ben R. Martin, "Technology Foresight: capturing the benefits from science-related technologies", *Research Evaluation*, Vol. 6, No. 2, August 1996, p. 158.

[17] Ian Miles, Michael Keenan and Jari Kaivo-oja, "Handbook for Knowledge Society Foresight, Annex A: Foundations of Futures and Foresight Research", available at http://forlearn.jrc.ec.europa.eu/guide/A1_key-terms/foresight.htm.

[18] Deborah A. Blackman and Steven Henderson, "How Foresight Creates Unforeseen Futures: The Role of Doubting", *Futures*, No. 36, 2004, p. 254.

[19] Richard A. Slaughter, *The Foresight Principle: Cultural Recovery in the 21st Century* (Westport: Praeger Publishers, 1995), p. xvii.

[20] *Ibid.*, p. 1.

Romania in 2030. Future Trends Impacting the Romanian Intelligence Service

Ionel NIŢU[*]
Gheorghe-Costinel ANUŢA[*]

Abstract

The paper is a prospective exercise based on the extrapolation of certain internationally wide accepted indicators (Failed States Index, Global Innovation Index, etc.), in the light of their historical evolution and also of some specific features (diffusion of power, demographic mobility, escalation of the competition for resources, etc.) considered to be relevant by currently applied prospective studies.

Based on the topics highlighted by the aggregation of the above-mentioned data, we have analyzed the impact of the mentioned indicators' evolution on some of SRI's policies, ranging from those related to human resources recruitment to elements likely to generate difficulties regarding the accomplishment of the service's missions. This work was also correlated with elements highlighted by SRI's recent strategic documents.

Against this backdrop, it was observed the necessity to approach the possibility to implement the concept of resilience within SRI, in order to reduce the consequences of any "strategic surprises" to the activity of the service.

Generally speaking, the current paper is about the possibility to take into account a possible role for foresight in the intelligence work. The use of foresight might have an important role for exploring not only a future environment, but also the future of an organization. Moreover, the intelligence sector doesn't have to build extensive capabilities and tools for exploring the future, but to connect to the existing flows.

However, as there are a lot of definitions in place regarding foresight, we will draw this study on a descriptive view on the term, meaning that this kind of products are projecting plausible future(s), being based on all our knowledge on the reality/the way the analyzed events are manifesting. As such, we will pay attention into our analysis to the outcomes of more than one plausible scenario for the future of Romania/SRI.

In the meantime, while we cannot compete with the visions of much more experienced researchers in the field (an interesting analysis on the topic was recently offered by Tetlock and Horrowitz[1]),

[*] Intelligence expert, Romania
[*] Intelligence expert, Romania

we will try to map some advantages and perhaps limitations in the use of foresight within the framework of an exercise regarding the futures of Romania and their impact(s) upon the Romanian Intelligence Service.

At the beginning of this research we had many doubts upon its usefulness - given at least two considerations: first the interest in the future or at least in a far-away future such as 2030 would be low, given the day-to-day priorities, secondly the limitations of such an endeavor are quite high and might decrease its value. Nevertheless we thought that it is better to give it a try than to wait for the future to happen.

However, given the two above-mentioned considerations, we decided to focus, for the beginning, on the future of a key priority during the SRI transformation – **the human resources** (as stated within the SRI 2007-2010 Strategic Vision) and particularly on the challenges regarding **the future pool of recruitment for our service** (since the intelligence work requires highly-qualified personnel). Pending on the interest shown in this particular research, we see it as a basis for a further endeavor, which has to include the other key dimensions of our service. A sound and comprehensive perspective on the future of SRI's key dimensions might be taken into account as a basis for the future strategic papers guiding the service's work as well as it might be factored into SRI's strategic planning process[2].

Another challenge related to the research pertained to the quest for the appropriate tools in supporting such an endeavor. For example, it is very difficult in a democracy to factor political decision-making into a research with such an extended horizon. However, in our case, we didn't take into consideration political decision-making in our analysis (except for the drivers already taken into account by the tools we used to project the future of Romania) since it is expected to have most probably a negative impact on the Service, given the current European (perhaps world) trends of downsizing the security sectors, as a result of the financial crisis.

As such, we have decided to use already validated software for estimates on the future (the *International Futures* programme at the Pardee Center of the University of Denver, version 6.61), and to combine it with current statistics (particularly withdrawn from the 2008-2012 editions of the *Global Competitiveness Report*, drafted by the World Economic Forum) and individual reflection.

Modeling Basics: International Futures Software and Global Competitiveness Reports

Before getting to the **International Futures** (IF) **programme** we thought of building our research on the extrapolation of certain internationally wide accepted indicators (Failed States Index, Global Innovation Index, etc.), in the light of their historical evolution and also of some specific features (diffusion of power, demographic mobility, escalation of the competition for resources, etc).

However, while studying modeling basics for the IF software we understood that it is the most appropriate tool for supporting our research since the advantages of using IF are enormous, especially with a view to the time needed to build such a model given its complexity. The IF model is built on **nine groups of indicators** – population, health, education, social/human needs, economy, energy, environment, international politics and domestic government – and the simulations are the result of modeling more than 800 parameters, with historical data, where possible. The simulations are also based on statistical data from current indexes calculated by widely acknowledged institutions such as Freedom House (economic freedom), Transparency International (corruption perception), World Bank (doing business) and other endeavors (Polity project, State Failure project, etc.).

Nevertheless, we were also influenced by the fact that Romania was one of the 183 countries modeled with the IF and we obtained, in this manner, a more accurate view on its evolution toward 2030 (a timeframe chosen in connection with some of the major foresight papers[3]).

The IF programme was initiated in 1980 and its functionality was very well described by Dr. Barry B. Hughes from the University of Denver, who was extremely involved in the development of the IF model, across four generations (1980, 1985, 1993 and 2000)[4]:

"*International Futures (IFs) is a large-scale integrated global modeling system. International Futures serves as a thinking tool for the analysis of near through long-term country-specific, regional, and global futures across multiple, interacting issue areas including human development, social change, and environmental sustainability*"[5].

Another plus of the IF is that the programme is a **focal point for a large network of researchers and organizations**. As such, while some parts of the IF were being funded by the TERRA project

of the European Commission and by the Strategic Assessments Group of the US Central Intelligence Agency, the global think-tank Millennium Project used, starting with 2010, the IF model for calculating the State Of the Future Indexes (SOFIs), an endeavor designed to show if the current policies will provide for a better future.

Last, but not least, an extremely important feature of the IF model is that it is designed across four basic scenarios. According to Roy Pearson[6], the four scenarios are build on the United Nations Environment Programme's "Global Environment Outlook GEO-4" of 2007 (pp. 400-401), to which the IF developers contributed, available online at http://www.unep.org/geo/geo4.asp:

- Within the **Markets First** scenario, "*there is a narrow focus on the sustainability of markets rather than on the broader human-environment system. Technological fixes to environmental challenges are emphasized at the expense of other policy interventions and some tried-and-true solutions*".

- **Policy First** scenario "*introduces some measures aimed at promoting sustainable development, but the tensions between environment and economic policies are biased towards social and economic considerations... the emphasis is on more top-down approaches, due in part to desires to make rapid progress on key targets*".

- **Security First** scenario, "*which could also be described as Me First, has as its focus a minority: rich, national, and regional. It emphasizes sustainable development only in the context of maximizing access to and use of the environment by the powerful*".

- As for the **Sustainability First** scenario, "*the government, civil society and the private sector work collaboratively to improve the environment and human well-being, with a strong emphasis on equity. Equal weight is given to environmental and socio-economic policies, and accountability, transparency and legitimacy are stressed across all actors*".

During the simulations, a fifth scenario arises, **IF Base**, not annotated in the model, but emphasizing, as Pearson mentioned, "*a central-tendency scenario, generally following a path that is an extension of the model's historical relationships*"[7].

However, the Security First and Sustainability First scenarios have a particular importance for the current research since they will emphasize some specific trends, different from the other two scenarios.

Even though the IF seemed to be such a comprehensive tool, we still wanted to fill some gaps in the research with the help of the statistics from the **Global Competitiveness Reports** (GCR). In that respect, our focus rested with the evolution of the labor market in Romania, and particularly the trends regarding the brain drain phenomenon.

Across the five editions of the GCR used for the current research, the study of competitiveness reached a significant number of 144 economies all over the world (including Romania). According to the latest report, the GCR "*contains a detailed profile for each of the economies included in the study as well as an extensive section of data tables with global rankings covering over 100 indicators*"[8]. Moreover, the GCR is based on the inputs offered by over 150 partner institutes worldwide, which are carrying out an Executive Opinion Survey for each of the countries analyzed by the GCR. Apart from the survey, the GCR uses statistical data obtained by internationally recognized agencies such as the UNESCO, the IMF and the WHO.

For benchmarking the competitiveness, the GCR is analyzing **12 factors** (called "pillars of competitiveness") – institutions (legal and administrative framework), infrastructure, macroeconomic environment, health and primary education, higher education and training, goods market efficiency, labor market efficiency, financial market development, technological readiness, market size, business sophistication and innovation. The index resulted from the study of the 12 factors indicates **the stage of development** for the analyzed economy - factor-driven (low-skilled labor and natural resources), efficiency-driven (efficient production processes and increased product quality) and innovation-driven (the most sophisticated production processes, and new/different goods through new technologies)[9].

Choosing the Indicators: IF Simulations and GCR Statistics

In studying the evolution of the recruitment pool for the SRI toward 2030, we took into account both a **quantitative** approach, oriented toward demographic shifts, as well as a **qualitative** one, more complex and multiple-faceted but having as the lowest common denominator the drivers facilitating the brain drain. The indicators chosen for both approaches are in line with the human resources

theories (e.g. population growth and distribution, financial motivations, values and so on), and in our view are the most relevant ones for such a research. However, we cannot rule out the study of other indicators (technological change for example), but we made sure that most of them were factored into the IF model, our main tool for the current research.

As such, while for **the quantitative dimension** of the recruitment pool we took into account three indicators – the evolution of the overall population, the level of education (particularly the enrollment for tertiary education) and the aging – **the qualitative side** was focused on Romania's ability to retain and attract talented people, the evolution of the wages (pending on the GDP growth), the human resources motivations and the brain drain (pending on the evolution of the above-mentioned qualitative drivers, as well as on the evolution in labor market efficiency).

The quantitative analysis is **entirely based on the IF simulations** (version 6.61), and particularly on the population module of the model. Nonetheless, we will not get into a detailed description of the way the indicators are computed and extrapolated with the IF, but we will refer to some features emphasizing the complexity of the IF population module. Though, according to Hughes and Hossain[10], the methodological approach of IF can be called "*Structure-Based and Agent-Class Driven Modeling*" and is designed around five key elements: organizing structures, stocks, flows, key aggregate relationships, and key agent-class behavior relationships. In an example presented also by Hughes and Hossain, the key elements for the population module would look like in the following table:

Table 1 – *Population module in IF: key elements*[11]

System/ Subsystem	Organizing Structure	Stocks	Flows	Key Aggregate Relationships (Illustrative, not Comprehensive)	Key Agent-Class Behavior Relationships (Illustrative, not Comprehensive)
Demographic	Cohort-Component	Population by Age-Sex	Births, Deaths, Migration	Life Expectancy (including HIV/AIDS) with Exogenous Technological Assumptions	Household Fertility and Migration

Whilst analyzing the simulations for the quantitative approach, we will notice that **the overall population is decreasing** (graph 1 from the annex) and there is **sharp disparity in aging** (graphs 2 and 3 from the annex) across the four scenarios.

On the other hand, an interesting evolution is displayed by the enrollment graph (graph 4). Even though there is not an overall significant difference, the highest enrollment percent would pertain to the Sustainability First scenario and the lowest to the Security First scenario. But the evolution is labeled as interesting since **the enrollment for tertiary education is the only indicator displaying a disparity across the four scenarios** and, in the same time, it has a particular significance given that, by 2030, the needs of SRI for fresh blood will increase, and as mentioned before, the service will be also calling for highly-qualified personnel.

Nevertheless, even though the enrollment is not connected to the evolution of the GDP per capita (another indicator used for the second part of the research) in the IF approach, despite some evidence on their linkage[12], the tertiary education's impact upon the economic growth is taken into account. As such, for example, an IF variable called knowledge society index is based on R&D spending as a portion of GDP and on the tertiary graduation rate as a percentage of population[13]. Just as a short note, the knowledge society index for Romania is registering a slight increase over the forecasted period, but it has to cope with a decreasing population and low R&D spending.

As for the second dimension of the exercise, while acknowledging the inherent difficulties in assessing the quality of the recruitment pool we have combined the IF simulations with some of the findings of the 2008-2012 GCR editions.

First of all, **Romania's ability to retain and attract talented people is perceived as low** in different polls across the 2008-2012 GCR editions (see figure no. 1, where the lowest level of the ability would be 1 and the highest 7). The perspectives for the talented people seemed to improve after Romania joined the EU (2007), with a peak registered during 2009, but afterward they turned to a decrease, which, in our view will be even sharper once all the EU states will give up the labor restrictions for Romania and Bulgaria.

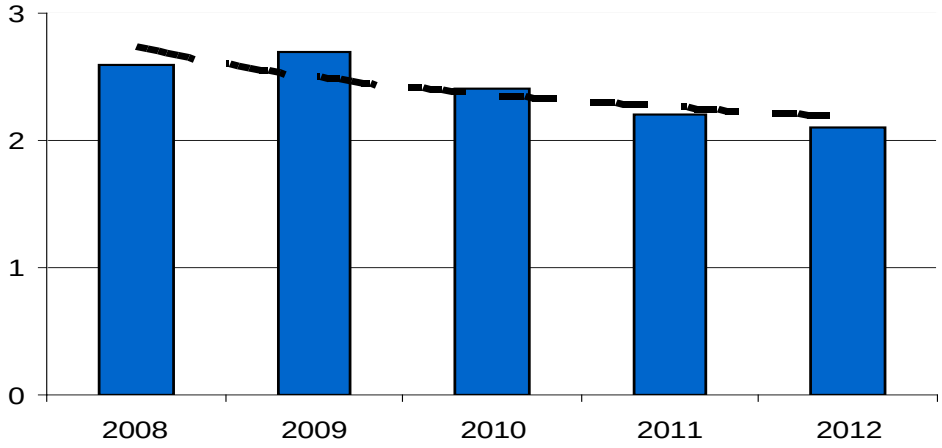


Figure no. 1: *The evolution of Romania's ability to retain talented people (2008-2012)*

Secondly, the above-mentioned negative perception is **stressed by a pessimistic perspective on the wages and pensions systems**. In order to have a more realistic view on the increase of the individual income, we chose the IF simulations for the GDP per capita at purchasing power parity/GDPPCP (see graph 5). While the GDP per capita is calculating by means of dividing "*the sum of value added across sectors, which would also equal the sum of production for final demand across sectors*", by the population number, the IF uses a purchasing power parity conversion value over time to obtain the GDPPCP[14].

Even though the GDPPCP is displaying in the IF simulations a slight increase by the 2030 frame (around 5%), we have to pay attention to the instability of the global financial system and its potential for a negative correction of the forecasted increase. Moreover, the sophistication of the threats the SRI has to deal with is increasing altogether with the amount of risks arising from Romania's position at NATO and EU borders or its involvement in strategic projects such as missile defense.

Since we are talking about perceptions and motivating the human resources, another important issue will be raised by a **certain shift in values** which might impact job-seekers preferences. The IF simulations based on the World Values Surveys[15]

(WVS) are showing for Romania a transition from traditional values toward secular-rational values, as well as from survival toward self-expression values. In the WVS language the secular-rational values are opposite to the traditional ones emphasizing the importance of religion, parent-child ties or the deference to authority, while the self-expression values include social toleration, life satisfaction or public expression. The cross-cultural variation is also connected to the transition from an industrial society to a post-industrial one, oriented toward well-being, self-expression and quality of life[16].

Last but not least, **the dynamics of the Romanian labor market**[17], as analyzed within the 2008-2012 GCR editions, cannot be perceived as following a positive trend, even though their evolution is steady around level 4, out of 7 levels (see figure no. 2), since Romania is constantly placed in the second half of the overall number of analyzed countries (for example, in the 2012-2013 GCR, Romania took the place 104 out of 144 countries).

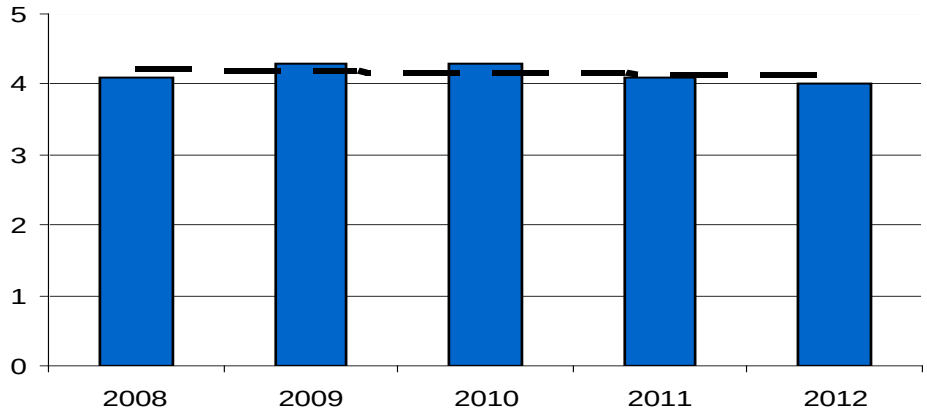


Figure no. 2: *The perceptions on labor market efficiency evolution (2008-2012)*

Beyond the current weaknesses of the inner labor market, the SRI will face a **double folded competition in the recruitment process**. On the one hand, the internal private sector could be a serious competitor (actually it is right now for some fields of activity) and on the other hand the further openness of the EU labor market will have a significant impact on the quality of the recruitment pool.

The four above-mentioned drivers of the qualitative approach could be also seen as facilitators for a currently increasing phenomenon - the **brain drain**. For example, according to some data, the number of researchers working inside Romania dropped to less than 50% of its 1993 value[18].

Findings and Way Ahead: New Strategies for a Potentially Reconfigured Labor Market

While it is less likely that the above-mentioned trends will suffer major alterations, given their similar evolutions across all the scenarios, **the recruitment pool for the SRI will suffer a medium decrease in dimensions, but an important decrease in quality**. These developments could be augmented by the restrictive selection criteria - e.g. the candidates have to possess Romanian citizenship – which will limit the flexibility in human resources policies.

However, some **disparities across the four scenarios** made us reflect a little bit on their likelihood, especially with a view to the Security First and Sustainability First scenarios, since there are significant differences between them. Even though a Security First scenario has a low probability since Romania will follow-up to 2030 and beyond – its Euro-Atlantic objectives as a NATO and EU member, a few foresight exercises emphasized some of the worrisome perspectives for the two organizations in 2030 or 2035.

For example, one of the scenarios highlighted by NATO's Multiple Futures Project is an "Old boys' lounge" Alliance, defined by a combination of total absence of US dedication to NATO, fragmented or cohesive Europe and common or diverse threat perceptions. Such a scenario will definitely have some negative impact especially on the South-Eastern European NATO countries, including Romania[19]. In the meantime, a "Nolens volens" scenario where the EU 2035 "*has no intention or strategy to carry out as a global actor*" and its "*action is limited because political, social and economic fragility of the Union and its Member States has slowed down capability development and considerably reduced the extent of usable force*" could push for a more security oriented approach across the European continent in the event of a major crisis[20].

In order to contain the gap which might be determined by the change especially in the quality of the recruitment pool, the SRI will have to build a **flexible long-term human resources strategy** comprising, among others, the following dimensions:

- a complex recruitment system, including for example some unconventional approaches for an intelligence service, such as the head hunting for particular positions (including middle to high level management positions, where possible);
- the adjustment of in-house training programs (extended use of e-learning) and the build-up of a continuous training system (including on the job training), supplemented by mentorship and coaching;
- a network of partnerships with academia and other institutions in order to be able to access a wide range of training programs at lower costs, while outsourcing intelligence knowledge and supporting the endeavors meant to enhance the outreach toward the civil society.

Even though some of the steps are already emerging (the SRI is in the process of creating links with the academia[21], one example being the development of a Master programme together with the Faculty of Sociology from the University of Bucharest), the SRI strategy will have to take into account an **ongoing paradigm shift in the intelligence-security continuum** based on significant transitions, such as the ones from linear risks to nonlinear risks, from state security to human security, from intelligence agencies to intelligence communities (including developments such as crowdsourcing intelligence), from information to knowledge, from need to know to need to share and even responsibility to provide and so on[22].

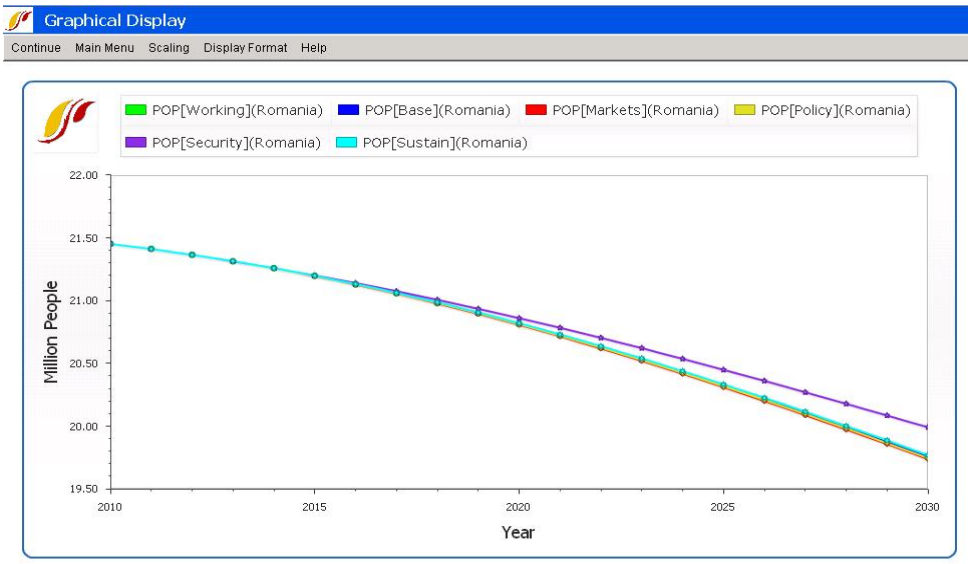
Nevertheless, the intelligence services are, by excellence, bureaucratic organizations. Therefore, an extensive change in order to meet the challenges related to the recruitment pool for the SRI will take some time. We might also be facing different delays given the sudden shifts in Romania's overall or security policies and priorities.

As such, although it may be seen as an early moment, we think we need to spend at least a little time to reflect on the future Romania might face in around 20 years and last, but not least, on the challenges to an optimal functioning of the SRI by 2030.

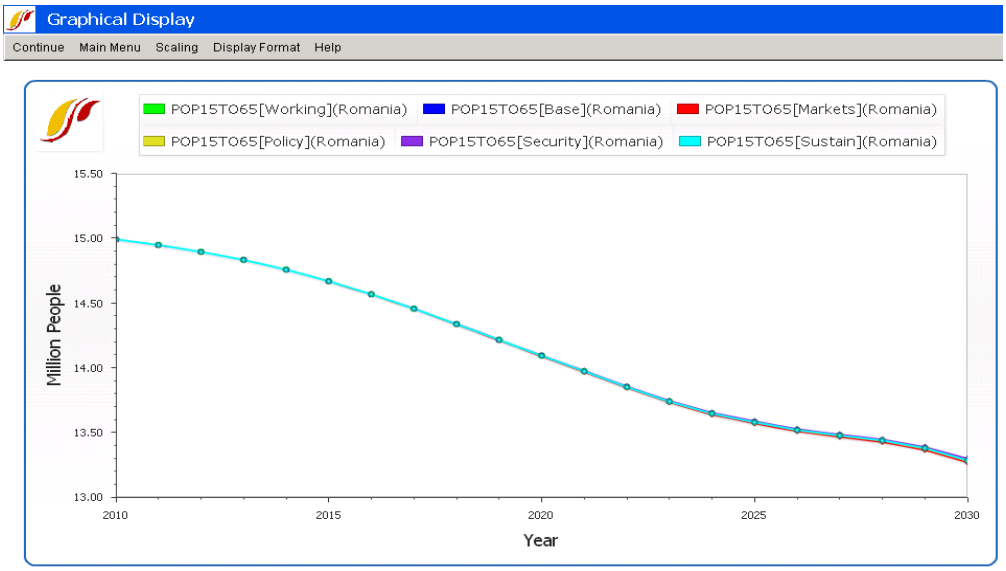
Annex

International Futures Simulations for ROMANIA (2012-2030)

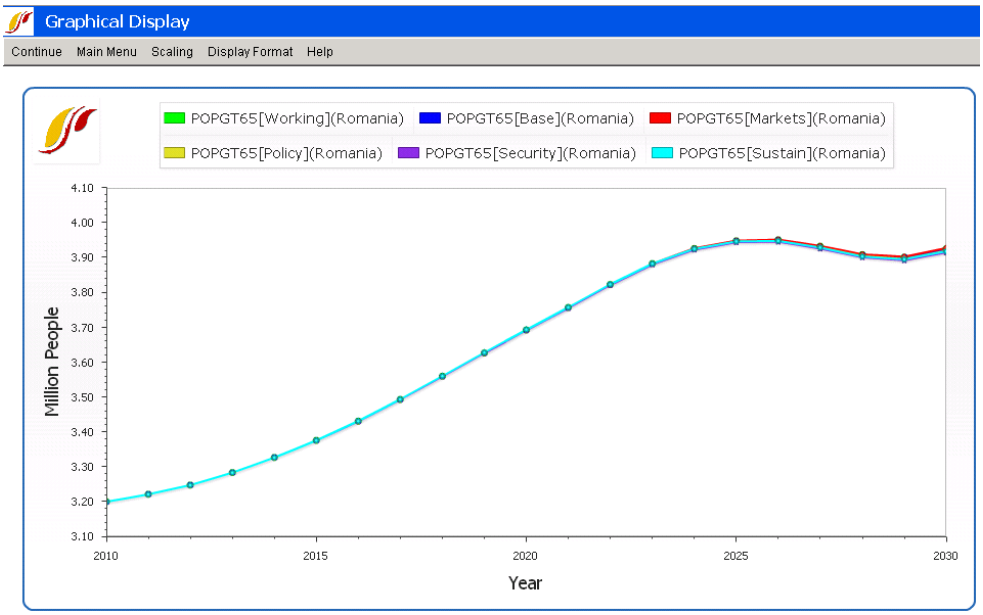
Graph 1 – *Population, overall*



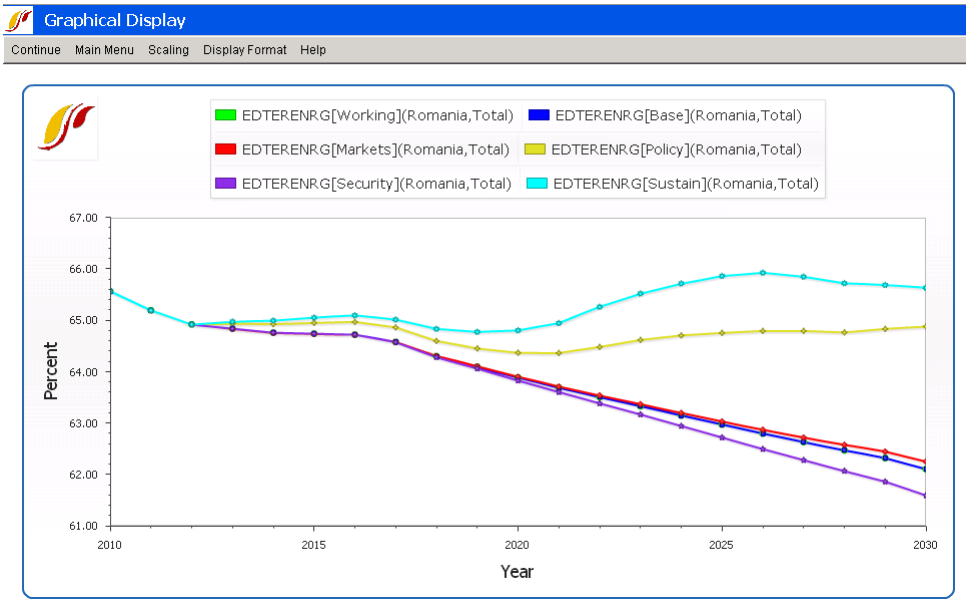
Graph 2 – *Population, aged 15 to 65*



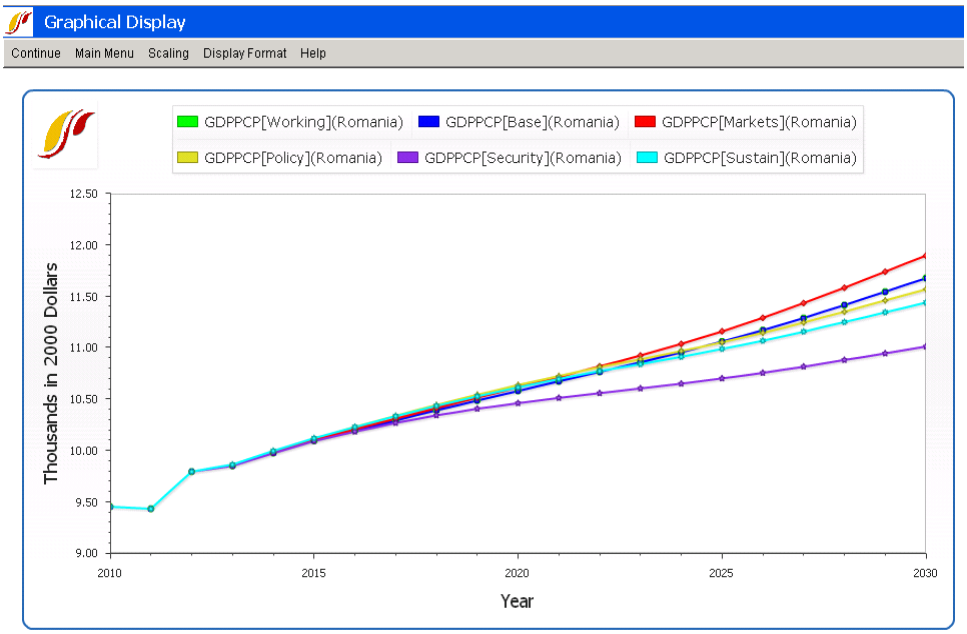
Graph 3 – *Population, aged more than 65 years*



Graph 4 – *Education, tertiary, gross enrolment rate*



Graph 5 – *GDP per capita at PPP in 2000$ (converting 2005$ from ICP[23] 2007 update)*



References

[1] Philip Tetlock and Michael Horowitz, "Trending Upward. How the intelligence community can better see into the future", *Foreign Policy*, September 2012, available at http://www.foreignpolicy.com/articles/2012/09/06/trending_upward.

[2] For details regarding the current strategic planning process of the SRI, see Nicolae Iancu and Gabriela Tranciuc, "Planning and Strategy in Reforming Romania's SRI", *International Journal of Intelligence and CounterIntelligence*, Volume 25, Issue 1, 2012, pp. 111-129.

[3] For example *Global Trends 2030: Alternative Worlds*, published by US National Intelligence Council or *Multiple Futures Project. Navigating toward 2030*, drafted by NATO's Allied Command Transformation.

[4] The main difference between the four generations is mainly related to the hardware used and the software run for modeling – from FORTRAN and mainframe computers toward functionality over Internet (including a kind of open source simulations) and current powerful personal or industrial computers.

[5] Barry B. Hughes, "Forecasting long-term global change: Introduction to international futures (IFs)", 2009, p.1, available at http://www.ifs.du.edu.

[6] Roy Pearson, "Using the International Futures Global Modeling System (IFs) for Alternative Scenarios by the Numbers", *Foresight: The International Journal of Applied Forecasting*, Summer 2011, pp. 6-7, available at http://www.forecasters.org/foresight.
[7] *Ibid.*, p.5.
[8] Klaus Schwab (ed.), *The Global Competitiveness Report 2012-2013* (Geneva: World Economic Forum, 2012), p. xiii, available at http://www.weforum/gcr.
[9] *Ibid.*, pp. 3-10.
[10] Barry B. Hughes and Anwar Hossain, *Long-Term Socio-Economic Modeling with Universal, Globally-Integrated Social Accounting Matrices (SAMs) in a General Equilibrium Model Structure*, University of Denver, 2003, p.7, available at http://www.ifs.du.edu.
[11] *Ibid.*, p. 8.
[12] Barry B. Hughes, *Forecasting Productivity and Growth with International Futures (IFs). Part 2: Driving the Drivers and Indices*, University of Denver, May 2005, pp. 37-41, available at http://www.ifs.du.edu.
[13] *Ibid.*, pp. 41-42.
[14] Hughes and Hossain, *Long-Term Socio-Economic Modeling*, pp. 29-30.
[15] "*The World Values Surveys were designed to provide a comprehensive measurement of all major areas of human concern, from religion to politics to economic and social life and two dimensions dominate the picture: (1) Traditional/Secular-rational and (2) Survival/Self-expression values*" (http://www.wikipedia.org).
[16] See http://www.worldvaluessurvey.org/ and http://en.wikipedia.org/wiki/World_Values_Survey.
[17] For the GCR analysis of the labor market efficiency, there are used around 9 indicators – cooperation in labor-employer relations, flexibility of wage determination, rigidity of employment, hiring and firing practices, redundancy costs, pay and productivity, reliance on professional management, brain drain, and female participation in labor force.
[18] Dan Irimia,"Exodul creierelor: Vezi cati cercetatori pierde Romania in fiecare an si cand cercetarea va disparea definitiv", April 20, 2012, available at http://www.econtext.ro/dosar--2/analiza/exodul-creierelor-vezi-cati-cercetatori-pierde-romania-in-fiecare-an-si-cand-cercetarea-va-disparea-definitiv.html.
[19] Stephan De Spiegeleire and Rem Korteweg,"Future NATOs", *NATO Review*, Spring 2006, available at http://www.nato.int/docu/review/2006/issue2/english/military.html.
[20] Alexander Siedschlag, Andrea Jerković and Brooks Tigner, *Syllabus of scenarios for EU roles. Milestone 4 document* (Vienna: Center for European Security Studies, Sigmund Freud Private University Vienna, June 2012), pp. 25-26, available at http://www.focusproject.eu.

[21] For details, see Valentin Filip and Remus Ştefureac,"The Dilemmas of Linking Romanian Intelligence, Universities, and Think Tanks", *International Journal of Intelligence and CounterIntelligence*, Volume 24, Issue 4, 2011, pp. 711-732.

[22] For a detailed view on SRI's challenges from a management of change perspective, particularly in the field of intelligence analysis, see Ionel Niţu, "Chapter 5 – The need for an integrated strategy for intelligence analysis: three critical factors (3P Project)", in Ionel Niţu (ed.), *Intelligence Analyst Guide. A Digest for Junior Intelligence Analysis* (Bucharest: "Mihai Viteazul" National Intelligence Academy Publishing House, 2011), pp. 56-63, available at http://www.animv.ro/files/Ghidul-Analistului--EN-.pdf or Ionel Niţu, *Analiza de intelligence. O abordare din perspectiva teoriilor schimbării* (Bucharest: RAO Publishing, 2012).

[23] "*The International Comparison Program (ICP) is a worldwide statistical partnership to collect comparative price data and compile detailed expenditure values of countries' gross domestic products (GDP), and to estimate purchasing power parities (PPPs) of the world's economies. Using PPPs instead of market exchange rates to convert currencies makes it possible to compare the output of economies and the welfare of their inhabitants in real terms - that is, controlling for differences in price levels*".

National Intelligence Estimates: A Romanian Perspective

Cătălina COSTEA[*]
Adrian ENE[*]

"If NIEs could be confined to statements of indisputable fact the task would be safe and easy. Of course the result could not then be called an estimate. By definition, estimating is an excursion out beyond established fact into the unknown".

***Sherman Kent**, 1964.*

Abstract

This paper briefly presents the perspective of the SRI and also of the National Intelligence Community (NIC) on one of the most well-known type of estimative analytical product – the (National) Estimate on major risks and threats to national security.

In an effort to strengthen its strategic analysis capabilities and to diversify the types of strategic intelligence products disseminated to the policy-makers, SRI took as a model the American NIE and tried to adapt it to national and organizational particularities. This process resulted into the making of an annual estimate offering the Service's integrated vision of the most important threats to the national security and their risk level in the year to come. A specific methodology was established, scientific methods and techniques have been applied and its use was extended even to county level (were local customers were offered an estimate tailored to their own needs).

More similar to the American model, the National Intelligence Community annually drafts a national evaluation of the most relevant risks to Romania's security, based on contributions from its four members. This document (approved by the National Defense Supreme Council) represents the grounds for the elaboration of the National Plan of Informative Priorities – the most important framework for strategic planning of our agencies' activities.

A Little Bit of History

In 2007, the SRI issued the Strategic Vision 2007-2010, an agenda for ambitious reforms which established among its major priorities the development of the analytical area through: optimization of selection, training and promotion policies, managerial flexibility,

[*] Intelligence expert, Romania
[*] Intelligence expert, Romania

investment in people, and integrated IT new platforms. Thus, one of the priorities of the transformation process that the SRI has undergone for the past six years was and still is the development of analysis, as a whole, and strategic analysis in particular, considered to be major tools for increasing the quality of our service's analysis and prognosis capabilities.

In that respect, significant efforts have been made to deal with all the three Ps relevant for every reform in intelligence analysis (as mentioned by Ionel Niţu in "Intelligence Analyst Guide, A Digest for Junior Intelligence Analysts") – people, processes, and products. The first step was to create a specific unit within the Central Department of Analysis with the responsibility to produce strategic analytical products in a multidisciplinary and trans-sectorial approach, using all source intelligence and having a strong anticipative dimension (complex evaluations, prognoses, policy analyses).

This structure was populated with senior analysts with significant experience, good overall expertise and the necessary degree of versatility for dealing with disparate national security issues in an integrated manner. They were expected to be open-minded, creative and work great as a team. The main objective of their activity was to deliver strategic analytical products that integrated all the existing knowledge in SRI on a specific national security issue, by using collaborative resources and applying analytical methods and techniques.

In terms of products, there was felt the need to expand the range of strategic documents. Of course, the most accessible models were the Anglo-Saxons ones, taking into account the amount of literature on intelligence analysis coming from that area. American National Intelligence Estimates seemed like a good starting point. So, SRI "adopted" and adapted this analytical instrument, in order to annually offer the Romanian policymakers the Service's integrated vision on the most important threats to the national security and their level of risk in the year to come.

In the last quarter of 2007 there started the first process of drafting an Informative Estimate of the risks and threats to Romania's national security. The result was delivered to SRI's customers in January 2008. Ever since, at the beginning of every year, SRI disseminates its Estimate to the central policymakers, as a way to cast a glance into the future and warn about potential risky issues.

In early 2012, SRI realized that this kind of document might be useful for local customers as well, provided that it focuses on evolutions of local interest. Therefore, before March 2012, estimates of the potential risks with county relevance (derived from the Informative Estimate with national coverage) were delivered to prefects and presidents of the County Councils all over Romania. The feedback was rather good, the document being considered useful, as a starting point in the development of local policies.

The American Model

The US intelligence community provides National Intelligence Estimates, which are meant to represent "the collective best guess of the nation's intelligence community as to what is likely to happen, or not happen, in particular parts of the world"[1] – events that might concern the US' national security. A National Intelligence Estimate (NIE) represents the US intelligence community's most authoritative and coordinated written assessment of a specific national security issue. The US Department of Defense defines NIE as a "*strategic estimate of the capabilities, vulnerabilities and probable courses of action of foreign nations produced at the national level as a composite of the views of the intelligence community*". Also, according to the National Strategic Intelligence Act (1994), NIE "*means the product of the process of considering and weighing the possibilities, probabilities and facts disclosed by national security intelligence with regard to any situation, and of drawing conclusions from such possibilities, probabilities and facts*"[2].

NIEs usually provide information on the likely course of future events and highlight possible implications. Unlike "current" intelligence products, which describe the present, NIEs forecast future developments and underline their effects on the security of the USA. A wide range of issues is covered, from military to technological to economic to political trends. NIEs are addressed to the highest level of policymakers, including the President. Limited-distribution NIEs covering issues meant to inform other consumers than the regular ones are called SNIEs (the "S" standing for "Special").

The concept of an "estimative" intelligence report was established by the National Security Act of 1947, following the surprise invasion of South Korea by North Korean troops. Ever since,

hundreds of NIEs and SNIEs where drafted and sent to the consumers, thus influencing the decision making on sometimes vital issues to the US national security.

Throughout the years, the process of making NIEs has undergone a series of overhauls to increase inter-agency collaboration. NIEs were first produced by the Office of National Estimates. This office was superseded in 1973 by National Intelligence Officers. This group of experts became the National Intelligence Council (NIC) in 1979. In the early years, the NIC reported to the Director of Central Intelligence in his role as the head of the intelligence community; however, in 2005, the Director of National Intelligence (DNI) became the head of the intelligence community.

Nowadays, intelligence estimates are coordinated by the NIC – the intelligence community's center for middle-term and long-term strategic thinking – which reports directly to the DNI. It employs thirteen National Intelligence Officers – senior experts from agencies of the intelligence community and from outside the government – who, among their other responsibilities, conduct the NIE writing process. The NIC serves as a bridge between the intelligence and policy communities, as a source of substantive expertise on critical national security issues, and as a focal point for collaboration within the intelligence community.

The NIE writing process progresses as follows:

- A senior executive branch official, a committee chair of the House or Senate or a senior military official can request a NIE. An estimate can also be initiated independently by the NIC. The request is authorized by the DNI.
- The NIC discusses key issues that are to be addressed and the main questions to be covered in the estimate. These are included in a Terms of Reference paper, or TR, meant to be circulated throughout the intelligence community for comments. The object of this paper is to define the subject matter of the estimate, its scope and time frame, but also to focus the forthcoming NIE on the major points that are considered to be the main concern of the requester. Many times, TRs have to be taken back to the requester, in order to precisely establish whether his area of interest is thoroughly covered.
- A draft is produced and reviewed by the NIC before it is sent to the members of the intelligence community. Agency experts review

the draft and prepare comments. Intelligence is vetted to eliminate potentially questionable or unreliable sources by discussing it to intelligence collectors within every agency.

➢ Afterwards, agency representatives meet and discuss the report line by line at an inter-agency coordination session. The members of the intelligence community have the right to dissent to some aspects of a NIE and their vision can be included in a footnote. A final draft is distributed for final review to intelligence community experts. The NIC reviews the final draft and then forwards it to the National Intelligence Board (NIB)[3], which is composed by senior representatives of the intelligence community and is chaired by the DNI.

Once an NIE is approved by the NIB, it is delivered to the requester as well as the president, senior policymakers and relevant members of Congress.

SRI: the Informative Estimate of the Risks to the National Security

The first annual Informative Estimate ever drafted by SRI was delivered to the decision makers in January 2008. It was inspired from the American estimates, mostly in what its strategic vision and integrated form were concerned.

However, there are major differences between the two kinds of documents:

➢ Our Estimate offers just SRI's perspective, whilst the original NIEs represent assessments based on contributions from all the agencies that are members of the intelligence community.

➢ Being the product of just one agency, it cannot afford to have dissenting judgments. Whenever two departments' perspectives on an issue differ, further verifying and validation are compulsory in order to provide the one correct coordinated interpretation of the facts.

➢ Most of the times, the American NIEs are made up to answer specific requests of the policymakers. SRI's estimate represents our initiative, in an effort to offer our decision-makers the most authoritative, integrated vision of what might or might not happen in the year to come with consequences to the national security.

➢ American estimates assess just one issue at a time, whilst SRI's estimate covers all the main potential risks and evaluates the

probability of their occurrence and the intensity of their potential outcomes, thus drawing a holistic picture of the potential risks.

- The process of making NIEs involves outreaching procedures – the use of the so-called Princeton Panel, or Princeton Consultants, whose job is "to give an enlightened outside view of work of a tight little inner circle"[4] – while, at the moment, SRI only resorts to its inner auditing resources when finalizing estimates.
- Some key judgments of the American reports have sometimes been declassified and brought into public attention. This wasn't the case for SRI's Estimate, which still remains entirely classified, though there are voices within the Service claiming it might represent – in a synthesized form – an opportunity to show the complexity and depth of SRI's activity.

The production of SRI's annual Estimate usually involves a few months of intense work (the period may vary from 2 to 4-5 months, depending also on conjectural, sometimes organizational issues). Relatively similar to the original NIEs, the process starts with consultations among the senior analysts from the Strategic Analysis Unit of the central department of analysis, in order to establish their perspective on the key issues that are to be addressed and the main questions to be covered in the estimate.

After that, a formal request is sent to the other central departments of SRI to deliver contributions to the estimate, that are to include their authoritative perspective on potential risks to the national security for the next year in their specific field of expertise and competence. The request underlines the necessity that the contributors evaluate the current situation and build prognoses for the main threats to our national security taking into account present and future changes in the security environment. They are specifically asked not only to assess the level of the risks that were addresses in the past estimates, but also to establish whether new risks and threats should be added to the list (and assessed accordingly).

When all the contributions are available, there follows a period of intense work for the strategic analysts whose job is to formulate predictions about evolutions relevant for the national security, based on the received input and also on their expertise in the field. They use methods such as brainstorming, the devil's disciple, what if?,

the scenarios method etc. in order to define their perspective on the addressed matters. The result of these activities is a draft of the Informative Estimate, a working sheet that represents the basis for further analytical interpretation.

The main method further used is (a variant of) the Delphi method. This type of approach is preferred to the scenario method out of reasons to improve the precision and accuracy of the forecasts. Through the use of consecutive rounds of consultation, it is also very useful in terms of managing disagreement and reaching a certain degree of opinion "convergence"[5].

The investigation group is coordinated by 2-3 senior analysts from the Strategic Analysis Unit and the advisers of the SRI's leadership. They are entitled to elaborate the list of experts who are to be consulted, coming from SRI's central operational units and the central department of analysis. Based on the draft of the Informative Estimate, the experts express their opinion on the relevance of each threat for the national security and assess the level of risk, taking into consideration the probability of its occurrence and its potential impact. The processing of the answers consists in gathering data, arranging the obtained range, respectively choosing the central (median) and the most frequent value. The participants whose answers situate outside the intervals are asked to substantiate their opinions or to review them. Then, the experts are informed about the results of the previous rounds, being subsequently asked to formulate a new estimate. The investigation continues until the number of participants sharing the same opinion or similar opinions is considered big enough. At this moment, the results are centralized. The final draft of the annual Informative Estimate, representing the SRI's integrated vision on the full range of potential threats to the national security, is handed to SRI's leadership for approval and then delivered to the legal customers.

It is a fact that this entire process depends a lot on the quality of the horizontal cooperation among experts from all levels – the analyst from the central department of analysis, the operational/case analyst or the analyst from the territorial units.

NIC: the National Consolidated Evaluation on National Security Issues

The establishment, in 2005, of the NIC was a potential revolutionary decision for the intelligence sector in Romania. The performance goal of this structure was the creation of an analytical community within NIC, a real competence platform for the delivery of strategic intelligence to the decision-makers. The achievement of this objective involved hard efforts to try to change mind-sets and develop mechanisms to increase collaboration, best practices sharing and set uniform standards.

The delivery of strategic intelligence on specific national intelligence issues (similar to the American NIEs) is the NIC's core business. Therefore, it was only natural to think about producing a document that integrated the visions of the community members on all the relevant (national and international) security issues, in a holistic approach. Starting 2009, the NIC annually produces, through its analytical core – the Office of Integrated Intelligence (OII), a National Consolidated Evaluation on the major security issues in our country – risks, threats and vulnerabilities to the national security.

The document is based on the contributions from the community members, but it also takes into good consideration eventual specific requests formulated by the legal customers. The writing process involves sessions of consultations, as a way to provide the most accurate analysis, but also to manage disagreement.

Mutatis mutandis, inter-agencies consultations that stand at the basis of the elaboration of NIC's Consolidated Evaluations may be methodologically assimilated to Delphi sessions. Analysts from the Office of Integrated Intelligence produce a draft that is sent to the members of the community. Agency experts review the draft and prepare comments. Intelligence is vetted to eliminate potentially questionable or unreliable sources by discussing it to intelligence collectors within every agency. In the end, the OII coordinates experts' consultations, with the specific goal to reach agreement. The members of the intelligence community have the right to dissent to some aspects of an evaluation and their vision can be included in a footnote (similar to US NIEs).

Although not very common, dissenting views may occur and solving such "opinion issues" is a real challenge for those responsible for the making of the National Consolidated Evaluation. The differences may range from slight nuances in formulating reasons and conclusions up to "arguments" on the opportunity to include a certain risk in the short list of those with enough relevance. The causes of these different views are multiple, but most commonly they have something to do with each agency's area of competence and expertise, and more precisely with the fact that each service tends to consider that its job is at least just as important as anyone else's, if not the most important. That is why consultations under the coordination of the Office of Integrated Intelligence are a must, to ensure that the big picture presents the actual reality and not the reality seen through the "eyes" of one agency or another.

The final form, after being approved by the National Defense Supreme Council, represents the basis for establishing the National Plan of Informative Priorities, which is the framework for the strategic planning of the NIC members' activities.

Way Ahead

As compared to our fellow colleagues' experience, we are only at the beginning of the development process of our NIEs. There are some main directions of action that should be addressed or at least considered in our efforts to optimize both de procedures and the product itself.

First, at the moment, the methodology used both in elaborating the SRI's estimate and the NIC's consolidated evaluation doesn't involve the consultation of experts outside the intelligence community. As a matter of fact, the practice of using outside contractors in the field of analysis and forecast is still at its very beginning in many Romanian intelligence structures, though there is great need for specialized expertise especially in what strategic analysis is concerned.

In his volume "The Future of Intelligence Analysis", William Lahneman prepared some recommendations for the US Intelligence Community with regard to the use of outreach programs as a way to improve the analytical expertise. "Expand and standardize analysts' abilities to consult and otherwise interface with nongovernment experts – including non-US nationals – by issuing appropriate IC-wide

doctrine. This doctrine must be biased toward enabling collaboration while preserving standards for protecting secrets, sources, and methods"[6]. This should be a perspective for the leadership of every intelligence agency and community to have in mind when addressing ways of improving their analytical performance.

In a similar way, Treverton states that analysts should become a dynamic for changing, working successively in other security agencies, employing personnel from outside and organizing brainstorming with personnel as routine actions, not as an exception. "They should spend time outside not in their offices, sharing assessments with other experts and verifying their agendas with decision makers"[7].

The majority of those involved in analytical activities in our intelligence community acknowledges the fact that increasing analysts' contact with the world beyond will allow them to tap the knowledge of world-class experts, which is more and more important when analyzing threats and other issues with non-military dimensions.

In the Foreword to Ionel Niţu's "Intelligence Analyst Guide, A Digest for Junior Intelligence Analysts", Florian Coldea, deputy head of SRI, explains that progress can only be achieved by "the standardization of analysis, the augmentation of the available information integration capability and the increase of the multi-source analysis products, the enlargement of the open sources capabilities, the improvement of the dissemination process and of the relations with customers, the co-operation with academia and other intelligence partners".

The dialogue with experts from academia or the civil society – be it punctual (about specific issues, at specific times) or quasi-permanent (through well-established mechanisms that facilitate rapid transfer of expertise) – represents a great knowledge resource which could and should be used for the writing of estimative products. That is why the main challenge for SRI is to introduce the outreaching practice into its standard procedures. Bringing in expertise from the academic and research institutes should not be a sequential approach, but a permanent endeavor.

In such a collaborative context, intelligence analysts, experts from the academia, and researchers may form working groups with variable geometry to discuss complex phenomena that usually

are referred to in SRI's or NIC's national or consolidated estimates. In order to maximize the benefits of such approaches, the dialogue should go beyond formal/formalized institutional cooperation towards a flexible, informal networking system, with experts from the intelligence world, other state institutions, universities, NGO's communicating outside the institutional boundaries.

However, such developments involve assuming the costs: financial resources should be allocated for this specific purpose (the expertise doesn't come for free), security policies should be adapted to the new reality (easy procedures for outsiders to get access to classified information). It is not about crossing the existing orders and regulations, but amending them to new realities. It is above all about building trust between the involved parties, an essential element that represent the sine qua non condition for the efficiency of the networking process.

It goes without saying that the introduction of this kind of practices in our daily activity doesn't exclude the use and development of our own training and research programs, which should remain a constant effort.

Second, we should all be more concerned about the use of new scientific methods in our prospective analytical efforts. Estimating the future is, as everybody knows, a very challenging activity. Maybe more than any other type of analytical approach, the analytical activity which represents the basis for the making of a national estimate faces the greatest temptation in this field – the elaboration of speculative explanations by 'breaking' the applicability of the used method and sliding towards intuitive, unsubstantiated assessments. Therefore, the need for the use of these methodologies in strict conformity to their scientific definition is ever bigger. The peril of superficially applying the analytical methodology is that it might lead to negligent conclusions which could be contradicted by the reality. This is something that no intelligence service (or community) can or should afford.

Third, we should include in the process of making estimates, as a compulsory step, the post-mortem analysis, which is the ex post facto examination of the estimates with an idea of identifying the most significant gaps in our knowledge, but also in our judgments. It takes courage to do so, the courage to eventually discover that you were wrong, but it also represents a very effective lessons learned mechanism.

Last, but not least, we should at least consider the possibility to declassify parts of our national estimates/evaluations, as a way to increase public awareness on the range of activities the intelligence services perform, but also to consolidate the security culture and the people's openness towards supporting our operations. Maybe not right now, because our society doesn't seem to be ready for this kind of approach, but in a few years' time, it might seem like a good idea.

References

[1] Abram N. Shulsky and Gary J. Schmitt, *Războiul tăcut. Privire asupra lumii informaţiilor*, 3rd edition (Iaşi: Polirom, 2008), p.75.
[2] *National Strategic Intelligence Act, Act 94-39, 02 December 1994.*
[3] *Established by the Intelligence Community Directive No.202/2007.*
[4] Sherman Kent, *Collected Essays, vol. II, The Making of a NIE,* available at http://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/sherman-kent-and-the-board-of-national-estimates-collected-essays/making.html
[5] Kesten C. Green, J. Scott Armstrong, and Andreas Monash Graefe, *Methods to Elicit Forecasts from Groups: Delphi and Prediction Markets Compared* (MPRA Paper No. 4999, November 2007), available at http://mpra.ub.uni-muenchen.de/4999/.
[6] William J. Lahneman, "The Future of Intelligence Analysis-Final Report", vol. I (Center for International and Security Studies at Maryland, 2006).
[7] Gregory F. Treverton, *Reshaping National Intelligence for an Age of Information* (Cambridge: Cambridge University Press, 2003), p. 246.

Mining Data for Intelligence
Data Warehousing and Data Mining: Analytical Tools for Business and Government Intelligence.

Davide BARBIERI*

Abstract

Business Intelligence (BI) is a broad term describing collection, processing, analysis and dissemination of actionable information for strategic decision support. Data Mining (DM) is a set of powerful and advanced analytical tools, providing state-of-the-art capabilities for "big data" analysis and exploitation. In particular, within the domain of BI, DM is widely used in order to automatically discover hidden patterns (in market and business-related data) which may give any corporation a considerable competitive advantage. BI can improve the way an organization does its business, especially offering its decision makers the proper information to take strategic decisions wisely. This is also true for government intelligence agencies, since analytical tools exploiting DM capabilities can be used in security-related fields like fraud detection and terrorist attacks prevention. In this paper we shall examine basic BI and DM techniques and methods, like data warehousing, multidimensional analysis, link or association analysis, classification, clustering and text mining for corporate and government intelligence.

Introduction

Intelligence can be defined as the collection, processing, analysis and dissemination of actionable, strategic information. This process is usually described as a cycle by some intelligence agencies[1] and it is initiated by a preliminary phase, called *Planning and directions*. The last step of the cycle should give the proper feedback to the first one to begin a new cycle (as in figure 1).

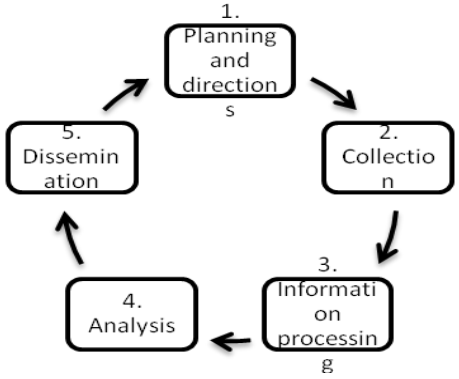


Fig. 1: *The intelligence cycle*

* PhD, University of Ferrara

Actually, the term intelligence may describe either the whole process or just the produced information.

Within the domain of intelligence, Business Intelligence (BI) can be defined as information gathering and analysis applied to corporate data, in order to provide decision makers with actionable information for strategic decision making. This process is meant to give any organization a significant competitive advantage. Usually, it is considered more as a linear process, rather than a cycle, comprising several phases:

- Data acquisition.
- Information processing.
- Analysis.
- Presentation.

As we can see, the classic intelligence life cycle and the BI process are actually overlapping, at least partially.

Data may come in different formats and from multiple sources, which usually include corporate databases, spreadsheets and the Internet (emails, news sites etc.).

Data which have been saved inside a consistent database are defined as *structured*. The basic data structure usually takes the form of a table, like in relational databases (Oracle RDBMS and Microsoft SQL Server are two popular examples). All data must have a defined data type, like text, number, currency, date etc. Relational databases implement a set of formal rules (the so-called *normal forms*) which provide an acceptable degree of data consistency. Structured data are properly called *information* and can be analyzed directly. This is not necessarily the case with unstructured data, which can be inconsistent or ambiguous.

Unfortunately though, most of the data which an organization possesses or can acquire from public/open sources, like the Internet, are unstructured[2]. Therefore, after acquisition, data must be filtered (since we do not necessarily want to use them all) and stored inside a database, which will serve as a consistent data repository for the following phases of the BI process. Information processing is a rather vague set of terms which may actually mean different things, like filtering, extracting, applying formal rules, eliminating errors and ambiguities etc.

At this point, information can be analyzed by means of a query language, like SQL (*Structured Query Language*) in order to provide

the BI project stakeholders with some basic statistics, like means, standard deviations or ranges, giving a synthetic description of the domain of interest (like the market and the main competitors) in terms of trends, peaks, variability etc.

For more complex analysis, more sophisticated data structures like *data warehouses*, are required. The process can then go through all the sub-phases of the analysis step, like data mining, and then disseminate the results in the last phase, *presentation*. An example of a possible BI roadmap is given in figure 2.

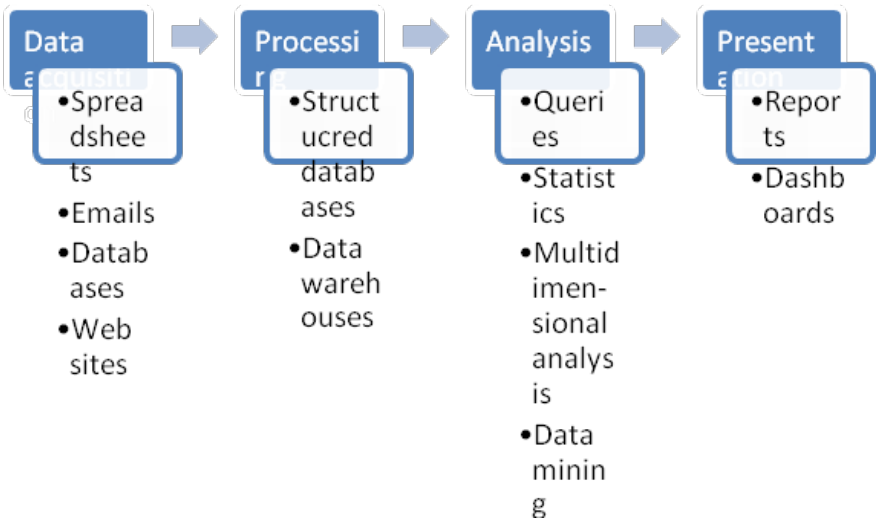


Fig. 2: *A BI roadmap*

Data Warehousing

A data warehouse is a multidimensional data repository, where stored variables can be analyzed along different dimensions[3]. Even though they are not necessarily part of a BI system, data warehouses have become almost a synonym for it, because of their many advantages. While a relational database contains flat tables, a data warehouse adds other dimensions to the basic two, in particular time and space. Contrary to operational databases, where data are dynamically stored, retrieved, modified or deleted, data warehouses offer a static picture of the data, in order to provide a single version of the facts.

To build a data warehouse with information coming from an operational database, we must first design a *star schema*, that is a data model where information is represented in terms of *measures* and *dimensions*. Measures are the way in which we quantify the data (e. g. Euros and quantity for sales) while dimensions are the variables along which we analyze them (e. g. month and shop or city).

In figure 3 we can see an example of a star schema for a retail company. At the centre of the schema, we have the *fact table*, the table containing the main facts, which in the case of a retail company are sales.

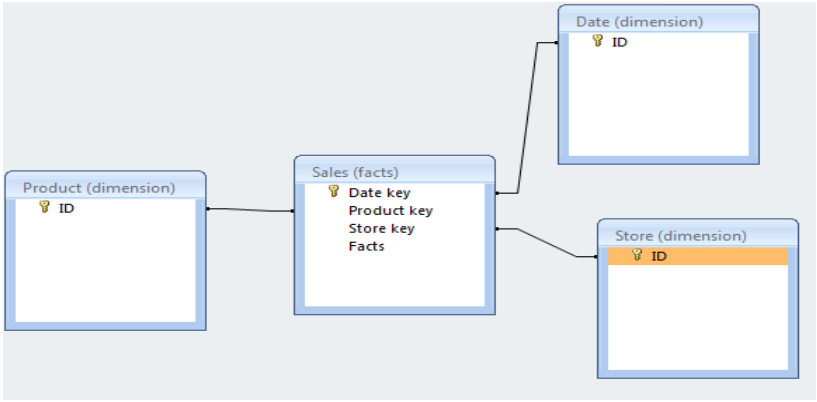


Fig. 3: *Star schema*

Once the schema of the data warehouse is ready, we must proceed to *Extract, Transform and Load* (ETL) the data from the data sources into the data warehouse. This can be the most demanding part of the project, since data may need lots of work before they are actually ready to be loaded into the multidimensional repository. The ETL process[4] can be summarized as such:

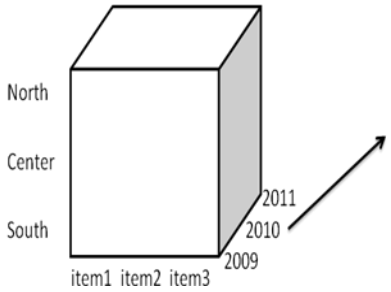
- Extraction of the data from the data sources.
- Transformation: eliminating redundancy, correcting misspellings, resolving conflicts, providing missing elements etc..
- Loading the data into the presentation area.

Extraction and transformation are performed inside the *data staging area*, which only skilled professionals are allowed to access. The *presentation area* instead is accessible also to the final users. These processes will lead to the creation of a *hypercube*, a multidimensional data structure. Now, information is ready to be analyzed along different dimensions.

Multidimensional Analysis

On-line Analytical Processing (OLAP) is a set of software technologies allowing multi-dimensional queries in data warehouses. The basic analyses which can be performed using OLAP are the following:

- Drill down, which means going into higher level of detail. For example, we may know the global sales in the last year in Europe, but we want to know the sales per month/week or per city store.
- Roll up, or consolidation, which is opposite to drill down. It allows evaluating facts at a lower level of detail, aggregating data per year or geographic area (region, country etc.).
- Slicing (see figure 4), which consists in extracting a portion (a "slice") of the data from a hypercube according to a given filter imposed on one of the dimensions of the data warehouse (e.g. only data regarding a certain area, time period etc.).



	Item1	item2	item3
North	20	35	90
Center	45	41	54
south	53	10	67

Fig. 4: *Slicing an OLAP cube*

- Dicing, which consists in imposing a filter on two or more dimensions, for example sales office, period of the year and clients' type of organization.

Results can be presented in a user-friendly format, eventually adopting traditional spreadsheet environments, like MS Excel Power Pivots. These tools allow charts to be shown beside the pivot table containing the data. The charts change accordingly to the performed function: they expand in case of drill-down or collapse in case of roll-up.

Data Mining

Data mining[5] is a set of powerful and advanced techniques used to extract meaningful, but often unpredicted, information from "big data"[6] repositories. Its aim is to find hidden patterns and models (associations, anomalies etc.), together with counter-intuitive information. Predictions can be used by big retailers, like Amazon[7],

to suggest future purchases, and by intelligence and police agencies, in order to optimize personnel deployment[8]. Data mining can be applied to databases or data warehouses, in order to discover knowledge without previously formulated hypotheses.

Some data mining techniques belong to a discipline called *machine learning*, a branch of artificial intelligence. Machine learning algorithms enable computers to "learn"[9] from empirical data, which can be provided by both sensors and historical archives, stored inside databases or data warehouses.

These techniques can be divided into two broad categories: unsupervised and supervised. Unsupervised algorithms do not need any input, other than the data themselves, to achieve results. Supervised algorithms instead need inputs (other than the data) to work properly. In the following paragraphs we shall briefly review some of the most important data mining techniques.

Clustering

Clustering is an example of unsupervised learning and can be applied to corporate databases in order to find groups of clients with similar purchase behaviors or other common characteristics, like cultural interests, income etc. Elements within a cluster are close (that is similar) to each other, while clusters are far from each other, according to the principle of strong cohesion and weak coupling.

For example, there may be a strong – but non-obvious – relationship between clients coming from different geographic areas, but having a similar income, and their purchase or eating habits. Customer cards may be used to archive information about purchase preferences and individual data, like profession and home address. Clustering will eventually provide meaningful correlations between these data, therefore offering strategic information to the marketing staff.

The union of all the clusters must contain all the elements, but no cluster can have any element in common, that is the intersection of the clusters must be empty. The two extreme cases of one single cluster, containing all the elements of the data set, or of one element per cluster are logically equivalent and it means that no effective clustering has been found inside the data set.

Clustering techniques can be employed by law enforcement agencies to analyze criminal careers[10] and profile offender descriptions, in order to reduce the variables involved in recognition and eventually identify the offenders who are involved in more than one crime[11].

Classification

Classification is a kind of statistical analysis which exploits historical data to predict future trends and behavior patterns, especially to give support to marketing and Customer Relationship Management (CRM). The basic idea is that the future is contained in the past.

This process is described as *supervised learning* and it is a form of induction, a way of reasoning which infers general rules from a set of individual observations. Usually, the larger the set, the more reliable[12] the rules. Still, even if an event was the rule in the past, it does not mean there will be no exceptions, or different trends, in the future. Therefore, induction is always statistical and rules are given with a degree of probability or *confidence*[13].

The available data set must contain complete and valid observations and all the records must have already been labeled, that is classified, by domain experts. This means that another field, the *class*, is added to the database table and correct values are inserted, dividing the data set into some sub-populations. For example, suppliers can be classified as reliable or non-reliable, in terms of delivery timeliness, raw material quality etc.

A subset of the available data (which could amount to 70% of the total number of records) is chosen as the *training set* and is given to the classification model as input. Once the model has been trained, a *test set*, consisting of the remaining 30% of the previously collected data, is given to the model. The class field though, is empty. The trained model, or *classifier*, must label the data, making predictions (see figure 5).

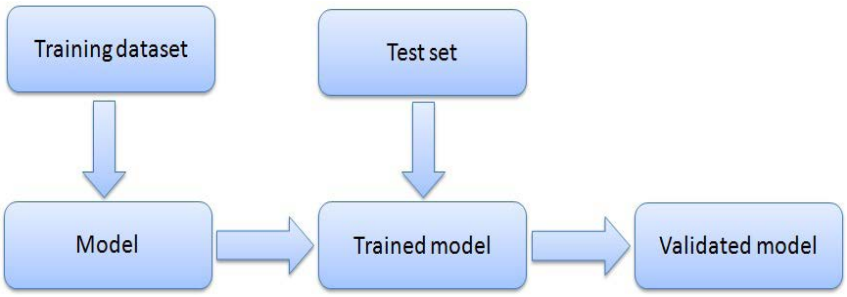


Fig. 5: *Classification*

Since the class of each record in the test set is known, the accuracy of the model can be evaluated as number of correct predictions on total number of records. If accuracy is satisfying (e.g. greater than 80% or 90%, according to a predefined threshold), then the model can be used to make predictions about new, unlabeled data.

Since tax auditing is a demanding task, classification could be used to predict the probability of being a fraudster. Auditing will then be enforced especially in the cases where probability is high. Reducing the rate of false positives (people who are believed to be fraudsters, but actually are not) will diminish the waste of government resources[14]. Different prediction techniques, like the *decision tree* classification algorithm, can be successfully adopted[15].

The case of VAT (Value Added Tax) is particularly interesting, since it can be widely evaded, under-declaring sales or over-declaring purchases. In the DIVA (Data mining IVA) project[16], around 34 millions of tax declarations where collected, containing data like city code, total sales, import, export etc. for each company claiming VAT refund. For a much smaller sample, also auditing results were available, including the amount of VAT fraud (that is, the difference between the claimed VAT refund and the actual due). Audited subjects were then labeled fraudsters (if VAT fraud > 0) or non-fraudsters (in the other case). Fraudsters were then awarded a score (a degree of interestingness) according to three criteria: profitability (a $ 100,000 fraudster is more worth to be audited than a $ 1,000 one), equity (to avoid that low-income individuals are never audited, since a $ 1,000 fraudster is more interesting if his/her business volume is $ 10,000 rather $ 100,000) and efficiency (an individual claiming a $ 1,000 refund but entitled to $ 800 is less interesting than an individual claiming $ 200 but entitled to none).

The main objective was to develop a rule-based[17] model which finds the individuals in the top class, minimizing the amount of false positives, taking into account both the probability and the severity of the fraud. The developed classifier, called *Sniper* (see figure 6), showed good confidence (>80%) and can therefore be used as a reliable tool in identifying tax avoidance. But one of the main outcomes of the study, validated on new real cases, is that it was able to identify fraudsters who would never be selected by domain experts, thus unveiling previously unknown fraudulent behaviors.

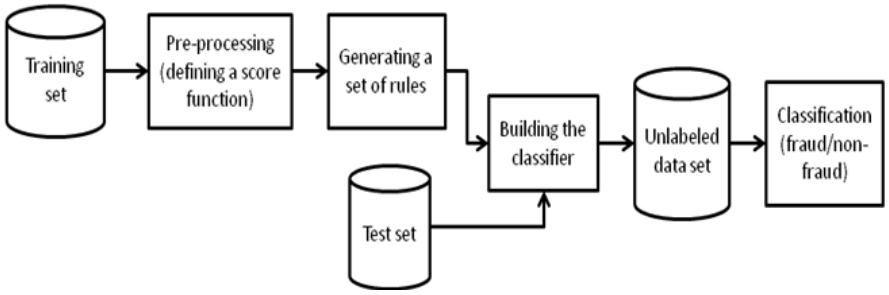


Fig. 6: *The Sniper model (source: adapted from Basta et al., 2009a[18])*

Link Analysis

Link analysis is mainly used to discover associations between purchased items. If the items are purchased within the same transaction (that is, one single visit to the shop) then it becomes a *basket analysis*. Focusing on consumers as groups of individuals with their own habits has led to one-to-one marketing, which has proved to be more effective than the traditional one. For example, if the management knows that adult male customers who bought a shirt may also be interested in buying a tie, then they may put them close together in the same aisle and properly advertise the interested audience.

Association rules usually take the following form: '76% of the customers who buy A then buy B'. Cross-selling techniques can be adopted by the retailer: there may be a discount on the second item (the "head" of the rule) whenever two or more of the first item (the "body") are bought. Rules can have body or head with more than one item, like in this example: *{tomatoes, chips}→{hamburger}*.

If the link analysis is conducted on transactions over a time range, then it becomes *sequential pattern discovery*. In national security-related intelligence, even though crossing a border with a single item may not arise suspicion, a sequence of related items passing custom over a week may eventually lead to the construction of weapons or explosive devices. Link analysis can unveil these patterns, which cannot be realistically spotted without data mining tools.

Deviation Detection

Outliers are values which are far from the mean or the median of a dataset. They are sometimes considered measurement errors (eventually, a human error) and therefore they may be discarded as if they were some kind of noise inside the data.

This is not always the case though. Sometimes, an outlier can be a correct measurement. In such cases, it is worth to investigate further, because the outlier can be an interesting value. For example, it can be a sign of poor/exceptional performance or of fraudulent behavior (since criminals do not conform to an established normal behavior, at least until we suppose honesty to be the norm).

Unsupervised deviation detection assumes that the majority of the data in an unlabeled dataset must be close to the expected value and then detects anomalies looking for items that are someway far from the rest of the dataset. Distance-based algorithms can be used, reducing the problem to a cluster analysis, which must label the data as *normal* or *abnormal*. A cluster having only few elements, compared to the rest, is supposed to contain outliers.

Supervised techniques instead require a set of labeled data to train a classification model. If it achieves a satisfactory degree of accuracy, then the classifier is applied to non-labeled data. If the training dataset has both normal and abnormal data, then supervised learning is used. If instead only normal data are present, then *semi-supervised* learning must be used to train the model. Accuracy must be evaluated against a test dataset, measuring the distance of an item from the normal data. If it is too high, then the item is labeled abnormal.

Compared to other clustering or classification cases, the specificity of anomaly detection is evident on the different dimensions of the two subsets, where the abnormal dataset has a much smaller item count compared to the normal dataset.

Deviation detection can be used to track money laundering. For example, in order to receive money, the member of a terrorist organization can export overvalued goods, which have been previously purchased at market price, to a foreign country, where they are imported at a much higher price by the members of the same, or of a supporting, organization. The member in the first country can use the difference between the total cost of the exported goods and the received money to finance criminal or terrorist activities. Also the opposite works: the exporter buys expensive goods at market price and sends them to a foreign country, where they are imported at a much lower price and resold at market price. Again, the difference can be used for criminal activities.

In general, an observed price deviation may be related to tax evasion, money laundering, or terrorist financing[19]. For this reason, the IRS (U.S. Internal Revenue Service) defines as suspicious those export prices that exceed the upper quartile export prices and those import prices that are less than the lower quartile import prices (see figure 7).

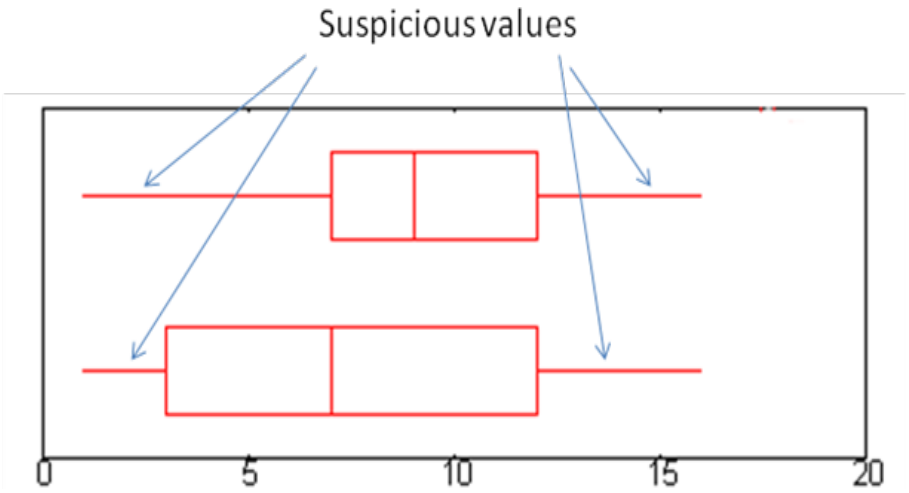


Fig. 7: *IRS price acceptance thresholds*

Text Mining

Text mining[20] consists in the application of data mining to unstructured data, specifically free text. In real life data are mainly unstructured, contained in paper documents, emails, blogs, forums, social networks etc. It is therefore necessary to apply typical classification or deviation detection algorithms to this kind of data formats.

Two of the main tasks of text mining are *information retrieval* and *information extraction*. The first task is concerned with finding information in text documents. Next, information extraction analyzes the retrieved documents, in order to find hidden, strategic information.

Text mining is complicated by the fact that natural languages may vary from English and French to Arabic and Chinese. Contrary to Arabic numbers, which have become the *de facto* standard to represent quantitative data, natural languages may take different,

exotic and vernacular forms, comprising lingos, slangs and jargons, which can be difficult to decode and require the dedicated support of domain experts. Therefore, text mining is a very inter-disciplinary job, involving many different skills, from statistics to linguistics.

Text classification aims at automatically assigning the text to a predefined class on the basis of linguistic features, like words' statistical frequency. Such a process has different useful applications, including email spam detection, web page content filtering and Open Source Intelligence. In particular it can be applied to news sites, blogs and forums in order to retrieve security-related information (on politics, religion etc.).

Since its inception, text mining has been traditionally applied to European languages. Still, studies regarding data mining techniques applied to other languages have already appeared. For example, an interesting paper by Al-Harbi et al. (2008)[21] describes automatic classification of Arabic texts. The purpose of this paper was to evaluate the accuracy of two popular classification algorithms, SVM (Support Vector Machine) and C5.0. Both performed well, especially in classifying Islamic topics, where accuracy was 86.4% and 92.1% respectively.

Due to the increased demand for transparency in financial statements, auditing has become a demanding and time-consuming task. Therefore, automated classification techniques have been applied to this issue[22]. In particular, text mining deviation detection has proved to be effective in identifying financial frauds. For the aim of optimization, auditing should be enforced in the direction of deviations from the norm.

Kamaruddin et al. (2007)[23] propose a conceptual framework (see figure 8) for the detection of extra-ordinary financial declarations. In this paper, text is tagged (each word is assigned a syntactic tag, like N for nouns, V for verbs etc.), parsed (to identify the sentence structure) and then represented in the form of a conceptual graph. A conceptual graph clustering algorithm assigns sentences to one of two non-overlapping groups: normal financial statements and abnormal financial statements (where auditing should be enforced).

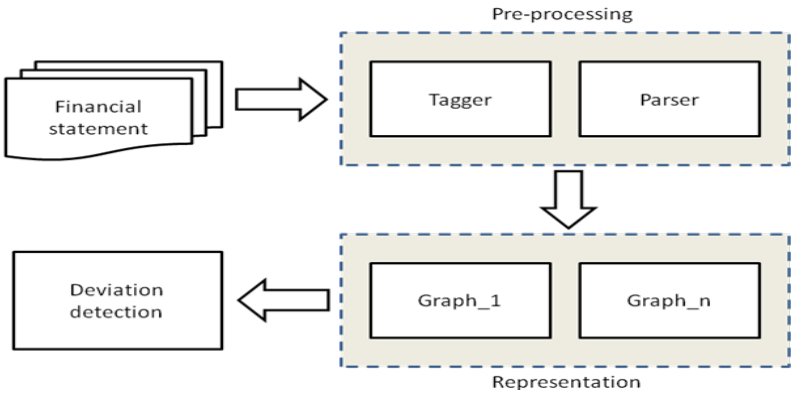


Fig. 8: *Text mining: deviation detection*
(Source: adapted from Kamaruddin et al., 2007)

Conclusions

Business Intelligence technologies, like data warehousing and data mining, can be successfully implemented in order to acquire information for either competitive advantage or security reasons. Efficiency in performing traditional law enforcement and government intelligence tasks, like data acquisition and analysis, auditing, crime prevention and detection etc. can be significantly increased.

This is especially true in presence of an outstanding amount of data, as it is the case today within most organizations, like multi-national corporations or government agencies. In the context of the information and knowledge society, where the Internet and many open sources have become widely available, managing the "information overload" is a top priority, to be tackled with state-of-the-art technologies.

References

[1] See, for example, the FBI intelligence cycle (http://www.fbi.gov/about-us/intelligence/intelligence-cycle, accessed 13/07/2012), the CIA cycle (https://www.cia.gov/kids-page/6-12th-grade/who-we-are-what-we-do/the-intelligence cycle.html, accessed 13/07/2012) and the Canadian Security Intelligence Service cycle (http://www.csis-scrs.gc.ca/bts/ccl-eng.asp, accessed 19/07/2012) on their respective web sites.

[2] This may be true also for databases: in fact, some can be used like basic spreadsheets, as it is possible with MS Access, for example.

[3] On this subject, see R. Kimball and M. Ross, *The Data Warehouse Toolkit,* 2nd edition (New York: Wiley, 2002).

[4] Kimball and Ross, *The Data Warehouse Toolkit*, p. 8.
[5] On this subject, see P. Cabena, P. Hadjinian, R. Stadler, J. Verhees and A. Zanasi, *Discovering Data Mining* (Upper Saddle River: Prentice Hall, 1998).
[6] Petabytes or more. On "big data" problems and opportunities, see K. Kukier, "Data, data everywhere", *The Economist*, 25th Feb. 2010, available at http://www.economist.com/node/15557443?story_id=15557443 (accessed 17/07/2012).
[7] Amazon and other on-line stores use data mining and predictive analytics, as any registered user knows. Suggestions come regularly into the users' mail box.
[8] C. McCue, "Data Mining and Predictive Analytics in Public Safety and Security", *IT Professional*, Vol. 8, No. 4, July-Aug. 2006, pp. 12-18.
[9] More precisely, *to infer* – that is to draw conclusions – by means of *inductive reasoning*.
[10] J. S. de Bruin, T. K. Cocx, W. A. Kosters, J. F. J. Laros and J. N. Kok, "Data Mining Approaches to Criminal Career Analysis", *Sixth International Conference on Data Mining 2006 - ICDM '06*, 18-22 Dec. 2006, pp.171-177.
[11] J. Mena, *Investigative Data Mining for Security and Criminal Detection*, (Butterworth-Heinemann , 2003), pp. 24-36.
[12] That is, statistically significant.
[13] The confidence of a rule A→B is the probability of finding A and B together inside a dataset, divided by the probability of finding A: P(A, B)/P(A). Here probability is defined as relative frequency.
[14] F. Bonchi, F. Giannotti, G. Mainetto and D. Pedreschi, "Using data mining techniques in fiscal fraud detection", *DaWak'99, First Int. Conf. on Data Warehousing and Knowledge Discovery*, 1999.
[15] Fan Yu, Zheng Qin and Xiao-Ling Jia, "Data mining application issues in fraudulent tax declaration detection", *International Conference on Machine Learning and Cybernetics*, Nov. 2003, pp. 2202-2206.
[16] S. Basta, F. Fassetti, M. Guarascio, G. Manco, F. Giannotti, D. Pedreschi, L. Spinsanti, G. Papi and S. Pisani, "High Quality True-Positive Prediction for Fiscal Fraud Detection", *IEEE International Conference on Data Mining Workshops - ICDMW '09*, 6 Dec. 2009, pp.7-12; and S. Basta, F. Giannotti, G. Manco, D. Pedreschi and L. Spinsanti, "Sniper: A Data Mining Methodology for Fiscal Fraud Detection", *ERCIM News*, No. 78, July 2009, pp. 27-28. IVA stands for *Imposta sul Valore Aggiunto* (the equivalent of VAT in Italian).
[17] That is, a model which makes predictions according to rules. Rules usually takes the form *if A then B*, e. g. *if (sales < 1,000 and empoyees > 30) then fraudster*.
[18] Adapted from Basta et al., 2009a
[19] Zdanowicz, 2004.
[20] On this subject, see Zanasi (2007).
[21] Al-Harbi et al. (2008)
[22] See, for example, Kirkos et al.,2007.
[23] S. S. Kamaruddin, A. Razak Hamdan and A. Abu Bakar, "Text Mining for Deviation Detection in Financial Statement", *Proceedings of the International Conference on Electrical Engineering and Informatics*, Indonesia, June 17-19, 2007.

Theoretical vs. Empirical Elements of Sociology as Science: What Intelligence Science Can Learn From Sociology's Progress?

Valentina MARINESCU*

Abstract

Science is a multi-layered complex system involving a community of scientists engaged in research using scientific methods in order to produce new knowledge. Thus, the notion of science may refer to a social institution, the researchers, the research process, the method of inquiry, and scientific knowledge. The concept of progress can be defined relative to each of these aspects of science. Hence, different types of progress can be distinguished relative to science: economical, professional, educational, methodical *and* cognitive. *These types of progress have to be conceptually distinguished from advances in other human activities, even though it may turn out that scientific progress has at least some factual connections with* technological *progress and* social *progress.*

The present article tried to approach the issue of scientific status of a science from a sociological point of view and to offer an answer at the following research questions:

- *"How people assessed the debate between theoretical aspects and the empirical ones in the case of sociology as science?" and*
- *"What intelligence science can learn from people's assessments of sociology in order to progress itself as science?"*

The research project uses the triangulation of methods, and favors both qualitative and quantitative approaches to the issue. The quantitative analysis is made on the set of data from 2009- the survey made by the Romanian Agency for Quality Assurance in Higher Education. The second analysis is a qualitative one, based on a set of 50 interviews with students from the University of Bucharest.

Introduction

Scholarly study and practitioner observation in the realm of intelligence organizations and analysts point to a failure to know or use highly applicable theoretical insights, a counterintuitively dangerous "paradox of expertise", undisciplined use of data, and an overreliance on situational logic and (often error prone) inductive methods[1]. Moreover, key instances of intelligence shortcomings have been attributed to an unhealthy emphasis on substantive expertise[2].

Some researchers have pointed to the higher education system to explain in part the skill composition and shortcomings in the

* Associate Professor, Faculty of Sociology and Social Works, University of Bucharest.

intelligence community[3]. Consistent with that view, Michael Collier (2005) wrote that graduate intelligence and security curricula provide a limited theoretical and methodological preparation, with only the more progressive programs giving students the advanced social science backgrounds needed for advanced analytic positions in the intelligence community. This sort of preparation seems wholly consistent with the mission of higher education institutions, particularly for graduate programs meant to prepare knowledge workers who will, as careers, probe and parse complex social systems and settings. Christopher A. Corpora[4] indicated that the work of intelligence analysts and social scientists, despite differing objectives and data, can be similar in process and methodology. Speaking of the fundamental objectives of educational (and training) programs in this area, Stephen Marrin observed: "In terms of intelligence analysis, the term 'training' is usually associated with internal government programs intended to provide specific instruction for the implementation of job-related tasks, while the term 'education' is normally associated with academic courses or programs geared to provided more conceptual and theoretical frameworks having less immediate effect on performance, but laying the foundation for improved performance over the longer term"[5].

The present article tried to approach the issue of scientific status of a science from a sociological point of view and to offer an answer at the following research questions:

- "How people assessed the debate between theoretical aspects and the empirical ones in the case of a science?" and
- "What intelligence science can learn from people's assessments of a science in order to progress itself as a valid domain of knowledge?"

Theoretical Framework

Science is a multi-layered complex system involving a community of scientists engaged in research using scientific methods in order to produce new knowledge. Thus, the notion of science may refer to a social institution, the researchers, the research process, the method of inquiry, and scientific knowledge. The concept of progress can be defined relative to each of these aspects of science. Hence, different types of progress can be distinguished relative to science: *economical*, *professional*, *educational*, *methodical* and *cognitive*.

These types of progress have to be conceptually distinguished from advances in other human activities, even though it may turn out that scientific progress has at least some factual connections with *technological* progress and *social* progress. Th. Kuhn's[6] theory understands science as a problem-solving activity. Paradigm-based normal science is cumulative in terms of the problems solved, and even paradigm-changes or revolutions are progressive in the sense that "a relatively large part" of the problem-solving capacity of the old theory is preserved in the new paradigm. For L. Laudan[7] the *problem-solving effectiveness* of a theory is defined by the number and importance of solved empirical problems minus the number and importance of the anomalies and conceptual problems that the theory generates. Here the concept of anomaly refers to a problem that a theory fails to solve, but is solved by some of its rivals.

Academic practices are multifaceted. Interesting instances will certainly be practices such as writing, reading, teaching, supervising, publishing, presenting, conferencing, discussing, advising, consulting, organizing meetings or hiring practices. While here is not the place to elaborate on the different versions of theories of practice, it is worth noting that a wide array of sites and objects are assembled in these practices. For instance, writing will involve the usage of a pen, paper, a computer screen, a keyboard, citing from books, going to the library, drawing empirical material together, discussing with your colleagues, re-writing, deleting, copy-editing, compiling literature lists and so on. Obviously, it will make sense to distinguish between different situations in which writing in a specific science takes place. Writing an article for a regular scientific seminar will not be the same as writing an article for an international conference; writing a grant proposal for the *European Science Foundation* will differ from writing a PhD in a specific science. Saying that it is useful to differentiate between situations does not mean that it is necessary to document all of the byzantine complexity we will face. It will often be more useful to provide overviews.

A promising starting point for categorizing situations in which scientific practices thrive is Pels'[8] triangle of politics/the state, culture/science and economy/the market. Pels argues that situations in which scientists find themselves can be interpreted as being influenced to various degrees by economic, political and cultural rationalities. For instance, writing a policy brief requires considering political and market rationalities to a much higher degree, than writing a theoretical article, which will be primarily influenced by cultural rationalities. Practices

contain normativity. Different collectives and disciplines will have different understandings of what constitutes a good piece of writing, what can be written and how. For instance a lengthy description of the preparation of a field visit will be appropriate in an anthropological context, but not in a specific and peculiar science. Or consider the example of chairing a conference panel. Chairing is, besides other tasks, about regulating scientific discussions, and about defining what is a worthy contribution to the discussion and what is inappropriate cheap talk. Dissections of practices in situation will assist in unraveling these regulatory norms. In reconstructing these practices in the light of the three objectives, the task will not only be to get an understanding of the community under study, but to investigate how relations to non-scientific actors are established and maintained in these practices, how disciplinarian power effects play out, and which norms govern the respective practice.

The sociology of science is rich in approaches useful for the study of various specific sciences. If the objectives are to unravel the performative capacity of a specific scientific domain and of a peculiar science, to conduct sociological studies in an ethical manner with an emancipatory interest, and to elaborate norms for education and evaluation based in scientific practice, then the approaches described as “cultural studies of science” are the most promising path to pursue[9]. Cultural studies of science take science to be a social formation constituted by practices and being in constant relation to other formations (such as politics, journalism or neighboring scientific formations). Science is moreover a continuously reconfiguring formation given the slippage of scientific practice and the recurrent introduction of new practices, objects and concepts.

The researchers associated with the macro-analytic *Strong Programme in the Sociology of Scientific Knowledge* (Barry Barnes, David Bloor) were particularly interested in the role of large scale social phenomena, whether widely held social/political ideologies or group professional interests, on the settlement of scientific controversies. Some landmark studies in this genre include Andrew Pickering's[10] study of competing professional interests in the interpretation of high energy particle physics experiments, and Steven Shapin and Simon Shaffer's[11] study of the controversy between Robert Boyle and Thomas Hobbes about the proper interpretation of experiments with vacuum pumps.

Science and scientific rationality themselves were gradually recognized as an everyday performative practice among many others. As Pels puts it, science has come to be theorized as: "...bad short-hand for a vast plurality of practices which are fragmented across many disciplines, niches, paradigms, and approaches. More dramatically, science has come to be viewed as just one culture of rationality among others, 'just another story', one among a plurality of perspectives, information bases, and interpretive communities, none of which can lay claim to an overarching or foundational status"[12].

This epistemological naturalization/socialization/contextualization explicitly showed that science, like any other ordinary social activity, conveys values, assumptions, presuppositions, implications and consequences which we could never ignore or bypass.

In particular, the reflexive awareness of the mutual dependency of sociological categories (such as risk, citizenship, space, time, modernity, morality) and social practice has been increasingly brought right at the forefront of various hot epistemological debates. In the general case of science, a model of social complexity has overwhelmingly emerged. This made clear how the establishment or institutionalization of "scientific knowledge" is directly followed by its technological "application" which self-consciously leads to a critical reflection on the unintended, unanticipated and unforeseen consequences[13]. The inherent unpredictability of knowledge production could be further elaborated through the empirical demonstration of its unavoidable Janus-faced character. That is, the impact of science and technology is both positive and negative: they are a "collective good" and a "collective bad" at one and the same time.

In a useful and compelling essay in this journal in 2006, Matthew Herbert argued that[14]: 'The Intelligence Community should recruit epistemological talent and cultivate epistemological skill across its organizations.''

Herbert began his argument by noting official critiques of the Intelligence Community (IC) for its mistakes in determining whether Iraq had weapons of mass destruction in 2002. The two basic problems, according to these critiques, were the American intelligence collection system in general, including, presumably, ''stove piping'' and faulty analysis. Suggesting that the second of these is the more basic problem - ''America's intelligence analysts must simply become better thinkers''- Herbert noted the officials' call for ''analysts to raise the rigor of their

methods, root out analytic bias, and demonstrate clear connections between judgment and evidence"[15]. In response to these critiques, Herbert suggested training analysts in epistemology and having an epistemologist on hand to help the analyst better do the job. This response might be characterized as an argument with four premises. First, an analyst's task is primarily epistemological. Second, the analyst can fulfill a task either knowledgeably and systematically or by haphazard trial and error. Third, this task is better fulfilled knowledgeably and systematically. The fourth premise is that there is epistemological expertise in intelligence sciences. The path to knowledge need not be improvised. A body of time-tested expertise exists on which to base the consolidation of analytic practices. The discipline of epistemology, or theory of knowledge, focuses 2,500 years' worth of erudition on the key issue encountered in intelligence analysis.

Herbert's article opens the way to the general view that there are a number of findings and perspectives in the intelligence literature that point to the need for contemporary intelligence analysts to be equipped with a heightened knowledge of advanced social science theory and methods. There is evidence that these foundations are sometimes lacking in the intelligence community, suggesting a shared failure on the part of the intelligence community and the educational programs meant to prepare its analysts. Consistent with other critiques of the intelligence community, Collier (2005) pointed to a cultural reliance on historical and inductive approaches to intelligence analysis. He pointed to a lack of analysts "trained in the proper development of theoretical frameworks and research hypotheses and in advanced-social-scientific analytic methods"[16].

The Research Project

The present article tried to approach the issue of scientific status of a science from a sociological point of view and to offer an answer at the following research questions:

- "How people assessed the debate between theoretical aspects and the empirical ones in the case of sociology as science?" and
- "What intelligence science can learn from people's assessments of sociology in order to progress itself as science?"

The research project uses the triangulation of methods, and favors both qualitative and quantitative approaches to the issue.

The quantitative analysis is made on the survey made in 2009 by the Romanian Agency for Quality Assurance in Higher Education[17] and it presents descriptive statistics of the survey's results.

The second analysis is a qualitative one, based on a set of 50 interviews with students from University of Bucharest. The data collection took place in 2012 and, in the same way, the descriptive elements are presented in the article.

Students, Professors and Employers – the Quantitative Secondary Analysis

A survey made in 2009 by the Romanian Agency for Quality Assurance in Higher Education[18] showed that Romanian students from the tertiary (university level) educational system positively assessed in 2009 the quality of the lectures: 79% of a national sample interviewed considered that the information is up-to-date and 66% agreed with the statement "The courses I learn put an accent on the practical elements of the discipline". At the same time, a percent of 42% of the sample of students assessed that the lectures stressed in a higher degree the theoretical aspect of the curricula, at the expense of the practical ones[19]. Also, 50% of the students interviewed in the same survey assessed that the lectures gave them "all the abilities and competencies they need at the work-place" and 66% of them assessed that the practical stages during the faculty's years were very useful[20].

As regards the involvement of Universities in finding a work-place for their students, 69% of the total sample of students assessed that the tertiary education institutions provides them with fellowships and 57% had indicated the internships the Universities provided to them[21]. Only 42% from the same sample of students named the presentations made by employers about the existing work-places and only 39% mentioned the fact that Universities had organized internship programs[22].

At the same time, the professors' assessments regarding the way in which the Romanian tertiary system prepares the students for entering the work-places are extremely positive. As the 2010 report from the Romanian Agency for Quality Assurance in Higher Education[23] showed, 90% of a total national sample of university professors assessed that the content of the courses they teach helped the students to acquire the abilities they need at their future work-place[24]. A percent of 88% of the same sample of university professors assessed that the internship program s organized by the

faculties are useful in training the students[25]. Other interesting results showed that 68% of the total university professors' sample assessed that their lectures covered the practical issues that the students could face at their work-place and 67% assessed the students will easily find a work-place after graduation[26].

One can, as such, notice the existence of a "gap" between the students' and professors' perceptions about the degree in which the faculty helps youth to obtain abilities they need at the work-place. This difference is of 40% between the two samples considered[27].

Table 1 – *Students and professor's assessments regarding the ratio between practical and theoretical abilities acquired during the learning process in the tertiary education*

Assessments of the professors	Little agreement	Great agreement	Difference in assessments	Great agreement	Little agreement	Assessments of the students
The lectures taught covers practical issues that the students will encounter at their future workplace	28%	68%	18%	50%	38%	The lectures taught covers practical issues that I shall encounter at my future workplace
The faculty helps students to acquire abilities they will need at their future workplace	9%	90%	40%	50%	40%	During my study-years I acquire abilities I shall need at my future workplace

(Source: Vlăsceanu et all., 2010a: 182)

The opinions and assessments of employers about the value of the University degree varied. As the 2010 report from the Romanian Agency for Quality Assurance in Higher Education[28] showed, 40% of a national sample of Romanian employers assessed that the university graduation diploma is not a guarantee of the quality of their employees[29]. In addition, the Romanian employers assessed that the university graduates were better trained from a theoretical point of view, at the expense of the practical ones: 51% of the total sample of employers declared that graduates had a good theoretical background in their field of expertise and only 27% assessed that graduates have practical skills[30].

The second relevant difference appeared among the perceptions of employers, students and professors regarding the type of skills students received during the tertiary level education cycle. Only 27% of the employers sample assessed that graduates had acquired good practical skills during the tertiary education cycle but

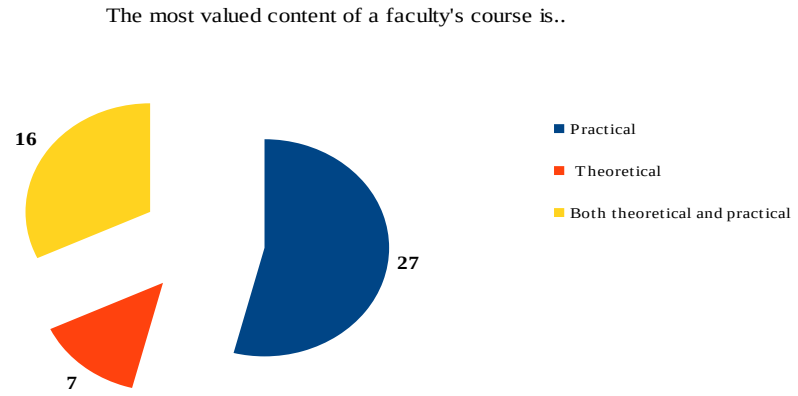
66% of the students and 68% of the professors assessed that graduates had acquired good practical skills during the tertiary education cycle[31].

The Qualitative Analysis

The quantitative research made in 2012 showed a shift in the students' opinions and assessments about the content of the lectures they attend at the faculty, and from here, a change in their opinions and assessments regarding the abilities and skills they need to enter workplace.

Thus, from a total of fifty answers at the questions "What is the most valued content of a faculty's course?" twenty-seven students answered "Practical content" while only seven students choose the strictly theoretical one.

Figure 1: *Assessments of the theoretical vs. practical content of the faculty's courses*



We recorded clear differences among the reasons behind different students' choices. The students who put a stress in the practical content of lectures also invoked the help this type of information provided to them in "real life", "learning how to do things", while the students who valued the theoretical content linked it to the more general "aim" of the education process: the progress in knowledge. For the third category – that is, the students who equally valued "practical" and "theoretical" contents for the faculty's lectures – the reasons behind their choice were "the complex relationship that exist between theory and practice in science".

Table 2 – *Reasons for assessing the content of the courses*

A. I.	Certainly, the term that better describes the course is "theoretical" and this is due to the fact that during the lectures we have learned information that enabled us to assess in a critical manner both the work of other researchers and our own work. But, at the same time, the course is also a practical one, because it made appeal at the benefits of empirical learning.
E. D.	It is a practical one, and I prefer it that way. Due to the fact that it is practical, it helps me more in real life. What's happening in reality has to be replicated in the classrooms. This is the aims of the faculty's lectures, isn't it?
D. G.	I would describe the course as being mainly theoretical because, aside from the fact that it presents some useful research means, it also builds a critical view on reality.
F.Z.	I shall choose the word "practical" to describe the course. We learn a lot of useful information but, at the same time, we did not reach that point at which we want to know more and this is, mainly, our fault.
B. M.	I shall choose the term "practical" because, each time when we attended a lecture, we also saw practical examples and, at the same time, the homework we did had required always a practical information.
C. D.	A practical one, due to the fact that the course did not intend to be a theoretical one, but a course applied to real situations, that someone can face at his or her work-place.
M. L	Both, because practice is provoking. It is about the experience one is acquiring during the education process, of reverting the initial plans, of assuming risks in knowledge. At the same time, in order that someone can make a judgment he or she needs a constant intellectual development.
T.L.	A practical one. The reason for that choice is the fact that you need this kind of information if you work somewhere. And, also, because the main objective has to be to learn "how to do something".

In the case of the survey made in 2009 three samples were used – the students' sample, that of the professors and the sample of employers[32] - and the answer at the three different questionnaires could be cross-checked and compared. On the contrary, the qualitative study from 2012 was made only on a single sample – the students' one – and we cannot compare their assessments with those of the professors and, respectively, of the employers. For that reason a prospective-type question (used in the guide of interview) requested respondents to explain how they would deliver a lecture (in the hypothetical case) if they were not students but professors.

Table 3 – *"In the case in which you are a professor how would you deliver a lecture that could be positively assessed by students?"*

A. I.	If I would be in the teacher's position certainly I shall present lectures that are based on empirical learning. I would do that because I know from my own experience that "experience is the best teacher".
E. D.	I do not like to read a lot of theoretical stuff, dozens of pages that only few men actually read. For me it is enough to pay attention to fundamentals and, more important, to know how we can apply the theoretical aspects of knowledge. If I were a teacher I would come in front of my students with real life examples. I would tell them stories about real life and, at the same time, I would try to involve them in my research projects. In this way they can learn useful things and acquire knowledge with a practical character. It is not so important for me that graduates have a "strictly theoretical" background because, as anyone can see, this can't help you to find a workplace. Instead, I should favor the students' acquisition of practical abilities.
A. P.	I would try to tell them a story at the beginning of the courses. This story would be related to the course's content so I could obtain the students' interest in the future lectures.
D.P.	I would make with them practical results, because this kind of skills are more desirable now at any work-place.
P. D.	I would put a stress on the practical aspects of the course. I am taking into account the fact that theoretical aspects can't be so easily learn and sometimes we forget them.
C. D.	I would try to make a creative course, involving students in a "role-playing" so they can easily teach practical aspects of the course.
M. L.	I would try to combine, to mix the theoretical aspects of the course with the practical ones. I love to enlarge my knowledge and I should like to see myself in the position of putting knowledge into practice. The theory helps you to increase knowledge and practice shapes you as individual.

The answers at this question proved the importance of practical elements in the education process, as this was assessed by students. "Real life example", "practical skills", "practical abilities", "being ready for the tasks at the work-place" - those are the main reasons behind the students' opinions and attitudes towards the University's curricula and lectures' content.

Conclusions

Sociology of science provides an alternative source of norms, or maybe better a different take on them. Sociologists of science aim to elucidate norms as they come from within concrete, historical and

observable scientific practices. Scientific practice is a continuous struggle about which norms are appropriate in given situations. The normative settlements different scientific communities and disciplines' reach, for instance by job interviews, peer review mechanisms, in board meetings or conference panels, are however hardly explicated. Yet, if they remain private, tacit, and implicit, they can neither be used in evaluation nor in educational processes. Sociology of science is not only a tool that allows one to get closer to practice and thus escape the entrapment of becoming the object of either the abstract generic norms of the philosophers or the absurd norms of the managers, but it is also one that favors a regain a meaningful autonomy for the knowing subject and its communities

Existing sociology of science already provides alternatives in discussing knowledge generation from a broader and indeed more practical perspective. Yet, the usefulness of sociological accounts for education and evaluation purposes is hardly apprehended or outlined in a straightforward manner. Indeed, a rewriting of the history of the first great debate[33] may help the student to gain critical distance to the stories teachers tell, studies of national disciplinary communities provide useful maps to access and navigate, a statistical analysis of career and publication patterns[34] may assist the early career researcher in choosing publication strategies, or a survey of top publishing houses, professors and graduate schools[35] may assist the student in identifying the best graduate school and publication outlets. As long, however, as the eye does not turn to scientific practices and to controversies and their settlement, a sociology of science undersells its potential in both educating its future members in how to practice in a specific science, as well as in offering alternatives to current norms of evaluation

The micro-sociological or laboratory studies approach features ethnographic study of particular research groups, tracing the myriad activities and interactions that eventuate in the production and acceptance of a scientific fact or datum. Knorr Cetina's[36] reports her year-long study of a plant science laboratory at UC Berkeley. Bruno Latour and Steven Woolgar's study[37] of Roger Guillemin's neuroendocrinology laboratory at the Salk Institute is another classic in this genre. These scholars argued in subsequent work that their

form of study showed that philosophical analysis of rationality, of evidence, of truth and knowledge, were irrelevant to understanding scientific knowledge. Sharon Traweek's[38] comparative study of the cultures of Japanese and North American high energy physics communities pointed to the parallels between cosmology and social organization without making such extravagant and provocative epistemological claims. The efforts of philosophers of science to articulate norms of scientific reasoning and judgment were, to all these scholars, misdirected, because actual scientists relied on quite different kinds of considerations in the practice of science.

What do studies of the social, institutional, and rhetorical aspects of science add to our practical understanding of science? From one perspective, the careful study of what scientists do, how they speak and write, is trivial. Of course science is uncertain, changes over time, is dependent on measurement devices, requires funding, involves human beings and social institutions, relies on language and persuasion, and so forth. Latour and Woolgar note that the reaction of the Salk Institute scientists they studied was that it was all rather unsurprising: How could anyone ignore the details of our daily work?

From the point of view of those who have adopted an idealized view of science, i.e. as formally constituted without regard to social, institutional, and rhetorical contingencies, a sociological or rhetorical analysis seems to be an attack on science itself a reduction of all science to junk science. From the sociological or rhetorical point of view, however, a social, institutional, and rhetorical account of science is merely descriptive of how science works, and is, therefore, critical only of idealized accounts. In short, if practitioners anticipate an attack on his or her own side expert as biased or interested, deposition of the opposing expert should attempt, using ethnographic methodology, to show that all science is biased or interested not perniciously but normally in its very constitution as knowledge.

When one first encounters the growth of the discipline of science studies, their prominence in numerous university programs, and the appropriation of anthropological methodology in ethnographic studies of scientific practice, one cannot help but think that the insights of this field would be useful to practitioners in cases

involving scientific expertise. As has been shown, however, science studies do not fit easily into the discourse of practitioners-science relations, where an idealized conception of science predominates. Interest, bias, and motivation are viewed in the courtroom as bases for impeachment and markers of junk science, in contrast to the bases of genuine scientific knowledge sufficient data and reliable methodology. Evidence that all science is socially motivated, institutionally interested, or rhetorically biased seems to have no place in the courtroom, since it casts doubt on the certitude of both sides expertise. The value of science studies for practitioners is therefore called into question. On the other hand, if science studies are viewed as a challenge not to science itself but to idealizations of science, then in certain situations namely when a practitioner will be challenged by an opposing expert as not meeting idealized standards ethnographic methodology could be usefully appropriated. A modest view of science tends to level the playing field in disputes between hard science and soft science experts.

A number of conclusions can be reached at the end of this article.

The first is that the fundamental purpose and role of higher education, particularly graduate education, is consistent with the teaching of advanced theory and methods. In the field of intelligence science this was stressed by S. Marrin[39] who differentiate between education and training in the curricula of intelligence sciences.

Secondly, as in the field of sociology, in intelligence science it is important to balance substantive expertise with theoretical and methodological expertise in the field of intelligence sciences. As Michael Corpora[40] indicated, intelligence analysts, after all, are knowledge workers, and their work, while having differing objectives and data, is not that dissimilar to that of social scientists.

As this article tried to suggests, it is desirable that much of this research would be undertaken in the context of longer term professional development and analyst performance in the intelligence community. This will help support the development of a more integrated intelligence analysis discipline and hopefully better analytic outcomes.

References

[1] M. Collier, "A pragmatic approach to developing intelligence analysts", *Defense Intelligence Journal*, Vol. 14, No. 2, 2005, pp. 17-35.; Jack Davis, "Why Bad Things Happen to Good Analysts" in *Analyzing Intelligence* (Washington, DC: Georgetown University Press, 2008); Richards J. Heuer, *Psychology of Intelligence Analysis* (Washington, DC: Center for the Study of Intelligence, Central Intelligence Agency, 1999); Rob Johnston, *Analytic Culture in the U.S. Intelligence Community: An Ethnographic Study* (Washington, DC: Center for the Study of Intelligence, Central Intelligence Agency, 2005).
[2] Davis, "Why Bad Things".
[3] Jeffrey R. Cooper, *Curing Analytical Pathologies: Pathways to Improved Intelligence Analysis* (Washington, DC: Central Intelligence Agency, 2005).
[4] C. A. Corpora, "The stone and quarry: Intelligence studies in a dynamic global environment", *American Intelligence Journal*, Volume 25, 2008, pp. 12-23.
[5] Stephen Marrin, "Training and educating U.S. intelligence analysts", *International Journal of Intelligence and Counterintelligence*, Volume 22, No. 1, 2009, p. 131.
[6] T.S. Kuhn, *The Structure of Scientific Revolutions* (Chicago: University of Chicago Press, 1970).
[7] L. Laudan, *Progress and Its Problems: Toward a Theory of Scientific Growth* (London: Routledge and Kegan Paul, 1977).
[8] D. Pels, "Unhastening Science", *European Journal of Social Theory*, Vol. 6, No. 2, 2003, pp. 209-231.
[9] J. Rouse, *Engaging Science. How to understand its Practices Philosophically (*Ithaca: Cornell University Press, 1996).
[10] A. Pickering, *Constructing Quarks: A Sociological History of Particle Physics* (Edinburgh: Edinburgh University Press, 1999).
[11] Steven Shapin and Simon Shaffer, *Leviathan and the Air Pump, Hobbes, Boyle and the Experimental Life* (Princeton, New Jersey: Princeton University Press, 1985)
[12] D. Pels, "Unhastening Science", *European Journal of Social Theory*, Vol. 6, No. 2, 2003, p. 210.
[13] C. A. Van Peursen, *Strategie van de Cultuur* (Amsterdam: Elsevier, 1970).
[14] M. Herbert, "The Intelligence Analyst as Epistemologist," *International Journal of Intelligence and CounterIntelligence*, Vol. 19, No. 4, Winter 2006-2007, pp. 666–684.
[15] *Ibid*., pp. 666-667.
[16] M. Collier, "A pragmatic approach to developing intelligence analysts", *Defense Intelligence Journal*, Vol. 14, No. 2, 2005, p. 21.
[17] L. Vlăsceanu, M.G. Hâncean, B. Voicu and C. Tufiş, *Starea calităţii în învăţământul superior. Barometrul calităţii* (Bucharest: ARACIS and QualMedia, 2010a); L. Vlăsceanu, M. G. Hâncean, B. Voicu and C. Tufiş, *Distribuţii statistice, interpretări şi opţiuni privind starea calităţii în învăţământul superior: Barometrul calităţii – 2009* (Bucharest: ARACIS and QualMedia, 2010b).
[18] L. Vlăsceanu *et al.*, *Starea calităţii în învăţământul superior*, 2010a.
[19] *Ibid.*, p. 159.
[20] *Ibid.*, p. 160.

[21] L. Vlăsceanu *et al.*, *Distribuţii statistice, interpretări,* 2010b, p. 17.
[22] *Ibid.*
[23] L. Vlăsceanu *et al.*, *Distribuţii statistice, interpretări,* 2010b.
[24] *Ibid.*, p. 19.
[25] *Ibid.*
[26] *Ibid.*
[27] L. Vlăsceanu *et al.*, *Distribuţii statistice, interpretări,* 2010b, p. 22.
[28] L. Vlăsceanu *et al.*, *Distribuţii statistice, interpretări,* 2010b.
[29] *Ibid.*, p. 16.
[30] *Ibid.*
[31] L. Vlăsceanu *et al.*, *Distribuţii statistice, interpretări,* 2010b, p. 25.
[32] L. Vlăsceanu *et al.*, *Starea calităţii în învăţământul superior*, 2010a; L. Vlăsceanu *et al.*, *Distribuţii statistice, interpretări,* 2010b.
[33] C.G. Thies, "Progress, History and Identity in International Relations Theory: The Case of the Idealist-Realist Debate", *European Journal of International Relations*, Vol. 8, No. 2, 2002, pp. 147-185.
[34] Th. Plümper and F. Schimmelfennig, "Wer wird Prof – und wann? Berufungsdeterminantenin der deutschen Politikwissenschaft", *Politische Vierteljahresschrift*, Vol. 48, No. 1, 2007, pp. 97-117.
[35] D. Maliniak *et al.*, *The View from the Ivory Tower*: TRIP Survey of International Relations Faculty in the United States and Canada, Williamsburg: Program on the Theory and Practice of International Relations, College of William & Mary, 2007.
[36] K. Knorr-Cetina, *The Manufacture of Knowledge* (Oxford: Pergamon Press, 1981).
[37] Bruno Latour and Steven Woolgar, *Laboratory Life: The Construction of Scientific Facts* (Princeton: Princeton University Press, 1986).
[38] Sh. Traweek, *Beamtimes and Lifetimes: The World of High Energy Physicists* (Cambridge: Harvard University Press, 1988).
[39] Stephen Marrin, "Training and educating" pp. 131–146.
[40] C. A. Corpora, "The stone and quarry", pp. 12-23.

Intelligence and the Neuropsychological Structure of the Brain

Richardo NEDELA[*]
Brânduşa ŢEICAN[*]

Abstract

The paper starts from a double observation. Firstly, it emphasizes the specialization of intelligence activity on the two basic components: information gathering – and here we have in mind collecting information from secret human sources - HUMINT –, and information analysis. Our next premises regard the neuro-psychical structure of the brain from the perspective of the theory of specialization or lateralization. According to this theory, there is a specialization of the cognitive functions that combine with a dominant of one of theirs.

Taking into account the various studies and scientific research that linked the prominence of certain cognitive functions to certain types of activities, professions and even cultures, we consider that the above mentioned observations represents solid starting points to conclude with the hypothesis that the same connection could be made between the cognitive specialization of the two cerebral hemispheres and the specific required skills in intelligence: HUMINT information gathering on the one hand, and information analysis, on the other.

Specialization in Intelligence

Whether it is seen as a cycle or as a field, as Shulsky and Schmitt do, intelligence has two essential components: "as an *activity*, this field involves collecting and analyzing information"[1].

With respect to the relationship between the two intelligence activities powerful schools of thought have been developed: "distance and proximate schools", as Mark Lowenthal put it[2]. But no matter the distance or proximity between the two functions, they are *different* and even from the beginning of the modern intelligence, at least in the U.S.A., these functions were performed by different officers, by different people. Garett Jones describes the history of this relation as follows:

"From the founding in 1947, one of the CIA's cardinal rules was that intelligence should be collected by a different group of people than those who analyzed what the intelligence meant and its

[*] Lecturer, "Mihai Viteazul" National Intelligence Academy
[*] Asistant Lecturer, "Mihai Viteazul" National Intelligence Academy

value. The CIA's founders understood that collector of intelligence invested far too much professional and personal energy into a source or a method to be able to evaluate the resulting intelligence in a unbiased manner. In fact, when the old CIA headquarters was first opened, the hallway doors between the DI (Directorate of Intelligence) and the DO (Directorate of Operations) were permanently locked. DI and DO personnel were not to mix. The DI had not staked in how much time and money the DO had expended in collecting a piece of intelligence. Their only task was to evaluate the accuracy and importance of the collected intelligence"[3].

The reason for this splitting seems to be the principle of checks and balances[4].

"Unfortunately, it has become common practice in many intelligence centers for analysts to both direct the collection of intelligence and, because of their training, make the first cut on the meaning and value of the intelligence. When it becomes time for the DI to produce a formal product, among the first people it sounds out on what the intelligence means are the analysts responsible for its collection. This is a fundamental error and may be at least partially responsible for the failures surrounding the Iraqi WMD question. This is not to say that collectors' opinions on the intelligence should not be considered: they often have subtle and meaningful insight into the situation. However, their opinions should be one data-point among many, not the first draft of a National Intelligence Estimate. The current practice is a profound violation of analytical tradecraft. If you are going to collect, collect; if you are going to analyze, analyze. Having analysts involved in the collection process is a good idea, but once they have invested themselves in collection, they must not be involved in the subsequent analysis"[5].

This is why today the specialization of intelligence in collecting and analyzing information has become commonplace in most intelligence agencies.

It is obvious then that the optimal performance of the two different functions requires different skills, different abilities, and different competences. Specialization itself requires improvement in one particular direction: one cannot be a specialist in everything, one cannot be good in anything, and if such cases do really exist, they can only be the exceptions that prove the rule.

To excel in what they do, the man or woman who collects the information must have different skills than an analyst. Their work may require less rational and more emotional intelligence, may involve less analytical abilities and more communicational skills. In order to obtain information from a human source, they might need less critical thinking and more creativity and imagination, less deductive reasoning and more persuasive capability. Conversely, the analyst might not need a better emotional relationship, but a more valid and pertinent logical relationship. They might not need to master non-verbal communication, but the verbal one, especially the written one, which is no longer directly connected to the transmitter. The analyst may have less need to think in images and more in concepts, less in concrete and more in abstract, because, in the first place, they are not "on the ground", as the gatherer, and in the second that, unlike the collector who, in collecting the information is much more connected to the present, the analyst assesses for the future.

No matter how important these components of intelligence cycle may be separately, both are equally important, their value being given by their complementarity, not their individuality. However, this specialization and complementarity of intelligence activities have a striking resemblance with the specialization and the complementarity of the brain functions. This is why, even if the specialization in intelligence was not caused by the neuropsychological specialization model, such a parallel can and should be done.

Brain' Functions

The brain is the core component of the central nervous system. It accommodates the cerebral hemispheres whose activity makes it possible for the psyche to be conscious. The rise of man from among the primates, from animality in general, as an evolution of hominids is attributed to the development of the brain, of its volume and weight.

The surface of the brain, the cerebral cortex, performs four functions: sensory, motor, psychic and vegetative. In the cerebral cortex there are the projection areas for the fibers linked to various sensorial organs – "the optical fibers in the occipital lobe, the auditory fibers in the temporal lobes, fibers from the skin (tactile, thermal, pain) on the anterior edge of the parietal lobes" – but also the various nervous centers which command movement, both

involuntary and voluntary – in the central anterior circumvolutions area – or those from the frontal lobe "which influence the sympathetic and parasympathetic nervous system, thus indirectly, the activity of the internal organs"[6].

As far as the psychic function is concerned, "it is being provided by the association of neurons, located between the projection areas, neurons that link the sensory areas to the motor ones, but also the cerebral cortex level to the subcortical areas. Those areas allow the formation of conditioned reflexes, learning, memory, perception, thinking etc. The motor centers of speech are found in the frontal lobe, the ones that ensure the understanding of speech, and the understanding of written speech is being coordinated in a lower parietal area"[7].

In connection with the function of cerebral hemispheres, even since the 19th century, there have been two opposing views: anti-localizationism and localizationism. Anti-localizationists, such as Karl Lashley, claim that "the cerebral cortex is more likely to function as a whole", that functions such as learning and memory "do not appear to be localized to a certain area of the cortex but are spread upon its entire surface"[8]. Localizationists, on the other hand, consider that each skill has a corresponding cortex area.

Nowadays an intermediate position upon this is the one of a dynamic localization according to which "there are main centers for some functions, but there are areas in the cortex connected to those centers, which can, when needed, have the same function"[9]. Moreover, the trend is to describe brain activity not by using strictly separated areas, but rather taking into account the integration of excitations on *levels* and branching (horizontally) resulting in "constellation of centers".

We would have here "*the block with the function of receiving, storing and processing information* from the external (and internal) environment. Most of the hemispheres contribute to this: the occipital lobes, temporal lobes, and parietal lobes. Besides the zones of sensorial projection we find large areas with integrating functions. Very important appears to be the zone of intersection (tertiary) between the optical, acoustic and tactile sectors which is represented by the inferior parietal circumvolutions, considered to be specific to humans. It is believed that it plays a major role not only in synthesizing sensorial information, but also symbolic processes, grammar and logic structures, allowing abstract thinking"[10].

On the other hand, we would have "*the block with functions in programming and planning activities*". This one "consists of the frontal lobes that allow the confrontation of performed actions with intentions and initial projects, the regulation and control of psychic functions. Damaging the frontal lobes does not appear to lower the intellect, but one becomes helpless (the ability to take initiative decreases) and irresponsible (the sense of responsibility fades away)"[11].

Then, it is both logical and, so to speak, bio-logical, that different functions be polarized in, and by different parts or areas of the brain. Specialization of the brain is just as natural as specialization of the whole body: we have the hand for grasping, holding or touching, not for seeing or hearing, for which we have the eye and the ear. Obviously, it's to our own advantage: we could hardly have all these capabilities with one organ only.

Specialization in the Brain

Before any consideration or speculation regarding the differentiation of brain functions, we need to consider the facts: "Whilst the coordinating centers are bilateral, those of speech and writing are found on the side of the brain which controls one's dominant hand; that is the left side for right handed people and the opposite for left-handed people"[12]. And, further: "Whilst the intellectual functions are on the dominant side for speech (left side for right-handed people), the other side assumes senso-motor functions. Those functions are coordinated through the Corpus Callosum, whose sectioning makes the two hemispheres better for separate learning"[13].

We notice the same observation of domination and laterality on Sheila Hayward: "For the majority of individuals, the dominant hemisphere is the left one; it controls the right side of the body. Some functions have centers only in a single hemisphere, for example the center of speech which is usually found in the left part of the brain"[14]. But the non-dominant hemisphere has its role as well: "The non-dominant hemisphere, usually the right one, is responsible for some functions, such as spatial location (the awareness of relationships between objects in the spatial field). Spatial localization is useful to people from several domains such as architects, artists and tennis players. It is worth mentioning that numerous tennis players and artists are left-handed. For those individuals, spatial representation takes place in the dominant hemisphere"[15].

In her argument, Sheila Hayward invokes Robert Ornstein's theory, suggesting that the left hemisphere specializes in analytical, verbal and mathematics functions, of successively processing information (one element at a time, on a straight line), whilst the right hemisphere is impressionistic, holistic and processes more than one element at a given time. Moreover, Hayward mentions Roger Sperry's scientific work, that appears to substantiate the necessity of a lateralization of functions (different functions being mediated by the parted hemispheres), even though some are without any doubt bilaterally represented.

Even if Sheila Hayward concluded that "scientists are not sure if other functions, besides speech, are located in a specific hemisphere"[16], the specialized functioning of the two hemispheres was emphasized by many authors as pairs of opposite, but complementary, terms.

Here's how Dr. Betty Edwards describes[17] the specifics of the two hemispheres:

Left	Right
VERBAL – uses words to name, describe, and define.	NON-VERBAL – aware of things, but minimal connection with words. It gives the pitch (verbal stimulation).
ANALYTICAL – discovers things step by step, element after element.	SYNTHETIC – puts things together to make wholes.
SYMBOLIC – uses symbols instead of things.	CONCRETE – relates to things as they are at the present moment.
ABSTRACT – extracts a piece of information using it to represent the whole.	ANALOGICAL – sees the links between things, understands metaphors.
TEMPORAL – follows the axis of time, it is framed in time organizing things sequentially, taking them one at a time.	ATEMPORAL – no sense of time.
RATIONAL – draws conclusions based on facts and reasoning.	NON-RATIONAL – doesn't need facts and reasoning. Tendency not to judge.
NUMERIC or digital – Uses numbers and their means.	SPATIAL – sees objects in relations with one another and as parts forming a whole.
LOGICAL – draws conclusions based on logical organization.	INTUITIVE – evolves in leaps, starts from impressions, feelings, visual images, informing elements.
LINEAR – thinks in terms of ideas linked to each other, convergent thinking.	GLOBAL – perceives assemblies, association of parts, divergent conclusions.

According to Dominique Chalvin, the dominant characteristic of the left hemisphere is rationality: "the typical feature for left hemisphere is rational approach"[18]. The left hemisphere encompasses reasoning, both mathematical and logical, which involves abstracting and procedures and rules – that is method, a rational method. Language is located in the left hemisphere because reasoning also implies language: thinking is impossible without language and – to some extent – vice versa. Thinking is also analytical. As Watzlawick put it, left hemisphere "sees the trees instead of the wood": "The main function of the left hemisphere is to translate any perception into logical, semantic, and phonic representations of reality and to communicate with the exterior on the basis of this logical-analytical coding of the world"[19]. On the other hand, and on the contrary, the left hemisphere doesn't care very much about deduction and explanation: it is "the world of thinking without language, of non-verbal understanding, of recognition, of spatial perception [...]. Its job is to synthesize and express our experience into an image. Its modes of expression are non-verbal; its functioning is based on associations. Imagination and intuition are its dominant functions; this is why it is considered the headquarters of artistic and musical competence"[20]. The left hemisphere's approach is not step by step, based on reason, but on intuition, leaping, seeing instantly the connections, the associations, and the wholes.

Although separate, the hemispheres function normally together, the psychic integrity is ensured by the integrated functioning of both hemispheres. The functioning of the brain is analogue with the functioning of the locomotory system: although each of the inferior limbs is necessary – none sufficient for completing the function of locomotion of the body. We need not forget that hemispheres are *parts* of the brain, not autonomous entities, and like any part of a whole find their fulfillment in the whole they belong to, not in reciprocal isolation. The expression "it takes two to tango" is a colloquial means to express this frequent phenomenon where the existence and functioning of a whole depend on more than one single element: they depend on a pair of elements equally important.

"It is important to mention that we do not have two brains functioning separately, independent from each other, but one single, total brain, working complementarily. That is why when we read a text the right hemisphere has its own role in decoding the visual information, appreciating the humor and the emotional content, understanding metaphors, keeping an integrated, unitary structure of the text. Creativity supposes collaboration, cooperation between the two hemispheres, and each grasping reality in their own way. From a psychological and physiological point of view, people differ from one another with respect to a balance between the two hemispheres. Thus, certain people approach a problem logically, analytically, displaying all the data before making a thorough analysis. Another category of people immediately see the solution without being interested in the analysis of all the details of minor importance, and also have the ability to see objects in space and to manipulate them through their tridimensional images"[21].

And, definitely, it must be mentioned the fundamental role of the prefrontal part of the brain with its critical unifying function: "True human intelligence, true reason, is not just the thinking machine of the noetic brain, but also the intelligence fully reflected which always involves an affective dimension, since the prefrontal part of the brain ensures unity of the intellectual level (noetic brain) and the affective level (primary brain) on a higher level where reason and heart are complementary"[22].

If lateralization – or hemisphericity – as a specialization of the human brain functions is today widely recognized beyond any doubt, some researchers have reached the conclusion that there are even various types of hemisphericity[23].

- *Execution hemisphericity* refers to the fact that certain activities – such as speaking, writing, recognizing faces, drawing etc. – uses more one of the hemispheres.
- *Individual hemisfericity* emphasizes the fact that through education, habits and profession, a person uses more one of the hemispheres.
- There would even be a *cultural hemisfericity*, certain groups of individuals – professional communities, social classes and even certain societies of a specific civilization – having the tendency to use more frequently one of the hemispheres.

As Dominique Chalvin[24] notices, there are professions and jobs that lead to the predominant development of one cerebral hemisphere. Thus, jobs such as engineer, technician, financial-administrative fields, doctor, jurist, IT specialist and the respective studies would be associated to the left hemisphere, and with the right hemisphere – musicians, dancers, writers, artists, poets, sculptors, psychologists, experts in inter-human relations, philosophers, politicians, entrepreneurs and the respective studies.

Sheila Howard also notices that the dominance of a certain hemisphere favours certain professions: "many high class tennis players and artists are left-handed. These individuals have the spatial representation in the dominant hemisphere"[25].

From our perspective, it doesn't matter where every particular function is localized – in the four lobes of the two hemispheres –, nor that they are close or distanced. The fact that we want to highlight is that these functions are *different*, and that specialization make the brain work as a whole. It is like language: the differentiating in the flow or continuum of sound and the differentiating in the flow or continuum of thought as well are the conditions of creating words.

The other fact we need to underline is that one of these functions – pertaining to a hemisphere or the other – is prominent and dominant.

These are strong, if not compelling, premises that leads us to the hypothetical conclusion that this might be the case in the field of intelligence also. That is why we start from the supposition that HUMINT collectors make use of certain cognitive functions, others than the ones used by analysts.

Our intention is to verify this hypothesis in a subsequent research, as well as to identify solutions to increase the abilities triggered by specialization on intelligence based on the same theory of specialization or lateralization.

References

[1] Abram N. Shulsky and Gary J. Schmitt, *Războiul tăcut* (Iaşi: Editura Polirom, 2008), p. 12.
[2] Mark M. Lowenthal, *Intelligence. From secrets to policy*, Fourth edition (CQ Press, 2008), p. 14.
[3] Garret Jones, "It's a cultural thing", in Christopher Andrew, Richard J. Aldrich and Wesley K. Wark (eds.), *Secret intelligence. A reader* (London and New York: Routledge, 2009), pp. 27-28.
[4] See https://www.cia.gov/kids-page/6-12th-grade/who-we-are-what-we-do/the-intelligence-cycle.html
[5] Jones, "It's a cultural thing".

[6] Andrei Cosmovici, *Psihologie generală* (Iaşi: Editura Polirom, 1996), p. 49.
[7] *Ibid*.
[8] Sheila Hayward, *Biopsihologie* (Bucureşti: Editura Tehnică, 1999), p. 73.
[9] Cosmovici, *Psihologie generală*, p. 50.
[10] *Ibid*.
[11] *Ibid*.
[12] Paul Chauchard, *La psychologie moderne de A à Z* (Paris: Centre d'Étude et de Promotion de la Lecture, 1971), p. 128.
[13] *Ibid*., p. 133.
[14] Hayward, *Biopsihologie*, p. 73.
[15] *Ibid*., p. 74.
[16] *Ibid*., p. 77.
[17] Betty Edwards, *Drawing on the Right Side of the Brain* (New York: Penguin Putnam Inc., 1999), p. 44, *apud* Mihaela Roco, *Creativitate şi inteligenţă emoţională* (Iaşi: Polirom, 2001), p. 53.
[18] Dominique Chalvin, *Utiliser tout son cerveau* (Paris: ESF, 1992), p. 39, *apud* Roco, *Creativitate şi inteligenţă*, p. 52.
[19] Paul Watzlawick, *Une logique de la communication* (Paris: Éditions du Seuil, 1983), *apud* Roco, *Creativitate şi inteligenţă*, p. 52.
[20] Roco, *Creativitate şi inteligenţă*, p. 52.
[21] *Ibid*., p. 44.
[22] Chauchard, *op. cit.*, p. 134.
[23] Chalvin, *Utiliser tout son cerveau*, pp. 36-37, *apud* Roco, *Creativitate şi inteligenţă*, p. 50.
[24] Chalvin, *Utliser tout son cerveau*, p. 118, apud Roco, *Creativitate şi inteligenţă*, p. 51.
[25] Hayward, *Biopsihologie*, p. 74.

Business Intelligence, a Company Profit Multiplier

Sergiu MEDAR*

Abstract

Business Intelligence is not a new concept in business. This concept started to prove itself as an excellent tool to enhance the profit of the companies. Business Intelligence can support the decision making process through a deep knowledge of the reality of the business environment as well with a realistic prognosis of the business future in the interested area.

Some of the current leaders of the economic organizations believe they already know how to catch and use some information in order to support their decisions. They are deeply wrong. The paper tries to explain the differences between "catch information" and "intelligence product support".

The concept is presented together with results belonging to USA companies.

In Romania Business Intelligence is a very new concept which started with much enthusiasm and with an unexpected success.

It is obvious that, for a long period of time from now on, the companies will carry out their activities against the background of economic and financial crises overlapping the process of globalisation.

The effect of these two simultaneous phenomena leads to the globalization of the crises and thus it becomes a major element of risk for the economic, and implicitly, financial development of companies. It is practically impossible for the development of companies, no matter how small they are, to remain untouched by the globalisation of crises,

Companies can no longer plan their activity without profound and professional understanding of all the elements necessary to manage a company in the decision-making process, among these elements being intelligence. The success, and sometimes even the survival of a company, depends on the quality of intelligence it acquires and which allows it to make correct decisions in an unpredictable environment in which the only predictable thing is its unpredictability.

There is a major difference between information and intelligence.

* PhD, Integrated Corporate Solutions

Information is a material often descriptive, not evaluated, which results from observation, discussions, reports, rumors or images. The pieces of information can be true or false, accurate or not, confirmed or not, real or fanciful.

Intelligence is a result of the collection, assessment and interpretation of the pieces of information. Intelligence is always checked using different sources, in a cross-check process.

The above definitions prove clearly that what companies need is intelligence and not information.

In fact, Robert Steel, the current vice-president of the Aspen Foundation, says that "information costs money...intelligence makes money".

The president of a company has said that he keeps gathering information and he is right since this is not intelligence.

Business Intelligence has two basic components:

- Competitive Intelligence (CI)
- Competitive Counter Intelligence (CCI)

The phrase "Business Intelligence" is often used with a limited meaning referring only to the IT processing and storing of commercial and financial information that a company holds. The "confiscation", on commercial purposes of this phrase by the IT companies, needs to be cleared up so that this concept to be well understood. The Romanian Business Intelligence Professionals Association considers that the phrase „Business Intelligence" (BI) means only "Intelligence for Business". The same point of view is shared by SCIP (Strategic and Competitive Intelligence Professionals).

Competitive Intelligence (CI) is the activity of defining, gathering, analyzing and disseminating intelligence products on clients, competitors and other aspects of business environment necessary to business decision makers to make strategic decisions.

If Competitive Intelligence means to get intelligence referring to the business environment a company is interested in, Competitive Counter Intelligence (CCI) means to ensure the security of a company against the competitors' attempts to get information which later is to be transformed into intelligence. CCI also deals with the physical security of a company: documents, personnel, IT systems (INFOSEC) and communications (COMSEC).

A company, in order to be successful, has to combine the two domains: Competitive Intelligence and Competitive Counter Intelligence.

In accordance with some evaluations, conducted by SCIP (Strategic and Competitive Intelligence Professionals) in the USA, between 65% - 85% of the big companies have a clear program of Business Intelligence. Among the companies that most successfully use Business Intelligence are: Motorola, Coca Cola, General Electric, Dell Computers, Merck, Procter and Gamble, General Motors.

According to the evaluations made by SCIP (vol.10, no.2, 2007):

- Procter & Gamble gained 40 million dollars a year, for the first five years, after they introduced a BI program.
- Motorola, relying on the intelligence provided by its BI department, bought a European company and the next years its profit was 10 million dollars.
- NutraSweet gained 50 million dollars, for five years, using a BI program on which it spent only about 450.000 dollars a year.
- NutraSweet also got 38 million dollars as, on the recommendation of its BI department, it did not join one of their competitors' initiative.
- Merck had a profit of 100 million dollars using, on the recommendation of its BI department, a certain sales policy for one of their products.

Unfortunately, most decision-makers of big companies are not interested in calculating accurately the profit obtained by their company as a result of putting into practice the BI solutions, being content to be permanently informed about the developments of the business environment they are interested in, the market trends, the main accomplishments and shortcomings of their competitors[1].

The leadership of the companies that do not do a hit-or-miss business consider that it is worth paying (even tens of thousands Euros) on a monthly, up-to-date, intelligence bulletin regarding a certain business domain or, from time to time, on a business research.

The Nutra Sweet CEO has declared that the BI program of the company helped him make better decisions, improve his strategic planning and make it more competitive and efficient, have successful products and services, contributed to the increase of their sales and also enabled him to identify new market opportunities[2].

On implementing a BI department in a company, the most difficult thing is to convince the company leadership that they need such a service. As soon as they become aware that this is necessary, BI becomes a multiplying factor of the company's performances. Thus, the leadership of a company will be able to identify:

- Market opportunities;
- Evaluate market niches;
- Current and future price trends and how prices are to be affected on a short or medium term by the economic and financial crisis;
- The impact of globalisation on a company;
- The impact of the political and security environment on one's own business;
- Future development of the political and security environment and its impact on one's own business;
- The impact of the competitors' ability of predicting the development of one's own business
- The current and foreseeable developments of the financial markets;
- The investment risk;
- The risk regarding the providers and their relationships with the competitors;
- The risk regarding the creditors and the evaluation of their current and future financial available funds;
- The risk of possible associations with other firms;
- The risk factor brought about by the appearance of new companies;
- The resources in one's own company;
- The specialized personnel on the market.

As far as CCI is concerned, a company will be able to improve its performances since there will be:

- An up-to-date security auditing;
- Programs and projects to ensure physical security;
- Programs to ensure a safe circulation of the company's sensitive documents;
- Assistance to implement modern methods of vetting when people are employed or promoted;
- Specialized training support for the staff in order to be able to protect themselves against the competitors' intelligence collecting attempts;

- Support for implementing protection methods for the IT systems;
- Support for implementing protection systems for the company's communications to prevent illegal access to its data and information from the company;

Douglas Bernhardt, president of a famous consulting company and expert in making big companies efficient, mentions in one of his books[3] that "strategy without intelligence isn't strategy, it's guessing".

In order to get the expected results from a Business Intelligence department the leadership of a company has to know some basic elements:

- In order to get the intelligence product referring to the Romanian business environment, it is advisable for a company to train its own personnel that is to plan, gather, process and analyze intelligence in order to hand the leadership the required product. The trained staff is certified.
- To get the intelligence products referring to investments, providers, competitors, financial markets etc. which are abroad a company has to sign a contract with a specialized firm with expertise in strategic intelligence and on this contractual basis to get a monthly intelligence bulletin and, on request, business reports on different issues. The company's decision makers should cooperate directly with this specialized firm.
- In order to implement a CCI position in a company it is advisable to set up a specialized department which is to propose the decision makers the measures to be taken to ensure the physical, personal, document, information, communications security.

Any decision maker who wants to set up a BI department in his company or to use a specialized firm for this has to have in view:

- Competitive Intelligence is not economic espionage. The former uses legal means to get information while the latter uses mainly illegal means;
- The quality of the final intelligence product depends on how accurate the request is made;
- The intelligence product can't provide everything the customer requires it can provide only the greatest part of the information required.

- The better accustomed the BI firm is with the activity of the company, the better it can anticipate the decision makers' needs;
- The relation between the organization leadership and the BI company is efficient only when this relationship is based on trust, otherwise, the cooperation comes to an end.
- Any BI activity is based on the existence or the setting up of a specialized IT system with a secured data base and a hierarchic access decided by the company leadership.

The existence, even on a low budget, of a BI department within a company with low budgets can grant the leadership of the company at least the comfort and self-confidence given by the fact that they will always be better informed than their competitors or associates.

Conclusions

The development of a BI Department in a company and a BI training of the company is very much depending on the leader.

If the President or CEO of the company is an open minded person he/she will be very much interested to understand the concept and to use it. I have seen leaders interested to have a training in this field by themselves. After such a training, they tried to build a BI department in their companies or they wanted to have a contract with a specialized company.

For intelligence professionals, business Intelligence, with less leverages but with more analytics, could be an exciting challenge.

References

[1] Jan P. Herring, "How Much is Your Competitive Intelligence Worth", SCIP, Vol. 10, No. 2, 2007.
[2] Jan P. Herring, "Create an Intelligence Program for Current and Future Needs", SCIP, Vol. 8, 2005.
[3] Douglas Bernhardt, *How to Acquire and Use Strategic Intelligence and Counter-Intelligence* (Financial Times management, November 30, 2003).

Romanian Entrepreneurs' Perception Regarding Security Culture

Ella Magdalena CIUPERCĂ*
Cristian Anghel CIUPERCĂ*

Abstract

Although the basic mission and challenges of intelligence have not changed, the profound transformation of the security environment in the recent years has led to a new view being shaped on security as a "common good". Therefore, ensuring security has become the responsibility of society as a whole, its effects concerning all citizens. In order to consolidate individual efforts to adjust to the specific needs of every national security paradigm, it is important to identify the mental map of each social category in terms of their social awareness and of their knowledge regarding national security. Because one of the key categories of every society is entrepreneurs, both in terms of their job but also in terms of the impact they have on how their employees use to interpret their environment, in this study we interviewed 35 managers to analyze their perceptions regarding security and intelligence specific issues, especially the factors they consider to affect the foundation of security culture among the citizens and the perception of vulnerabilities endangering the community.

Introduction

Although the mission and the fundamental challenges of the military intelligence have not changed since the days of Moses who ordered the Jews to spy the land of Canaan ("Who is the enemy?, Where is he?, What is he doing?"), the profound changes of the security environment in recent years[1] have led to a new vision of the nature of security, seen as a "common good" that should be ensured by the contribution of all citizens. Such a paradigm requires that each actor should turn into a "prosumer", who should serve both as a producer and a consumer of intelligence.

In order to make such a situation true every member of the community should have the necessary knowledge that makes him able to detect threats and risks to national security[2]. Therefore, their education must be a priority for the government of every state.

An educational policy is due to start from the pieces of information authorities have regarding the target population. While

* Associate Professor, "Mihai Viteazul" National Intelligence Academy
* Researcher, National Institute for Intelligence Studies, "Mihai Viteazul" National Intelligence Academy

a few social categories have been subjected for scientific knowledge, a very important one – the entrepreneurial field has been overlooked in terms of research.

Methodology

Therefore, we decided it is important to identify managers' perceptions on the security issues, to assess their level of understanding on the phenomenon, but also to make a review of perceptions on variables that shape citizens' current level of security culture.

In order to choose the appropriate method to investigate such subjects we rely on the knowledge that managers are people with a high level of expertise and understanding of the situation, but whose main characteristic is a severe lack of time and a desire to get a high profit out of every minute. Therefore, a questionnaire would not produce enlightening results. Moreover, pilot surveys based on a questionnaire conducted on a total of 10 cases revealed a tendency to give only schematic answers to the questions. Conversely, raising issues during the interview and asking questions with direct reference to managers' life history and personal experience allow the dismantling of very valuable information for understanding the issues at stake[3].

The interview guide that we used consists of 30 questions formulated so that the necessary knowledge would be provided and was applied between March-October 2011. The pieces of information provided by the subjects were relevant only insofar they illustrated real experiences and the subjective account of the caller. Therefore, answers will bear the seal of the subculture to which respondents belong and would be interpreted only in relation to a specific social context.

The subjects are managers of large companies, representative for the community. The premise was that companies with considerable economic scale have reasons to use security expertise and it is more likely to be informed regarding this problem (financial instruments field, pharmaceutical industry, chemical industry). The existence of such concerns is a reason to extend the research to a lower level. On the contrary, their absence induces a very high probability that such concerns are nonexistent in the medium or small business echelon.

The selected sample is a "chain" type: each interviewee was asked to recommend another entrepreneur willing to carry that discussion with the researcher. We chose this method because of the extremely difficult access to this category of individuals, less willing to cooperate

with the researcher in the absence of a request coming from someone they know. Recommendations proved to be almost an indispensable condition for the interview to be granted. Moreover, the recommendation of an acquaintance has the advantage of eliminating the feeling of insecurity and anxiety that the subject may have against a person who asks about personal views, especially as the person would have later no longer control on how they will be used.

The number of interviews was determined by the extent to which the obtained information was saturated: when the new interviews are only repeating the old ones having nothing new to say[4], we decided to finish the investigation. Thus we interviewed a total of 35 managers (7 women and 28 men), aged 30 to 60 years old, with activities carried out in different areas of economy and different social statuses according to level of education and the importance of the business.

We didn't explain the concepts of "security" and "intelligence" before the interviews as the main idea of the research was to find out how subjects were referring to such issues. But in spite of a frequent use of this terminology in everyday discourse of media and people, their answers revealed an approximated knowledge of the dimensions of concepts or even an extreme reductionism. Only a few subjects realized the polysemy that such terms subsume:

"*There is job security, work security, there is security of information or "Securitate" state body as it was understood during the communist regime." (S27-RI).*

Results and Discussion

In order to know the place security holds in the axiological and priority hierarchy of every manager, the subjects were asked about the social subsystem that would produce the most important changes in their business when something would change. Their answers were not uniform. Although the economical system was frequently indicated as the main provider of welfare for the business they run (25,7%), we expected even a higher percentage because this is an important source of welfare. Despite our expectations, most reviews were not referred to the economic sector, but focused, in different forms, to other areas of society. For example, the political subsystem is often iterated as a factor in the responses of managers (25,7%), being referred in various forms such as ideology, foreign policy, domestic policy. The social subsystem (20%) is also considered with reference to the mentality

of the majority, considered to be retrograde and a deceleration factor for business, but also in reference with opinion makers, surprisingly considered to be a risk variable.

Although uncommon, security has not been absent from the responses provided by managers (11,4%). It is true that opinions are pros and cons:

"Greatest significance is attributed to the economic field – a change of VAT tax... security being lowest ranked..." (S31-ZU)

For a large part of managers, the security of business is limited to computer security or the security and protection of the technology that each company incorporates:

"I think security (is important), because we work in an environment in which liquidities are not used much. What we deal with is a pile of sensitive data and most of the time we do not realize the effects that these data can produce if disclosed. Because you cannot feel, taste or smell them. The immaterial nature of information has direct effects on the way it is perceived. Security is very important! Money cannot produce such effect on business. The level of securing business in Romania is dependent on technology, but managers refuse to use it. We know how it should be done, but there is often a high strength to do that." (S35-VG)

Still, there are managers (8,5%) that consider that security is the most important area that allows private business continuity:

"Everything is connected. Changes in one area lead to changes in other areas ... But if we talk about conflicts, I think this is the worst situation ... the only thing we still have is the security of the state. Otherwise, economic crisis came, people are discontent with these prices and cuts, what to say about politics ... so I believe security should come first because everything else can be solved easier. Politics can change, the economic crisis can go, but security is more serious." (S33-SI)

Some managers have offered deep analysis of the security phenomenon in Romania, emphasizing also the way in which national interest is focused on:

"In the pharmaceutical industry, we do not normally think about what might affect national security... But I think that the withdrawal of producers from the Romanian market would be a big problem ... if things will continue like this with all the restriction and pressure on industry profitability... it can be ... I'm not saying we will go, but it is possible for others to decide they no longer want to be in this country. And while some drugs are unique and cannot

be replaced by other drugs, I see it as a threat to national security. There will be a number of patients who cannot be treated and I see it as a very dramatic situation." (S9-AC)

"I believe that macro security, national security would be the most important. After this it would be politics and politics can have influence on economic and social issues. It can make them raise or collapse. It is clear that a state of war suspends all normal economic activity. But, also, there are security related issues in time of peace – there are no businesses without credit. All businesses develop based exclusively on credit and loans and in Romania credit means 99.999% bank loan. Funding in the capital market is almost nonexistent in Romania. And when you want to get bank financing, the problem is that there are only two Romanian banks: CEC and Eximbank. When banks make an analysis of performance of the company, they say they need to secure their loan and ask you the list with representative customers, from whom you buy resources; in fact you have to tell them everything for free. Like this, they find out extensive information about the business or company. Apparently the aim is to secure their business – in fact, there are back-office sites of all banks operating in Romania. There, bit by bit, they dissect all economic activity taking place in Romania and send info to their countries. After that they base their investment decisions in Romania as they have all the information about Romania. And when 90% of all the banking system is foreign banks: Austrian, French, Italian, and Greek, and Israeli banks, in fact there is no economic secret for any of them.

What affects me? I have to face the fact that all these information reach the authorities of those countries. Those ministries firmly support businesses and economic interests of their companies so that they send to the interested companies the information they need for them to have competitive economic decisions in our country. And therefore, a company that has never developed any business in Romania, an Austrian or Italian or Greek or French or Israeli company, has instant access to all features of the Romanian economic environment. That company knows even the price I am selling a product with, who are the consumers and so on. For them it is easy to come to Romania and sell. And moreover they receive all these information without any cost. Because I am the one who pays for this study.

As a principle, there is a similar manner of working everywhere. But only in Romania, approx. 90% of the banking system has foreign capital. Of course that all companies are looking

for profits, but they are also protecting their national interest first of all and they hardly accept foreign companies. And they are transferring money and make payments inside their national banks. Otherwise when I find a good supplier they will instantly find about him, only because they have my bills... Well... if I go to CEC Bank this is a happy situation because the information no longer goes beyond." (S21-NS)

Another example that should be considered:

"Different aspects of national security have different places in a hierarchy. Some of them are determined by undertaking certain industries by foreign groups. That way we almost lost the cement industry, and then we lost the energy distribution... We're about to lose all the energy independence and energy production... and then we can talk about ownership transfers of strategic enterprises through stock and share market... Also terrorist activities can use the market and its instruments as money launderings tools. It is true that the Romanian market is too small to enter these flows of international money laundering, but it is possible." (S32-SA)

The counteracting of the mentioned problems is possible through: *"... Great political will and political awareness of national interest, economic interest, national identity... Solutions are known.... But there is a lack of will to apply the*m. (S21/NS), while other managers consider that: *"It's too late to find solutions... they sold everything ... even the supermarkets are foreign brands now. In France you can see Carrefour at every street corner, not Metro. In the Netherlands they have only local shops, money are circulated inside the country..." (S33-SI)*

The situation of national security is primarily determined by the security culture of each member of society. Therefore, authorities should consider a strategic approach aimed to implement the security culture in Romania.

Being questioned regarding the variables that can influence the security culture, subjects most frequently spotted the common people's quality of life, which is considered to be the main responsible for the lack of people interest for security issues:

"The troubled and the poor are concerned with anything else than security culture. Wealthy people who have something to lose are the ones thinking about safety issues. I think this is the link ... but we must get more documentation to get a conclusion... You took me by surprise." (S7-CI)

"From leisure to extra job activities, when you have a good quality of life you do not have the same worries as the others. It is typical for any person. When someone managed to accumulate some savings he is thinking of investment, while a poor man struggles to pay daily bills. People think of immediate needs. Security does not seem to be an immediate need. Immediate needs are related to food, children's education. When the standard of living increases, then security becomes an issue." (S32-SA)

"The higher is the standard of living, the better. A poor man has nothing to secure, what should he secure, the food of his children? Conversely, if a person or a company has a certain level of wealth it needs security, because without it they would not be able to maintain their standards." (S2-DB)

"When a community lacks the necessary minimum, it's hard to believe it thinks of safety culture. When the standard of living is higher you may find at least a 10% that have the time or inclination or training to do so. Some poor people may not even understand what this means." (S25-SB)

Therefore the low interest of common Romanian people to understand security issues is considered to be a consequence of low living standards of the Romanian communities. The aggregation of managers' opinions indicated a score of 4.40 for community poverty on a scale of 1 to 10.

Still, some managers identify a different connection between security and the standard of living.

"When the standard of living is higher, the level of civic education is higher. I do not mean Americans although I was thinking to them first, because that's where I acquired a model that population can be educated on safety rules and can react very well and very quickly. But I was impressed by the Japanese – a disciplined educated people that know how to react to an unusual situation. And they are those who have the highest standard of life. ***In fact, their security culture is responsible for their living standards because 50 years ago they were so poor! It's an important relationship! It just occurred to me! It is the opposite of what one would usually say, but this is it****." (S20-MN)*

"Yes, definitely, it is linked with what we use to name as sustainable development: as long as we have economic activities and make business with Romanian companies, the community wealth remains in the community. Therefore a high safety culture leads to higher living standards." (S21-NS)

"Definitely, there is a link between the standard of living and their security system. But I do not know which one was the first: the egg or the chicken." (S10-TK)

"But, of course, physical misery generates moral misery and moral misery generates physical misery. The existence of a strong security culture generates a better life, but it is just contributing as there are many other variables. What is its percentage... I cannot say without research." (S5-BR)

Education is considered also responsible for the developing of the safety culture, in a comparable extent:

"...An educated person has at least a vague idea about security culture." (S32-SA)

...although most of the answers refer to the disastrous situation of the education in Romania, which is criticized because of its incapacity to produce specialists able to work according the needs of the economy:

"Everything begins with school... My parents thought the child must learn. And now all are bachelor graduated. The other day I was watching a commercial for Spiru Haret University and I swell laughter: "School is not what it was; now it's better!" What nonsense! There is no school ... there is no education, no practical abilities; they cannot even knock a nail. They are leaving school ignorant... There are two important things that were destroyed in the last 20 years: education and health. Without them... these kids should look after me and pay my allowance. Do you have any kind of expectations from them?" (S5-BR)

"People have more and more degrees, but no deep knowledge, so they live better than they think anyway... we have very good people, and very weak people. Moreover, after the Revolution, 7000 colleges with many graduates cannot find jobs in this market. Elsewhere, the state invests in a person and after that it squeezes value. But we train doctors, engineers, architects, but do not know what to do with them. And so they go with all the investment." (S2-DB)

"I have nobody to hire. These faculties are supposedly to be technical, but all subjects are theoretical, they have no idea about anything when they come to work... I am overwhelmed and cannot delegate because I do not find any business specialist..." (S26-PF)

"As long as they do not know their rights they cannot protect them. We, as a country, are vulnerable and our level of knowledge is very low. Therefore a better culture would provide a better living standard" (S14-GI)

On the other hand, the positive impact of a proper education is recognized:

"... If they had a bit of culture and state cared for people it should be different. At the end of 2007 year I refuse to give my employees any certificates for loans, especially mortgages. I explained that why: you have a salary of 800 RON and you have to pay bills, the usual cost of life and a credit. But if the bank increases rates, what will you do? I may go bankrupt, but you may lose your house! And then you will come to me to ask for more. I have two options: to pay you or to dismiss you, which is even worse for you ... They were upset, but now they come and thank me ... just like that I tried to make a financial culture for them. But I didn't think of security culture, mainly because it did not affect me directly, but would equally have beneficial results." (S33-SI)

"... We have a habit when changing the mayor or councilors and so on... we take them in a tour of the factory, explain its specifics, we are polite and ask them what we can come up for the community and then tell them what needs we have... We know that those who run the community should understand our specific and they will be more attentive and prepared - we invite them to our training exercises, fire brigade, civil defense and simulations of fire, explosion. How could they know about all these if nobody tells them?" (S1-BI)

"A serious accident can force us to look with the desire to know how to avoid it next time. That would affect positively in terms of security needs. Otherwise, if "it works everyday" it's unlikely that anything will change." (S20-MN)

In an attempt to explain why Romanian firms do not try to solve some of the problems they face and to manage issues that affect them involving in activities aiming to improve the safety culture, managers refers to a situation somewhat paradoxical: firms that are involved in civic and community activities come to be perceived negatively, perhaps because of a still communist mentality:

"In Romania, Petrom has a lot of money and can invest, but it doesn't do it because it would be perceived differently, as related to activities specific to the former Securitate state body. I had a huge surprise in Russia when talking with someone from the presidential area, I was told "Well, we do not understand you, to us it's not like this - why do you blame "the Securitate"? Here, these employees are considered heroes and treated as such by society. Not that we did not have the political police or people who profited from the position they had. But anyway, those were a few in total. But the others are

considered heroes because they put their life and family in the service of ensuring state security!" Then I was thinking they were right even when they had had even worse practices than ours. But their culture was built differently. Our culture was destroyed by politicians who wanted to destroy it at all costs. Now you avoid saying you work for a secret service because you may be wrongly perceived." (S32-SA)

"Looking back, it is clear that the destruction of safety culture was a terrible thing. Companies involving in strengthening safety culture would be more likely to have strong effects abroad. The main reason why I am not doing this is that the perception of the community is not very favorable to such issues. It is much better to say that you fight for the environment, for children. So the very lack of safety culture block these actions. It's a vicious circle." (S17-RC)

An unexpected variable that shapes security culture – age – was invoked by some of the managers (42,8%), though their opinions are contradictory and perhaps a new research is needed to clarify this issue:

"Age is significant for the level of security culture. As you grow older, you start to think more and more of the need for safety and security. Therefore, such an educational programme should be started with the older people, as they are the most likely to take on responsibilities. A young person will not have such problems. He is planning to raise money to buy a house, a car, he doesn't care about security. Only after 30 years old one begins to have such worries." (S32-SA)

"It's difficult to convince the elders as they are influenced by the past. The youth are likely to be more concerned." (S24-LM)

The job of a person was also an expected variable invoked by managers:

"In fact, a farmer would not be interested in security issues... there are areas that, at least at first glance, do not need it. But an agricultural enterprise with hundreds of employees, that applies innovative technologies, would need it." (S32-SA)

"Someone who works in a bank but is unaware of document security regulations may represent a problem. All jobs require a minimum of knowledge in this area; therefore all jobs should become part of a global security protection scheme." (S9-AC)

Some of the family characteristics (such as the number of children or the specific of socialization) are also considered important for the way people evaluate security issues:

"The number of children matter because it involves responsibilities and also a different strategy comparing to what you had before." (S32-SA)

"Family environment matters. If the family was interested in such issues... or you had peers that talked about this..." (S4-VN)

Another pointed variable consists in deficiency of collective mentality that should be influenced in the desired direction:

"If the state creates a system with clear laws... when everybody is acting correctly the system will perpetuate. When you see your father acting in a way you will do the same. Good or bad." (S11-DP)

"Perhaps the influence of the media is too high. Especially poor people use to say "It is true! I heard on TV!". We had a public relations officer which was prepared to talk to press to tell them our realities not what they imagine to be." (S1-BI)

"In small towns there is still a fear of authorities, the mentality is totally different. Including what people think about public order and security... in a big city you can hardly influence." (S2-DB)

Conclusions

The present empirical approach has as a fundamental premise that the security culture of Romanian entrepreneurs has low amplitude and, consequently, the effects that its existence should produce are nonexistent. The objective of this research is to assess the level of managers' involvement in the development of security culture of their employees and of the members of the community to which they belong.

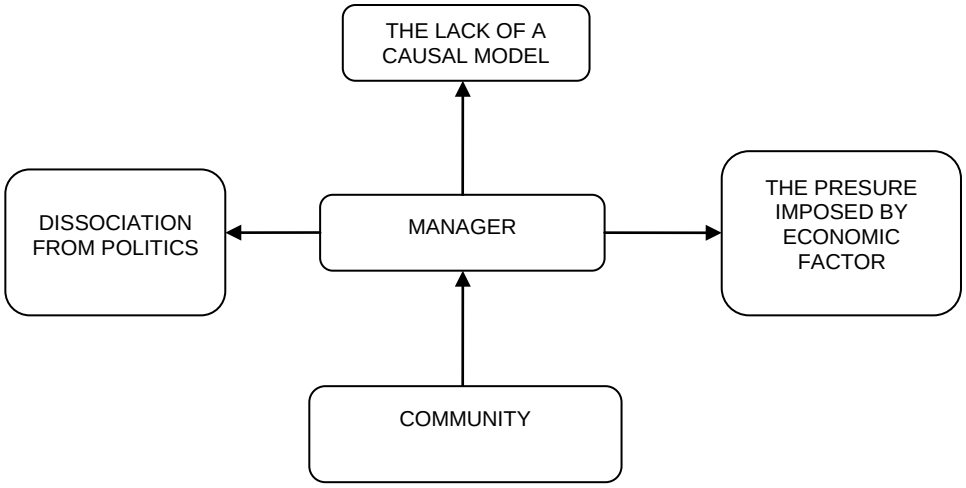
The answers show that only a few managers really know the problems the communities to which they are belonging face. Their responses invoked general problems of our country such as poverty, unemployment and low skilled jobs. They also show a lack of interest which can be explained by economic pressure, the pursuit of profit accumulation, the need and the desire to survive in a harsh and unpredictable market economy.

A significant number of managers consider that economic factors are the only ones that matter. The political factor is mentioned as having some influence, but they almost ignored other factors (e.g. social, cultural), which shows an immaturity to identify connections between different factors. The lack of a causal model of factors that act synergically may justify entrepreneurs' indulgence towards community issues.

Summarizing, we can say that the three indicators (dissociation of the political factor, the pressure of the economic

factor, the lack of a causal model) induce a passive behavior of managers regarding involvement in community to which they belong.

Although there may be other factors of influence, the most striking seem to be:



These dimensions of managers' perception are extremely important in drafting effective measures aiming to improve the situation and to design awareness and educational effective programs.

References

[1] Buzan B., *Popoarele, statele şi teama (*Chişinau: Editura Cartier, 2002).

[2] Donovan L.A., "Citizens as Intelligence Volunteers: The Impact of Value Structures", *International Journal of Intelligence and CounterIntelligence,* Vol. 18, 2005, pp. 239-245.

[3] Bailey K. D., *Methods of Social Research*, 2nd edition (New York: The Free Press, 1978).

[4] Chelcea S., *Metodologia cercetării sociologice. Metode cantitative şi calitative,* 2nd edition (Bucureşti: Editura Economică, 2004).

National Security and Intelligence[1]

Antonella Colonna VILASI*

Abstract

After the end of the Cold War and the fall of the Berlin Wall in 1989 the international system is in a continuous and turbulent transformation. The national system itself no longer exists. Not as a part of the international one. The old-style concepts cannot fully represent our contemporary world any more.

The idea of National security refers to a Nation not only perceived under an ethnic profile, but in its broadest sense: defense of the state as a center of attribution of political, economic, social and cultural rights. In the past centuries the only priority was the defence against external threats, apart from maintaining the internal order. However, with international relations increasingly complex, the concept of national security extends and involves activities, citizens and their tangible and intangible assets, culture and cultural identity. Modern nations need to foster intelligence power, due to the evidence that the possession of information, and its control, constitutes a security factor. Furthermore, the formulation and definition of a concrete "national interest" is of utmost importance in policy and strategy.

Without a stable policy it is not possible to have an appropriate national safety system, and without clear objectives the same cannot be ruled at its best. Nations must therefore hunt for other Nations' information, prevent "enemies" from acquiring sensible information and try to keep an information advantage in order to protect their national interests. It could seem a Machiavellian statement, but that is how it works. The advantage can take different forms, ranging from the knowledge of the vulnerability of the adversary, to the knowledge of political intentions, up to the definition of objectives and goals. as in poker or chess, it is important to understand the game without revealing information to your opponent.

Information processing is the fundamental imperative of security. National security is a concept that refers to the idea of nation not only perceived under an ethnic profile, but in its broadest sense: defense of the state as a center of attribution of political, economic, social and cultural rights.

According to an obsolete view of state security, typical of an old constitutional doctrine, the only priorities were the defense against external threats and maintaining internal order.

*President of the Rome-based Centro Studi 'Inteligence, Scienze strategiche e Sicurezza' (Research Center on Intelligence, Strategic Studies and Security)

However, with current international relations increasingly complex, the concept of national security extends and involves also all the activities of a country, the people and their tangible and intangible assets, culture and cultural identity.

Modern nations need an improvement of intelligence agencies forcefulness, due to the evidence that the possession of information, and their control, is a security factor. Furthermore, the research, formulation and definition of a concrete “national interest” is crucial in establishing possible choices in policy and strategy as far as the concept of security is concerned.

Without a clear policy it is not possible to have an appropriate national safety system, and without clear objectives the system itself cannot be ruled at its best.

Nations must therefore hunt for other's Nations information, prevent “enemies” from acquiring sensible information and, if necessary, try to keep an information advantage in order to protect their national interests. It could seem a Machiavellian statement, but that is how it works.

This advantage, in fact, can take different forms, ranging from the knowledge of the vulnerability of the potential adversary, to the knowledge of their political intentions, up to the definition of their objectives and goals to be pursued.

As in poker or chess, it is important to understand the game without revealing information to your opponent.

In this context, the activities of world intelligence agencies are similar in their aims, (the military defense of the State) a priority since the beginning of the concept of national security.

Priorities are also the integrity of the country and the organization of the same. To reach such a definition we must take into consideration the national territory and the exclusive economic zone, public and private institutions, people and goods, nationals and their goods abroad, the economic, social and all lines and areas of supply of strategic materials, without any geographical limitation; global economic interests, the financial situation, focusing attention primarily, though not exclusively, to the geopolitical area of main interest.

Once you have defined national interests, therefore, you should be capable of defining implicitly those limits concerning national security and, therefore, restrict the objectives of our

research. In this way, through the definition of national interest we can describe those parameters related to the term “national security information” and its objectives.

Intelligence agencies tasks are focused on assuring safety, tending to the satisfaction of the information needs of the Nation (research-espionage) and the maintenance of a suitable defense, in order to protect the country from any kind of threat and risk (counterintelligence), with particular emphasis to all operations aimed at maintaining its defensive potential.

The political nature and purpose of the intelligence system, indeed, determine the kind of activities of such National agency and also the function of unconventional assets used in order to protect the Nation from dangers.

Clearly, the objective criterion of legality as strict observance of the law cannot suit to intelligence agencies. Only a criterion of conformity and adherence to government legitimate purposes can be reached, as determined by the Government in accordance with constitutional procedures.

The activities aimed at the defense of the Nation are: the research carried out by state organizations, by criminal organizations and, nowadays, even by private companies.

A valid national security should focus on the analysis of threats, thus assigning objectives and tasks to national intelligence agency, with counterintelligence and defense function, and most important, in order to identify “enemies” research and espionage areas of interest.

Threats to state sovereignty are various: real or potential. And that can be summarized in three types:

- threats to homeland security;
- threats to the stability of the Nation;
- threats to national interests.

The classic form of threat, until the Second World War and for a good part of the Cold War, was the threat to „ homeland security”.

The territory has always been the reason for disputes between States, from dynastic wars to colonial expansion and conquests.

The strategy adopted was a military classical approach. Opposing armies clashed in order to control and dominate the territory. Nowadays in our new international scenario we must face

a meta-real situation, which implies a multi-level threat. It is then necessary to develop new concepts of war, related to the world of computer science and new technologies: softwar, netwar or cyberwar, that putting aside the concept of territory and physical strength, insists on the capability of information technology in multiplying the threats. Military threat is always an element of potential danger but of lesser relevance.

The second type of threat is referred to the stability of the Nation. The so-called "unorthodox threat", completely different to the concept of traditional warfare, indicates internal or external threats designed to subvert the political and legal order.

The third form, not less dangerous, is the threat to national interests through economic menaces, proportionally inverse to the potential and capacity of economic systems, banking and finance.

The last two forms of attacks, unorthodox threat and economic threat, can be defined as "surrogate war"; conducted through offensive strategies, coordinated or not with the military classic instrument. Surrogate war includes: espionage, sabotage, subversion, terrorism, guerrilla warfare, interference, propaganda, influence, separatism and disinformation (unorthodox threat). Economic threats include: illegal trade, technology transfer, economic penetration.

Once identified all threats, we can define the "defence potential" of the Nation, which is the set of resources, production capability, organization, spiritual and immaterial assets of a Nation.

Objectives are therefore all economic resources, energetic, industrial, mining and farming, in particular industrial, transport and commercial and, last but not least, the spiritual potential seen as intellectual, cultural, social, scientific and political treasure of the Nation.

After the end of the Cold War and the fall of Berlin Wall in 1989 the international system is in continuous and turbulent transformation. The national system itself no longer exists. If not as a part of the international one. The old-style elements are skipped, or at least not capable to fully represent our contemporary world any longer. How Rosenau says[2]: "Politics is not international any more, but postinternational." A policy that no longer acts only between "nations", but rather among subsystems, a "turbulent" policy, with one major characteristic: uncertainty. Political turbulence implies a change of parameters, the system boundaries are no longer able to contain the fluctuations of the variables. Turbulence, just as in physics where it refers to fluids, is a flow regime characterized

by stochastic changes, and random properties. It is unstable, with random movements. Even today's computing system is defenseless before the irregular motion of fluids, if you do not fully calculate every possible variable. Nature is irregular, but the degree of irregularity remains constant at different scales, is "fractal". This can suit to many fields. Structural parameter in transformation is marked by "bifurcation": this means that a tiny change in the parameter values of a system causes a sudden change in "quality". In other words, this means that "state-centric" world currently coexists with a "multi- centric" one, equally powerful, though more decentralized. Systemic interdependencies make the international system so complex, turbulent and "chaotic" to warrant a new look. The international system coevolves with society and is then sensitive to events of feeble importance which may have serious consequences. Such a new world should be interpreted with a "systems" approach, or holistic approach. Consequently, we must almost abandon exclusive linear and Cartesian approaches, that are nowadays obsolete. Uncertainty is today the rule. The so-called unexpected events become common cases, the faults are normal and minor accidents give rise to serious consequences. In complex systems, in fact, interactions cannot be provided separately from the "action" of each factor; and strategies depend on the strategies of others. The only way to master change and win such turbulence is the capability of learning and fitting to new situations. This requires analytical skills, intelligence, forecasting and planning/programming, in a word, strategic analysis capabilities. In order to analyze such a mobile and dynamic system, it is necessary the updating of all methodological tools at reach. The causal principle is in crisis. The causal determination principle is not the only one available in helping you to determine the right decision. Among these methods, or categories, there are three priorities: interaction (or causal connection between them, or functional interdependence), a statistical approach (in other words the final result by the joint action of independent entities, or quasi-independent), and an holistic structural determination (with a global effect). In other words the quasi-denial of Cartesian way of thinking and the assessment of a systemic principle. Only a systemic approach, in fact, can help us in understanding the context in which each problem develops and each solution should be pursued. It is therefore important to refer to the theory of chaos and complexity. Complexity is "order", organization, complexus, woven together.

Chaotic systems behavior appears "random", but is actually "deterministic" in the sense that their future dynamics is defined by their initial conditions. Thousands of years ago echoed the teachings of Hermes Trismegistus, the Thrice Great: "*For every cause an effect and every effect has its cause; everything happens in accordance with law. The case is just the name we give to the unknown. Many are the plans of reason but nothing escapes the Law*".

It is mathematically demonstrated that even a very simple nonlinear system can behave in a complicated way.

Therefore we cannot analyze a complex system like that of the world in the era of globalization with simple linear coordinates. It is necessary to refer to such complexity taking into account the interaction between systems.

The laws thus obtained will be more "conditional", and "probability" could allow a high degree of predictability.

In short, we must have an approach based on the **complexity of social systems**, taken as constantly in a learning phase, a sort of reaction, adaptation and change even in a stable situation.

The "forks" mentioned by Rosenau are part of the complexity theory. Stability and instability are equivalent. And the more complex a system, the more disturbances, noise and fluctuations would threaten systemic stability.

Obviously, stability depends on the amount of disturbance, its magnitude, and is connected to the sensitivity of the system. It is the so called "butterfly effect" that makes a precise forecast impossible.

The mechanistic Cartesian and Newtonian view and linearity cannot tackle complexity. In fact, if you still want to manage complex processes with old tools you should abandon policy, which is the art of managing complexity and drive change.

Social systems are open systems, there are no mechanisms or structures. Their subsystems are related with an internal link to each other, not an external one.

The only form of control that can be exercised over them is macroscopic, through an influence on systemic parameters, and not with a microscopic one, exerting control over subsystems.

In nowadays world, in which we live, whose future will most likely not adjust to our expectations, intelligence and strategic warning intelligence are a precondition for security. Until a few years ago, intelligence was able to let us know the capabilities of the enemy, its material means of power. Today the effort to understand its history, its culture, its psychology, its intentions is a priority.

The enemy is often invisible, its structure, the product of globalization processes, is now “snap” and “ubiquitous”: nothing to do with the traditional organizations.

The selection of countermeasures depends on the speed with which dangers and threats are identified and the choice of the appropriate action is undertaken.

The analysis of a strategic situation and its development, and the evaluation of risks and opportunities are, moreover, the functional definition and pursuit of national interests, as well as crisis management.

Analysis begins with intelligence data, but it is aimed at elaborating forecasts. Intelligence, in short, is the functional activity of prediction, subsequent to its planning activity. Indeed, one can argue that there is no intelligence without foresight, and without forecasting.

Intelligence worldwide failures are due to a lack of knowledge in history, culture, psychology and of the geopolitics and geo-strategy in the areas observed. An obvious default if compared to the knowledge that our “enemies” have of our culture and society.

The intelligence process is developed into three different and complementary phases: description, explanation and prediction. The purpose of intelligence, such as science, is then to predict the future in order to control the environment in any way we consider it.

While science operates with a nomothetic approach and tries to reach a general and universal rule, intelligence analysis should use an idiographic and analytical approach, with a special attention to the knowledge of the particular.

The particular can turn into the universal.

The intelligence cycle is carried out through various analysis steps that follow a scientific method:

- assignment;
- collection;
- evaluation;
- classification;
- collation;
- analysis;
- prediction;
- dissemination.

Intelligence, both in gathering secret information and in providing all-source assessment, remains pivotal to estimating threats and risks, and to policy-making at national and international level. In the case of intelligence analysis, deception is the rule; the validity

of the data is always uncertain. Moreover, intelligence analysts are specifically trained to take deception into account as part of the process. Analysis is both a process and a collection of specific techniques. Analysis is an action that incorporates a variety of tools to solve a problem. Different analytic methods can offer different analytic tasks.

The analytic process is a construction of the human mind and is significantly different from individual to individual, or from group to group. Intelligence analysis is art, tradecraft, and science. There are specific tools and techniques to help perform the tasks, but, in the end, it is left to individuals to use their best judgment in making decisions. Clearly, intelligence moves from collection to analysis, as the Intelligence Cycle holds. The job of the analyst is, in part, to evaluate raw material and put it in perspective. In order to analyze the data, the analyst compares the new material with the existing data base and previous analysis.

Intelligence collection and intelligence analysis are operating in parallel rather than sequentially. In the final stages of the Intelligence Cycle, finished intelligence is supposed to be delivered to policy (the so called "dissemination" step). Estimates are a forecast of the future which decision makers can use to build policy, just as the Intelligence Cycle proposes.

Conclusions

The only way to master change and tackle international turbulence is the capability of learning and fitting to new situations. This requires analytical skills, intelligence, forecasting and planning/programming, in a word, strategic analysis capabilities. In order to analyze such a mobile and dynamic system it is necessary the continuous updating of all methodological tools at disposal.

References

[1] This text is taken from the author's publication: *Handbook of intelligence studies* (Città del Sole Publisher, 2011), pp. 20-29.

[2] James N. Rosenau, *Turbulence in world politics: a theory of change and continuity* (Princeton: Princeton University Press, 1990).