Editors

Niculae IANCU   Irena CHIRU

INTELLIGENCE
IN THE KNOWLEDGE SOCIETY

Proceedings of the XX^th International Conference

EDITURA
ANIMV

Bucharest – 2015

Editura Academiei Naţionale de Informaţii *„Mihai Viteazul”*
Telefon: 021 4106550/1172,1204,1186
Fax: 0213104714

Bun de tipar:09.10.2015 *Apărut: octombrie 2015*
Tipărit sub comanda nr. NS9021481/01.10.2015

EDITURA
ANIMV

ISSN 2392 – 7542

PROCEEDINGS
# of the XXth International Conference
INTELLIGENCE IN THE KNOWLEDGE SOCIETY 2014
TABLE OF CONTENTS

PERSPECTIVES ON STRATEGIC INTELLIGENCE

SECURITY TODAY: NEW DRIVERS, CHALLENGES, AND OPPORTUNITIES

Foreword

The *Intelligence in the Knowledge Society* International Conference (IKS), taking place every autumn in Bucharest, under the aegis of the “Mihai Viteazul” National Intelligence Academy, has become a genuine landmark for the evolution of intelligence and security studies in this part of Europe.

Its purpose of developing a transnational, multi- and interdisciplinary network of scholars, practitioners and experts coming from the private and governmental milieu has been partially attained, as one can notice from the heterogeneous nature of the participants that have made us the honor of putting forward their valuable perspectives during the 2014 edition of the event.

But there is still much work to be done in order to frame some of the puzzles and mysteries that make up the emergent field of security and intelligence studies. Moreover, paradoxically, as more knowledge about the field is collected and shared, the more questions seem to be arising, and the need to transparently debate key questions becomes more and more stringent. That is why events such as our Conference, turn into “intelligence hubs”, contexts within which the gap between intelligence services and external experts is being narrowed, as the two parts consolidate a fruitful long-term relationship, based on mutual trust and the transfer of know-how.

The 20th edition of the Conference has dealt with two main subjects: 1) *the re-conceptualization of security and 2) strategic intelligence.*

Thus, the debates focused on one hand, on how to efficiently integrate the different dimensions of security at national, regional and international level, capitalizing on both academic and practitioners’ expertise in order to envision a shared understanding of existing and potential future threats. The new drivers of change in the social, legal, technological, economic and political fields have opened up the practice of security organizations towards new skills and instruments which need to be shared and build into a common body of knowledge across disciplines.

On the other hand, the participants to the debates tried to find answers to questions such as how to define strategic intelligence? How is the strategic intelligence produced by national security institutions different from the one produced in the private sector? Which are the best analysis methods to produce strategic intelligence? Is strategic intelligence influenced by national cultures and most importantly are there any blueprints to be used in building national intelligence systems?

Though, in most cases no consensus has been reached, the discussions opened up many pathways that could and will be explored in the coming events. This volume integrates some of the valuable academic papers delivered during the event, and the publishing of the conference's proceedings represents our contribution to building up an intelligence theory. It is also an important step towards consolidating a Romanian intelligence culture, as it shades a glimpse of light upon the controversial world of intelligence and its role within the democratic societies faced with an ever-growing uncertainty.

We dedicate the current volume both to intelligence practitioners, but also to the intelligence stakeholders: scholars and researchers, decision-makers, representatives of the private sector and non-governmental organizations, and to all citizens that might be interested in knowing more about the topics related to intelligence and security studies.

The editors

PERSPECTIVES ON STRATEGIC INTELLIGENCE

Starting with Sherman Kent's famous book Strategic Intelligence for American World Policy published in 1949 the topic of strategic intelligence has constantly been a subject of intense debate. In the intervening years the literature on strategic intelligence has grown exponentially. Nowadays, in a time when decision-makers are constantly put under pressure to produce viable and innovative strategies to counter the multiplicity of challenges encountered both at state and organizational level, a new awareness takes shape regarding the critical role of intelligence in strategy formulation. Consequently, a whole array of questions arise dealing with topics such as how to define strategic intelligence? How is the strategic intelligence produced by national security institutions different from the one produced in the private sector? Which are the best analysis methods to produce strategic intelligence? Is strategic intelligence influenced by national cultures and most importantly are there any blueprints to be used in building national intelligence systems? The reform of the intelligence enterprise as well as the reshaping of its mission and goals in the last decades has deeply influenced the study of strategic intelligence by opening up new debates on issues concerning strategic intelligence priorities, integration, products, customers as well as its overall role in supporting decision-making.

COMPETITIVE INTELLIGENCE IN THE PUBLIC SECTOR?

Marius MITRUŞ[*]

Abstract

The purpose of this paper is to question whether or not competitive intelligence can be implemented in public sector organizations. Even though the concept of competitive intelligence has a widely spread acceptance and a fair utilisation in the private sector, implementing it in public sector organizations seemed, for a long time, „mission impossible", due to specific constraints. The shift of paradigm, by setting the public sector on the road to good governance, involves better connecting with the needs of the general public using, more often, advanced or new techniques (e.g.: the internet), as well as implementing the general concept of competition in the governmental area. In the following paper we will try to demonstrate that the main objectives of a public organisation can more easily be achieved by using C.I. techniques.

Keywords: competitive intelligence, public sector organizations, C.I. practitioner, innovation, good governance

Not very often one can find the term „competitive intelligence" (C.I.) associated with the decision making process in public organisations and, for sure, the limited amount of scholar by articles addressing this topic could lead us to mistakenly believe that the correlation, into practice, of the two notions it is very unlikely to occur.

Therefore, the question mark in the title is intended to raise the debate not just on the necessity of competitive intelligence activities in public organisations, but also on the possibility of a real and effective implementation in the public sector.

Taking this into consideration, first of all we must define the notions that we are trying to associate in this paper, as follows: „Competitive intelligence" is, commonly accepted, as „the action of

[*] Strategy advisor, National Bank of Romania.

defining, gathering, analysing and distributing intelligence about products, customers, competitors and any aspect of the environment needed to support executives and managers making strategic decisions for an organisation."[1]

One of the main functions of C.I. is that of early warning about the changes (risks and vulnerabilities) of the environment in which the organization is acting, and providing the decision makers with real, valuable and trusting data, in order to better sustain the tactical or strategic decisions, that make the company more competitive to its entire environment and stakeholders.

C.I. is also used by major companies as a method for finding new opportunities and trends[2], for competitive benchmarking and to test their strategies against market response.

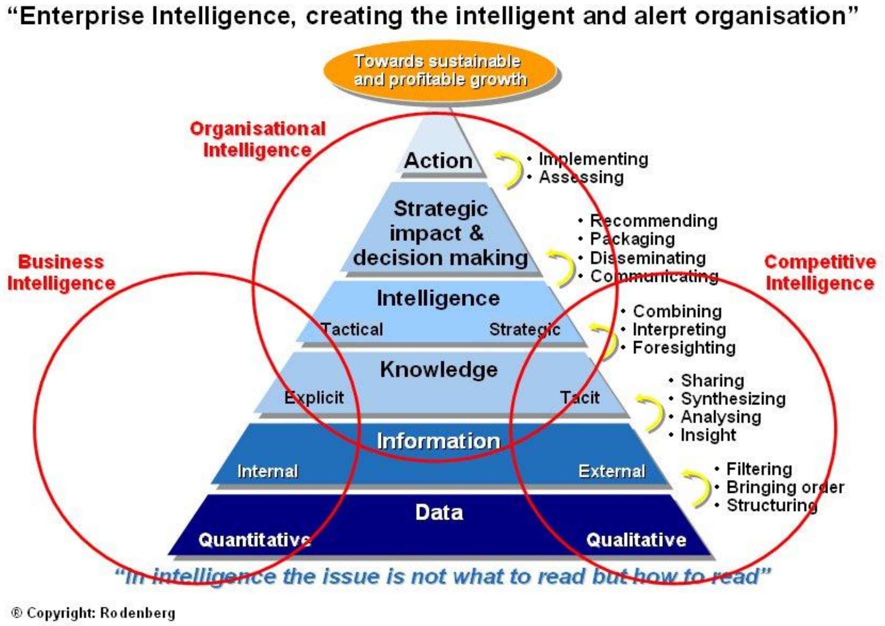


Figure 1: Enterprise intelligence, creating the intelligent and alert organization
(Source: http://www.rodenberg.nl/publications/rechts13-1.php)

The public sector „consists of governments and all publicly controlled or publicly funded agencies, enterprises and other entities that deliver public programs, goods or services"[3].

In order to understand the paradox of implementing, in publicly controlled organisations, C.I. procedures and activities – which were by default created and are custom tailored to improve the competitive advantage of a private business, it is useful to analyse what are the objectives, as part of a strategy and in accordance to a specific mission, that can be achieved by a public organisation using C.I. techniques.

If we accept that a public organisation's main mission is to provide good governance by delivering programs, goods and services to the general public and private sector, undoubtedly we can state that the quality of this outcome can be constantly improved. One of the ways of achieving this legitimate goal is by becoming more aware of and connected to the real needs of the final beneficiaries (people and companies) that it serves, thus for upgrading the decision making process and becoming more cost efficient. So, in large terms, better serving the public interest with less budgetary spending should be the basic paradigm of the public sector organisations and one of the main criteria of grounds the use of C.I. techniques, which have already proven their effectiveness in the private sector.

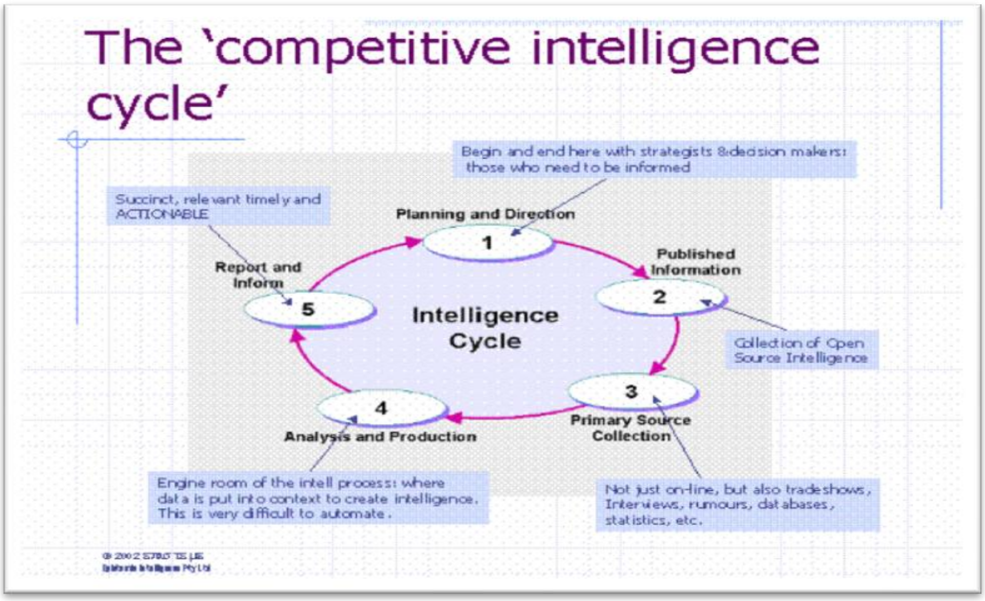
A more complex approach grounds the necessity of driving the public sector organisations towards achieving what is called the invisible component of the strategy – the competitive advantage, seen as providing services that differentiates itself through their qualities from similar products offered by others or by the most competitors[4].

From this view point, the main task is to implement the general concept of competition in the governmental area seen, too many times, as paradoxical by public authorities. Although good governance is often statistically measured by comparison with the specific indicators (GDP, inflation, unemployment, etc.) of other countries and thus – even though the choice of changing the „service", by changing the government, occurs, usually, at a pre-established fixed period and it is not a strictly an individual choice – one of the main assets of an organisation, private or public, can be radically affected if one country's governance is positioned below the average of the region, which can be abstractive seen as the „market" on which each country („competitor") is activating.

In fact, at least two other categories of competition appear as relevant for the public organisations[5]:

- Competition for funding (internal and external). For example, the issuing by the Finance authority of treasury or sovereign bonds is influenced by competition with other investment opportunities or with similar public organisations from different countries.
- Competition for personnel. In a free workforce market, both public and private companies compete for attracting and retaining skilled personnel.

The C.I. unit and the C.I. practitioners have the clear primary objective of identifying the competitors as well as establishing what will generate the competitive advantage for the public organisation. One of the main sources of competitive advantage is reckoned to be innovation[6], defined by Schumpeter as „emergence of a new service, introduction of new management methods, and generation of a new form of organisation." In this context, how can a public organisation better adapt to social demand/need, improve the goods/programmes/services it provides and become a stronger competitor, even in terms of reputation, than by formally adopting a set of C.I. procedures?



The 'competitive intelligence cycle'

Begin and end here with strategists &decision makers: those who need to be informed

Succinct, relevant timely and ACTIONABLE

Planning and Direction

1

Published Information

2

Collection of Open Source Intelligence

Intelligence Cycle

Report and Inform

5

3

Primary Source Collection

4

Analysis and Production

Engine room of the intell process: where data is put into context to create intelligence. This is very difficult to automate.

Not just on-line, but also tradeshows, Interviews, rumours, databases, statistics, etc.

Figure 2: The competitive intelligence circle
(Source: http://conferences.alia.org.au/online2003/papers/ford.html)

According to the Publin D9 Report[7], innovation in the public sector can be divided into several types, as follows:

- a new or improved service (for example health care at home);
- process innovation (a change in the manufacturing of a service or product);
- administrative innovation (the use of a new policy instrument, which may be a result of policy change);
- system innovation (a new system or a fundamental change of an existing system);
- conceptual innovation (a change in the outlook of actors, accompanied by the use of new concepts, for example integrated water management);
- radical change of rationality (the worldview or the mental matrix of the employees of an organization is shifting).

The public sector is generally viewed as unadaptable to user needs and preferences, although informal C.I. techniques are mostly unwarily carried out by civil servants on their daily basis interaction with the general public. The lack or insufficiency of knowledge about the real needs or the impact of programmes and services provided (one of the most common tasks of a C.I. unit) can lead to public dissatisfaction which can be a strong pull for innovation in the public sector.

More and more often, the scholar is debate on whether or not the public sector can be analysed from an economic perspective, is leading towards the conclusion that similarities with the private sector are now predominant and the need for reshaping the public sector, based on market principles, is becoming easier to sustain.

A cultural shift away from rules and regulations towards a more adaptive, responsive and client-oriented culture[8] is reshaping the public sector organizations of today', with the focus on quality of the provided services, the orientation on achieving the „customer" (former citizen) satisfaction and the constant need to gather and analyse data regarding the perception on the effectiveness of public policies.

According to OECD[9], the public sector is currently facing some key challenges, such as:

a. delivering better public services under fiscal pressure;

In order to address this challenge many countries have assumed three main objectives:

- do more with less, also by using IT and innovative practices;
- build and keep trust, mainly by communicating results;
- engage with the public and the stakeholders.

b. a more effective and performance-orientated public service;

The main three strategies used in order to accomplish this objective were:

- expanding and strengthening resource management, by using new technologies to upgrade resources;

- improving strategic management and matching it with expectations, including strategic foresight, governance for performance, using performance information, social dialogue and communicating with stakeholders and their expertise networks;
- reaching out to facilitate effectiveness and performance, meaning that stakeholders are invited to provide significant input.

c. **open and transparent government,** with the objectives of restoring trust in government and aligning the public sector with modern information management practices and to provide policy levers to facilitate capacity for change and for sustainable reform in the public sector**.**

Nevertheless, taking into account some specificities of the public sector organisations, there are some issues that have to be addressed and mitigated, before implementing a C.I. programme, such as:

a. **acceptance of practices and terms;**

If in the private sector the ethical use of CI techniques is broadly acknowledged and accepted. It seems hard to justify, in public organisations, the establishment of an independent structure/department that deals „only" with gathering and analysing data about public need and perception regarding public policies impact.

b. **accountability in using budgetary funding**;

This issue resides in the difficulty of sustaining the necessity of public funds allocation for a detailed analysis and, furthermore, for the implementation of the results, with the sole objective of strengthening the competitive position of the organisation.

c. **reluctance to change**;

Common also to private organisations, the lack of motivation in improving the way „business is done", is more often encountered in the public sector where some constraints (rules, procedures, and reglementations) are intentionally exaggerated, in order to justify the resilience of the current state of being.

d. **difficulties in measuring the outcome**;

Contribution to profit or value added to the shareholders, as results of applying C.I. techniques, can more easily be assessed in a private company, then the „improvement of quality of life" as a possible outcome of the use of C.I. activities by a public organisation.[10]

After the decision of implementing/developing a C.I. function is taken and widely accepted and the objectives (intelligence needs) are clearly stated, the manner in which the intelligence function will be secured, should be selected, from the following options:

- by designated middle managers (in case of small public organizations), with the council of a C.I. expert;
- by establishing a dedicated structure (department/unit) and clear procedures, including for internal and external cooperation;
- by contracting a C.I. specialised company;
- by a team of employees from the public organization, under the supervision of an external C.I. specialist.

Whatever the solution adopted, transparent and clear formulation and communication of the objectives and specific procedures to all employees involved in any kind of professional relation with the general public is needed (as they can act as „data collection antennas"). Also, taking into account the risk of not being accepted of the terms used, of an external or even internal structure dealing with gathering of data, it may be useful to consider, just as an informal measure, renaming the structure/service, for example strategic analysis or strategic projects.

According to Bartes[11], the process of introducing C.I. systems, should take place after the phases of preparation of the management, the personnel and the organization, as a whole. Preparation of the management includes familiarization with C.I. scope, grounds the decision of implementing C.I. system and identifying the best ways to do it and designate the project manager.

The second phase, of personnel preparation should involve evaluation, selection and training of the future C.I. practitioners of the organization. Organizational preparation should cover the establishing of internal procedures (setting the „intelligence map"), functional and operational hierarchy and ethical deontology. It is highly important that, in this phase, the criteria of evaluation of the effectiveness of the C.I. system should be set and acknowledged by all parts involved (decision makers and personnel) as well as the internal public audit principles and specific tasks for this area.

The need for measuring the C.I. system resulting from connecting them to the performance of the organization is best emphasized by the surveys carried out by SCIP (Strategic and Competitive Intelligence Professionals), which show that the average lifespan of a C.I. structure is between three to four years, proving that, still, C.I. is not broadly accepted as a performance booster.

Conclusion

The purpose of this paper was to question whether or not competitive intelligence can be implemented in public sector organizations. The specificities of public sector organizations (hierarchy, budgetary founding, and public accountability) make it difficult to sustain the need of implementing a C.I. system within.

Innovative government can facilitate the acceptance of C.I. programmes. Similarities with the private sector are now predominant and the need for reshaping the public sector, based on market principles, is becoming easier to sustain. Therefore, there is a need to clearly emphasize the relation between C.I. activities and one of their main objective in the public sector - credibility and reputation growth, as a result of better knowledge, understanding and serving the general public needs.

References

[1] *Small business encyclopaedia*, available at Entrepreneur.com, accessed, 2014.06.09.

[2] Calof, J., Wright S., Competitive *Intelligence: A practitioner, academic and interdisciplinary perspective*, European Journal of Marketing, 2008.

[3] *Supplemental guidance: Public sector definition. The institute of internal auditors*, December 2011.

[4] Porter, M., *Competitive Advantage*, The Free Press, 1985.

[5] Fleischer, C.S., Blenkhorn, D.L., *Controversies in competitive intelligence: the enduring issues*, Praeger Publishers, 2003.

[6] Popa, I., *Management strategic*, Editura Economica, 2004.

[7] Halvorsen, T., Hauknes, J., Miles, I., Roste, R., *On the differences between public and private sector innovation*, PUBLIN, 2005.

[8] Hauknes, J., *Some thoughts about innovation in the public and private sector compared*, STEP, 2003.

[9] „The call for innovative and open government. An overview of country initiatives”, OECD, 2011.

[10] Fleischer, C.S., Blenkhorn, D.L., *Controversies in competitive intelligence: the enduring issues*, Praeger Publishers, 2003.

[11] Bartes, F., *The process of implementing Competitive Intelligence in a company*, in *Acta Universitatis Agriculturae et Silviculturae Mendelianae Brunensis*, 2013.

SMART GOVERNMENT: BUSINESS/COMPETITIVE INTELLIGENCE, THE KEY FOR DECISIONS IN PUBLIC SECTOR

Virgilius-Traian STĂNCIULESCU[*]

Abstract

Public Sector is critically in need of the technology to improve decision making and choose the best options for modernization. CI and BI tools can ensure operational efficiencies and performance improvements thereby helping policy-level decision making. With CI/BI, public sector agency can have all the information that it can at its disposal for decision making, planning and monitoring. CI/BI is the cornerstone of decision making based on facts rather than perceptions With CI/BI investment, government departments and other public sector organizations make better informed decisions. They can ensure that the public sector meets its key performance indicators (KPIs), and manages its limited resource well.

Keywords: competitive intelligence, public sector, strategic decisions, planning, policy

Public sector and business/competitive intelligence

A government must define S.M.A.R.T. politics in terms of Sustainable, Manageable, Achievable, Resourced, Tangible and Traceable goals. To define and to apply political strategy, the government, the public administration needs "to decide". One of the words that starts to produce actions is "decision". This paper tries to respond to the question of what helps the right decisions.

[*] Head of IT Administration Office, National Authority for Management and Regulation in Communications (ANCOM)

Competitive Intelligence/Business Intelligence can have a determinant role for decision making processes in Public Sector (PS) and, approaching this concept, it is to be remarked that Competitive Intelligence/Business Intelligence is widely applied in private sector and very restrictively in the public sector. Let us try to respond to questions like “why private business apply CI/BI and public sector not?”. Why private business is considered a more suitable area to apply CI/BI than the public sector?

The role of Competitive Intelligence/Business Intelligence in Public Sector area is minimized because there is considered to not be a classic business oriented profit. But this is not true. Government wants to have good politics, good plans, suitable decisions to apply, wants to collect and reinvest money, to have rational expenses, efficiency and many other goals. All of these requests knowledge, about the needs and about the perceptions, to construct applicable and sustainable politics.

The public sector is a very complex system. It can be described:

- with the different types of public policies that organizations implement;

- or by political and administrative dimensions;

- but also it can be described by the services that organizations deliver to citizens[1]

The paper will refer to the public sector as the ensemble of all organizations providing public services to the society as a whole: government, state agencies or companies, public administrations. These types of services range from health services, and education, to social and cultural services, infrastructure, and so on. A shared classification of public sector services includes: public administration, defense and compulsory social security, education, health and social work, other community, social and personal services.

Differences on applying Competitive Intelligence in Public and Private Sector

It is worth to understand the public sector`s distinctive characteristics and to focus on the differences between the public and the private sectors in terms of objectives, information and knowledge exploitation, and decision-making processes.

An obvious difference between the public and private sectors is that the public sector is not profit driven and its primary goal is not to maximize profits. Nevertheless, this should not lead us to believe that public sector employees and managers are not concerned about financial matters. Similarly to private companies, public organizations fight for funding and power, and mainly for costs saving, but operate in a political environment and basically work to reach political goals. Public organizations service delivery has to meet objectives regarding productivity, efficiency and quality of services. Public sector services depend on revenues that are allocated according to political decisions rather than market performances. The central government funds public sector activities to cover the costs. The national budget makes public sector activities possible, and its allocation defines the boundaries for such activities. In particular, the way political goals are reached is influenced by decision-making processes which are mainly conditioned by available information and knowledge. Knowledge is essential to support decision-making activities and to deliver better services[2].

The private sector is typically associated with market forces while the public sector is more shaped by political considerations: one is about "business" and the other is about government"; one tends to be decentralized and the other centralized. The typical public sector decision-making process begins with the definition of objectives or goals. In the public sector decisions are often the result of compromise, bargaining and political debates. The process of making a decision is often more important than the decision itself. The result may not be the most cost-effective, but it is the result of a consensus developed to satisfy most of the constituents' interests. In fact, public sector decisions have many stake-holders who believe they have a right to participate in the process of making a decision. Moreover, the public sector requirement for transparency increases the importance of the clarity of objectives[3].

Citizens demand for better services while supporting Public Sector with their taxes. Therefore, two requirements deserve special attention among public sector: cost reduction; and service improvement, the latter involving concepts like service quality, effectiveness, and efficiency. [4]

Public Service improvement may require several actions: to modify the service processes, to improve the information quality, and possibly to carry out strategic knowledge management activities. Knowledge is a key factor in affecting service quality: knowledge is required to design, produce and deliver better services, furthermore knowledge may also represent the main output of some services. Public Service quality improvement relies on evaluation, which requires useful and measurable indicators.

In the private sector, efficiency and effectiveness measures are ultimately related to profit maximization and to profitability for stakeholders. Therefore, in the private sector a classic performance metric is the return on investment (ROI) and the set of related indicators.

However the public sector does not have profit maximization as its main objective, but it rather focuses on policy and service outcomes improvement. Unfortunately outcomes indicators are hard to identify since they are strictly domain dependent, and they are affected by the complex set of factors influencing the customer perception and service satisfaction[5].

The Opportunity of Competitive Intelligence in the Public Sector

The public sector is operating today like a commercial organization. It faces unprecedented pressure to improve service quality while progressively lowering its costs. At the same time, it is expected to become more accountable, transparent, customer focused and responsive to stakeholder needs in a climate of shrinking budgets and resources. Government agencies are tasked with more than simply reducing costs and increasing service levels. They face increased scrutiny from legislators, executives, and even the public through Right to Information Act. This brings about the need to increase transparency, accountability, and performance as well as solve operational challenges, improve customer service, maximize resources and eliminate fraud, abuse, and waste[6].

Speaking about knowledge we must speak about intelligence, and applying competitive intelligence. Applying CI/BI in the public sector can support almost all activities, including:

- Policy formulation and enactment;
- Planning and budgeting, Tax Plan, Financial Systems;
- Service management;
- Acquisition, Logistics and Supply Chain;
- Health & Human Services;
- Citizen Relationship Management;
- Education;
- Fraud prevention and national security;

And not on last positions even the

- Knowledge Management;
- Intelligence Assessment itself as a strategy to grow up the use of CI as a continuous process.

There are a lot of opinions defining the CI as[7]:

- collecting information about competitors to gain a competitive edge in the marketplace
- as an organization's commitment and ability to study competitors and to anticipate their actions
- a formalized, yet continuously evolving process

In the public sector, the CI can be defined as a continuous process of collecting information, specific public and private environment monitoring, analysing and disseminating the intelligence products to assist political and administration decisions followed by operational adequate decisions.

The process of knowledge creation starts from information and with knowledge. Information becomes knowledge when it is assimilated into some useful form. This progression can be considered as a continuum where information and knowledge represent two ends, and CI resides in the middle given the fact that it is neither raw data nor an ultimate knowledge product.

Applying Business/Competitive Intelligence in Public Sector

We must think at CI in the Public Sector as a continuous process applied by 2 categories:

- employees itself;
- specialised CI units.

This process involve 2 actions:

- Growing up the CI culture of the state organizations employees, and the learning process to adapt the working way as a CI process.

Why? Because an important part of the intelligence needed by a state organization is possessed by its employees, who collect vast amounts of information as they interact with citizens, partners, organizations, state and private companies, political factors, and their experience should be also a source of data for the specialized CI units

- Creating specialized CI units at the level of state organizations.

Why? Because these are focused on the selection, gathering, and analysing of information of the environment in order to provide correct intelligence products related to the strategic or operational decisions to be taken.

Three levels are proposed to be part of a CI framework in a state organization, and each level focuses on an important form of analysis that can be good for decision making mainly at the different levels in an organization. These levels can be identified as:

- **Strategic level**: The first level represents analysis of information that can assist the government or state organization at the strategic decision-making level. This level also provides a framework within which other levels (tactical & operational levels) of intelligence collection and analysis take place, and it assists the organization in identifying important trends and patterns that emerge in its environment as well as the threats and opportunities available to the organization. Practically this level has the focus on environmental analysis.
- **Tactical level:** Level two represents the analysis of information that can assist mainly in tactical decision making at the level of the organization, and it also supports the strategic level. A symbiotic relationship exists between the strategic and tactical levels of intelligence analysis. This level is represented by the service-business analysis, evolutionary analysis and financial analysis.
- **Operational level:** The third level represents the operational level of information analysis, and it focuses on the low-level decisions and delivery of public services. This level is, therefore, related to social impact analysis and citizens satisfaction as a result of previously or present applied decisions.

Thus the public sector needs a proper, powerful and robust information infrastructure, which allows the usage of all data for making the best operative, tactical and strategic decisions in a competitive economic environment which is permanently changing, offering the ability to use information in an intelligent way, in order to cope with challenges and to benefit for opportunities

Business/Competitive Intelligence systems

There are specialized information infrastructure systems for CI/BI, generally called BI systems (the "BI systems" were borrowed by the IT industry and became a standard, but, in reality, they are just another way to do a part of what CI presumes):

- BI systems are evolved decision **support** systems, capable to assist tactical and strategic decision making, operations and business processes improvement.
- But it is necessary to estimate the future evolution too, in order to anticipate events and make the most appropriate decisions. BI systems join various activities within the company and raise relationships that are difficult to be observed. So, BI overdraws the borders of a standalone activity and becomes an integral part of the way politics are applied and the administrative act is conducted.

CI/BI systems aims to provide to the decision making process accurate, consistent and pertinent information. They make possible developing of evolved decision support systems, capable to assist tactical and strategic decision making, operations and business processes improvement. Thus, these systems contribute to profitability increasing and gaining competitive advantages.

BI systems can provide historical reports, data analyses and alerts that signalize problems and possible threats. Analysing historical information, managers can evaluate the former activity. But it's necessary to estimate the future evolution to, in order to anticipate events and make the most appropriate decisions. BI systems join various activities and emphasize relationships that are difficult to be observed. So, BI overdraws the borders of a stand-alone activity and becomes an integral part of the way the business is conducted.

It is necessary that BI solutions are available not only for managers, but also for a great number of employees. At the same time, they must be able to be used by external users, such as customers, business partners, and providers, and to take into consideration the requirements of each user category.

BI can be implemented in all areas and levels of government. Correctly implemented, BI provides executives, administrators, managers, partners, and even individual citizens with the important information necessary to perform their jobs and make decisions more effectively, resulting in better government service.

About interoperability and the amount of data

There is a lot of information and data held within the public sector but who needs to know what? What information is appropriate for which department or for which agency? It is important that information to be found effectively by the interested agency or department.

Public agencies can elevate their performance with the unprecedented visibility and control with Business Intelligence/ Competitive Intelligence software tools.

A condition for obtaining good results in applying competitive intelligence in state agencies and implementing BI/CI, is the interoperability of all the informational systems of governmental and state agencies, and sharing the specific databases, all of this being possible in a **governmental cloud.** The benefit of this new approach of the IT world is huge, because it appeared to be not only the opportunity to share the governmental and public or non-public data, but also the easiest way to put together, in a interoperable way, all what was separately until now. Of course, cooperation is needed between all the institutions, and also access levels defined, but now everything is possible by cloud interfaces. There is no need for big investments, but there are a lot of benefits offering to governmental CI a comprehensive source of aggregated data.

Moreover, as the Big Data phenomenon is increasing, the CI/BI units can benefit from this huge source, and it is a must to take Big Data into consideration, once major companies already have, and once a lot of useful information can be mined from there.

Big data is a popular term used to describe the exponential growth and availability of data, both structured and unstructured. And big data may be as important to business – and society – as the Internet has become. Why? More data may lead to more accurate analyses. More accurate analyses may lead to more confident decision making. And better decisions can mean greater operational efficiencies, cost reductions and reduced risk.

Big data can be characterized by 3Vs: the extreme volume of data, the wide variety of types of data and the velocity at which the data must be processed. Although big data does not refer to any specific quantity, the term is often used when speaking about petabytes and Exabyte of data. And is happening right now, being the new phenomenon like the Internet was yesterday.

Implementation issues

The development of a BI/CI system is a very resource consuming task, the projects are on/off investments: they return positive results (i.e. they provide value to the decision-making activities) only if:

- the decision maker's needs are correctly identified,
- useful indicators and measures are computed,
- data quality issues are resolved,
- the technological support is correctly deployed,
- the data provision system is user-friendly,
- the decision-making processes and the overall service provisioning processes are affected.

If only one of this aspects is not properly managed, the resulting decision support system will fail to provide an added value to its users. The costs and the probability of failure are lower when prior knowledge about the domain and the project are available in the users and in the ICT personnel involved in the project (e.g. because people already worked on similar contexts). However, fewer successful projects are available in the public sector compared to the private one. For these reasons, it is reasonable to suggest starting projects in the public domain where the probability of failure is low and where the expected benefits could be very high. Public sectors (or services) having high knowledge intensity could benefit from the introduction of BI/CI systems, and the decision-making activities would benefit from it. The introduction of BI/CI systems could lead to huge savings in sectors having high expenditures, or could lead to a service level improvement without cost changes. Services or sector having a high degree of decision will have a relief from the introduction of BI/CI systems, while a high level of automation is an indicator of the availability of electronic data upon which the BI/CI can be more easily built. Indeed a lot of useful information can be identified and extracted with low effort when a lot of electronic data is available. Thus, a high level of automation may contribute to lower the costs of a BI project[8].

Conclusions

To resume in a few words the line of success of implementing CI/BI in public sector, the key factors must be raised:

- establishing internal Competitive Intelligence units involving specialists;
- increase the Competitive Intelligence culture at the employees level;
- understand the political factors;
- benefit and involving the academic resources;
- interoperability between public and private systems;
- mining in big data systems;
- benefiting and involving the academic resources.

In this way, a public sector can achieve its S.M.A.R.T. goals, acting smart, up to date, from the strategy definition to short and long term decisions

References

[1] Peters, B. G. (2006): Understanding the Public Sector: The Significance of Size and Complexity?. The Asia Pacific Journal of Public Administration 28 (2), pp. 99-116.
[2] Roberto Boselli, Mirko Cesarini, Mario Mezzanzanica , Public Service Intelligence: evaluating how the Public Sector can exploit Decision Support Systems.
[3] Bozeman, B.; Pandey, S. K. (2004): Public Management Decision Making: Effects of Decision Content. Public Administration Review 64, pp. 553-565. Dillon, S.; Buchanan, J.; Corner, J. (2010): Comparing Public and Private Sector Decision Making: Problem Structuring and Information Quality Issues. In proceedings of the 45th Annual Conference of the ORSNZ, pp. 229-237.
[4] Langergaard, L.L.; Scheuer, J.D. (2009): Specificities of public sector service innovation. ServPPIN Deliverable 2.1.
[5] Roberto Boselli, Mirko Cesarini, Mario Mezzanzanica , Public Service Intelligence: evaluating how the Public Sector can exploit Decision Support Systems.
[6] Maia Intelligence, 1Key Agile, Business Intelligence *for* Public Sector | Government.
[7] Sina Soltani Mollayaaghobi, A Comparative study of competitive intelligence in Public Sector.
[8] Craig S. Fleisher, David L. Blenkhorn, Controversies in Competitive Intelligence, the enduring issues.

INTELLIGENCE SUPPORT TO THIRD PARTY INTERVENTION

Cathryn Quantic THURSTON[*]

Abstract

In the post-Cold War world, many conflicts are internal to states or regions, and the international community is still grappling with their role in helping to resolve these disputes. The academic community, especially in conflict analysis and resolution, has been working steadily towards a shared understanding of and practice for resolving conflict. This paper discusses how intelligence could assist the international community in 1) understanding what motivates actors at different levels to behave in certain ways, and 2) how outside intervention can be useful in moving warring parties to a solution. Intelligence could play a beneficial role in this process, but that will require intelligence agencies and partners to collaborate on a regular basis.

Keywords: conflict analysis, intelligence support, resolution, international community

Third Party Intervention between Warring Parties

The United States national security community has struggled since the end of the Cold War to evaluate the effectiveness of intervening between warring parties, whether the U.S. is supporting multilateral or UN peacekeeping operations or making a unilateral decision to intervene between warring parties with humanitarian aid, economic sanctions, diplomatic activities, or military assistance. Generally, from a conflict resolution point of view, the purpose of third party intervention is to halt or reverse violence, either bringing a bad situation back to a status quo, or helping two opposing sides move towards a new future together.

[*] Ph.D., National Intelligence University. This paper is solely the work of the author and does not reflect the official position of the United States Government, Defense Department, or the Defense Intelligence Agency. This paper is cleared for public release.

The United States and her allies are increasingly summoned to intervene in many types of conflict. For example, the current list of joint military publications includes a range of operations: special operations, antiterrorism, joint urban operations, stability operations, peace operations, joint counterdrug operations, joint security operations in theater, information operations, military information support operations, multinational operations, joint forcible entry operations, foreign internal defense, counterinsurgency, counterterrorism, foreign humanitarian assistance, and civil-military operations.[1] While some of these operations clearly support traditional "interventions" between warring parties, such as peacekeeping and foreign humanitarian assistance, some of these operations are also useful when embedded within interventions, especially in post-conflict reconstruction and stabilization activities. However, the lack of an overarching framework and clear understanding of what is required for third party intervention activities means that military planners must be adaptive as the conflict unfolds. Likewise, intelligence support to these different types and levels of operations must also be flexible, depending on the conflict.

Understanding Conflict Intervention

Third party conflict intervention is further complicated by a lack of understanding about why conflict exists in the first place. Academics and international security experts, non-governmental organizations, and governments have many different ideas on why and how to intervene in conflict. For example, if an intervening organization believes the source of a conflict is rooted in negative attitudes, then a "hearts and minds" intervention plan might focus on changing the way people view their situation or their adversary. Alternatively, if an intervener believes the conflict is caused by a destructive governing system, then the intervention will focus on "correcting" the government, which might even mean installing a new one. In practice, intervention often takes place even when there is only a vague understanding of the sources of the conflict. After all, members of the international community intervene between warring parties for many reasons including self-interest, cultural affiliations, treaty obligations, etc. Therefore, just as there is no one "theory of conflict" there is also no single "theory of intervention." Consequently, organizations design conflict interventions based on many theories, which in turn makes it difficult to evaluate the efficacy of the intervention.

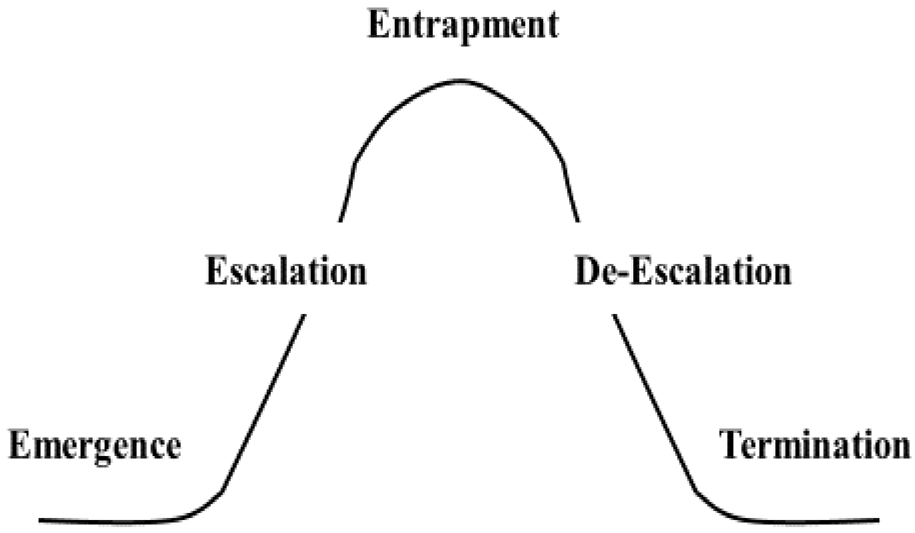
Though intervention may be situational and understanding of conflict may be unclear, every intervention includes explicit and implicit goals and intentions. Current practice in international conflict intervention is a little like a "trial and error" experiment. A potential intervener looks at a problem, hypothesizes as to the source of the conflict, decides what kind of intervention is best, weighs the pros and cons of intervention, and plans an intervention with specific goals in mind. Once the intervention is underway, the intervener reassesses the conflict, trying to understand if the activities are actually causing the "right" kind of change. The current U.S. military approach to this is called "adaptive planning."[2] The concept includes multiple in-progress reviews (IPRs) primarily to check the interagency dialogue and coordination and planning exchanges with civilian and multinational counterparts, but also to allow for updates on the conflict itself.

Because the situation and planning assumptions are changing constantly, and so many actors are involved, it seems imperative that someone, perhaps intelligence support, perhaps not, creates a baseline understanding of the conflict, and then tracks changes in the conflict in a systematic way. This baseline assessment of the conflict itself would give planners a way to measure impact of their intervention activities.

Strategies for Third Party Conflict Intervention

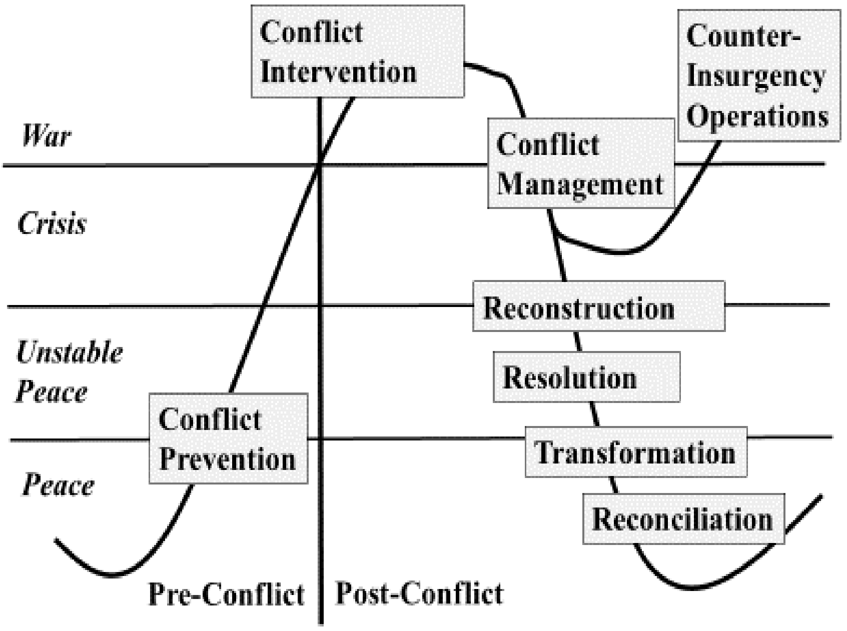
The conflict life cycle, shown in figure 1 below, treats conflict as a wave, or a series of successive waves.[3] The model illustrates how underlying "latent" conflict emerges and becomes "manifest," is eventually recognized as a crisis by external third parties, then escalates, becomes entrapped, and de-escalates. However, these stages are not necessarily set in stone and can act concurrently with other conflicts, remain "stuck" for years, or reignite.

Figure 1: Conflict Life Cycle



Still, over time, the international community has developed different interventions for the different stages of conflict. Figure 2 below shows some of these options: conflict prevention, conflict intervention, conflict management, counter-insurgency operations, reconstruction, conflict resolution, transformation and reconciliation.

Figure 2: Life Cycle and Intervention Options



These intervention options are designed to do different things; therefore, the understanding of the conflict itself and the thinking behind intervention planning will be very different depending on the option taken. In the past two decades, the drive to be more explicit in goals and intentions in peacebuilding is rooted in a general feeling of uncertainty and hesitancy about conflicts occurring after the end of the Cold War. Conventional wisdom says that the end goal of any intervention should focus on finding a nonviolent solution to a problem. But is this enough? In the post-Cold War era, some (but not all) conflict resolution activities have moved away from a focus on *resolving* a conflict, which seems to focus on stopping conflict (negative peace), to *transforming* a conflicted community or society towards a new shared future (positive peace). [4] In the past twenty years, the strategies used in conflict intervention at the international level have become fairly standardized. These basic strategic approaches and some common associated goals, objectives, and tasks are outlined below in Table 1.[5]

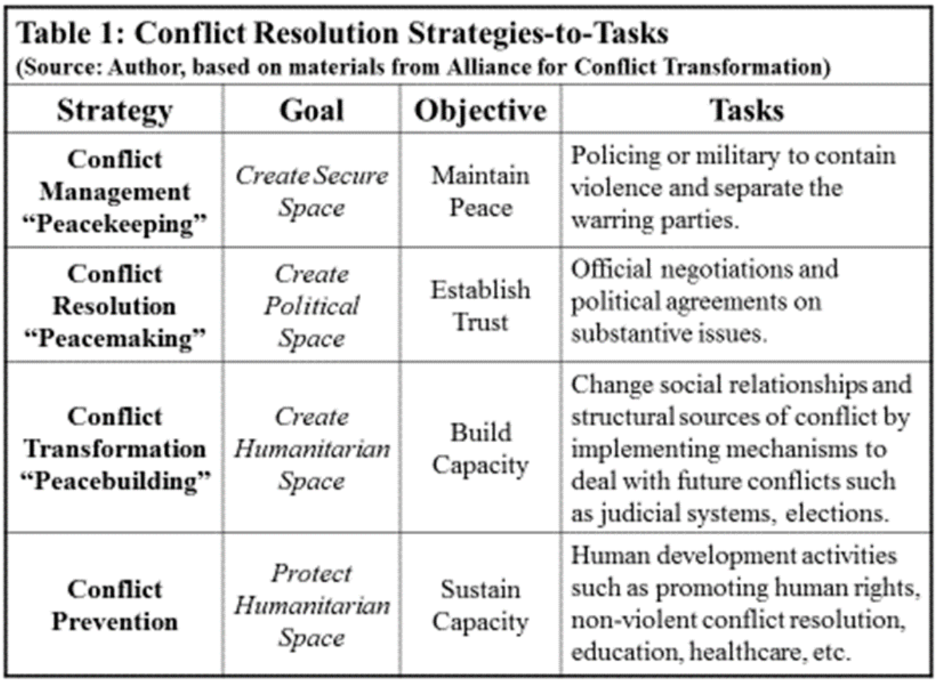


Table 1: Conflict Resolution Strategies-to-Tasks
(Source: Author, based on materials from Alliance for Conflict Transformation)

Strategy	Goal	Objective	Tasks
Conflict Management "Peacekeeping"	*Create Secure Space*	Maintain Peace	Policing or military to contain violence and separate the warring parties.
Conflict Resolution "Peacemaking"	*Create Political Space*	Establish Trust	Official negotiations and political agreements on substantive issues.
Conflict Transformation "Peacebuilding"	*Create Humanitarian Space*	Build Capacity	Change social relationships and structural sources of conflict by implementing mechanisms to deal with future conflicts such as judicial systems, elections.
Conflict Prevention	*Protect Humanitarian Space*	Sustain Capacity	Human development activities such as promoting human rights, non-violent conflict resolution, education, healthcare, etc.

Table 1 locates the traditional intervention strategy of *conflict management*, or "peacekeeping," at one end of a spectrum. The peacekeeping goal is to create a safe space for official talks, and the main objective is to manage the conflict. The activities conducted by the international intervention force normally focus on physically separating the two warring parties and monitoring and reporting the parties' compliance with a cease-fire. The theory of change is that, by separating the two warring parties, the leaders of each side can concentrate on finding a nonviolent political solution to the conflict. This type of intervention strategy is the foundation for the United

Nations Peacekeeping Force, which was established at the end of World War II by the UN Security Council.[6]

The middle-range of the intervention spectrum includes the strategy of *conflict resolution*, or "peace-making." The goal of a conflict resolution intervention is to create political space for two sides to talk constructively and resolve the conflict peacefully. Therefore the main objective is to establish a level of trust between the parties. Traditional conflict resolution focuses on coaxing the parties to the negotiating table, which could include activities such as military observer missions, conducting "track two" diplomatic activities, retreats, or sending intermediaries. The theory of change is that a neutral third party, usually representing another government, can work with the two warring parties to help them come to some kind of political agreement over the conflict issue. A good example at the international level is Norway's effort to broker peace between Israel and Palestine via the Oslo peace process during the mid-1990'.

The third range on the intervention spectrum involves a strategy to *transform* a conflicted society into a peaceful one. This strategy is often called "peacebuilding" and it focuses on building or re-building a nation's capacity to settle disputes peacefully. The intervention goal is to create humanitarian space so that the basic needs of a population are supported while the government rebuilds social structures. Therefore, the objective is to build capacity. The associated activities include re-building or creating a new judiciary system along with local and national police forces, writing a new constitution, establishing a representative government and holding elections, training the military, setting up education and health systems, launching economic infrastructure projects, and developing business incentives. The idea is to transform the relationship between two warring parties by repairing the social structure so that the two parties can resolve future disagreements in a non-violent manner. The theory of change is that a destructive social system can be made "right" when the international community transfers skills to help build indigenous capability. Then, private citizens, businesses, and non-profit organizations can rebuild the damaged society. This strategy underpins the United States' post-Cold War focus on "nation-building" in Europe and the Middle East.

Finally, the last range on the intervention spectrum represents both old and new ideas on *conflict prevention* strategies through humanitarian aid and development. The goal of this kind of intervention is to protect humanitarian space and support basic human needs so that a society can build more sophisticated political and economic capacity. The objective is to sustain capacity, and the activities rely on international organizations working together to strengthen existing national conflict prevention structures such as education systems, agriculture, or regional economic and health organizations. The theory of change is that healthy societies do not go to war with each other (or with themselves) and will work to solve their problems peacefully. This strategy underpins the international development field, where governments fund activities around the world in an effort to prevent some future conflict by working to improve the human condition. A good example of this strategy is the United Nations' Millennium Development Goals, which focus on reducing hunger and improving access to education and health care across the globe.[7] The difference between the strategies and goals of conflict transformation and prevention is narrow; the former is conducted in a post-conflict environment and the latter is focused on struggling countries who are trying to avoid conflict in the first place.

In practical terms, the lofty intervention strategies and goals are realized through their more concrete objectives: *Maintain Peace, Increase Trust, Build Capacity*, and *Sustain Capacity*. Each of these objectives is a reasonable reflection of the strategy, and each is also measurable; any associated activities conducted under their auspices can be evaluated for their contributions to reaching the objectives. Finally, the connection between these strategies and goals, objectives, and tasks employed by governmental, non-governmental, and private organizations on the ground is the ***theory of change***.

Once the intervention planners understand the strategic goals and build the objectives, they will choose the main organizations that will deliver activities to the audience. There are formal and informal types of activities. Formal activities include traditional "track one" diplomatic and military activities such as negotiations and peacekeeping. Informal activities, however, include a vast array of possible "multi-track" activities conducted by individual military units, foreign and local non-governmental organizations, private citizens, etc. Some of these activities could include conflict resolution skills training, truth and reconciliation commissions, youth retreats, cooperative business initiatives, or community health and education programs to name a few.

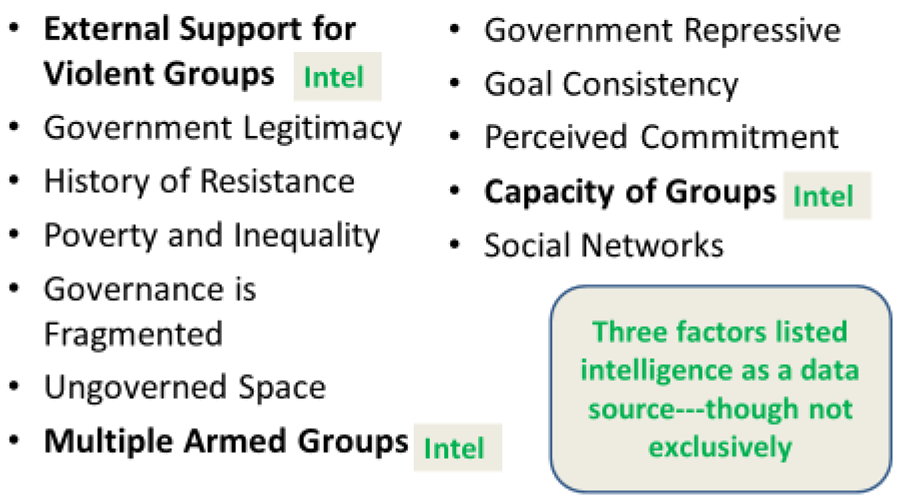
Creating a Baseline to Measure Progress

Several problems arise when decision makers cannot assess the impact of activities and programs against the conflict itself. First, decision makers ask, do the activities actually increase the capacity of the receiving nations? Secondly, the budget folks need to know the value of intervention programs. What would be the impact if the program was cut? Finally, planners also have questions. Which activities are the best? What is the appropriate sequence of activities to create the largest impact?

Traditional intelligence analysis, especially in a military context, focuses on giving the commander a good idea of the diplomatic, information, military, and economic (DIME) conditions of an adversary, otherwise known as the "instruments of national power." More recently, and in response to "new" types of military operations described above, the analysis also includes financial, intelligence, and law enforcement information (DIME-FIL). Another set of requirements for planning uses PMESII (Political, Military, Economic, Social, Information, and Infrastructure System Analysis).[8]

The U.S. military community continues to look for a better way to understand the conflict situation. For example, a 2014 RAND study entitled, *Improving U.S. Military Understanding of Unstable Environments Vulnerable to Violent Extremist Groups* surveys social science research to determine 12 main indicators of instability.[9] These indicators are included in Figure 3 below:

Figure 3: 12 Indicators of Unstable Environments



- **External Support for Violent Groups** Intel
- Government Legitimacy
- History of Resistance
- Poverty and Inequality
- Governance is Fragmented
- Ungoverned Space
- **Multiple Armed Groups** Intel
- Government Repressive
- Goal Consistency
- Perceived Commitment
- **Capacity of Groups** Intel
- Social Networks

Three factors listed intelligence as a data source---though not exclusively

Interestingly, only three of the 12 indicators have intelligence means identified as possible sources of information. The vast majority of information sources needed to "track" these indicators come from open sources such as UN reports, news organizations, and non-governmental organizations.

Possible Areas for Intelligence/Information Sharing: Problems and Prospects

Unclassified information comes with two main challenges: the quality of the source of information, and the categorization of vast amounts of information. The sheer volume of information available, especially news reports and social media, makes it hard to select and then verify. Plus, new data mining software and other online services have their own limitations that require the user to learn how to use complicated search mechanisms. In many cases, international conflict information gathered by non-profit organizations and academics requires intelligence analysts to understand complex algorithms or datasets. This is an important point because constructing a dataset of conflict information is complicated by the conflict itself. Anyone gathering data in a conflict zone must pay particular attention to missing data, and the quality of the sources of information. Furthermore, many intelligence analysts do not have the academic backgrounds to really understand the methodologies that social scientists use to build information. In addition to understanding the quality of the source of information, it is also difficult to know which information to focus on. The unclassified information available on conflict in general and on specific conflicts is vast and essentially unorganized. Even if the analyst knows exactly what he or she is looking for, it is difficult to know where to go to get the information. The explosion of online resources available almost requires a research librarian or other information sciences professional to help explore the data in a meaningful way.

It seems clear that the many intelligence organizations supporting third party interventions cannot possibly produce and manage the vast amount of information needed to support decision makers, especially in multilateral interventions. A partnership could be formed, however, between the producers and consumers of information. If the majority of information on unstable environments and intrastate conflicts comes from open sources, perhaps intelligence agencies should think about how to share this information with each other, with allied intelligence organizations, or even the general public, to include non-profit and peace organizations.

One possible group to explore collaboration could be conflict analysis and resolution academics and practitioners who focus on helping people resolve their own conflicts. In a workshop conducted in 2010, the United States Institute for Peace asked participants to compare intelligence and conflict analysis.[10] Participants agreed that the two approaches endeavour to understand very complicated conflict situations, often for the benefit of senior level governmental or military decision makers. Workshop participants acknowledged a need to better collaborate, especially due to the enormous amounts of information available. However, the two groups come from different backgrounds and see their missions in very different ways. Figure 4 below shows a commonality between intelligence and conflict resolution missions as conflict emerges, a divergence during crisis operations, and then a commonality in post-conflict.

Figure 4: Mission Similarities and Differences Between Intelligence and Conflict Resolution

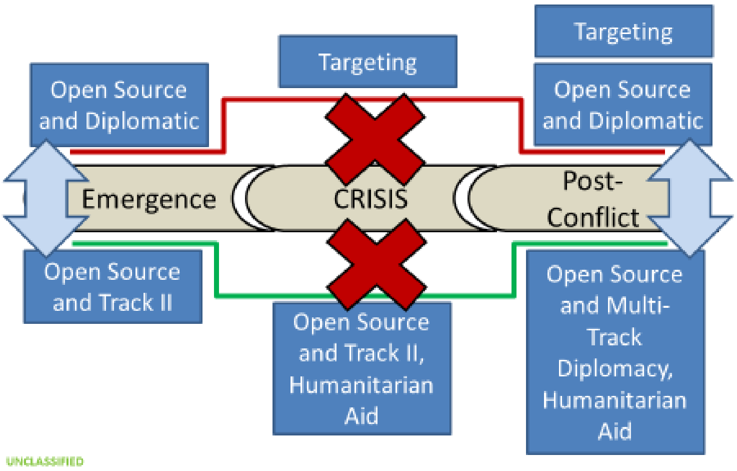

Targeting
Targeting
Open Source and Diplomatic
Open Source and Diplomatic
Emergence
CRISIS
Post-Conflict
Open Source and Track II
Open Source and Track II, Humanitarian Aid
Open Source and Multi-Track Diplomacy, Humanitarian Aid
UNCLASSIFIED

Figure 4 shows commonality of information requirements as well in the emergent stages of conflict, where the international community is working to prevent conflict. During this timeframe, intelligence agencies are assisting the diplomatic mission to resolve conflict, while non-governmental groups are working to do the same in the unofficial "Track II" arena. However, if the conflict escalates and breaks into violence, the intelligence agencies and non-governmental groups part ways. During this timeframe, intelligence agencies are supporting military operations while the non-governmental organizations may be focusing on humanitarian crisis operations such as helping refugees and internally displaced persons. However, when the conflict dissipates or comes to a point where fighting has lessened, intelligence and conflict resolution organizations come back together again with similar missions and information needs. The post-conflict timeframe again requires information to support diplomatic and peacebuilding activities. Figure 5 below shows the same information only displayed on the conflict life cycle.

Figure 5: Possible Information Sharing

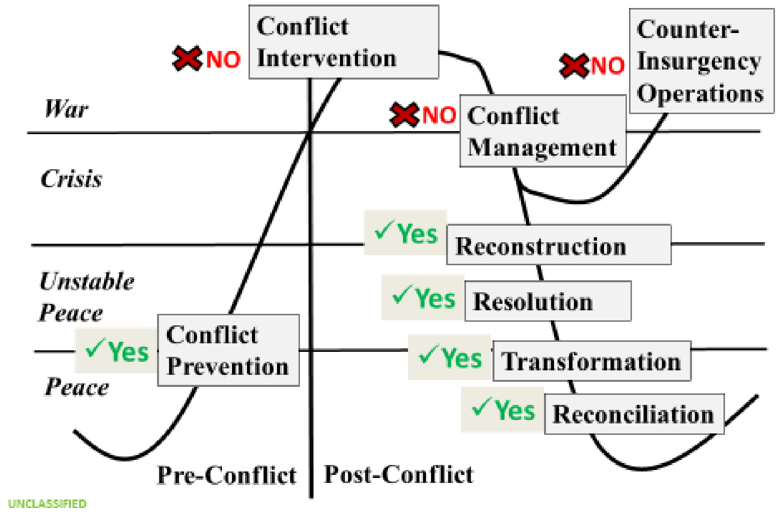


Figure 5 is helpful to see the categories of information that intelligence and conflict resolution practitioners need for specific intervention strategies. Specifically, information could be shared in the following areas: conflict prevention, reconstruction, resolution, transformation and reconciliation. However, it seems unlikely that information could be widely shared on conflict intervention during active fighting, conflict management activities such as military operations, or counter-insurgency operations. Figure 5 suggests that information on emerging conflict could be a prime category of shared information. This paper could be the start of that conversation, especially in helping to begin categorizing the specific types of information needed.

Conclusion

As third party intervention grows and evolves, intelligence has an opportunity to assist decision makers in understanding what motivates actors at different levels to behave in certain ways and how and when outside intervention can be useful (or harmful) in moving warring parties to a resolution. Intelligence agencies could partner with non-governmental organizations in some cases to share information important to third party intervention. In particular, information on emerging conflict could be the best place to find ways to collaborate.

References

[1] See the Joint Electronic Library at: http://www.dtic.mil/doctrine/new_pubs/jointpub_planning.htm.

[2] Joint Publication 5-0 „Operations Planning", August 2011, available at: http://www.dtic.mil/doctrine/new_pubs/jp5_0.pdf.

[3] Figure 1: Life Cycle and Conflict Intervention Options. Source: Author based on: Fisher, Simon, Dekha Ibrahim Abdi, Jawed Ludin, Richard Smith, Steve Williams, and Sue Williams. „Working With Conflict: Skills and Strategies for Action". London, (UK: Zed Books, 2000). There are many versions of the Life Cycle Model. It is unclear who originally developed the Life Cycle Model, but Michael S. Lund has a very nice version in his book, *Preventing Violent Conflict: A strategy for preventive diplomacy*, Washington, (D.C.: United States Institute of Peace Press, 1996, p. 38).

[4] John Paul Lederach, Reina Neufeldt, and Hal Culbertson, „Reflective Peacebuilding: A Planning, Monitoring, and Learning Toolkit" (Notre Dame, IN: Joan Kroc Institute for International Peace Studies and Catholic Relief Services Southeast, 2007): Available online at: www.crs.org.

[5] Dennis J.D. Sandole, „Chapter 3: Typology", in *Conflict*, edited by Sandra Cheldelin, Daniel Druckman, and Larissa Fast (New York, NY: Continuum, 2003.

[6] United Nations Peacekeeping Department website: http://www.un.org/en/peacekeeping/.

[7] United Nations Millennium Development Goals, available at: http://www.un.org/millenniumgoals/

[8] Joint Publication 5-0 „Joint Operations Planning", 2011, p. III-9.

[9] Thaler, David E., Ryan Andrew Brown, Gabriella C. Gonzalez, Blake W. Mobley, Parisa Roshan. „Improving the U.S. Military's Understanding of Unstable Environments Vulnerable to Violent Extremist Groups
Insights from Social Science", Santa Monica, CA: RAND Corporation, 2014.

[10] Woocher, Lawrence, „Conflict Assessment and Intelligence Analysis", USIP Special Report, Washington, D.C.: United States Institute for Peace, June 2011.

PLANNING FOR THE PROGRESS OF THE INTELLIGENCE ORGANIZATION IN THE 21ST CENTURY

Anca PAVEL[*]

Abstract

Looking, in a synthetic manner, at the main features that should define the intelligence organization today, in the "knowledge society" and "informational era", profoundly marked by the effects of globalization, we can highlight two essential aspects: very rapid adaptation to the security changes in the environment, always in a continuous transformation and also successful anticipation of the issues or future events with a major impact on the organizational capabilities.

In this regard, a successful 21st century organization cannot be built without developing planning capabilities whose mission is to help the organizational leadership to reach the efficiency of the specific activities, in a world which has become more globally connected and where the opportunities, threats and challenges seem to be increasing. Two questions arise in this regard: how does integrated planning activities help the decision - makers of the intelligence organization and what are the attributes that make them useful?

With regard to the first question, integrated planning can be useful in four distinct areas: organizational policymaking; warning; monitoring phase outcomes and assessing specific activities. Nevertheless, for maximum utility, planning activities must concern relevant institutional processes and also poses the attributes of quality and timeliness. Therefore, special planning capabilities sustain and participate in implementing the interdependency of actions, taking into account that strategy and tactics are part of the same overarching process, having an inherent relationship.

Keywords: planning capabilities, integrated planning, strategic management, organizational flexibility, alignment

Today, the planning capabilities within the intelligence organization play more than ever a very important role and also a difficult one. The importance derives from performing specific tasks in order to support the organizational management, a management of change, in a period of

[*] Intelligence expert, Romanian Intelligence Service

upheavals, such as the one we are living in, when change is the norm. The difficulty derives from the fact that the intelligence organization has the features of the traditional structures - more rigid and less flexible than others, and far more deeply rooted in the concepts, the assumptions, and the policies of yesterday – therefore, it is designed for continuity and special efforts must be done in order to be receptive and able to change.

Planning aims at the organizational success and this can be achieved only by creating the right balance between change and continuity. For that, organizational policy should pay special attention to sustain the continuity of values and rules of the organization, also regarding definition of performance and results, which are shared along communicational processes, in order to make the institutional environment predictable, understandable and known.

Challenges for tomorrow

The fundamental direction, regarding the legal mission's accomplishment in terms of performance, is provided by strategic planning activities, involved in designing organisation's strategic documents such as the vision and the strategy, which establish and define the values and operational priorities. Subsequently, their statements are implemented at all managerial levels, with the participation and support of integrated planning.

Today, this type of strategic documents must concern two important aspects which define the security environment:

a) the beginning of the 21st century, reflects times of great uncertainty and unpredictable surprises, a period of turbulence, with rapid and profound economic, social, political and technological changes, which will surely continue in the future[1];

b) the profoundly changed organizational world politics - especially those in the field of the intelligence services, whose legal mission is to provide a stable security environment, along with safeguarding their specific practices and methods – as a result of the terrorist attacks on America in September of 2001 and America's response to the terrorists.

The purpose of strategic planning is to enable the organization to achieve its desired results in a future security environment by sustaining the identification of organisational and institutional objectives which implement the global strategy and also to focus on defining the needed results. Planning activities aims to convert strategy into performance and therefore allow the organization to be aware of the challenges and opportunities that it faces in a meaning period. What is an "opportunity" can only be decided if there is a strategy, otherwise nobody can underline what genuine advances the organization has made toward its desired results, and what is diversion and splintering of resources.

The issue which arise is: what can strategy be based on in a period of rapid change and total uncertainty? Are there any certainties that intelligence organization can consider?

Peter F. Drucker, in his book, *Management challenges for the 21st century* identifies five phenomena, primarily social and political, which he calls certainties. Starting from these points, a possible intelligence organization strategy may be formulated from the perspective of some realities which will manifest in the future, with an impact upon defining the global security environment, such as:

1. The collapsing birth-rate in the developed world[2]

The assumption of a shrinking population and especially of the young population may cause two important implications for the security environment:

a) in the next years we'll face an unprecedentedly massive immigration as an effect of population decline in the developed countries, accompanied by population growth in most of the neighbouring and poor countries of the Third World.

That means the intelligence organizations will have to concentrate their efforts to counteract and to prevent the threats and vulnerabilities which could emerge from this status-quo.

One of the concerns on the intelligence organization agenda should be intelligence gathering, having in view the potential impact that these realities can have on the security environment by taking into account that social security is threatened by large-scale immigration, especially from countries of different cultures and religion.

b) The political response to the problem will inevitably imply politics of great turbulence, because no country is prepared for the issue. Political parties have their own vision and solution in this matter and the population will not agree to any of the political solutions adopted by legal norms. Therefore, government instability is likely to manifest or dominate in all developed countries.[3]

2. Shifts in the distribution of disposable income[4]

The economic crisis effects will be felt on a long term and will affect the intelligence organizations' budgets. That is the reason why, one of the main challenges that the intelligence organization should manage in the future will be to increase its products's quality and to streamline processes taking place at organizational level along with the reduction of sums allocated to different categories of expenditures.

The intelligence organization must not expand or grow – especially not by acquisition – unless they fit into the organization‘s realities and overall strategy. If what looks like an opportunity does not advance the strategic goal of the organization, it is not an opportunity it is a distraction.

The planning capabilities will play a very important role because one of their tasks relates to support organizational efforts to plan its operational activities according to identified strategic priorities and in the same time to allocate resources related to these ones.

3. Defining performance[5]

The intelligence organization's strategy will have to be based on new definitions of performance and to develop new concepts of what "performance" means in the organization. The planning capabilities, based on the conclusions resulted from assessing specific activities will identify and argue for new measurements which will define the set of performance indicators at the organizational level. Along with a communicational process, these new parameters will have to be meaningful to the knowledge workers and to generate "commitment" from them. The idea of performance will need to reflect the answers to how to balance short term results with the long range prosperity of the intelligence organization.

4. Global competitiveness[6]

Today, no intelligence organization can achieve success alone, unless it measures up to the standards set by the leaders in the intelligence field. It is no longer possible to prevent and to combat the globally emergent threats from a national level. The cooperation between intelligence organizations all over the world is well-known and it has become a common thing. But this cooperation with the international intelligence partners implies, more than ever, to be equal in results to that of the world leaders in the field.

Therefore, in order to achieve great results, comparable with those of the leaders in the field, the organization's costs of development will reflect high prices. That implies to take action to become one of the best, by developing new technological capabilities in order to allow interdependency between the technologies and requirements of partners and to be on top regarding the intelligence productivity.

5. The growing incongruence between economic globalization and political splintering[7] represents another reality on which the intelligence organization's strategy will have to focus in a period of worldwide structural change and uncertainty.

The world economy is increasingly becoming global and we felt, we'll still do in the future, the effects of this reality during the economic crisis. But at the same time, political boundaries are not going to go away despite the European Economic Community rules and legislation.

Despite partnership economic treaties, political dissensions are obvious, and an economic war would be difficult to wage without affecting all the parties involved. An example is the way in which the European leaders have recently decided a range of sanctions against Russia as a response to the Russian government's policy and actions that threaten Ukraine's territorial integrity, its sovereignty and independence. Although they announced severe economic penalties, due to subsequent economic implications affecting not only Russia but Germany, France and other European countries, the sanctions have proved not to be effective in changing Russia’s policy lines.

It is obvious that the intelligence organization, in defining its strategy, should start out by considering these realities, in order to be prepared for the challenges that the next years are certain to raise. Also it has to be aware that the organization’s development will increasingly not be based on mergers or acquisitions or even on starting new valuable practices. It will have to be based on partnerships, joint ventures and all kinds of relations, with intelligence organizations located in other political jurisdictions.

Strategic planning is constantly challenged, and today more than ever before, with the issue that must support the intelligence organization to adapt rapidly to the security environment and with the best results. Progress is something that we all are trying to achieve, and planning makes it tangible, an integrated part of the organizational life, because through its processes it ensures the desired orientation. In an ideal way, a strategic plan serves as an instrument for continually reminding managers to evaluate the direction of their specific activities, according to their overall goals. In this way it helps them make solid, reliable decisions on how to best execute the objectives that advance the organizational strategy.

Building performance in the intelligence organization

In order to pursue incremental advantage while threats, vulnerabilities and challenges fundamentally reinventing the security landscape, intelligence organizations moved ahead and have already done much of the hard work of catching up on quality, speed and flexibility. Planning capabilities play a significant and important role in this matter, because along its developed processes and specific activities allow and support flexibility, speed and quality of the whole operational systems.

The specific vocabulary used by planning, indicates the goal as something that the intelligence organization want to accomplish within a specific time frame (often interchangeably called a strategic objective or a strategic priority), the strategy is the organizational long term plan or alternative methods of accomplishing that goal and the tactics are the short term actions required to fulfil a selected strategy. Goals, strategy, tactics and execution are part of the same dynamic process through which are long terms implemented priorities through short term daily operations.

Due to the dynamism of the actual security environment, when an organization sees an opportunity or realizes a threat, it can't apply the old solutions of yesterday because most of the time, all new challenges require new solutions operationalised by smart plans. From this point of view, the intelligence organization's strategy must be extremely flexible in its tactics, so that the officers be encouraged to determine how best to achieve it.

Today, achieving maximum results requires faster goal setting, in order to make the employers of the organization to act quickly and to make them aware that their activities must align with the organization's strategic objectives. One of the task of the planning officer is to monitor the implement of the organization's goals and objectives, process which involves a good communication with managers, those which must be aware when a new opportunity is identified. In order to make the organisation's vision and strategy well known and understandable inside the organization, good quality communicational processes accompany planning activities.

Planning offers a holistic point of view, sustaining the managerial act and the managers of the intelligence organization to have a complete perspective and to be able to move forward with clarity, because the right understanding leads, in most of the times, to right action. In problem analysis, the holistic approach takes into account the whole system of causes and effects that have an impact on the problem. We can say that planning officers offer to the deciders the whole image of a puzzle, the way in which different segments of activity are interconnected, and therefore they are able to identify viable solutions to the punctual organizational problems that arise.

As I illustrate in the next figure, planning capabilities play a significant role in four internal organizational functions: organizational policymaking, warning, monitoring phase outcomes, assessing specific activities – all of them in relation of interdependency.

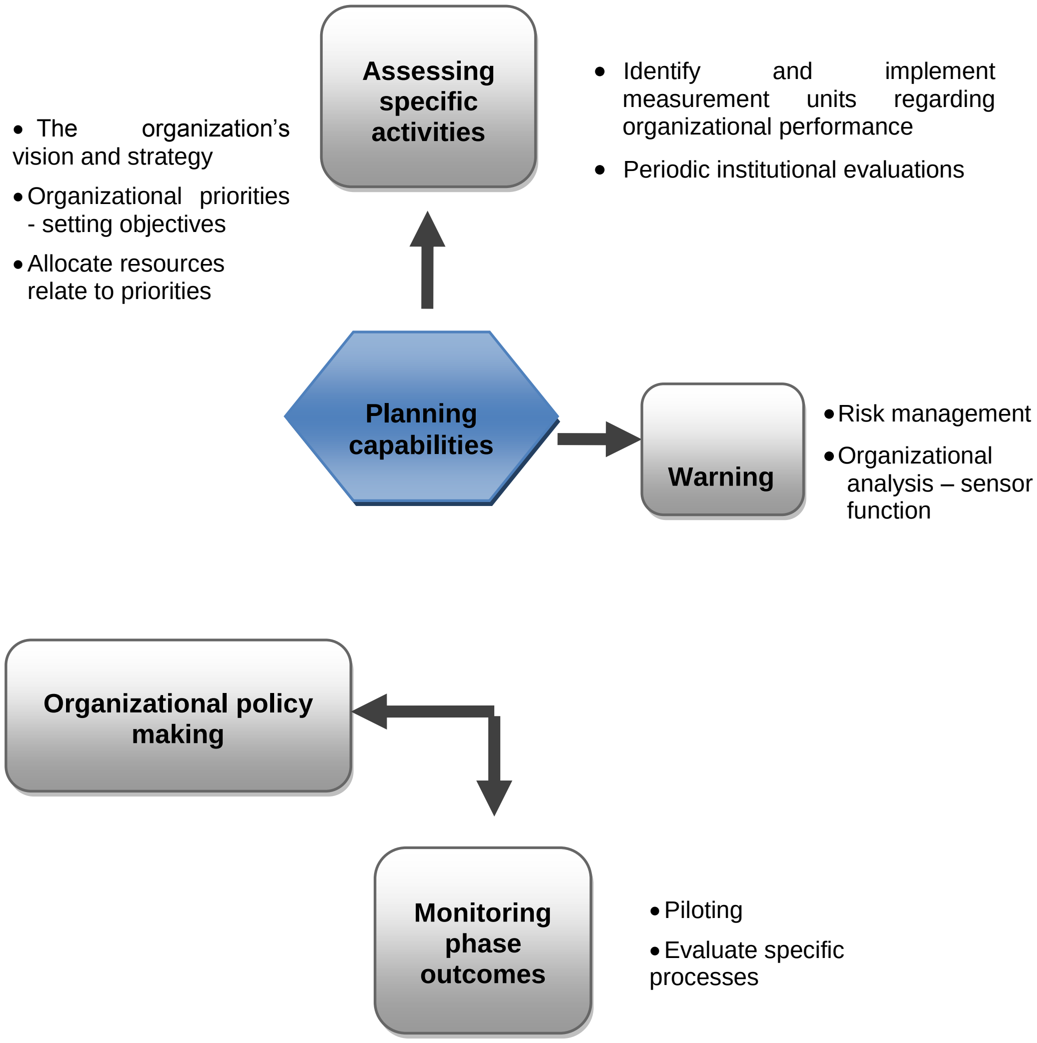

Assessing specific activities
• The organization's vision and strategy
• Organizational priorities - setting objectives
• Allocate resources relate to priorities
• Identify and implement measurement units regarding organizational performance
• Periodic institutional evaluations
Planning capabilities
Warning
• Risk management
• Organizational analysis – sensor function
Organizational policy making
Monitoring phase outcomes
• Piloting
• Evaluate specific processes

Figure no. 1: The role of planning capabilities

Also, *planning* within intelligence organization *provides alignment,* in order to support managers from all organizational levels to make decisions and to act faster, allowing the organization to get feedback and grow more quickly. It helps to create the organizational context, those fundamental references, being a promoter of change: it adapts and implement rapidly the needed solutions, reviews the plans annually, by semester, or even sooner, in other words sustains and permits the change which is frightening for most of us in opposition to the static which feels comfortable. But we must be aware of the fact that the most static systems are most fragile – changing is a natural and a defining aspect of life and we can't escape from it, that's why when we try to force to adopt a solution against the law of nature we fail.

A multiannual planning, having an annual review, will allow permanent adjustment to current challenges and the creation of unitary action guidelines will offer flexibility to the organization leaders' operational orientations for the solving of organizational needs. Therefore, a rapid translation of new requirements within the current activities plan is ensured by identifying objectives of different managing levels, starting with the strategic level to the tactical operational level. That is why one of the major tasks the responsibility of planning capabilities in the intelligence organization is identifying fundamental references for organizational managers to help them provide guidance needed to coordinate specific activities. These references are identified by analysing the external security environment, threats and opportunities that occur or are likely to occur in the future, as well as by analysing the internal organizational environment, those needs that once overcome lead to successful action.

At the same time, planning departments participate at creating a compelling view of tomorrow's opportunities and they move pre-emptively to secure the next organizational steps. That means taking into account issues like: resource effectiveness, operational consistency, identifying right goals and strategic objectives and making them tangible and real to employees at all levels.

To achieve the progress of the intelligence organization means to successfully manage in the next society, as Peter F. Drucker shows in one of its works, meaning to understand the realities which characterize the present and the future society and to base organizational policy and strategy on them, in order to be able to exploit the changes as opportunities for the organization.

"The goal is not to predict the future but to imagine a future made possible by changes in technology, global geopolitics, regulation, global climate, social movements and the like. For the future is not what will happen, the future is what is happening. The present and the future don't exclude each other, neatly divided between the five-year plan and the great unknown beyond. Rather they are intertwined. The long-term is not something that happens someday, it is what the organization is building or forfeiting by its myriad daily decisions."[8]

Planning capabilities are useful in *warning* the organization's decision makers about the problems and the opportunities with regard to the tasks included in the activity plans of the different organizational departments, we can say they assume the role of the organizational sensor, developing organizational analyses based on strategic organizational priorities underlining also the positive aspects of the organizational segments.

In this regard, their role is to make widely understood the potential threats to the specific actions developed at different organizational departments.

Another major task of planning departments is to focus every six to twelve months, on changes that might be opportunities - in two main areas:

a) The organization's own unexpected successes and unexpected failures in different segments of interest's activity - reflected by the conclusions reached by evaluating these segments - ;

b) Incongruities, especially incongruities in the process and also the process needs – especially when it comes to testing a new organizational process.

The officers of planning departments are often involved in participating in organizational pilot projects. Every improved or new organizational process needs first to be tested on a small scale - it needs to be piloted. Most of the times, planning officers offer support to a successful change through *monitoring phase outcomes* of the organizational pilot projects in order to find the possible problems or opportunities nobody anticipated. In other words, to ensure that the inevitable risk of change is small and it is clear where to place the change, how to place it and what steps to follow next.

The planning cycle reflects that the whole planning system is fundamentally based on *assessing the organizational specific activit*ies. Therefore, planning officers hand over to their beneficiaries' periodic reports which underline the problems and also areas where results are better, by evaluating certain organizational processes. The evaluation processes developed in a specific period of time and a specific area of interest provide the needed feedback from all organizational departments. This type of comprehensive feedback assessment enables the organizational leadership to see the problems that arise and which interfere in achieving the specific goals and objectives.

Hopefully that...

Hopefully in today's rapidly changing world, all intelligence organizations will develop planning capabilities to provide constantly answers to the leaders' challenging questions, such as: How can we keep improving? What can we do that is better? How can we provide a better security environment? Which are our next valuable steps?

In order to answer these questions, the intelligence organization must have a viable strategy that can actually achieve quantifiable goals within specific constrains of time and cost. Also, it needs special departments whose activities ensure monitoring of organizational processes in order to be able to track the direction as needed, ensuring through specific tasks that the organizational leaders don't choose a bad strategy and that they are not speeding in the wrong direction?

Managers look for creating high performance cultures, accelerating organizational growth and identifying the opportunities and the weak organizational areas. Therefore, planning capabilities are of real help for them, supporting all daily activities to move toward the accomplishment of the organization's ultimate goals.

In addition to its value in policymaking and guiding decisions concerning alternative courses of action, planning is a key element to the organization's top management and some of the top management's decisions may be concerned with the costs implied by each segment of activity or regarding the main areas which need a higher attention and new operational priorities, also.

In this matter, the conclusions of the periodical assessment of all of the activities developed in the organizational environment, by analysing information from the organizational structures, is a potential benefit of the planning capabilities. It underlines that the management of the entire intelligence effort involves the planning and direction process, starting from the identification of the need for data to the final delivery of an intelligence product to a beneficiary.

Supporting managers from all organizational levels to innovate is another potential benefit of the planning activities because every organization today, including the intelligence organization, has to be designed for change as the norm and to create change rather than react to it. Planning must be aware that the results of any organization exist only on the outside and for that the organization must develop great concern with the environment, which is beyond its control.

Managers also should focus on the results and performance of the organization, which is one of the most difficult, one of the most controversial, but also one of the most important tasks. It is therefore the specific function of planning to organize the resources of the organization for results outside the organization, starting from relating the needed results in correspondence with the priorities.

Therefore, planning puts first the intended results helps to organise the resources of the organization to attain these results by making better known that it is a necessity to make the intelligence organization capable of producing results outside of itself - and this will represent one of the major future concerns of the planning departments in intelligence organizations.

To define quality in intelligence work and to convert the definition into intelligence organization activity is to a large extent a matter of defining the task. It requires the difficult, risk taking and always controversial definition as to what „results" are for the organizations in the field. The starting point is to know how to do the specific task. For that issue planning officers participate in identifying the main measurement units, which reflect the performance of the intelligence organization.

Ultimately, planning involves most of the time analysis activities, in order to relate its specific processes to the requirements and needs of the organization's leaders and managers – as one category of beneficiaries of its activities. From this point of view, planning officers should look for the most useful information for elaborating and delivering their reports. That's why planners must make seasoned judgements and issue warnings based on their mastery of analytic tradecraft.

In conclusion, one thing is certain for the intelligence organization: building planning capabilities is a necessity in times of profound and rapid changes. Not to develop such a capabilities doesn't ensure the organizational failure, but it doesn't guarantee its success either. An intelligence organization that doesn't develop its own structure to support the organizational management, incorporated throughout its structure, meant to implement the overall strategy – through the participation in identifying the next steps to a future progress – would rather reflect its lack of concern to become one of the best organizations in the field.

That is why, in a professional intelligence organization of the 21st century, building the planning capability is a must!

References

[1] Gary Hamel, Bill Breen, „The future of management", Harvard Business School Publishing, Boston, 2007, pp. 9.

[2] Peter F. Drucker, „Management Challenges for the 21st Century", HarperCollins Publishers, Inc., 200, pp.44-69.

[3] Ibidem.

[4] Ibidem.

[5] Ibidem.

[6] Ibidem.

[7] Ibidem.

[8] Gary Hamel, C.K. Prahalad, *op. cit,* p.7.

BUILDING THE FRAMEWORK FOR USEFUL INTELLIGENCE – THE CONTEMPORARY NEEDS AND RISKS

Antonia COLIBĂŞANU[*]

Abstract

The paper assesses how the current phenomenon of 'information overload' redefines the architecture of intelligence processes, underlining their utility function. The architectural design of intelligence processes today focuses on functions that allow flexibility, working with concepts borrowed from the economics, psychology and neuroscience. The conclusion underlines the interdisciplinary characteristic of intelligence systems at the organizational level and the need for its implementation considering the increasing importance of rapid reaction and adaptation of the function of competitive intelligence processes.

Keywords: competitive intelligence, intelligence process, strategic analysis

Introduction

Companies and nation states' governments both confront the phenomenon of "information overload". As technological progress facilitates speed, the information needs of all global actors seem to grow at an accelerated pace. From the companies' board meetings to nation states' military conferences, the common preoccupation refers to ways of making better use of technology for information sharing at the organizational level. As opportunities open and close in a matter of hours and technologies emerge in weeks and mature in months, there's a feeling of urgency for investment in technology that will enable us "know more". Nevertheless, the general complaint of today is the same as the one decades ago, when information was more difficult to acquire: decisions are made without *enough* information and both businesses and governments are suffering from lack of *sufficient* knowledge. The key word, intrinsic to the intelligence concept: *usefulness,* is gaining even more importance.

[*] Stratfor Romania

What is *Useful Intelligence?*

Acquiring knowledge is the single most important, strategic need of any organization today. Apparently a pleonasm, as intelligence is considered to be by definition useful, the global environment today, characterized by the high level of inter-connectivity and a constantly accelerated technological progress, forces organizations to adapt their information architecture and produce intelligence that is effectively used by the decision-makers. This emphasizes the 'utility' concept for the intelligence process developed at the company or government level.

In economics, utility is defined as the ability of a good to satisfy the needs or wants of the economic actor. Game theory works with 'expected utilities', associating utility[1] with the concept of options that an actor has at a certain point in time, each option having an assigned risk level.

$$U = f(needs, wants) = f(option_x * associated\ risk_x)$$

Simply put, *useful* intelligence is the process that transforms data and information into actionable knowledge for decision-makers. The utility of the process comes from answering the right questions – those supporting the strategic pillars and the overall long-term strategy of the organization. The definition, selection and prioritization of relevant questions is dependent on the organization's needs. The utility of the intelligence process is defined by the degree to which it responds, in real time, to the specific needs of the organization.

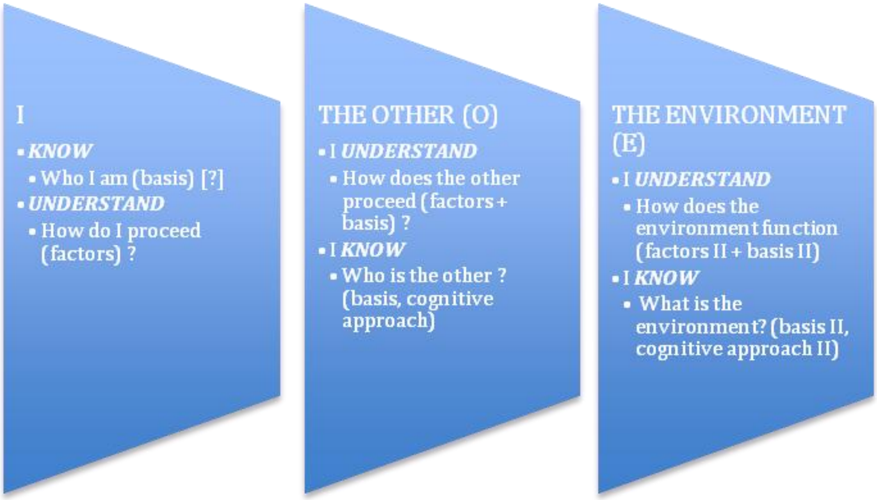
The economic intelligence process is generally built considering the three major needs of organizations, following on their goal to increase and maintain their competitive advantage: 1) understanding the external forces, 2) protecting itself from risks arising from within the organization or from the outside world, 3) understanding and influencing the external environment, in order to support its position[2]. The three needs – and functions – of organizations are interlinked, depending on the type of organization, its development level, its long term strategy as well as its immediate concerns and constraints. A global company that looks to expand its services branch to accompany production in all countries it operates, will focus on first understanding the external environment. In the second phase, of making the services branch operational, it is likely that its influence needs will grow and therefore marketing efforts, projecting internal values on to the surrounding environment, will intensify.

Creating the *framework* for the intelligence processes

Our decisions and ultimately our activities are influenced both by the persons with whom we interact, the general environment that we live in as well as ourselves, our personal history – that creates both our personality and defines our attitude towards certain factors. At the same time, everything that we decide to do and end up doing adds one more page to our personal history, leaving a mark on our personality and influencing our future decisions. If we were to describe the individual decision-making cycle, we would start by referring to the bases: the decision maker and his/her knowledge about things, defining the ways in which he/she proceeds – leading to the process of understanding what internal factors influence the decision. The second step considered when taking a decision is understanding the factors affecting the other – the decision-making partner or competitor, in an attempt to define the other's basis and therefore have the decision-maker acquire knowledge on opportunities and constraints regarding the behavior of those with whom he/she interacts with. The third step refers to the environment – understanding the factors affecting the general environment that affects both the decision-maker as well as the people with whom he/she interacts with (the others). This builds up knowledge on constraints and opportunities, common for all actors, not only the decision maker, but in relation with whom a new basis is created.

The model for the simplest individual decision-making process, as presented in the figure bellow is based on the generally accepted assumption that human cognition – both conscious and unconscious is transforming information – what we *know* – into knowledge – what we *understand*.

Figure 1. The decision-making process


I
▪ KNOW
▪ Who I am (basis) [?]
▪ UNDERSTAND
▪ How do I proceed (factors) ?
THE OTHER (O)
▪ I UNDERSTAND
▪ How does the other proceed (factors + basis) ?
▪ I KNOW
▪ Who is the other ? (basis, cognitive approach)
THE ENVIRONMENT (E)
▪ I UNDERSTAND
▪ How does the environment function (factors II + basis II)
▪ I KNOW
▪ What is the environment? (basis II, cognitive approach II)

Source: author

At the organizational level, the intelligence process supporting the decision-makers needs would recreate the same process while taking into account the specifics of the enterprise.

Considering the specific organizational needs mentioned in the earlier chapter, the *protective function of the intelligence system* refers to the *"I"* from the generalized model above, defining what the organization is and fears most, considering its past and present activity. A company's protective intelligence system would therefore focus on the following activities:

- identify the vulnerabilities, risks and needs of protection both at the level of the company's operational systems and global level;
- establish and monitor the physical and IT security system protocols that will be implemented through of the company's code of conduct, limiting informational leaks as well as direct attacks on the organization's activity;
- monitor, control and revise efficiency of protection measures employed;

- adapt protection measures to new needs, new risks and vulnerabilities that may appear;
- create a reporting system on major developments, risks and improvements at the level of organization.

Regarding the *"others"* from the model above, organizations interact with their peers: competitors, partners or suppliers. At the level of the intelligence system, this refers to the organizational need of *understanding the external forces*, notably external players that it depends on, in one way or another. At this level, the intelligence process focuses on the following activities:

- establish the specific informational needs for the organization, depending on the relationship and level of dependency on the external players (competition vs. cooperation);
- conduct research for information on external players; research can focus on structured and/or non-structured information, external and/or internal information;
- establish formal and informal networks of information within and outside the company that supports the activity of gathering information on the external players;
- create an analysis system for the information, considering the specific requirements and needs of the organization
- create a reporting system on the analyzed information about the external players.

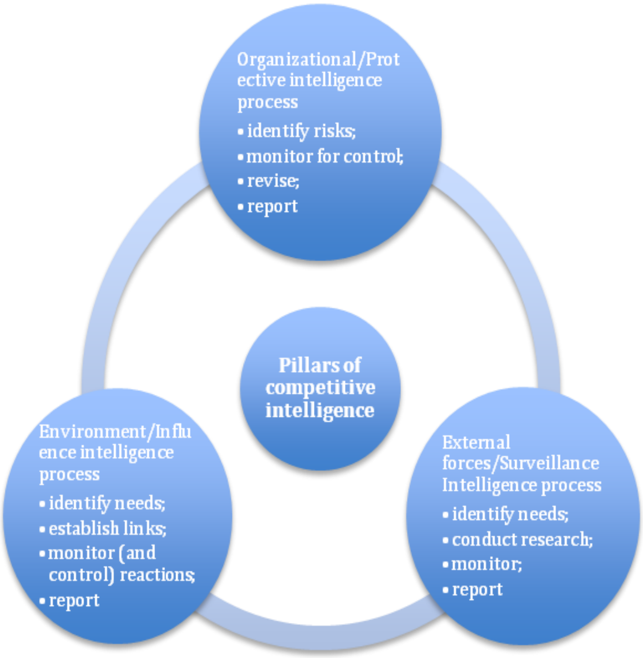
The *environment,* as it is shown in the model is considered through the third dimension of the intelligence system, coming out of *the need for the organization to understand and be able to influence the external environment, with the goal of promoting, supporting its own position*. This function of the intelligence system is supported by the following activities:

- identify the needs for influence based on the existing dependence links (clients vs. suppliers, potential clients – civil society, etc.)
- identify tactical and strategic objectives – differentiate between short and medium-long term in considering influence intelligence tactics

- identify methods and channels to be used for influence and monitor their efficiency – PR activities, lobby activities, informational intoxication, disinformation
- monitor the influence activity of the other players and their efficiency
- create a reporting system on the results for the decision makers

Just like in the model above, the three areas intersect and reciprocal changes are created, which leads to the three pillars of the intelligence process has a dual-use function, as they're both sending and gathering information, both depending and creating dependencies with the outside world. Just as in the model

Figure 2: The three pillars of the organizational intelligence process


Organizational/Protective intelligence process
• identify risks;
• monitor for control;
• revise;
• report
Pillars of competitive intelligence
Environment/Influence intelligence process
• identify needs;
• establish links;
• monitor (and control) reactions;
• report
External forces/Surveillance Intelligence process
• identify needs;
• conduct research;
• monitor;
• report

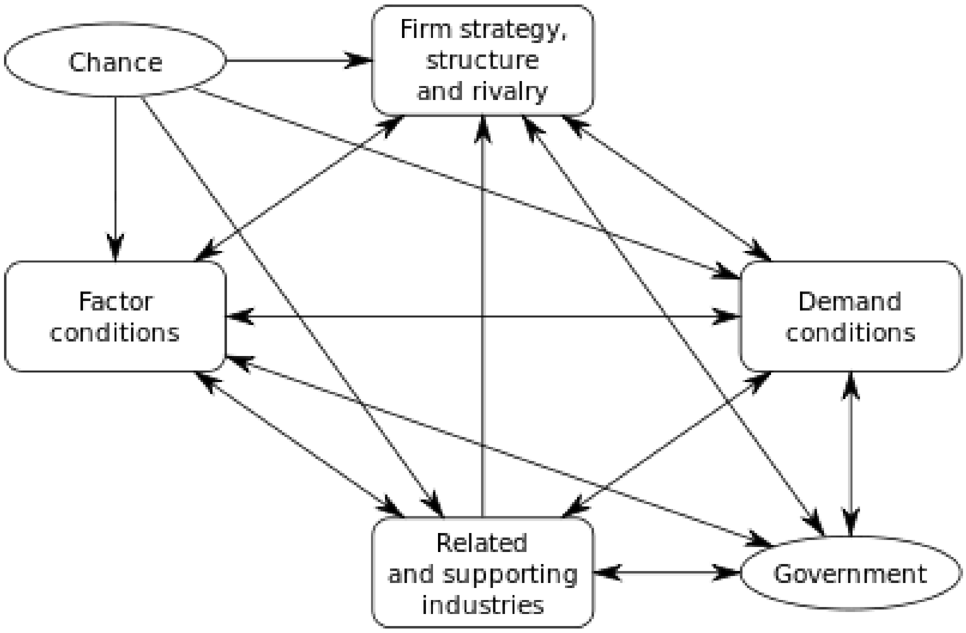
Source: author

The purpose of intelligence is to serve the decision making process. This is why it goes hand in hand with strategic management, always serving a precise goal. In this sense, economic intelligence and strategic planning are depending on one another at the organizational level. The organizational situational awareness is key to both processes, constituting the base for establishing objectives and long-term goals. Referring to the “I” level of the model described above, the situational awareness at the level of the company or any other kind of organization is maintained through periodical SWOT (Strengths-Weaknesses-Opportunities-Threats) analysis.

The initial results of the SWOT analysis give the initial information about the organization referring to its perceptions on the internal stability (economic, security dimensions both considered), external environment and competition. Such knowledge on the organization is the platform for the strategic planning process, establishing resource allocation rules and sending a clear message on priorities, risks and objectives, channeling the information into the intelligence process. The periodical SWOT assessment serves the first pillar of the intelligence process as it allows the organization to identify (new) risks for pursuing the long-term goals of the company and to outline critical parameters that support the long-term goals.

Michael Porter’s diamond model is also essential for the intelligence process and strategic planning. The economic model that he described in the ‘90s in his book “The Competitive Advantage of Nations” has been reshaped to fit current organizations’ needs, as the intelligence process gathers and analyzes information of a constantly changing environment.

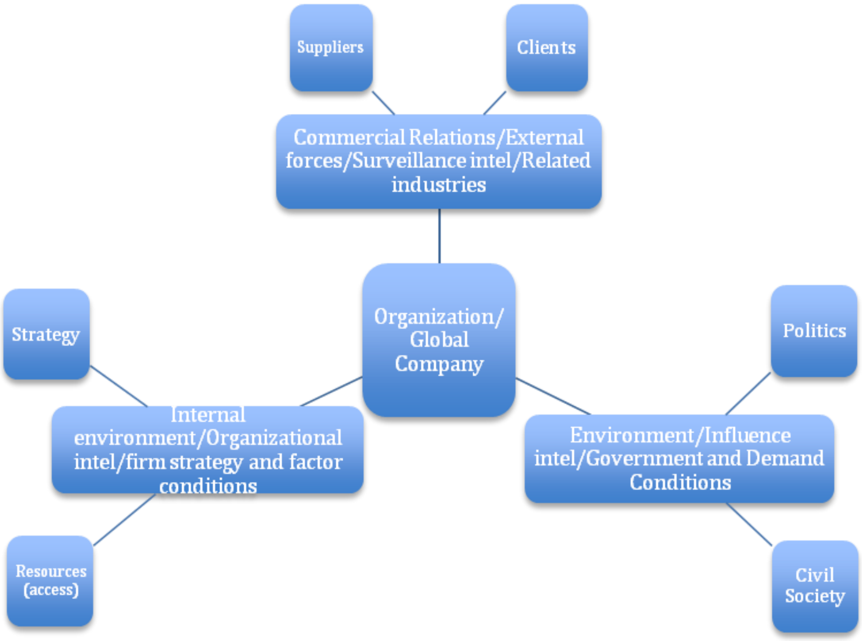
Figure 3. Michael's Porter economic model


Chance
Firm strategy, structure and rivalry
Factor conditions
Demand conditions
Related and supporting industries
Government

Source: Traill, Bruce; Eamonn Pitts (1998).
Competitiveness in the Food Industry. Porter (1990, p. 127), Springer. p. 19.

Considering the three pillars of the intelligence process, the factors that Porter considered for his model, as well as "chance" as the necessary setting for the positive outcome of the environment conditions, have been rearranged around the organization, as it appears in the figure bellow. The protective function of the intelligence process gathers the factors under firm strategy, structure and rivalry as well as the factors relating to access to resources (factor conditions as it appears in the original model elaborated by Porter). The influence function is served through all public relations, communication and lobbying activities towards governments and the civil society - therefore gathering both the governmental and demand conditions from the initial Porter model. Surveillance intelligence for external forces is looking at the related and supporting industries.

Figure 4. Michael Porter's diamond re-written for intelligence processes


Suppliers
Clients
Commercial Relations/External forces/Surveillance intel/Related industries
Organization/ Global Company
Strategy
Politics
Internal environment/Organizational intel/firm strategy and factor conditions
Environment/Influence intel/Government and Demand Conditions
Resources (access)
Civil Society

Source: author

Based on the interaction between the six factors that the intelligence process is analyzing using Michael Porter model, decision makers will be able to establish operational plans that support the overall strategy serving the long term goals of the organization, always at the center of any decision. The information flow under this model would come both from internal (accounting, production, commercial departments, etc.) and external sources (clients, suppliers, governments, civil society, etc.). The intelligence process also has to take into account the information coming from employees that can refer both to internal and external factors affecting the organizational operational and strategic plans.

Considering the realities of the 21st century and the constant technological process, under such processes, organizations are facing the "information overload" problem where, because of too many sources and channels for data and information, the system often deals with more information than it needs. This adds to the goals of the intelligence process design: it needs to be flexible in selecting and validating sources of data and information, while ensuring a structure of information that allows good, efficient synthesis. Documentation analysis helps eliminating the surplus of unwanted information as it not only serves for researching good sources of information but also validates and create networks for collecting information according to the needs. Such analysis needs to be implemented at the level of all three pillars supporting the intelligence process.

Knowledge building and *the contemporary needs and risks*

The ultimate purpose of the intelligence processes developed both at the companies and a governmental level is acquiring knowledge. This relates to the contemporary need of being able to make information actionable so that it prevents organizations from falling behind, and not being able to adapt to the constantly changing environment and treating change as a risk more than an opportunity. In a way, this relates to the dual face of crisis – if we are to understand constant transformation as constant crisis mode: some see the opportunity that may lead to future success, some see the risks and negative effects that may lead to failure. Perception is what ultimately makes the difference, being dependent on the one hand on the formation of the decision maker and on the other on the analysis of the organization's intelligence process.

Basic neuroscience teaches us that the human brain functions, generally speaking, on a dual dimension framework: where automatic, parallel processes of the unconscious are supplementing the controlled, serial processes of the conscious. The decision-making model described in the chapter above is a map of a serial process, therefore a controlled action at the brain level. However, the very first question relating to the "I" element – "who I am" includes the automatic, parallel unconscious processes summing up what is subjective to human beings. Automatic processes do not refer only to affectivity, but also to cognition. While a person likes another person without initial reasoning, the positive of the affection may in time transfer into models – thus creating cognitive processes where what was liked multiple times and therefore positive transforms into a "true value" for the entire system. We recognize the value of a certain object or person as they relate to our own system of values, developed in time through the process of recognizing such values.

Brain mapping can certainly give interesting models for management and leadership. If it would be possible to completely untangle the secrets of the human "black box". What we do know however is that "the brain performs a huge number of different computations in parallel. Because of the massively interconnected 'network' architecture of neural systems, computations done in one part of the brain have the potential to influence any other computation, even when there is no logical connection between the two"[3].

Extrapolating, the very same is true for an organization. In fact, the network architecture of the neural systems can be assimilated to the decision-making model and therefore, to the three pillars of the intelligence system already described above. However, the difference is that while it is natural for human beings to sustain the computational level constantly, day and night, the organization can only design a controlled process where automation is dependent on the efficiency of collective information mining and analysis.

While for humans "controlled processes occur at special moments when a person encounters unexpected events, experiences strong visceral states or is presented with some kind of explicit challenge in the form of a novel decision or other type of problem"[4], controlled processes are constantly shaping up organizations. It is them who define 'perception', linking the functions of the three pillars of the intelligence system.

The knowledge curve, defined through the needs that an organization has at a certain moment, is dependent on the interdisciplinary evolution of the three pillars supporting the intelligence system. Being linked to the organizational planning activities, the knowledge curve is less about information and more about the reaction time.

New environmental risks relate to both slowness in reaction to expected events and incorrect or no reaction towards the "black swan" type events. Human instincts are usually the guarantee of good reaction towards the 'black swan' type events even if they don't always support a quick reaction towards all other expected events occurring. This is why, generally, the intelligence processes have been designed to primarily support the decision-making systems under normal conditions, with calculated risks. Current conditions force organizations to adapt to the unexpected – and therefore intelligence processes are likely to suffer transformations, in the sense of focusing analysis capabilities on both situational awareness and forecasting functions.

In this sense, recent studies – especially in what regards behavioral economics[5] – show that neuroscience, along with psychology have started to become more common in analyzing the way in which organizations operate and are structured. Considering this, we can also draw parallels in what regards the intelligence process architecture.

Taking into account the human features, characteristic to both the automatic and controlled processes, needed for the success of an intelligence operation[6], we obtain the following list, in relation to the three pillars that were mentioned in the chapter above:

- **a neutral to negative mindset** is necessary for both organizational and surveillance intelligence processes, a process that is based on finding the right questions to answer, **under the premises of suspicion** being necessary especially in the initial steps of the process – this is founded on the idea that it is the job of marketing to sell a project and to be optimistic about it, not of the intelligence process as intelligence looks at the milestones of the project more than at the project itself
- the architecture needs to ensure that **clear missions/goals** are being set up for all projects undertaken by the intelligence system from the very beginning – the intelligence department

doesn't need to report "everything about the project", but respond to finite and clear questions. It needs to **tell what and why you need to know something**.

- the architecture must be built in such a way that it **ensures and checks trust levels** for the relationship between the intelligence process and the organization – in order to provide information about topics of interest the intelligence team needs to deeply know the organization is ("I" function)
- the **specialization in the general**: the architecture of the intelligence process needs to ensure the system is **connecting the dots**. This ensures that the primary function the system responds to is always assess by needs, something that is requested by each of the three pillars above
- the process needs to **identify the knowledge base** – the process must never rely only on the information given by the client (a department within the organization) but do its own inventory
- the architecture of the intelligence process needs to ensure **coordination between time-money-optimal position between the two** to get the most useful information and transform it into knowledge in due time. It needs to provide answers, on each of the three pillars for the following questions: "how long do I have to get the answers? What is the budget and the return? Can the job be done?"
- the architecture needs to be designed in such a way that the intelligence processes **take advantage of the knowledge and experience of others** and avoid the high cost of moving up the learning curve of the intelligence system. The system doesn't need to become an expert into a field, it needs to assess needs and solve problems of various fields that the organization is concerned with
- the architecture needs to **provide quick ways to identify the sources of information – documentation analysis** is very important considering time constraints
- the intelligence process, through the three pillars has to always ensure the **retasking function** is embedded in the system – it is essential to be able to stop and evaluate after each step

taken in the process of finding solutions or identifying new risks related to a certain area relevant for the decision makers

- considering the current conditions in the environment, the intelligence system architecture needs to ensure that it is able to push the passive to the limit: intelligence process needs to offer **active, actionable intelligence** for the decision makers in a timely manner (meaning there is no need for the problems to be solved and final reports to be sent to the decision makers – but, now more than ever, the focus is on feeding the decision makers with knowledge needed during the process of finding ways for a solution)
- final analysis and evaluations need to **raise new questions** and therefore, the intelligence process cannot be designed as a finite one, but, in a way, a cyclic one.

The adaptation of the intelligence process is synonymous with adding flexibility to the system. Parallel and serial architecture is synchronized, increasing the general usefulness of intelligence.

Conclusions

Organizations need to support architectures that are designed to be flexible and adaptive to the changing environment. 'Information overload' is a growing concern for both private and public decision makers. International business and security is greatly dependent on actionable information rightfully analyzed. Information needs to be rapidly transformed into knowledge. At the core of the transformation process stands, more than ever, perception, a qualitative function that only the human being is capable of having.

Perception and utility both are concepts that are largely discussed in behavioral economics. Considering both technological progress as well as the contemporary risks that organizations face today, the intelligence systems need to learn and import "human functions", learn from neuroscience and psychology.

Working with the general equation of the utility, as defined by economists, we conclude that, ultimately, in the intelligence process usefulness comes from answering the right questions – those relevant to the decision makers in what regards the long-term strategy of the organization. However, to be sure that the organization is responding, in a timely manner, to the environmental challenges of today's world, looking at serial models that indicate that is cyclical but focused action on the information available is key. Based on a simple, three factor model, I have outlined the intelligence framework as a three pillars model that goes hand in hand with strategic analysis. In this framework, the model that Michael Porter outlined in the '90s, has been transformed to serve each function that the three pillars indicated, also considering the realities of the business environment at the beginning of the XXIst century.

Going further, considering the high level of interconnectivity at the global level – both between people and organizations, I have taken into account neuroscience findings supporting behavioral economics and realized a list of functions that, similarly to the human processes, are adding value to intelligence architecture developed at the organizational level. The practice of intelligence systems has developed as a reaction to the changing world and the new risks – from "black swans" to anticipated events. Flexibility is probably one of the most important characteristics of the intelligence processes today, especially when we talk about competitive and economic intelligence.

Bibliografy

1. Camerer, Colin and Loewenstein, George and Prelec, Drazen, *Neuroeconomics: How Neuroscience Can Inform Economics*, Journal of Economic Literature, 43 (March), pp: 9-64,.http://people.hss.caltech.edu/~camerer/JELfinal.pdf.
2. da Rocha, Armando Freitas and Rocha, Fábio T., *Free Will from the Neuroscience Point of View*, September 14, 2013, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2325902.
3. Heuer, R.J., Jr., Psychology of Intelligence Analysis, Chapter 4 "Strategies for Analytic Judgement", Washington D.C.: CIA Center for the Study of Intelligence, 1999, http://www.odci.gov/csi/books/19104/art7.html
4. Bargh, John A. and Tanya L. Chartrand. 1999. "The Unbearable Automaticity of Being." *Am Psychol,* 54:7, pp. 462-479.
5. Waltz, E., "Knowledge management in the intelligence enterprise", Artech House, 2003, pp. 27-43.

6. *Friedman G., Friedman M., Chapman C., The Intelligence Edge,* Century Business, 1998.

7. Cunningham W., McNamara P - *Business Intelligence and Strategic Choices*, BenchMark Consulting International, Internal Documents, January 2007.

8. Nicolescu O., *Management bazat pe cunostinte,* note de curs – Scoala Doctorala ASE 2007, nepublicat.

9. Rodenberg J. H. a. M. - *Competitive Intelligence and Senior Management*, Eburon Uitverij B.V., 2008.

10. Moffet M., Stonehil A., Eiteman D. - *Fundamentals of Multinational Finance*, Prentice Hall, 2008.

11. Gilboa, I., Theory of Decision under Uncertainty, Cambridge University Press, 2009.

12. Begin L., Deschamps J., Madinier H., Une approche interdisciplinaire de l'intelligence economique, Cahier nr. HES-SO/HEG-GE/C—07/4/1/CH, 2007.

References

[1] Gilboa, I., Theory of Decision under Uncertainty, Cambridge University Press, 2009, pp. 51.

[2] Begin L., Deschamps J., Madinier H., Une approche interdisciplinaire de l'intelligence economique, Cahier nr. HES-SO/HEG-GE/C—07/4/1/CH, 2007, pp. 4-5.

[3] Camerer, Colin and Loewenstein, George and Prelec, Drazen, *Neuroeconomics: How Neuroscience Can Inform Economics*, Journal of Economic Literature, 43 (March), pp: 9-64, http://people.hss.caltech.edu/~camerer/JELfinal.pdf

[4] da Rocha, Armando Freitas and Rocha, Fábio T., *Free Will from the Neuroscience Point of View*, September 14, 2013, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2325902.

[5] Camerer, Colin and Loewenstein, George and Prelec, Drazen, *Neuroeconomics: How Neuroscience Can Inform Economics*, Journal of Economic Literature, 43 (March), pp: 9-64, http://people.hss.caltech.edu/~camerer/JELfinal.pdf.

[6] *Friedman G., Friedman M., Chapman C., The Intelligence Edge,* Century Business, 1998, pp. 56-84.

RESHAPING INTELLIGENCE AND SECURITY IN THE 21ST CENTURY

William J. LAHNEMAN[*]

Abstract

The 21st Century security environment contains threats and opportunities that require intelligence agencies to adopt new structures, processes, and skill sets – in essence a new intelligence paradigm – if they are to continue to provide effective intelligence products to policymakers. This paradigm must be capable of producing effective intelligence on both traditional state actors and transnational trends and actors. These products must identify potential opportunities as well as threats. In contrast, the traditional intelligence paradigm that this new paradigm will replace focused on identifying threats posed by state actors.

Since the new paradigm must be effective against both traditional and new threats, it must include the old one in its entirety. Both old and new elements must function smoothly without creating destructive interference.

Constructing the new paradigm involves developing new collection methods covering a much wider range of sources than has traditionally been the case. These new methods must include data management technologies to allow for the analysis of these massive volumes of information plus all of the raw intelligence collected by the INTs. Much of this information must be provided voluntarily by its owners.

The collection and management of such large volumes of information require a change in the way that intelligence agencies view information flows. A new category of information, trusted information, must be added to and treated co-equally with the traditional categories of open and secret (classified) information if intelligence organizations are to gain access and be able to effectively analyze the necessary information. The introduction of the concept of Controlled Unclassified Information (CUI) in the U.S. government indicates that needed revisions to traditional concepts of information flows are already being initiated. However, while necessary, the adoption of CUI will not be sufficient for managing 21st Century information flows successfully. Rather, to be effective, trusted information networks must be global and include both public and private sector participants.

Keywords: intelligence, security, threats, opportunities, new intelligence paradigm

[*] Embry-Riddle Aeronautical University Daytona Beach, FL USA

The changing security landscape

National intelligence organizations will need to change their organizational structures and processes, as well as the skill sets of their knowledge workers, to remain effective at providing intelligence as the 21st Century continues to unfold. To add value to the policymaking process, intelligence products must give policymakers a decision advantage. This advantage must come not only from the timely warning of impending attacks but also by providing leaders with knowledge that enables them to improve their policies across a wide range of domestic and foreign policies.

Three principal factors drive this need for change. First, the security environment itself is in flux. This environment, which used to be characterized by threats posed by various state actors, has now transformed into a landscape in which non-state, transnational actors compete with state actors for the attention of intelligence organizations. This is an important change, since the nature and operational methods of transnational actors such as terrorist organizations and organized criminal networks are different than those employed by states. Perhaps the emergence of the Islamic State of Iraq and the Levant (ISIL) – a quasi-state entity capable of controlling territory – arguably constitutes a third kind of threat, a "blended threat" that embodies both state and non-state actor qualities. Lastly, the increasing awareness of the threats posed by certain emerging global trends – climate change, energy dependency, and disease outbreaks, for instance – has added these and related topics to the list of intelligence requirements. Such tectonic shifts in the international security environment point to the need for extensive changes in how intelligence organizations are structured, how they process information, and how their workers are educated and trained.

Second, the requirements that policymakers place upon intelligence agencies have expanded beyond the kinds of threats listed above. In addition, policymakers also desire intelligence agencies to provide *opportunity analyses* to help them optimize their country's navigation of emerging economic, military, and social trends. Policymakers want to be able to learn of opportunities to enhance the physical security of their citizens, improve policies to foster economic growth, and make progress on democratization and human rights.

Third, the rate of technological development continues to accelerate, and such developments combine to form mega-trends such as globalization, the information revolution, the rise of social media, and the emergence of big data. And the rate of change is accelerating. One study asserts that the amount of data stored in electronic form worldwide is increasing at over 50% per year![1] These developments pose both threats and opportunities to intelligence agencies. They constitute threats when adversaries utilize new and emerging technologies in innovative ways to avoid detection by intelligence organizations and perpetrate attacks. They provide opportunities to the extent that intelligence agencies harness new technologies to provide them with powerful new collection and analytic tools. Of course, since emerging technologies are just that – *emerging* – their full capabilities, functionalities, and applications are unclear. When combined with the fact that government bureaucracies tend to resist innovation, intelligence agencies might not embrace new approaches as readily as their more agile adversaries.

Intelligence organizations' response to the changing security environment

During the 20th Century, intelligence agencies spent the preponderance of time and assets providing intelligence about state-based threats. By the dawn of the 21st Century, however, policy makers and their national intelligence organizations also had begun to focus on transnational threats such as transnational criminal networks and other disturbing global trends. Following the attacks by the al Qaeda transnational terrorist network against the United States on 11 September 2001, providing effective intelligence against transnational threats became the top priority.

Intelligence agencies' efforts to develop sources and methods to collect information and produce intelligence about state-based threats were largely successful. They produced what we call today the five INTs: SIGINT, HUMINT, GEOINT, MASINT, and OSINT.[2] These

INTs are optimized to collect the most important elements of intelligence pertaining to state-based threats. However, using these collection techniques to gather intelligence about transnational actors has proven inadequate. While many traditional techniques remained necessary, they were not sufficient to produce effective intelligence against transnational threats. This condition resulted from the fact that the characteristics of each type of threat are different and demand different approaches. Table 1 displays some of these significant differences.

At the same time that transnational threats were moving to center stage in the intelligence world, policymakers also increased their demands on their intelligence agencies for opportunity analyses. In the highly uncertain atmosphere of the post-Cold War world, policymakers wanted their intelligence organizations to help them optimize their countries' national interests, not just warn about impeding threats. How to enhance the physical safety of citizens, how to sustain and improve economic growth, how to support human rights and democratization?

Policy makers wanted answers to questions like "How does globalization work and what are its next developments? Can we improve our indications and warning for disease outbreaks and pandemics? How will the rise of big data and the growth of electronic information exchange change how economies operate? How will climate change affect the world in twenty years?

Providing effective intelligence about these threats and emerging trends requires that intelligence agencies collect and process vast amounts of information from nontraditional sources. The scale of these information demands mandates that intelligence organizations become adept at large-scale data management functions, including data mining activities employing pattern recognition, artificial intelligence, and extensive use of IT utilities and middleware. Furthermore, collection on such a large scale means that intelligence agencies cannot achieve these results alone, but rather must depend on the voluntary contributions of many entities, including foreign governments and private firms.

Table 5-1. Differences Between State-based and Transnational Threats

	State-based Threats	**Transnational Threats**
Nature of Threat	Predominantly military	Predominantly non-military
Information Requirements	Limited: emphasizes secrets	Enormous: most required information is not secret
Nature of Indicators (pieces to puzzles/adaptive interpretations)	Large and small pieces	All pieces are small. There are no large pieces.
Importance of Pieces	Large pieces are more important than small pieces. Values are static.	The value of each small piece can change from moment to moment
Durability of Solutions	Relatively constant: "Picture" experiences slow, incremental changes	Dynamic: Values of pieces and, therefore, meaning of adaptive interpretation, changes rapidly
Need for updates to analysis	Periodic (to detect major changes)	Continuous

Source: William J. Lahneman, *Keeping U.S. Intelligence Effective: The Need for a Revolution in Intelligence Affairs* (Lanham, MD: Scarecrow Press, 2008):

The need for a new intelligence paradigm

When all of these developments are considered, it is easy to be overwhelmed by the sheer scale of what is required for intelligence agencies to provide effective intelligence on threats and opportunities in the 21st Century security environment. However, it is useful to keep in mind that any new approach to intelligence must provide four major functions:

- It must retain and provide ways to refine and enhance intelligence organizations' traditional strengths. This is because state actors still remain the predominant players in global affairs. Many pose potential threats to other states and thus require the continued close attention of national intelligence agencies. As a result, intelligence agencies must continue to refine the collection and analytical tools that proved successful against actors such as the USSR during the Cold War. These methods – essentially the five INTs – remain the most appropriate way to penetrate these actors, and they are the only way to provide intelligence on secretive, authoritarian states such as North Korea, Iran, and, increasingly, Russia. This does not mean that current tolls will be sufficient to track state-based threats. On the contrary, the incorporation and continual refinement of new technologies to enhance the five INTs will be critically important. The advancement of unmanned aerial systems (AES) as both collection (SIGINT, GEOINT, MASINT) and operational tools is a case in point.
- However, adding new technologies for improving the performance of traditional collection activities is not sufficient. The new intelligence paradigm must master new processes, structures, and workforce skills to allow intelligence agencies to be leaders in information technology applications. This includes managing massive amounts of data and information to enable effective data management and analysis of information pertaining to non-traditional threats and issues.

Intelligence organizations will need to be leaders in data mining methodologies, developments in artificial intelligence, and knowledge creation techniques.

- Since the massive amounts of data required for effective analysis of transnational threats resides in many places, the new intelligence paradigm must develop ways to master large scale cooperation with other governments, business firms, and non-profit organizations to elicit their voluntary contributions of needed information.
- The new paradigm must organize overall collection and analytical efforts in ways that avoid *destructive interference* between their secret and open activities. The WikiLeaks (Bradley Manning) and Project Prism (Edward Snowden) disclosures of classified information arguably show the kinds of counterintelligence nightmares that can happen when intelligence managers make large databases of classified information available to many analysts in attempt to improve the intelligence community's ability to "connect the dots" in an effort to avoid another 911 intelligence failure. The point is not that expanded distribution is wrong and restricted distribution is correct. Rather, it is that both need to coexist without causing destructive interference.

These four characteristics fall into two main categories, *technology* – i.e., new ways of collecting and analyzing information – and *organizational factors* – i.e., structures, processes, and personnel competencies that place the right information in the right hands at the right time.[3] Keeping at the forefront of technological developments in information and knowledge management is challenging, but U.S. intelligence organizations have a history of achieving such goals. Accordingly, the outlook for success in this area is good if intelligence agencies recognize the need. The Edward Snowden disclosures indicate that they do. The prognosis for mastering the organizational factors needed to develop appropriate structures, processes, and skill sets to produce appropriate information sharing is less promising, however. Since intelligence agencies are secret organizations at their core, efforts to develop new ways of looking at the secret/open categorization of information in order to facilitate the sharing of massive amounts of information will encounter resistance. Such efforts go against the long established principle of limiting distribution of information as much as possible in order to preserve its secrecy.

In his remarks during the plenary session at the beginning of this conference, Philip H. J. Davies opined that, if current interpretations toward privacy rights in democratic states continue along present lines, intelligence organizations might be legislated out of existence as legislatures and courts slowly but surely limit intelligence agencies' ability to obtain the information needed to provide effective intelligence because accessing this information would violate privacy laws. While Davies might have overstated his dire prediction for purposes of illustration, it is worthwhile to consider how failure to resolve the current issues surrounding privacy and the government's access to various kinds of information will reduce the ability of intelligence organizations to provide the intelligence that policymakers demand.

Information security and information flows in the new intelligence paradigm

Intelligence organizations possess institutionalized information security practices that remain necessary to limit the distribution of certain kinds of sensitive information. However, these practices create problems when trying to manage and share the large amounts on non-traditional information required to produce intelligence on many transnational threats and issues.

Essentially, a problem arises when intelligence agencies try to fit all information that they collect into two categories – secret (or classified) and open source (OSINT) – when, in fact, all information actually falls into the categories of *proprietary* and open source. Proprietary information is any information over which some entity claims ownership and thus incurs either the right or the responsibility (under the law) to control its distribution. Proprietary information, in turn, is divided into "Government Proprietary Information" (GPI) and Non-government Proprietary Information" (NGPI). GPI is what intelligence organizations and governments in general refer to as "classified information." Distribution of GPI is limited to those with a "need to know" by the use of security classifications such as Secret and Top Secret. NGPI has proven more confusing and therefore troubling. At the end of the Cold War, after the existence of the "Open Source Revolution" became clear and the increasing value of OSINT was recognized, many tended to conflate NGPI with open source information in the belief that all information that was not classified was open source. This misconception could persist without causing too much harm to information processing as long as most intelligence analysis and production relied on secret information from sensitive sources.

The need to produce intelligence on transnational terrorism has changed the significance of this misconception. It became increasingly clear that Intelligence analyses on transnational terrorist organizations and their plans depended on large volumes of NGPI, and that this information was not open source but rather required either warrants or voluntary disclosure by the governments or the private firms (e.g., airlines, telecommunications companies) in question because of legal rights pertaining to privacy. In the United States, the intelligence community labeled such information "gray information" in recognition that it was neither open source ("white") information nor secret ("black") information, but rather constitutes a third type of information.

In hindsight, it is clear that the U.S. government has acknowledged the existence of NGPI for decades. For instance, information that was not classified but that nevertheless did not warrant open distribution to the public for one reason or another was sometimes labeled "For Official Use Only"(FOUO) or "Law Enforcement Sensitive." However, in practice, government officials tended to treat these categories of information as classified because it was the conservative thing to do.[4]

The result has been that, over time, various government agencies, including intelligence organizations, developed different systems and designations for their use of NGPI. Then, following the 911 attacks, the volume of such information collected by intelligence agencies and other parts of government increased dramatically as the need to provide intelligence on transnational threats became top priority. In addition, the need to share extensive amounts of this information proved difficult and began to impede the production of effective intelligence.

One result is that, in 2010, the Obama administration issued Executive Order 13556, which "created a category called 'Controlled Unclassified Information' (CUI) to handle information that is sensitive but not classified and to create uniform standards for handling unclassified information."[5] E.O. 13556

> Establishes an open and uniform program for managing information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, *excluding information that is classified* under Executive Order 13526 of December 29, 2009, or the Atomic Energy Act, as amended . . . . At present, executive departments and agencies (agencies) employ ad hoc, agency-specific policies, procedures, and markings to safeguard and control this information, such as information that involves privacy, security, proprietary business interests, and law enforcement investigations. This inefficient, confusing patchwork has resulted in inconsistent marking and safeguarding of documents, *led to unclear or unnecessarily restrictive dissemination policies, and created impediments to authorized information sharing*. The fact that these agency-specific policies are often hidden from public view has only aggravated these issues. [Italics added][6]

The Obama administration's designation of CUI demonstrates that the government's use of NGPI has become sufficiently widespread and important to acknowledge it as a separate form of information that requires handling procedures distinct from those used for classified information. In short, it acknowledges that the government must learn to handle three types of information rather than the traditional two forms comprised of classified and open source information. The above excerpt from E.O. 13556 also clearly states that current practices interfere with the smooth sharing of information, which remains a critically important element for providing intelligence against transnational threats.

Trusted information

The development of CUI is a *symptom* of the problems of managing information flows in the 21st Century security environment rather than a cure for this condition. CUI is a step in the right direction. It indicates that the U.S. intelligence community is aware that its current information management system based on categorizing all information into classified and open categories is not capable of managing its 21st Century information requirements. However, since CUI is a U.S. government initiative, it will not provide intelligence organizations with access to NGPI on the global scale required for effective intelligence production on transnational threats. Rather, achieving information dominance on a global scale requires unprecedented cooperation from many other states and other international actors, such as transnational corporations and nongovernment organizations. Nevertheless, if today's CUI initiatives enable the U.S. government to share and analyze large volumes of NGPI effectively, then further "globalization" of this effort to include sources of NGPI on a worldwide basis will be greatly improved as other actors perceive that such efforts are not only possible but also provide better intelligence products that give policymakers a decision advantage.

In *Keeping U.S. Intelligence Effective: The Need for A Revolution in Intelligence Affairs*, I used the term "trusted information" to describe a new category of information that was necessary to enable the seamless collection and management of NGPI globally. Use of the word "trusted" rather than "controlled" (as in CUI) emphasizes the need for partners who voluntarily share NGPI within "trusted networks" because they understand the need for such sharing and expect to reap benefits from their cooperation. Benefits might include the detection and prevention of terrorist attacks within their territory or the early detection and tracking of the progress of disease epidemics.

> Trusted information circulates within trusted networks. A trusted network is one in which all of the members are trusted to enter only validated information and to use network information responsibly. Within these constraints, network members can be any organization that can provide needed information. This will include government agencies, private firms, IGOs, NGOs, and even individuals in various informal communities of interest. Since their purpose if to address transnational issues and threats, trusted networks must be global in scope. The overriding principle is that members of a trusted network must agree to share voluntarily their own information to be able to access the network's contents. In short, the network depends on mutual trust among its members.
>
> Only the entities that are members of the network have access to its information, and these organizations have access to all of the information in the network at all times. This means that trusted information is not open source information because it is not available to the public. Nor is trusted information classified information, since its distribution is not restricted to a small number of persons with a need to know.[7]

Trusted information has a number of characteristics that distinguish it from classified and open information. First, all contributions are voluntary. Second, all contributors get access to all of the information in trusted databases and networks. This is necessary to incentivize private sector actors to share their NGPI. Third, each network containing trusted information must be designed so that it is compatible with all other trusted information networks. This practice will facilitate knowledge sharing and will enable data mining where appropriate. Fourth, publics must perceive that the use of trusted information is a mainstream activity of government rather than something that secret organizations such as intelligence agencies perform. Otherwise, the numbers of organizations that voluntarily share their NGPI will be low.

Regarding this last characteristic, there are already many cases of public acceptance of government collection and data warehousing and analysis of CUI/NGPI. In the United States, the Social Security Administration, which is tasked with administering the social welfare system for senior citizens and other dependent groups, maintains large volumes of personal information in its databases. So does the Census Bureau, which performs a census of all persons living in the United States every ten years as required by the U.S. Constitution. The census includes questions about demographics, income, employment, educational data, and many other pieces of personal information. Another excellent example is the Internal Revenue Service, which collects taxes and monitors citizen compliance with the tax code to minimize tax evasion and fraud. In these and several other cases, U.S. citizens accept that government agencies need to collect and analyze this information in order to perform their missions and, in the vast majority of instances, they accept these inroads into their personal privacy as legitimate.

References

[1] Martin Hilbert and Priscilla Lopez, "The World's Technological Capacity to Store, Communicate, and Compute Information," *Science* 332, no. 6025 (February 10, 2011): 60-65 (60).

[2] SIGINT – signals intelligence; HUMINT – human intelligence; GEOINT – geospatial intelligence; MASINT; measurement and signature intelligence; and OSINT – open source intelligence.

[3] For more information on structural, process, and skill set considerations to improve the effectiveness of intelligence on transnational threats, see William J. Lahneman, *Keeping U.S. Intelligence Effective: The Need for a Revolution in Intelligence Affairs* (Lanham, MD: Scarecrow Press, 2011) and William J. Lahneman, "Is A Revolution in Intelligence Affairs Occurring?" *International Journal of Intelligence and Counterintelligence*, 20, 1 (Spring 2007): 1-18.

[4] Based on author's experience while serving as a U.S. naval officer.

[5] Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 6th Edition (Washington, DC: CQ Press, 2015): 93.

[6] Executive Order 13556, *Controlled Unclassified Information*. Washington, DC: The White House, 2010.

[7] Lahneman, *Keeping U.S. Intelligence Effective: The Need for a Revolution in Intelligence Affairs*, 130.

SEVERAL ARGUMENTS FOR USING QUALITATIVE METHODS OF RISK ANALYSIS IN INTELLIGENCE

Valentin-Ionuţ NICULA[*]

Abstract

The paper aims to provide reasons for the widespread use of qualitative methods of risk analysis in the intelligence activity. Based on the current context in which intelligence organizations operate, and on the specificity of their work, the article presents some methods of risk analysis that can be used in various situations in intelligence.

Keywords: quantitative method, risk analysis, intelligence, qualitative method

The research hypothesis

The assumption we start from is that at the level of intelligence organizations the issue of risk analysis is one of the central pillars of the intelligence analysis activity by providing the proper tools for risk management, anticipation and estimation.

Since the beginning of our approach, it must be taken into account the premise that the intelligence activity, unlike other activities that rely on machines or systems, has as central element the human being, both as a source and as a resource, with all that this entails: the human being is unpredictable and the consequences of its actions and intentions cannot be calculated with "engineering" accuracy. Therefore, the question that arises is whether the risk related to this type of activity can be measured as the strength of materials in construction or by other mathematical methods specific to other industries that require systematic activities/mechanized operation or production.

[*] National Institute for Intelligence Studies, “Mihai Viteazul” National Intelligence Academy

Thus emerges the need to develop and adapt to the field of intelligence analysis those methods involving more the human factor in analysis, both by the importance given to human activity in the process of analysing and by valuing teamwork through this process.

The context

Initially developed in economics, the field of risk analysis has exceeded the boundaries of a single discipline, and is used today in a broad scientific spectrum, from studies on climate change to political science. The trans-disciplinary characteristic of this area of theoretical and practical intervention was valued in intelligence, with the proper methodological adjustments and reconfigurations, enabling the adaptation to the specific of intelligence analysis, covering a constantly changing security environment where risk and uncertainty are landmarks depending on which the analyst must outline the optimal analytical products in order to support the strategic decision. To these elements, which shape the environment in which the intelligence organizations act, the changes that have occurred in the information age can be also added, which moves the centre of gravity to information explosion, the development of new communications technologies and collaborative platforms. In this regard, the issue of estimation, anticipation and risk management is emerging as a central field of activity for the intelligence organizations, which need to provide appropriate responses at various levels of action.

As knowledge becomes not only the constituent of the modern economy and of the production processes, but also of the relations and social cohesion, as well as a primary source of the problems and conflicts of modern society, knowledge society becomes the appropriate term to describe the nature of the contemporary society. This requires that we build the reality we live in on knowledge, but we cannot equate between all forms of knowledge. According to Stehr, in the media, the term knowledge society is sometimes treated as a synonym for information society and used with some concepts related to the fact that we live in a globalizing era, that we move from things to ideas, from cars to software, that we focus on symbolic goods or in political life, transforming from distant observing to direct participation. The transformation of modern societies into knowledge-based society can be summed up in these clichés, but can be much more[1].

Stehr argues that the term knowledge society is more appropriate than information society or post-industrial society for being used in relation to nowadays society. In order to do this, he exemplifies by describing the various meanings of the term knowledge and its different uses in relation to terms such as human, cultural or social capital. In this context, he states that the concept of economic capital, which is the source of growth and of value-added activities, is based on knowledge. The transformation of the structures of the modern economy, based on knowledge as the main productive force, constitutes the material basis and justification for the current modern society name as knowledge society. The world today can be described as a knowledge societies because all its spheres were penetrated by the scientific and technical knowledge[2].

On a different level of discussion, another feature of the contemporary society is the uncertainty and a way to describe it is the mental state of doubt, uncertain meaning unknown or unstated, questionable, undetermined or undecided, about which there is insufficient knowledge. Also, another common approach is that we have an abundance of information that becomes harmful. In the absence of a process to treat these two situations, both tend to generate uncertainty and, how is advancing more towards one end of the continuum, the greater will be the resulting uncertainty. Speculation instead of information is the usual reaction to the lack of information and it tends to emphasize a situation which is already problematic. In many cases, the abundance of information creates confusion, frustration and despair[3].

Risk and risk analysis

At the international level, the concerns of the experts in risk management and risk analysis were pooled and standardized by the International Organization for Standardization in the ISO standard 31000: 2009, which developed some earlier efforts of experts from Australia and New Zealand described in the Directive AS/NZ

4360:2004. The specifications of the two documents can be applied to various fields, from the private sector to the public and military sector[4].

Following the guiding principles and rules outlined by the ISO standard 31000: 2009, organizations of all types and sizes face internal and external factors that make uncertain the reach of objectives. The effect that these uncertainties have on the organizations objectives may be defined as risk. From this point of view, all the activities involve risks and to manage them properly, organizations seek to identify, analyse them and then evaluate whether and how they should be treated to meet specific needs[5].

However, the same standard defines risk in terms of the effects of uncertainty on objectives, with the following mentions:

- The effect is a deviation from what was expected, either positive or negative;
- The objectives may have different aspects (financial, health, environmental protection, etc.)
- And can be applied to different levels (strategic level, the entire organization, the project, products or processes)

Risk is characterized through comparison with the consequences of possible events, or a combination of these; the risk is often expressed as the product of the consequences of an event and the probability of that event; uncertainty is the state of lack of information, even in part, related to understanding or knowledge of an event, its consequences or the probability of occurrence[6].

According to ISO 31000:2009, risk analysis is defined as the process that understand the nature of risk and determine the level of risk. Risk analysis provides the basis for risk assessment and decisions concerning the proper way for addressing the risks[7].

At the conceptual level, an important contribution is also put forward by the Society for Risk Analysis (SRA) - the international organization that brings together specialists in management and risk analysis. According to them, risk is defined as the potential achievement of unintended consequences on life, health, property humans or the environment. Risk estimation is usually based on the value of the conditional probability of an event, multiplied by the consequences of that event occurred[8].

Risk analysis is defined as the detailed examination that includes analysis/assessment of risks, risk evaluation and management, conducted to understand the nature of unintended negative consequences on life and human health, on property or the environment. It is an analytical process that provides information on undesirable events, a process of quantifying the expected probability and consequences of the identified risks[9].

According to the Lexicon developed by the US Department of Homeland Security (Department of Homeland Security - DHS), risk is defined as the potential of an undesirable outcome as a result of an incident, event or occurrence, as determined by the likelihood and consequences associated with it. In a broader approach, risk is defined as the potential occurrence of a negative result, analysed as a function between threats, vulnerabilities and the consequences associated with an incident, event or occurrence. This potential occurrence is measured and used to compare different possible or future situations. However, the risk can manifest itself at the strategic, operational and tactical level. In the case of terrorist attacks or other criminal activities, the probability of an event or incident can be estimated by taking into account the threats and vulnerabilities[10].

The DHS Lexicon defines risk analysis as the systematic examination of components and characteristics of risk. Thus, risk analysis involves aggregating the results of several risk estimates, which are translated into information products for beneficiaries entitled to make decisions. Moreover, risk analysis can undertake on alternative risk management strategies to determine the likely impact of the overall risk strategies[11].

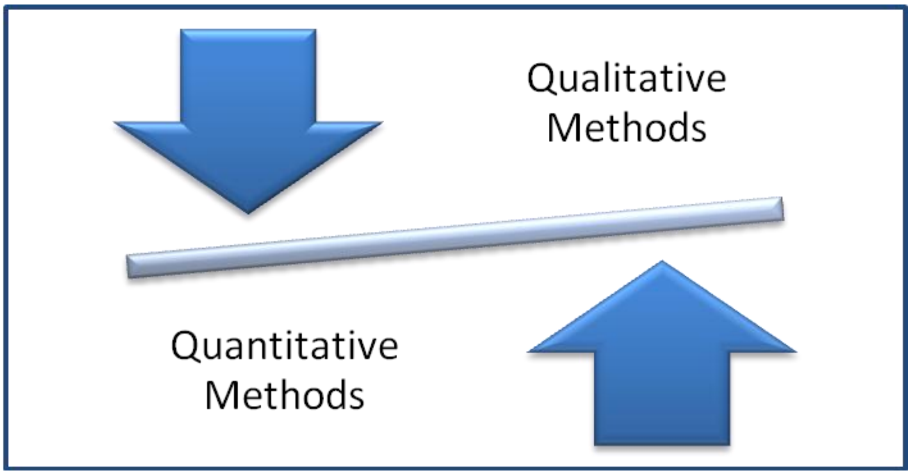
Following the traditional pattern, Hank Prunckun believes that **risk** can be defined as a function between probability and consequences. The author indicates that risk analysis can be performed for different types of situations that may be faced by the intelligence organization, not just those of a particular severity. After the application of risk analysis one can recommend certain measures to provide beneficiaries the ability to accept risk as it is or to address the identified risk in various ways, either to avoid risk or to mitigate its effects[12].

In the field of intelligence analysts can address a wide range of risks, from critical infrastructure and risk of a corrupted government to the democratic system of government, the impact of transnational actors, organized crime, ultra-radical, political or religious groups. Risk assessment is the whole process of analysis and risk assessment and risk management is defined as the culture, processes and structures that are directed towards the achievement of potential opportunities whilst managing adverse effects[13].

In intelligence or in early warning systems we are not operating with binary constructions such as: an attack will take place or not, but with uncertainties related to the time, place and manner of the attack as well as various combinations of these elements that represent risks and uncertainties of the above mentioned systems[14].

Some proposals of qualitative methods of risk analysis for the intelligence activity

According to Thomas Peltier, a risk analysis can be done for a specific task, a project of the organization, for an idea to be implemented etc. so that it can be established whether a project should be developed, implemented, purchase a particular product or a particular system or if the organization is subject to certain risks and threats. Hence, one of the great benefits of risk analysis that it is indicating to the organization managers whether a forward direction is good. This allows for decision-makers to examine all identified threats, prioritize resources, based on the weaknesses identified and to take appropriate measures or to accept and assume the risk identified. The purpose of risk analysis is not to completely eliminate risks but to be a tool through which decision-makers reduce risks to an acceptable level for the organization[15].



a) Preliminary Risk Analysis

Preliminary risk analysis is a systematic approach aimed at identifying and characterizing risks associated with accidents that may occur during the course of operations.

It is a team approach that is based on systematic examination by experts of a wide range of issues related to a system or activity. For conducting the analysis, it is used a standardized form with the following elements:

- Identification and description of the accident;
- qualitative description of potential problems (causes and factors) including the most important factors in the development of the accident;
- current safety measures;
- qualitative risk estimates;
- list of recommendations for reducing risk and quantitative assessment of the recommendations.

Preliminary risk analysis technique is used to generate risk profiles in a wide range of activities[16].

Usually, preliminary risk analysis is conducted by dividing the subject of analysis in parts (sub-items) followed by the conduct of actual risk analysis for each of these items separately. In most cases, risk analysis is conducted in a standardized form and it is used to describe risk categories covering all possible adverse events with probability and expected consequences if such undesirable event is happening. When estimating probabilities, T. Aven recommends avoiding terms like *often* or *seldom* as they may give rise to different interpretations. The author proposes as a solution the clear and direct affirmation of the findings of the analysis working group set up because it is not helpful to hide behind phrases mentioned without being explained clearly what is meant by these terms[17]. Preliminary Risk Analysis identifies the most important factors causing risk, furthermore the causal picture or the picture of the consequences being analysed in depth, using more detailed methods.

In intelligence, this risk analysis method can be applicable in different situations, whether we consider the operational field – launching of new projects (anti-terrorist operations, cyber-crime, traffic, etc.), whether we refer to analytical projects to substantiate the strategic decisions of importance, or we consider launching large scale investment projects necessary to undertake for the organization in order to support tactical, operational or strategic level.

b) Facilitated Risk Analysis Process - FRAP

The facilitated risk analysis process was originally developed for information security risk analysis. The procedure entails analysing a system, an application or a segment of an organization's operations by a team that includes both managers who are aware of the organization's information needs and technical staff, to be able to understand the potential system vulnerabilities and appropriate control measures. Sessions should be done according to a standard agenda and are facilitated by a member of the project team or among personnel responsible for protecting the information. The facilitator is responsible for ensuring that all team members communicate effectively and comply with the proposed agenda. During brainstorming sessions the team identifies potential threats and vulnerabilities and fixes negative impact on data integrity, confidentiality and availability. Later, the team will analyse the effects on their operations and classify risks in relation to the prioritization accepted[18].

The objectives of the facilitated risk analysis process are represented by identifying unauthorized incidents and risks that may have a negative impact on the organization's objectives or missions. After identifying and prioritizing these risks, appropriate measures will be identified for responding and correcting the risk level[19].

In intelligence, the facilitated risk analysis process can be used in particular to the ongoing operational activities and for technical projects, applicable in OSINT or to support current operative informative activities.

c) Failure Mode and Effects Analysis - FMEA

FMEA is a structured qualitative analysis method that is used to investigate how a system or the components of the system can cause performance problems. The key steps covered in the analysis include:

- The identification of the causes and contributing factors;
- The description of the protective measures in place;
- Identifying current and potential effects;
- A list of recommendations for risk management. [20]

In order to calculate the risk through the FMEA method, the term risk is analysed in terms of three components that are multiplied to obtain a risk priority number (RPN):

• Severity (S) - is calculated on a scale of 10 points - 10 is the largest

• Appearance (A) - is calculated on a scale of 10 points - 10 is the largest

• Detection (D) - is calculated on a scale of 10 points - 10 is the largest

RPN = S * A * D

(RPN may have minimum value equal to 1 and a maximum value equal to 1000)

To understand the decision-making process when one wants to prioritize a particular process, it should be specified that if it has not been set a threshold for the RPN, a value above which it is mandatory to take a particular decision or action to be triggered some or conversely, a value below which team should not act. It should also be noted that 0 quotations there are not allowed for those three items[21].

The FMEA method can be used to analyse risks, both at the system as a whole and at the level of its components, it is applicable to any well-defined system. Often the FMEA analysis is used to facilitate planning and optimization of system maintenance procedures.

FMEA can provide analysis and quantitative frequencies and / or estimates of consequences and classifications. A quantitative version of the FMEA method is the analysis of the effects and the likelihood of errors/defects and critical aspects (Failure Modes, Effects and Criticality Analysis - FMECA), a method using a formal procedure that begins with the systematic listing of all system components. The list commonly includes the following items:

- The component name;
- The function of the component;
- possible malfunctions/failures;
- causes and contributing factors of defects;
- indication/fault detection;
- primary effects on the functioning of the system malfunctions and the other components;
- protection measures implemented and preventive and reconstruction actions taken;
- estimation and classification of frequency and severity of defects;
- list of recommendations for risk management.

Risk analysis depends largely on the quality of data and the experience of the analysts involved. In this regard, the relevant data and information is collected through interviews, site inspections and documentation. The method can be applied by one analyst, by a group of experts or by interdisciplinary teams whose members have diverse knowledge and experience[22].

According to Aven, FMEA is essentially an inductive method, for each component of the system being investigated what happens when that component undergoes a failure/error. The method is a systematic analysis of the components of a system, carried out in order to identify possible ways in which an error can occur and quantifying their importance for the overall system performance. During the analysis is being considered, in turn, each part of the system, others being considered as functioning perfectly. It follows that FMEA is not suitable for the identification of critical combinations of failures of the various components[23].

Strengths and weaknesses of FMEA[24]

- The first comment on the strengths of the method is that the FMEA method provides a systematic analysis of the major faults that can occur in a system, forcing managers to assess the reliability of the overall system.
- In addition, the method is a good starting point for more comprehensive quantitative analysis subsequently undertaken such as Fault Tree Analysis or Event Tree Analysis.
- the FMEA method offers no guarantee that all the critical components defects have been identified, but most of the vulnerabilities of a system caused by malfunction of individual components can be identified.
- the FMEA analysis sometimes focuses too much on technical failures, leaving unanalysed the contributions of human error. This can be offset by the inclusion of human functions as one of the system components.
- One of the biggest drawbacks of the method is that the method examines all system components, even those whose failure causes weak or insignificant consequences, which makes the application of the method very demanding because of the extensive nature of the documentation necessary for the analysis. This problem can be reduced by clearly defining the system components.

In intelligence, the FMEA method can be applied at all levels - tactical, operational or strategic - because of its possibility to analyze the system, and some part of that system.

So, FMEA can be used both for analytical work for each project or for the entire process of analysis and information entitled.

Similarly, at operational level it can be applied at one particular operation or for the overall phenomenon or issue that is in the responsibility of that intelligence organization.

Conclusion

Whether we consider the qualitative or quantitative approach, in intelligence - like in any scientific endeavour - to overcome common knowledge, hypotheses are generated and tested through methodologies, models and specific research techniques, then conclusions are drawn about the processes/actions/events analysed, thus obtaining knowledge. The same guidelines are considered when it comes to the issue of risk analysis.

In this study we tried to present some methods of risk analysis and to evaluate them in the light of the valences they can prove for the intelligence activity, staring from the premise that one can find tools for risk analysis at the reach of any analyst. From this point of view, it is important to calibrate the method on the situation/event/issue considered and respect the methodological steps of the method chosen.

Also, our approach can provide an extra-argument to the widespread use of risk analysis methods in intelligence, showing results that substantiate the solutions and the strategic responses offered to decision-makers, regardless of the envisaged level – be it tactical, operational or strategic.

Bibliography

1. *** *DHS Risk Lexicon 2010 Edition*, Risk Steering Committee, Department of Homeland Security, Washington, 2010, available at: http://www.isn.ethz.ch/isn/Digital-Library/ Publications/ Detail/?id=150902&lng=en, last accessed on 14.11.2012.
2. *** International Standard Organization ISO/FDIS 31000 Risk management — Principles and guidelines.
3. Arben Mullai, *Risk Management System – Risk Assessment Frameworks and Techniques*, DaGoB Publication Series, 2006, available at http://www.rop.lv/ru/smi/zagruzki/doc_download/42-risk-management-system-risk-assessment-frameworks-and-techniques.html, last accessed on 13.06.2013.
4. Aven Terje, *Risk Analysis: Assessing Uncertainties Beyond Expected Values and Probabilities*, John Wiley & Sons, Ltd, 2008, available at: http://media.wiley.com/product_data/excerpt/ 60/04705173/0470517360.pdf, last accessed on 14.11.2012.
5. Lefayet Sultan Lipol şi Jahirul Haq, *Risk analysis method: FMEA/FMECA in the organizations*, în *International Journal of Basic & Applied Sciences* IJBAS-IJENS Vol: 11 No: 05, available at

http://www.ijens.org/Vol_11_I_05/117705-3535-IJBAS-IJENS.pdf, last accessed on 14.11.2012.

6. Longford Steve, *Uncertainty in Decision-making: Intelligence as a Solution* în Bammer Gabriele, Smithson Michael edit., *Uncertainty and Risk. Multidisciplinary Perspectives*, Earthscan Londra, 2008.

7. Peltier Thomas R., *Information Security Risk Analysis*, Auerbach, Boca Raton, Londra, New York, Washington, D.C., Taylor & Francis e-Library, 2005.

8. Prunckun Hank, *Handbook of Scientific Methods of Inquiry for Intelligence Analysis,* Scarecrow Press, Lanham, Toronto, Plymouth, 2010
Stehr Nico, *The Fragility of Modern Societies. Knowledge and Risk in the Information Age*, Sage Publications, Londra, 2001.

9. Uzi Arad, *Intelligence management as risk management: the case of surprise attack* în Bracken Paul et. al. (coord.), *Managing Strategic Surprise. Lessons from Risk Management and Risk Assessment*, Cambridge University Press, 2008.

10. http://www.sra.org/resources_glossary_p-r.php, last accessed on 14.11.2012.[25]

Acknowledgments: This paper is made and published under the aegis of the Research Institute for Quality of Life, Romanian Academy as a part of programme co-funded by the European Union within the Operational Sectorial Programme for Human Resources Development through the project for Pluri and interdisciplinary in doctoral and post-doctoral programmes Project Code: POSDRU/159/1.5/S/141086

References

[1] Nico Stehr, *The Fragility of Modern Societies. Knowledge and Risk in the Information Age*, Sage Publications, Londra, 2001, p. IX.

[2] *Ibidem,* p. 19.

[3] Steve Longford, *Uncertainty in Decision-making: Intelligence as a Solution* în Bammer Gabriele, Smithson Michael edit., *Uncertainty and Risk. Multidisciplinary Perspectives*, Earthscan Londra, 2008, p. 219-220.

[4] Hank Prunckun, *Handbook of Scientific Methods of Inquiry for Intelligence Analysis,* Scarecrow Press, Lanham, Toronto, Plymouth, 2010 p. 173.

[5] *** International Standard Organization ISO/FDIS 31000 Risk management — Principles and guidelines, p. v.

[6] *Ibidem*, p. 1-2.

[7] *Ibidem,* p. 5.

[8] http://www.sra.org/resources_glossary_p-r.php, last accessed on 14.11.2012

[9] *Ibidem.*

[10] *** *DHS Risk Lexicon 2010 Edition*, Risk Steering Committee, Department of Homeland Security, Washington, 2010, p. 27, available at: http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?id=150902&lng=en, last accessed on 14.11.2012

[11] *Ibidem*, p. 27.

[12] Hank Prunckun, *op. cit.,* p. 172-173.

[13] *Ibidem,* p. 173.

[14] Uzi Arad, *Intelligence management as risk management: the case of surprise attack* in Bracken Paul et. al. (coord.), *Managing Strategic Surprise. Lessons from Risk Management and Risk Assessment*, Cambridge University Press, 2008, p. 45-46.

[15] Thomas R. Peltier, *Information Security Risk Analysis*, Auerbach, Boca Raton, Londra, New York, Washington, D.C., Taylor & Francis e-Library, 2005, p. 1-3.

[16] Arben Mullai, *Risk Management System – Risk Assessment Frameworks and Techniques*, DaGoB Publication Series, 2006, p. 113, available at http://www.rop.lv/ru/smi/zagruzki/doc_download/42-risk-management-system-risk-assessment-frameworks-and-techniques.html, last accessed on 13.06.2013.

[17] Terje Aven, *Risk Analysis: Assessing Uncertainties Beyond Expected Values and Probabilities*, 2008, John Wiley & Sons, Ltd, p. 57-58, available at: http://media.wiley.com/product_data/excerpt/ 60/04705173/0470517360.pdf, last accessed on 14.11.2012.

[18] Thomas R., Peltier, *op. cit.*, p. 69-70.

[19] *Ibidem*, p. 72.

[20] Arben Mullai, *op.cit.*, p. 116.

[21] Lefayet Sultan Lipol şi Jahirul Haq, *Risk analysis method: FMEA/FMECA in the organizations*, in *International Journal of Basic & Applied Sciences* IJBAS-IJENS Vol: 11 No: 05, p. 74-75, available at http://www.ijens.org/Vol_11_I_05/117705-3535-IJBAS-IJENS.pdf, last accessed on 14.11.2012.

[22] Arben Mullai, *op. cit.*, p. 116.

[23] Terje Aven, *op. cit.*, p. 64-65.

[24] *Ibidem*, p. 69.

SYMBOLIC INTERACTIONISM AS KEY CONCEPTUAL FRAME FOR INTELLIGENCE ANALYSIS

Cristina POSAŞTIUC[*]

Abstract

The goal of this paper is to explore the potential of using sociological paradigms as analysis frameworks within the intelligence tradecraft. Although macro-oriented theoretical systems (e.g. structuralism, functionalism, conflict theories) have tried and tested uses in intelligence, especially when it comes to making sense of large-scale phenomena, events and trends, there is still little attention given to the paradigm of symbolic interactionism. At first glance, intelligence analysis has little to gain, knowledge-wise, from an empirically untestable scientific perspective which deals with the social micro-cosmos. Nevertheless, keeping in mind the fact that societal systems are constantly negotiated, consolidated and reformed through the most minuscule of daily interactions, understating the latter can help paint a correct picture of the "shared reality" of large or small groups at any given moment. I believe that intelligence practitioners can use insight derived from symbolic interactionism to better apply their tradecraft in an extensive palate of cases. Moreover, in an increasingly virtualized social universe, human interactions take new forms and generate new types of shared meanings and symbols, altogether changing the very social structure that fosters them. For intelligence practitioners that operate online, from all-source strategic analysts to OSINTers and SOCMINTers, understanding how this new medium emerges is of the utmost importance.

Keywords: symbolic interactionism, intelligence analysis, collective behavior, observer-expectancy effect, OSINT

Introduction

In the simplest terms, intelligence analysis aims at limiting or eliminating the ambiguity of certain situations characterized by a high degree of uncertainty using human cognition. To do so, the

[*] Romanian Intelligence Service. Parts o this paper have already been published in the no. 13/2015 of Romanian Intelligence Studies Review.

analyst mixes and matches data and information in order to evaluate the tableau of knowledge about target situations and entities. The analyst must also always keep in mind the blank spots that inherently appear on any knowledge map and focus on shaping and reshaping the constructed narrative through problematization. By checking all these items off of the "best practice" list, he or she can generate valid inferences at the operational, tactical and/ or strategic level regarding future developments.

While this rather simple, albeit abstract, recipe has not changed profoundly since the "birth" of the intelligence practice, the backdrop of this process is today greatly different. Avoiding intelligence failures is, after 9/11, a task that is said to require a greater emphasis on what makes good analysis. Strategic surprises stem today not so much from poor collecting but from poor analysis.

The nexus of the scientific process and intelligence analysis

Augmenting the quality of intelligence analysis has been done through borrowing and adapting models, frameworks, methods and techniques from the outside. One of the most selfless "donors" has been science. For example, the fields of economy, psychology, sociology, history or anthropology (just to name a few) offer a huge volume of knowledge that can immediately be put to use in intelligence analysis. In sociology, functionalism, structuralism, conflict theory and interpretative sociology are the basic paradigms that build analysis frameworks for phenomena, processes and trends that define the social dynamic. The same cannot be said, unfortunately, for symbolic interactionism and phenomenological sociology, as intelligence analysts have yet to harness the explanatory power of these paradigms.

At first glance, the critique of symbolic interactionism as a "bad" theory, one that cannot be empirically validated and, by only dealing with the micro-cosmos of social interaction, circumvents the required criteria for paradigmatic frameworks, is persuasive.

This paper aims to argue that symbolic interactionism dully deserves a role in the paradigm repertoire of any sociologist that practices intelligence analysis.

Conceptual pivots of the interactionist paradigm

Symbolic interactionism stems from the idea (Thomas Theory) that "if men define situations as real, they are real in their consequences" (Thomas & Thomas, 1929, p. 572). In other word, reality is a social construct which is constantly generated, consolidated, and negotiated through the multiple daily interactions of the participants to the social life.

Through these repeated interactions, symbols are created (habits, rites, rules etc.) and the individuals assigns means and significance to the things, events, and situations around them, and also interpret them accordingly.

Thus, symbolic interactionism presumes that people do not actionably respond to what we might call „reality", but to the socially and individually accepted meaning of reality.

Herbert Blumer, the creator of symbolic interactionism, most clearly underlies the main ideas of this sociological perspective, stating that the significance the social actors convey about things and other persons, the bargaining they carry out and the interpretations generated in this way are being read in this paradigm.

Exponents of the Chicago School analyzed the way individuals socially act, considering the subject of *projected self-image*. George Herbert Mead coined the term „self", meaning that image about him/herself, equally composed from social ego (as a result of interiorizing social roles) and psychological ego (as a personal, intimate component) (Doise et al., 1996), where Charles Horton Cooley handled (1902) differently this matter, stating that there is a „looking glass self", amid an image about your own person which is build from the interaction between individual's image about himself and the image the individual thinks others have about him.

Erving Goffman introduced the concept of "dramatic perspective" into the social daily analysis. Through „ The Presentation of Self in Everyday Life" (1959), he proposed the theatre metaphor in order to explain the emergence of some particular features related to social context: in public, individuals "perform", trying to present themselves as favorable. They choose a "mask" (meaning they exhibit those features considered to be preferred in that particular social context), they use appropriate settings and props and, then don't find themselves in front of the audience, they use the back of the stage to temporary renounce the role that they assume.

Despite the critiques of conceptual incongruence and lack of empirical testability[1], symbolic interactionism takes advantage at the fact that it conceptually concatenates the way *some* social symbols are generated through a *particular* type of interaction that takes place in a *particular* social structure. This interaction produces also a *particular* type of interpretation and internalization of structure. Symbols, in turn, become a part of the social structure, feeding a cycle of social regeneration. This circular causal concatenation allows us to understand the smooth relation between macro- and micro-social frames – from social structure to group interaction.

Nevertheless, the reasoning of the present paper does not support the preeminence of symbolic interactionism over the other paradigms, but the fact that there are a series of relevant social instances in the security field that can be more easily understood through explanations originated from the interactionism.

Symbolic Interactionism and intelligence

Strategic surprises

Despite the discussion about "objective" and "social" reality may seem philosophical and less important in terms of practical consequences, some social phenomena do emerge on the score of symbolic inter-individual negotiations and do modify tangible reality. For intelligence analysts, the emergence of these phenomena takes the form of a strategic surprise when they have important implications in the field of national security.

For example, during an economic crisis, the diffuse perceptions such panic related to the banking systemic sustainability may generate phenomena with actual consequences, even if, objectively speaking, banks are stable. To that effect, the most famous

[1] These critiques are the result of treating symbolic interactionism as a theory not as a scientific orientation. More underlain critics reproach this paradigm the fact that it studies a very narrow social niche, meaning the interaction inside small groups and specific psychosociological phenomena. Obviously, no sociological paradigm ever reached the performance of delineating a theoretical frame that „explains everything".

example regarding the effects of emotional spiral that validates Thomas's Theorem in Black Tuesday, that historical day from October 1929, when the Wall Street Stock Market precipitated and provoked an economic collapse.

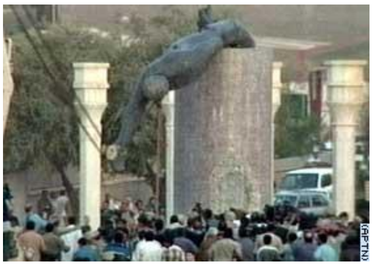
Amid a pronounced dynamic of the transactions, the Stock Market closed in October 24th with a 6.38 points decline of Dow Jones Index. During the weekend, the US newspapers heavily reported about the skid on the Wall Street, generating a large sense of panic amid investors. After the weekend, from Monday to Thursday, the Stock Market collapsed in a rapid pace because everybody tried to sell and get out of the market.

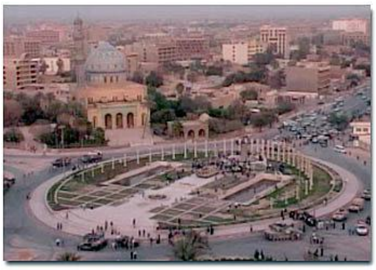
Of course, Black Thursday only officialised the unsustainability of the speculative bubble that hallmarked the `20 in the United States of America. Despite this, the trigger was based on the spreading of rumors, false information or assumptions that, once considered as being the truth, brought into play actions that validated wrong premises.

Analyzing the causal chain of the events that generate "announced" crisis, Robert Merton proposed the term „self-fulfilling prophecy" (Merton, 1948, p. 195). In intelligence, generating self-fulfilling prophecies is a specific objective (example below) of influence operations. Black and grey propaganda are meant to create and disseminate a product-message that present a version of reality according to the interests of the issuing entity. Their scope is to obtain a certain reaction or non-reaction from the target.

The example from below, largely mentioned among experts, had a very ample social impact at its time: in the left image there is the picture press channels broadcasted after the statue of Saddam Hussein from Firdos Place in Bagdad was pulled down (April 9, 2003).

Press reports insisted on the large support of the Iraqi population for the military operations. In the right picture is the same picture but from another angle.





Influence operations that intend to coagulate a general consensus („all the Iraqi population in 2004 wants to throw down Saddam Hussein's regime") presenting a false local consensus („all the persons in Firdos Place participated to the pulling down of the Saddam Hussein's statue") work by the Keynesian principle of rational agent's action – individuals action according to their own assessment about majority's opinion (Keynes, 1936, p.100).

Tagging

Another situation intelligence analysts often confront when they try to anticipate the actions of a hostile actor is the confirmation of the most dangerous scenario, despite the premises that might underpin less dramatic trends. Sometimes, the future seems to confirm the gloomiest expectations.

Howard Becker, a well known symbolic interactionist, proposes a social deviance theory derived from that of „looking glass self". *Social tagging* (Becker, 1963) is the trigger phenomenon of the deviance, not because of the intrinsic features of the acting, but as a result of the social network it generates.

The theory of social tagging is similar to the self-fulfilling prophecy theory, inserting in the explanatory circuit the driver of "others' expectations" and the of the way these expectation are internalized by the social agent. In intelligence, Zulaika (2009) states that this sort of mental frame usually emerges from cases related to preventing and countering terrorism. If authorities anticipate the fact that a specific group manifest violent tendencies (ideological radicalism, terrorism etc.), prevention and countering measures they adopt might push the members of those communities to that specific type of behavior they try to alleviate.

The example Zulaika offers related to military operations in Iraq, where the US Army and its allies intervened in order to eliminate Saddam Hussein, under the suspicion of Hussein developing chemical weapons of mass destruction and financially and logistically supporting terrorist organization such as al-Qaeda. Actual proofs for both hypothesis were not found, but the presence of US Army in Iraq favored the emergence of a high scale terrorist and insurgent phenomenon. If Iraq was not a propitious environment for terrorism before 2003, it surely became one after that.

Online collective behavior – the contribution of symbolic interactionism to understanding the emergence of new psycho – sociological phenomenon

Neither symbolic interactionism nor other paradigm will ever make „unknown unknowns", the field where strategic surprises develop, to disappear. According to Donald Rumsfeld's taxonomy (2002): "known knowns, unknown knowns, known unknowns, unknown unknowns". Nevertheless, a better understanding of the profound mechanisms of social emergence may diminish the field of „the unknown that can not be known" and the *effects* of strategic surprises.

Intelligence analysts became more and more interested in understanding the virtual space, a space of interaction and an informational resource with extensions that have never been substantially explored so far.

Hybridization of collective behavior, with emerging and actionable components both online and offline, generate surprising effects for those organizations responsible for preventing violent social movements.

Today, the daily global society is networked (Castells, 2004) and virtualized. The social density is exponentially growing, generating a "conductive" infrastructure that encourages social interactions using symbolic interactionism. That is why it is easy to understand the mechanism used to augment the velocity and frequency of generating new social symbols which, in turn, became part of the social structure, bolstering new interactions and internalized interpretations. This self-propelled cycle of symbol development will generate structural mutations at the limit between chaos and complexity, inducing more volatility in the security environment that seems to lose its sense of equilibrium.

Even if does not always permit this identifying of the next strategic surprise, this key of interpretation allows the intelligence analysts to be more alert in a renegotiated space between the participants to the social life, in a more alert pace than B.I. (*Before Internet* era).

Conclusions

Considering things in retrospect, the inability of intelligence analysts to foresee the moments of inflexion seem to be a natural consequence of cause-evolutions and is often due not only to the superficial knowledge of analyzed spaces, of history, of geopolitical profile, of culture or of psycho-social determinants regarding the targeted population.

Most of the time, this inability is generated by the social structure whose agent the actant is (the analyst), its features reflecting, at least partially, in his perspective, predilections, and preferences. Understanding this connection is very important in intelligence analysis, and the reasoning of the present paper is that symbolic interactionism, along with other scientific perspectives, may contribute to avoiding cognitive biases.

References

1. Becker, Howard Saul (1963). *Outsiders: Studies in the Sociology of Deviance*, New York: Free Press (Simon and Schuster), retrieved from www.personal.psu.edu/exs44/406/becker_outsiders_from_witzer.pdf (accessed on 01.02.2015).

2. Castells, Manuel (coord.) (2004). *The Network Society* (vol. 1), Massachusetts: Edward Elgar Publishing Ltd.

3. Cooley, Charles Horton (1902). T*he Looking-Glass Self, Human Nature and the Social Order*, New York: Scribner.

4. Doise, Willem, Mugny, Gabriel, Deschamps, Jean-Claude (1996). *Psihologia socială experimentală*, Iaşi: Polirom.

5. Goffman, Erving, (2007), *Viaţa cotidiană ca spectacol*, Bucureşti: Comunicare.ro.

6. Keynes, John Maynard (1936). *The General Theory of Employment, Interest, and Money*, s.l, retrieved from cas.umkc.edu/economics/people/facultypages/kregel/courses/econ645/winter2011/generaltheory.pdf (accessed on 01.02.2015).

7. Merton, Robert (1948). *The Self-Fulfilling Prophecy*, in *The Antioch Review*, vol. 8, nr. 2, pp. 193-210, retrieved from entrepreneurscommunicate.pbworks.com/f/Merton.+Self+Fulfilling+Prophecy.pdf (accessed on 01.02.2015).

8. Pherson, Randolph, Richards, Heuer Jr. (2011). *Structured Analytic Techniques for Intelligence Analysis,*Washington: CQ Press.

9. Thomas, William Isaac, and Thomas, Dorothy (1929) *The Child in America*, New York: Alfred Knopf, p. 572, retrieved from https://archive.org/details/childinamerica00thom (accessed on 01.02.2015).

10.Zulaika, Juleba (2009). *Terrorism. The Self-fulfilling Prophecy,* Chicago: The University of Chicago Press, retrieved from http://tinyurl.com/3knrm56 (accessed on 01.02.2015).

PERFORMANCE IN INTELLIGENCE AND OSINT ANALYSIS. THE KSAO OF AN ANALYST AND ITS ROLE IN A NETWORKED INTELLIGENCE PLATFORM

Daniela MITU[*]

Abstract

The purpose of this article is to present the main characteristics of performance in intelligence and OSINT (Open Source Intelligence) analysis. Being no perfect "recipe" for the top performer intelligence or OSINT analyst, my proposal consists in adapting the KSAO model knowledge, skills, abilities and other characteristics - to the intelligence field.

Thus, I propose the general requirements of a top performer OSINT analyst, as they are reflected in an ideal profile. With the help of Peter Drucker, Doug Cooper, and Wolfgang Reinhardt' concept of "knowledge worker", I underline the role of the analyst within the project of a networked intelligence platform. This platform represents, in my opinion, a possible alternative to the future of intelligence. Inside this platform, OSINT is the most important brokerage node that makes connections between intelligence organization, Academia, private sector, and civil society.

Keywords: performance, intelligence analysis, knowledge, skills, abilities

Introduction

The words "performance", "performer" and "to perform" belong to the same semantic and lexical field and refer to an outstanding activity and excellent results both in sports and acting. The meaning of these words implies a lot of talent, imagination,

[*] "Mihai Viteazul" National Intelligence Academy

skills, abilities, but also a lot of training, practice, exercises, in brief, experience.

The fact that intelligence analysis lies at the crossroads between art and science has become a common place in the discourse about intelligence. But in the intelligence literature, there are few references to the meaning of performance or to a top performing intelligence analyst and even fewer about the success "recipe" of how to become such an analyst.

My research in recent years and my personal experience have shown that there are no commonly known definitions of performance in intelligence or intelligence analysis, and even less in open source intelligence (OSINT) and open source analysis.

Generally speaking, performance in intelligence is synonym to lack of failure and to success of governmental or national intelligence organizations' operations on the national territory. To avoid strategic surprises, Romanian intelligence services work together, make predictive assessments, and get, what in our National Security Strategy is called, appropriate capacity in order to come up with the best response to security threats.

Seen from the analyst`s point of view, this effort implies providing assistance to beneficiaries in their strategies and action plans in order to prevent security risks and adopt proper measures to promote national security interests. To achieve this goal, the analytical product has to be delivered in due time and must contain all elements necessary to prevent and counter security threats.

The working assumption of this paper is that performance in analysis and OSINT is the result of putting together knowledge, skills, abilities and other characteristics in an ideal profile and my contribution consists in finding the general requirements of these KSAO of performance in intelligence analysis and OSINT. In my opinion, the way in which these general requirements are reflected in the current activity depends on the analyst's personality, organizational habits and rules, as well as group of people the analyst works with - colleagues, teams, task-forces and so on.

KSAO requirements

KSAO are the activity-related knowledge, skills, abilities, and other characteristics that a person must have to perform successfully in a certain position, whatever its nature, especially in those activities related to Peter Drucker, Doug Cooper, and Wolfgang Reinhardt' concept of "knowledge worker". These are workers whose main capital is knowledge. Thus, they analyse, make connections between information, evaluate complex situations, find causalities, and assess trends and their consequences. Due the complex nature of his or her activity, the intelligence analyst is a knowledge worker with multiple roles, such as: gathering and disseminating information, creating and sharing knowledge in a flexible and disciplined manner, monitoring topics, organizing information, searching solutions to specific problems, and networking people[1].

In an intelligence organization, knowledge implies, first of all, the national security issues the analysts are specialized in, such as economy, terrorism, conflict areas' security, critical infrastructure, cyber security etc. In the second place, it is also important to have a good knowledge of the issues' background, namely the history of the issue - what has been said and who said it before. It's useful to know the "voices" behind previous assessments on the issue, and, in the OSINT realm, this is even more important because there is a higher risk of manipulation. To get this knowledge in OSINT there are used open source platforms, on which analysts work on common spaces and within common projects, and where they share expertise and information. The main advantages of this approach are the possibility to have an integrative perspective on an issue, avoidance of fragmentation and of redundancy in analysis, and increase in response capacity to threats. In brief, the work of the analysts is more efficient.

This knowledge is attained in an intelligence organization, especially in OSINT, by a proper training and educational system that incorporates intelligence education offered by intelligence academies' programs and specialized training in intelligence and OSINT provided by internal courses.

In a paper published in 2009, Stephen Marrin makes the distinction between education and training. According him, both systems help to form the analyst by providing both the conceptual or theoretical frame, and the practical one. According to Marrin, education is delivered by the academia and includes bachelors and master's degree, and doctoral studies, while the training is performed within the in house developed intelligence organizations' programs[2].

Despite this institutional effort, an analyst cannot achieve excellence in his or her activity, without lifelong learning, which is a permanent, a constant attitude of openness to learn from the others, from the teams the analyst is part of, from senior analysts. It is the analyst's constant interest in self-development, in learning new things, and in investing in himself or herself time and resources.

In my opinion, skills can be divided in two main parts: individual and group related. The first category includes a high level of intelligence and imagination. Both are relevant to identifying new directions of investigation, especially in OSINT, where the analyst has to deal with plenty of sources and information. The security environment's changes and challenges - uncertainty of evolutions and trends, the mixture of state and non-state actors, the growing number and the complexity of symmetrical and asymmetrical risks - put a great pressure on knowledge providers, in this particular case, intelligence and OSINT analysts, in finding undiscovered, and always new sources and resources. Intelligence and imagination are also useful tools to finding the appropriate manner to evaluate security threats, outlining the main drivers of plausible evolutions, and possible discontinuities, building scenarios, and proposing alternative solutions in order to generate strategic advantage.

A top performer analyst has to develop enough criticism and self-criticism to accept ideas and the arguments of others and to go beyond his or her own biases. To accept others' criticism, analysts have to be adaptable, and flexible. Another requirement of the analytical job is the rigor of judgment, which is necessary when the analyst has to replicate the analytical conclusions in a scientific manner. Communication abilities are also relevant when the analyst presents his or her ideas, especially in writing. He or she should express clearly and convincingly. All these skills of the analyst are reflected in the main criteria that govern the elaboration process of an analytical product (the rigor to be accurate, logical, comprehensive, objective, and resource efficient, timely delivered, useful)[3].

As regards the group related skills, the top performer analyst should know best how to work in teams and, as the leader of a group or a task-force, how to organize and plan the activity, in brief, how to manage the team. From my experience, these skills are extremely important, because OSINT analysts are often part of working teams on different national security issues: permanent working groups or particular task-forces within the intelligence organizations.

The profile of top performer OSINT analyst is not complete without specific abilities. The ability to synthesize information from many sources plays an important role in the OSINT daily work. A top performer analyst should be able to draft complex OSINT products addressing complex issues. From this perspective, OSINT is a very valuable and rich intelligence source (country reports, reports on different conflict or instability areas from multiple points of view - economic, political, social, cultural, and military), where evolution patterns are outlined, generated scenarios and facts are seen in larger pictures.

This complex level of synthesis and analysis is achieved after acquiring long experience, practice and training, as well as good knowledge of national security issues and a constant interaction with other analysts. The natural effects of developing these abilities are the appropriate use of structured analytical methods and techniques[4] and analytical software. Implementing structured analytical techniques help to address the intelligence information needs. These techniques are used to depict, explain and predict, to generate hypothesis, to test them, to interpret complex relations between items and classes of items, between the system and its parts, and to identify causality relations.

The ideal profile of top performer OSINT analyst cannot be complete without other characteristics. These features refer to the willingness to become a top performer analyst, dedication to the analytical job and a permanent self-reinvention. Top performing analysts should be aware of their limits and recognize their mistakes. And last, but not least, analysts should be open-minded to new things, to asking, receiving and providing help.

Different proposals

According to Joel Gardner[5], scholar and educator in the field of instructional technology and design, there are seven “crucial” skills, abilities, and other characteristics to success in our day's knowledge society:

- thinking skills (the ability to work with information to solve problems, perform tasks, and design solutions);
- communication (the ability to understand and share ideas);
- teamwork and leadership (the ability to work with others to achieve a common goal);
- lifelong learning and self-direction (continual self-improvement through the constant gathering of knowledge);
- technology use (use and select tools and technologies to appropriately complete tasks and to accomplish goals);
- ethics and professionalism (an ethical person makes him or herself personally accountable for their own actions and work);
- personal management (manage habits to maintain physical, mental, emotional, and spiritual health)[6].

A similar perspective belongs to Jelena Vukašinović, from Singidunum University, Serbia, according to which the information society is based on computer technologies which rely on the knowledge of workers. Consequently, “the information society presupposes an environment which nourishes creativity and innovativeness, and is based on knowledge and constant learning and acquiring of hard and soft skills”[7].

In the intelligence field, and in the OSINT realm, there is an impressive requirement of knowledge, as well as the need of constant innovation, in accordance with ever new demands of technology and security challenges, combining and connecting skills and abilities, by applying information and communication technologies in order to approach any problem from many aspects and thus maximize the value of intellectual capital[8].

Paul K. Davis[9], policy analyst and Senior Principal Researcher at RAND Corporation, is the author of the FAR model, meant to provide help to professional analysts and decision makers in order to assume new responsibilities and to identify strategies. The main characteristics of this model are:

- flexibility - to accommodate changes in missions, objectives and constraints;
- adaptability - to cope with new circumstances;
- resilience - to absorb shocks.

Paul K. Davis highlights the ways in which intelligence analysts can respond appropriately to decision makers' requirements:

- by ensuring that they examine an available set of options and to use multiple criteria for their evaluation;
- by notifying uncertainties and demonstrating determination in the distillation of their implications;
- by identifying hedging measures available that allow subsequent adjustments;
- by supporting the organization in their efforts to obtain flexibility and resilience.

OSINT in intelligence

OSINT is an important source of intelligence, providing understanding of evolutions, situations or events. It offers experts' opinion in various security domains - for example journalists, scientists or academicians having a long experience in certain areas or that are familiar with the social, economic and political context of various countries. It also covers fields of interest that otherwise cannot be filled by secret sources, such as macroeconomics, demography, political transformations, or security strategies.

The multidisciplinary view and the predictive-anticipative perspective in the analytical products can easily be met with the help of open sources or, better, with a mixture, the so-called integrated intelligence analysis of open and secret intelligence. Grey literature, scientific papers, works of scholars, think tanks and research are important open sources used in both tactical and strategic intelligence.

In the last years, a complex review of the intelligence process within the Romanian Intelligence Service has been recorded, beginning with the development of the "Strategic Vision 2007 - 2010". Some of the priorities of the transformation process that the SRI has undergone were and still are the extended role of OSINT. The role of OSINT in the strategic analysis as a brokerage node in the knowledge network composed by intelligence services, academia and civil society, was strengthened by the "Strategic Vision 2011 - 2015" ("SRI in the Information Age") according to which one of the open source priorities is drafting strategic assessments on medium and long-term threats and risks.

OSINT as brokerage node in a networked intelligence platform. The role of KSAO

In our daily networked society, the intelligence organizations and the intelligence analysts cannot all by themselves find complex answers to complex issues. In line with current intelligence policies, government and private organization's contribution to national security is increasingly emphasized, as result of the need for a large participation to protect the national security, which is considered a common good.

There is an impressive need to attract the expertise of the outside stakeholders - the Academia, the private sector, and civil society - in order to co-generate knowledge for smart decisions, especially at strategic level.

Due to its diversity, open source information represents the main resource for strategic intelligence. Using different structured analytical techniques and software, using knowledge and experience from different national security fields, analysts can develop plausible alternative scenarios, helping them to explain causes of potential situations or events and identify trends of action.

Given its open nature, OSINT facilitates access to much more lax practices of sharing ideas and information, than those used in other sources of intelligence (human or technical), characterized by the need of preserving secrecy. OSINT is consequently the most appropriate intelligence resource to introduce the expertise from outside into the intelligence system.

Based on the expertise gained from the collaborative work initiated on different platforms, analysts can develop an OSINT based networked intelligence platform that facilitates interaction between intelligence organization and external knowledge. The idea of analytic hubs "borrowed" from the business sector could represent the solution to put in practice this conceptual system.

The purpose of analytic hubs' is to provide dedicated storage, tools and processing resources to establish a foundation for recurring discovery needs[10]. Analytical hubs are used for developing predictive models and to integrate, in a single common work space, available technologies into an automated architecture, in order to manage the entire informational flow, through its five components: business analytics (includes the tools used for discovery and situational analysis), advanced analytics (includes analytical tools used for statistical analysis, predictive modelling, data mining and data visualization), analytical hub platform (provides the processing storage and networking capabilities), predictive modelling (analytical servers, statistical databases and predictive modelling engines) and data access and delivery points (enables accessing and integrating a variety of structured and unstructured data)[11].

Bringing knowledge and expertise together from different fields allows one to: develop cooperation among collectors, analysts and beneficiaries of intelligence products; integrate information from different expertise fields; build a collaborative mechanism useful to the elaboration of analytical products as response to various national security issues. The collaborative work facilitates the dissemination of high standard analytical products, in order to complete with discursive and meta-discursive criteria, such as accuracy, completeness, usefulness, objectivity, and resource efficiency.

Inside this collaborative and analytical frame, there is a considerable increase of the importance of the intelligence analyst`s roles as knowledge worker, as presented at the beginning of this paper. The roles of the analyst as retriever, learner, sharer, helper, linker, solver, networker, and organizer, whether he or she works in teams or individually, are strengthened. In absence of these complex roles, none of the processes of collaboration is possible.

As participant on different work teams, the analyst retrieves and shares by himself or herself relevant information, helps the others learn new things and improves collaboration, by linking persons, departments or projects to each other. He or she should be a problem solver, by finding or proposing innovative solutions to specific challenges (national security, technological, informational, communicational etc.). As team leader, the analyst should be both a networker between team members, and an organizer of the entire team`s activity.

More than ever, collaboration with experts from Academia, private sector and civil societies is meant to enhance knowledge, skills, abilities, and other characteristics of the OSINT analyst.

Knowledge means not only accumulated intellectual capital, but also a basis for sharing data, opinions, and ideas on different tactical and strategic issues between representatives of intelligence organization and experts from outside - national think thanks, research centres, universities, business organizations, non-governmental organizations etc.

The specific skills and abilities necessary to draft complex analytical products are equally important in relation with the so-called outside experts, namely the fresh view, the imagination, the critical thinking, the talent, the creativity, the high capacity of organizing activities and ideas, the communication skills, the flexibility and the mind openness.

Conclusions

A growing body of literature advocates the need for performance in intelligence and analysis. In this paper performance in analysis and OSINT is considered to be the result of putting together knowledge, skills, abilities and other characteristics in an ideal profile.

The general requirements of this profile are necessary to accomplish the complex and diverse roles of intelligence and OSINT analyst as knowledge worker in an integrated and networked intelligence platform, which is meant to bond intelligence organizations with outside expertise, in order to improve the intelligence production and provide it with a deep insight.

A collaborative work platform based on open sources, with tactical and strategic input and output, could be developed having as central node intelligence services and as its “alters” the Academia, the civil society and the private organizations.

Bibliography

1. Brei, William S., *Getting Intelligence Right: The Power of Logical Procedure. Occasional Paper,* no. 2, Washington D.C., Joint Military Intelligence College, 1996.
2. Craig S. Fleisher and Babette Bensoussan, A FAROUT Way to Manage CI Analysis, accessed 15 May 2015 http://mindshifts.com.au/articles/the_farout_method.pdf.
3. Davis, Paul K., *Analysis to Inform Defense Planning Despite Austerity*, 2014, RAND, accessed 15 May 2015, http://www.rand.org/pubs/research_reports/RR482.html.
4. Gardner, Joel, *The 7 Skills of Knowledge Work*, 27.10.2014, accessed 15 May 2015 http://joelleegardner.blogspot.ro/2014/10/the-7-skills-of-knowledge-work.html.
5. Heuer, Richards J. and Pherson, Randolph H., *Structured Analytic Techniques for Intelligence Analysis*, Washington D.C., CQ Press, 2011.
6. Marrin, Stephen, *Training and Educating U.S. Intelligence Analysts*, "International Journal of Intelligence and Counterintelligence", 22 (1).
7. Phythian, Mark, *Intelligence Analysis Today and Tomorrow*, "Security Challenges", vol. 5, no.1, 2009.
8. Reinhardt, Wolfgang, Schmidt, Benedikt, Sloep, Peter and Drachsler, Hendrik, "Knowledge Worker Roles and Actions", *Results of Two Empirical Studies in Knowledge and Process Management* (2011), DOI: 10.1002/kpm, accessed 15 May 2015 http://www.researchgate.net/profile/Hendrik_Drachsler/publication/216015967_Knowledge_worker_roles_and_actions_--_Results_of_two_empirical_studies/links/0fcfd50eacf0f3df01000000.pdf.
9. Sherman, Rick, *Analytics Best Practices: The Analytical Hub*, 2013, accessed 15 May 2015,
10. http://stats.manticoretechnology.com/ImgHost/582/12917/2013/Resources/whitepapers/AnalyticalHub_Composite2013.pdf.
11. de Valk, Guillaume Gustav, *Dutch Intelligence - Towards a Qualitative Framework for Analysis*, 2005, accessed 15 May 2015 https://www.rug.nl/research/portal/publications/dutch-intelligence--towards-a-qualitative-framework-for-analysis%28dc65b14e-788b-45c7-b830-f68032256e55%29.html.
12. Vukašinović, Jelena, *Impact of Internet on Business activities in Serbia and Worldwide*, "Sinteza", 2014, accessed 15 May 2015, http://portal.sinteza.singidunum.ac.rs/Media/files/2014/476-479.pdf.

References

[1] Wolfgang Reinhardt, Benedikt Schmidt, Peter Sloep and Hendrik Drachsler, “Knowledge Worker Roles and Actions”, *Results of Two Empirical Studies in Knowledge and Process Management* (2011), DOI: 10.1002/kpm, accessed 15 May 2015 http://www.researchgate.net/profile/Hendrik_Drachsler/publication/216015967_Knowledge_worker_roles_and_actions_--_Results_of_two_empirical_studies/links/0fcfd50eacf0f3df01000000.pdf .

[2] Stephen Marrin, *Training and Educating U.S. Intelligence Analysts*, “International Journal of Intelligence and Counterintelligence”, 22 (1), p. 131.

[3] William S. Brei, *Getting Intelligence Right: The Power of Logical Procedure. Occasional Paper,* no. 2, Washington D.C., Joint Military Intelligence College, 1996, pp. 51 - 70; Guillaume Gustav de Valk, *Dutch Intelligence - Towards a Qualitative Framework for Analysis*, 2005, pp. 103 - 115, accessed 15 May 2015 https://www.rug.nl/research/portal/publications/dutch-intelligence--towards-a-qualitative-framework-for-analysis%28dc65b14e-788b-45c7-b830-f68032256e55%29.html; Mark Phythian, *Intelligence Analysis Today and Tomorrow*, “Security Challenges”, vol. 5, no.1, 2009, p. 81; Craig S. Fleisher and Babette Bensoussan, A FAROUT Way to Manage CI Analysis, accessed 15 May 2015 http://mindshifts.com.au/articles/the_farout_method.pdf.

[4] Richards J. Heuer and Randolph H. Pherson, *Structured Analytic Techniques for Intelligence Analysis*, Washington D.C., CQ Press, 2011.

[5]Joel Gardner, *The 7 Skills of Knowledge Work*, 27.10.2014, accessed 15 May 2015 http://joelleegardner.blogspot.ro/2014/10/the-7-skills-of-knowledge-work.html.

[6] *Ibidem.*

[7] Jelena Vukašinović, *Impact of Internet on Business activities in Serbia and Worldwide*, “Sinteza”, 2014, pp. 476 - 479, accessed 15 May 2015, http://portal.sinteza.singidunum.ac.rs/Media/files/2014/476-479.pdf.

[8] *Ibidem.*

[9] Paul K. Davis, *Analysis to Inform Defense Planning Despite Austerity*, 2014, RAND, accessed 15 May 2015, http://www.rand.org/pubs/research_reports/RR482.html.

[10] Rick Sherman, *Analytics Best Practices: The Analytical Hub*, 2013, p. 3, accessed 15 May 2015, http://stats.manticoretechnology.com/ImgHost/582/12917/2013/Resources/whitepapers/AnalyticalHub_Composite2013.pdf.

[11] *Ibidem.*

STRATEGIC INTELLIGENCE AND ORGANIZED CRIME

Lucian IVAN[*]

Abstract

When establishing proactive solutions to constrain organized crime opportunities, the challenges for strategic intelligence are to create assessments that capture risks and opportunities from an organized crime perspective and to be able to find those factors that can disrupt or prevent organized crime opportunities. In this regard, this strategic intelligence could reduce the time between deciding on a law enforcement strategy or action and implementing an effective operation to disrupt the organized crime. Intelligence-led policing could be more strategic in term of detecting organized crime opportunities and fragilities rather than targeting groups. Thus, to have an effective imaginative entrepreneurial response to organized crime, law enforcement must concentrate on market evolution rather than groups make use of a large number of data sources and enhance partnership in law enforcement and collaboration in law enforcement community.

Keywords: intelligence, strategic analysis, organized crime, law enforcement

According to the EUROPOL, we are facing today an estimated 3600 Organized Crime Groups (OCGs) active in the European Union (EU). These groups are becoming increasingly networked in their organization and behavior characterized by a group leadership approach and flexible hierarchies. International trade, an ever-expanding global transport infrastructure and the rise of the internet and mobile communication have engendered a more international and networked form of serious and organized crime. There is an increased tendency for groups to cooperate with or incorporate into their membership a greater variety of nationalities.

[*] Ministry of Internal Affairs, Department of Intelligence and Internal Protection

This has resulted in an increased number of heterogeneous groups that are no longer defined by nationality or ethnicity. Serious and organized crime is fundamentally affected by the process of globalization with none of the crime areas or criminal groups insulated from the changes involved.

Criminals act undeterred by geographic boundaries and can no longer be easily associated with specific regions or centers of gravity. Despite this, ethnic kinship, linguistic and historical ties still remain important factors for building bonds and trust and often determine the composition of the core groups controlling larger and increasingly diverse criminal networks.

The complex structure and expansion of organized crime is characterized as a growing threat to national security and the stability of communities. There is a common understanding between academics and professionals regarding the abilities of organized crime: they have their own network structure; they move rapidly to exploit opportunities and they tend to obscure the boundaries between licit and illicit activities in such a way as to enhance asset maximization.

To better assess organized crime and law enforcement reaction to it, police have three major roles:

1. produce threat assessments;
2. act as global police;
3. increase police capabilities worldwide.

Thus, intelligence is an essential component of law enforcement capability and exists at all levels of decision-making to support leaders and policy makers to make effective decisions. Intelligence analysis provides the decision-maker with a timely and accurate understanding of criminal threats and the components of operational environment.

In the law enforcement context, it is sometimes difficult to obtain the factual information necessary for effective planning and decision-making. This is principally because much criminal activity is undertaken in such a way that it is deliberately concealed; empiric evidence is not readily available. The whole rationale for developing criminal intelligence analysis is therefore to assist law enforcement agencies to plan, and trough planning to maximize their operational and organizational effectiveness.

Strategic intelligence is that required by the senior executive and policy makers for the formulation of strategy, policy and long-term plans. It may have current or explanatory components by its nature, but given the requirement to service forward looking decisions, it must inherently have a “futures” component. Given a wide range of clients that can include government ministers, senior law enforcement executives and policy makers, a comprehensive service will need to include a mix of national current intelligence, forward looking assessments, open source reports and strategic warning. The purpose of future work in strategic intelligence is to:

- provide a strategic context within which to understand emerging threats;
- provide a foresight capacity to allow the development of targeted strategies (provide warning of the need for new and different capabilities, policies, responses, priorities, powers and so on);
- narrow the range of uncertainty;
- and ensure that this understanding is provided in an appropriate form to the appropriate policy makers at the right time.

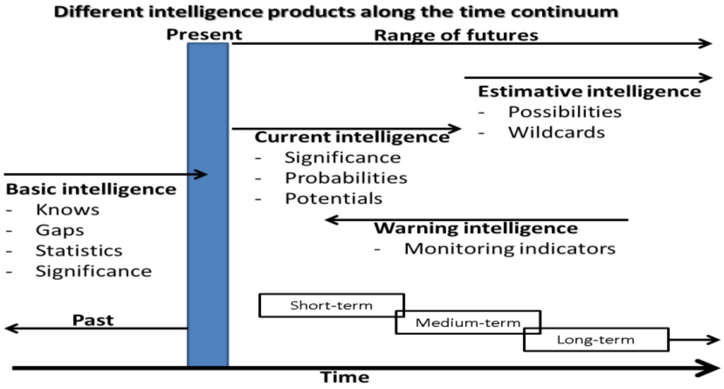
Importantly, strategic analytical product must always be explicitly policy relevant. It is less about descriptive intelligence and more about explanatory and estimative (predictive) intelligence. In the “estimative” sense, this means providing a range of possibilities, with attendant assessment of likelihood, such that decisions are made with full view of the range of possibilities and the potential consequences of actions.

A significant difference between futures work conducted in law enforcement and the national security service, is that strategic criminal is often oriented towards consequence management rather than situation management. That is, national security related intelligence often focuses on event issues, whereas, strategic crime assessments are often focused on consequences of future trends, such as the mutation of criminality, the unintended consequences of social experimentation or legislative or regulatory reform.

Products for futures analysis

- **Basic (background) intelligence** (What has happened?) This type of product contains background intelligence, usually encyclopaedic in nature, that provides a broad range of baseline information and intelligence. While not futures based, such products provide a useful historical start point for analysis of futures.

- **Current intelligence** (What is happening?) Specific assessments related to the status and significance of an ongoing operational threat, event, environmental condition or indication of illicit activity. Usually incorporates a section of the issue or indication and an assessment of implication by "who/what/why/when/were/how". An assessment will normally be made on the significance of the problem over the short term.
- **Warning intelligence** (Is the future unfolding?) Warning intelligence is that which provides warning of threats to law enforcement or national interests in time to take effective action. Warning intelligence bridges the current and estimative intelligence gap by focusing on agreed warning problems as part of a decision support mechanism that requires rapid alert and some form of policy, intelligence or operational response.
- **Estimative intelligence** (What could occur?) Estimative intelligence is that which provides forward looking assessment and predictive judgments, and attempts to project probable future developments in the law enforcement environment and analyses their implications. Assessments normally have an explanatory section (environmental and stakeholder analysis) culminating in a discussion of key change agents or drivers. Finally the types of futures or future implications are discussed.



General tools

New and evolving trends in criminality flow from a combination of political, economic, technological and social factors epitomised by continuing globalisation, alertness to international terrorist and transnational threats, and myriad domestic pressures. This provides a complex qualitative problem for strategic analysts – not resolved through the application of simple scenario generation tools.

No matter what type of product, strategic intelligence normally has the following ingredients:

- description of events or a situation with an eye to identifying essential characteristics (what, who, when, where, how);
- explanation of underlying causes (why);
- what could happen or develop (so what?);
- and implications (now what?).

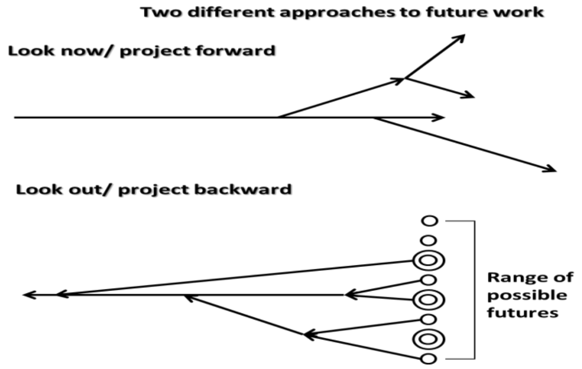
Hence analysis normally follows the stages of consideration of: Environment – Stakeholders – Causalities – Futures – Implications. For an analyst dealing with an issue on a daily (current) intelligence basis, aspects of a study of the environment and stakeholders may be intuitive, but they still need to be ordered logically for the less-aware customer. It is useful to keep the same terms of reference for analysing the current situation as for the future.

Reference points are generally divided conceptually into:

- **events** – observable actions or activities that provide a conceptual framework for "what has happened" and "what may happen";
- **patterns** – partially observable relationships related by time, sequence, association and/or effect. These patterns allow the analyst to link and associate events and stakeholders; and
- **drivers** – an inffered fundamental force that creates or underpins change over time (the drivers are also often called change agents, underpinning influences, or causal factors). These are inferred factors that assist the analyst to understand to explain why something is occuring, why it will change, and how patterns and events may emerge over time.

Using events, patterns and drivers as a central framework, there are two general approaches to considering the futures part of this process. First, it is possible to examine the present in order to extrapolate change out into time. A second option is to examine possible futures and consider the range of events and factors that may connect "there" to "now". The first option can entail the use of tools that "look from here to there".The first set of tools are designed to do precisely that. The second range of tools allow the analyst to "look from there to here".

These two different approaches to futures tool are shown diagrammatically in the figure below. We begin with tools that "look from here to there".


Two different approaches to future work
Look now/ project forward
Look out/ project backward
Range of possible futures

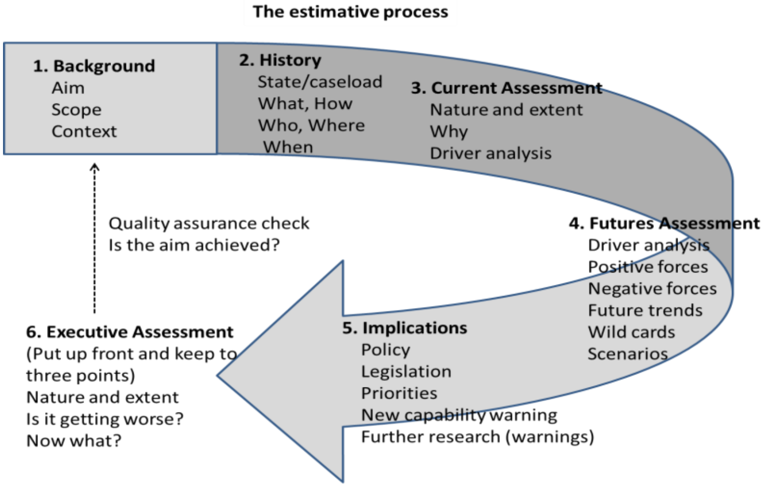
Written estimates

The most common form of futures tool used is the individually written analytical paper in which analyst wades through a series of deductive and inductive thought processes on the environment, stakeholders, influencing or causal factors, future scenarios, and implications. This is quite a useful tool as the "estimative" narative may translate readily into the ultimate product released to the client. This saves formatting time. It is also useful where one individual is charged with carriage of most of the analysis. Critically, the estimative flow often provides the best framework for the inclusion of results of products from other types of analysis.

Strategic intelligence estimates normally consider the range of events, patterns and drivers associated with the topic under analysis. The aim of such work is to support deliberate decision-making and planning processes which may act on only the key judgements but must be informed by the supporting analytical process. Additionally, aspects of such analysis will be useful to a range of associated intelligence analysts and hence, if the analysis is packaged as a complete product, it usually gets broader dissemination than other more tailored products.

For example, an analyst tasked with completing a quite complex strategic assessment on the nature and extent of an issue that is not quantifiable – as often occurs in the law enforcement environment – will need to develop a number of methodologies with which to assess the extent of the problem. Methodologies should provide a minimum size and a maximum size, with several methodologies providing indicative numbers in between. With commodity imports (for example, people or drugs) the minimum way be what we seize or find while the maximum may might be extrapolations of the highest estimated import rates internationally. Mid-range figures can be estimated based on extrapolating from various control groups, such as the potential consumer base or the known criminal base.

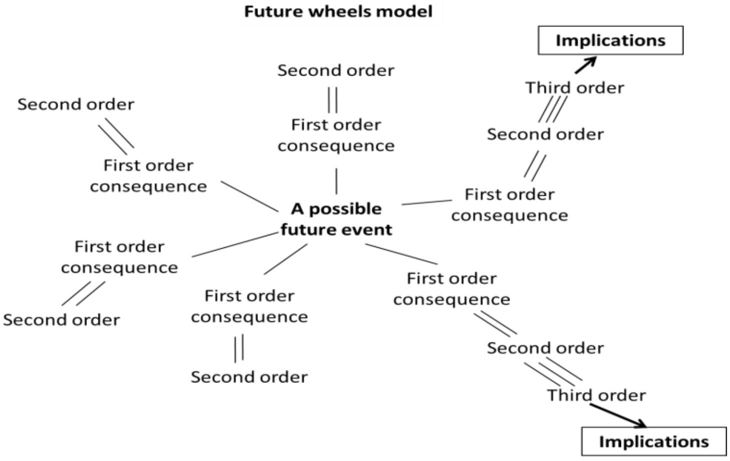
The future then can be assessed based on drivers affecting these control groups as to whether they will seek to import more or consume more.



Pulling it all together using an Estimative approach

Futures wheels

The futures wheel is a consequence analysis tool mainly designed to consider the effects of an event of action, but may be used to consider a particular trend. Diagrammatically dispayed, this tool provides rapid visualisation of the cause and effect relationship of consequences.



Description of the method

Step 1 – scope of the future of the event to be tested. Such events are normally expected to happen based on current or historical occurrences – such as an election, an economic downturn, a trade pact being signed and so on. The event to be examined is placed in the center of a visual display.

Step 2 – 'Big picture' or first order results are arranged out from the event and connected by solid lines indicated direct outcomes. The first-order result is surrounded by secondary results, associations or consequences and connected by double lines. A good place to start is what happened last time this event occurred.

Step 3 – the process is then continued by using triple lines to add third-order consequences, and may be developed to further levels of consequences, and may be developed to further levels of consequences and beyond. All of these stages can be seen in the figure below.

The tool is often useful in brainstorming sessions that have already successfully employed such tools as Ishikawa diagrams to explain the current context.

For example, as a strategic criminal intelligence is frequently a study into unintended consequences, futures wheels are often used when considering an event that could possibly impact on the shape of the environment, for example, impending legislation.

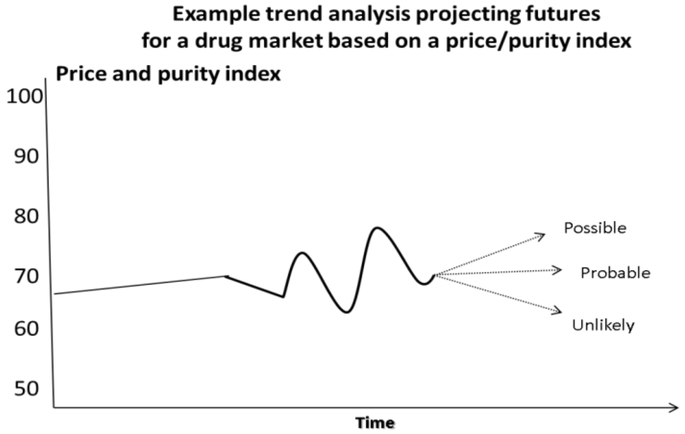
Trend analysis (time impact analysis)

Trend analysis is one of the most common futures tools because it is one of the most common explanatory tools and is supported by a wide variety of commercial software applications.The common problem in extrapolating from existing trends is that it is comfortable for both the analyst and the customer to believe that existing trends will continue. Without the addition of other tools, on perspectives, such analysis will display only limited possibilities and hence be of less use in intelligence terms; leaving the decision-maker prone to 'strategic surprise'.

The process of extending trends through a time-impact analysis into the future has, as its basis, the assumption that the future is an extension of the present. It is therefore important to start with a graphical, statistical, or some other representation of historical and current trends. The analyst then asks the following questions:

- What are the current observables and drivers of the trend?
- What forces are acting on this trend causing it to continue? Will those forces continue in the future?
- If the direction of the trend continues, what will be some positive or negative consequences?
- What is likely to alter the trajectory of the trend over time in terms of event or drivers?
- What forks in the trajectory will this produce?
- What are the positive or negative consequences of these forks?
- How much of this trend can be influenced by actions of the supported decision-maker?

A graphical example of a trend analysis is shown in figure below. The example projects three scenario futures for a hypothetical drug market, based on a price and purity index. Three outcomes are depicted from the current time into a future. The outcomes are shown by dashed lines. In the example shown in the figure, the analyst goes against the statistical trends of previous years, assessing that a paticular driver will impede a recurrence of the previousm cyclical peaks and thoughs.



Analysing drivers with 'Force field' analysis

Force field analysis is a comparative tool that assists the examination of the relative weights of drivers that act for (facilitators) or against (inhibitors) change. The concept may also be used to assist weighing the pros and cons of consequences arising from decisions or future events.

Before conducting force field analysis, the key drivers should have already been identified by another analytical process. An explanation of the relative strenghts of drivers on the current situation can be displayed as follows:

- list all forces for change in one column, and all forces against change in another column;
- assign a score to each force, from 1 (weak) to 5 (strong);
- the table may be converted readily into a diagram showing the forces for and against change. Show the size of each force as a number next to it or by different sized arrows pushing at a

centre line forming a pendulum effect. Or if turned on its side a see-saw display can be created, which is often more effective as it shows the relative strengths of each driver.

Threat assessment

Much of criminal intelligence processes have a genesis in security intelligence processes. Hence there are a range of threat assessment and risk assessment tools that assist an articulation of threat levels and potential priorities of response. Many techniques that are based on an attribute weighting system – that cumulative provides a threat assessment – are relatively difficult to apply in a futures context.

Capability and intent are two further perspectives on threat that can be analysed a futures context, where capability relates to the means and knowledge to facilitate a crime, and intent relates to the willingness to conduct the crime. Capability atributes can be given a relative weighting according to the potential or willingness to develop levels of capability related to the crime type under analysis. A level of subjectivity needs to be imposed by the analyst by considering emerging ways to conduct criminality in the face of likely environmental change.

An area of difficulty remains when attempting to quantify future intent. This is often speculative in explaining current threats, let alone considering future criminal issues. A useful approach here may be to retain intent as a constant from current assessments, allowing a controlled variation of capability to assist in assessing the impacts of targeting capability over time.

Competing hypothesis

Competing hypothesis is an analytical techniques used to objectively create a range of possible answers to a question.

This technique uses a multi-step technique to explore a range of hypotheses in order to evaluate them and identify the most plausible of the options. As such it is a useful technique to establish a current perspective on an issue and especially as a framework to collect against components of the problem. However, it can also serve as a futures tool, in that subsequent analysis of unfolding events or patterns (through the examination of indicators of evidence) will be conducted against these hypotheses.

Combining techniques

Like any use of tools, the best analysis is achieved from a combination of approaches. A particularly useful combination is to take time lines or pattern lines forward and add the balance of competing drivers in a weighthed fashion over time.

This not only provides an interpretation on how trends may branch or emerge over time, but also which key drivers are required to create that divergence.

Conclusion

If a strategic intelligence system does not include a futures function, then it inherently does not fulfil a strategic intelligence function. As an extension of a strategic decision-making system that involves policy, capability, strategy and operational development, strategic intelligence must include analysis of significance and consequence over time.

Such futures work does not have to be necessarily lengthy, involved or grounded in the unknown. It should, however, seek to challenge and provide the broadest context for decisions and be supported by a robust collection system. The analysis required to support such intelligence processes can be assisted by a range of futures tools usually aligned to either look out from where we are or look back from where we may end up.

References

1. Gray Colins, *Transformation and Strategic Surprise* (Strategic Studies Institute of the US Army War College), accessed October 2014 at http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB602.pdf.

2. EUROPOL, *EU Serious Organised Crime Threat Assessment*, accessed October 2014 at https://www.europol.europa.eu/sites/default/files/publications/socta2013.pdf.

3. Keith B. Payne, *The Fallacies of Cold War Deterrence and a New Direction* (University Press of Kentucky, 2001).

4. Colin S. Gray, *Maintaining Effective Deterrence* (Strategic Studies Institute, U.S. Army War College, August 2003).

THE WEB OF TRUST AND DILIGENCE

Dan MAZARE[*]

Abstract

Bridging academic, governmental and business intelligence while looking for a competitive edge leads to sewing a web of trust, connecting different entities' interests according to a common goal. More than a network, which usually emerges out of some entities' spontaneous behaviour, the web encloses a well-defined goal. It takes hard work and diligence to sew a web, supporting and adding value to the web itself. The current paper argues that, first, the quality of the thread empowers the web (content matters), and second, one should also look for blue ocean strategies not only for competitive edges (it is not only about competitiveness but also about value innovation).

Keywords: innovation, competitiveness, network, web, intelligence

> Kublai Khan: "But which is the stone that supports the bridge?"
> Marco Polo: "The Bridge is not supported by one stone or another, but by the line of the arch that they form."
> Kublai Khan: "Why do you speak to me of the stones? It is only the arch that matters to me."
> Marco Polo: "Without stones there is no arch." ...
> Italo Calvino, *Invisible Cities*[1]

Bridgeheads and the Weaver

The literature addressing intelligence is most of the time biased towards the peculiar context of its emergence. Academics are addressing issues using tools specific to their academic specialization and their sources of financial support, while managers, officers, businessmen or statesmen alike, are facing the same subjects from a different angle of responsibility, as the profit or the national interest

[*] PhD candidate, "Mihai Viteazul" National Intelligence Academy.

might require. It is even this superficial but recurrent point of reference, literature *per se*, revealing that bridging these worlds is a terrible task. Beyond literature one would also find differences tributary to the way in which human nature mingles with the democratic framework and its modern characteristics: bureaucracy, meritocracy, idiosyncrasy and political correctness at least.

The roots of discontent might be diverse, yet solutions for bridging different perspectives on intelligence are being feverishly sought-after, as the promise of competitiveness is the main prolongation of our current mainstream understanding of economic development.[2] From this point of view, bridging different perspectives on intelligence is similar to bridging different perspectives on international relations or policy analysis: a route through which science becomes more directly and deeper linked with our risk society[3] and risk prone behaviour, addressing issues as diverse as global warming, genetic modified organisms and last but not least, the trade-off between security and freedom, for example.

There are at least three labels attached to the word intelligence, defining different context into which the "terms of bridging" were sought: intelligence as a field of work for some categories of professionals, intelligence as a particular (pseudo-)scientific domain, or intelligence as a process and its corresponding organization of work. In all these cases, the "terms of bridging" define the categories of entities having different interests yet a potential common goal. Therefore, when addressing the subject, we have to note the different entities involved, their intentions and the bridgeheads they intend to acquire or are currently occupying.

As a field of work, intelligence gathered in time distinct approaches from academic, business and governmental professionals. The context is very well described by one of those anecdotes which emphasize the differences between "the good, the bad and the ugly", the professor, the businessman and the statesman, not necessarily being listed in this order. Adding an additional layer of humour, one could not that there are many roles of bad guys and many roles of good guys, while some good guys may also be ugly guys and thus these cases become as bad it gets etc. Attending a business conference and targeting intelligence subjects is a matter of an adventurous endeavour, as you can meet software evangelists disguised as business intelligence specialists, former officers playing the intelligence target centric approach in a complex business environment, marketing and sales professionals selling themselves as competitive intelligence professionals, and academics specialized in environmental scanning looking after research funding. The state owned ecosystem does not lack complexity either, as the intricacies of the so called national intelligence community prove it. It is a characteristic of the Euro-Atlantic space during the last decade, no matter the national surroundings and their corresponding national intelligence system, to develop national intelligence communities[4]. Despite such optimistic targets, institutional fragmentation continues to remain visible, at least as a norm and code of professional behaviour. There is the task force of the law enforcement institutions, the army's personnel, the "army" of the national security professionals, and a myriad of other specialized teams across institutions; they are all addressing intelligence, establishing specific approaches and standards. IALEIA and IAFIE are not just acronyms, but communities of practitioners and academics, having their own regulations and organizational policies, developing their own perspectives dubbed by standards, in education and daily routine. It is thus a difficult, if not an intractable problem to establish bridgeheads, no matter that a line of arch is well defined and pieces to be merged are hard as stone.

As a particular (pseudo-)scientific domain intelligence gathered much attention during the last twenty years. In the early '90s the study of intelligence was distributed across eight reflexive dimensions[5], four of them being embedded in an "archaeological" approach (memoirs, historical documentations, journalistic investigations, and activities supporting literature as popular culture on intelligence) and four of them targeting the meta-level of the "semantics of intelligence" (the search for a definition of intelligence, of research in intelligence, of a particular methodology of research, and last but not least of the way in which intelligence entered the debate concerning civil liberties). Two decades later, each of the initial dimensions is divided across many others: intelligence became much more present in the public debate, as the so called open source paradigm, the democratic developments in former closed societies and the technological innovation led to issues not met before.

One would find intense debates on "extraordinary renditions", "surveillance laws", "complexity and non-linearity", "asymmetric threats", "analytics and big data", "rebirth of geopolitics". The Truth with its attached conceptual avatars, in this case primarily "security" and "intelligence", is imbued with the lyricism or realism of the time, as a distinguished admirer of Hegel and The Frankfurt School would note[6]. Thus, the study of intelligence as "time grasped in concepts" is not more helpful in finding bridges and competitive edges. The currently flourishing debates tackle the development of a theory / or just a theorization aimed at establishing a conceptual framework of intelligence[7], the development of the analytic culture towards importing scientific methods from various disciplines[8], the comparison of intelligence evolution in diverse cultural settings[9]. Not only different subjects on the agenda but also different approaches of the subjects, as there are differences between education and training, between those who aim at developing the public education on intelligence as a public good and those who train future public professionals for profit. Despite these differences there is a tendency towards increasing dialog in the civil-military relations, without many tangible results in terms of mixed intelligence studies programs.

As a process and its corresponding organization of work, intelligence is also subject of heated debates, with entities proposing different developments to the classic intelligence process. Most of the radical different positions are rooted in traditional challenges: the role of decision makers like active and not passive entities in the intelligence process[10], the questioning of the cyclic pattern employed in the process[11], the centralized or distributed approach of the process[12]. These older debates got a new life as speed and reach, time and global coverage are constraints that gained relevance during the last decade, so that tweaking the intelligence cycle became a challenge. Technology and the open source intelligence paradigm are shaped by, and shape the estimate that 90% of required intelligence is available in open source - an imperative for intelligence collectors and analysts to “mine” the open sources. Another level of discontent in connecting potential bridgeheads grows out of the differences between operational and strategic perspectives on intelligence. While, theoretically, such an issue received a plethora of solutions, starting with balanced scorecards, strategic maps, and results-based management conceived as the supporting instruments, the practice of intelligence continues to emphasize the lack of integrative viewpoints – as “surprises” continue to propagate among the operational and strategic levels. To this picture, one could also add all those issues emerging out of the “need to know” versus the “need to share” approaches, being reluctant in front of any proposed bridging framework not including a transparency – opacity policy.

One of the hypotheses on which the argumentation is based comes from the fact that bridging supports two approaches. There is the spontaneous behaviour of the myriad of entities, as they establish connections at all three levels mentioned before, defining edges and thus networks. Complexity research shows that, in most of the cases, a social system has properties that are difficult or impossible to derive from the features of the units it is comprised of: the system does not necessarily emerge as the sum of its parts; rather the system goes beyond the aggregation of localized behaviour[13]. By taking into account this viewpoint, a second approach on bridging arrives. There must be a weaver: regulator, architect or constructor, whatever the label, it has to emphasize and reinforce what goes beyond the mere interest of the parts, adding trust and coherence. It is the weaver the one who directs the emergent behaviour towards the benefit of the system, transforming the network into a web of trust.

The Promised Land

The mystic role the weaver gets might seem inappropriate in a competitive, mundane environment, such as the world of the intelligence affairs. Intelligence is aimed at supporting decision making and one could infer that entities involved in producing intelligence are themselves intelligence enabled entities, perpetrating a set of actions aimed at enforcing their own competitive advantage. So, bridging and networking is the exception and not the rule, it refers to transitory state when approaching the world of intelligence affairs. What might be the promised-land on which all these emergent bridges will hold more than the blink of a transitory state?

Some argue that bridging the national intelligence institutions, civil-society's special organizations (NGOs, think-tanks, associations, foundations etc.) and the business environment is the route to enhancing the democratic values of the society, the freedom of speech, markets and the participative behaviour. Building the democratic ship at sea takes risks and diffusing responsibility of decision making at all levels of the society might generate social cohesion in times of potential prolonged predicament. More than this, there are voices that claim that diffusing open source intelligence principles to the public is the way towards developing a smart nation, a nation of intelligence enabled citizens[14]. This point of view directs us to the fact that bridging becomes sustainable beyond a transitory state if and only if there is a goal rooted in principles and values: a common vision to be achieved by the web of connected entities.

The case of the former communist regimes in the Central and East-European countries might shed some light on the role of the weaver. Some of these countries experienced the fall of the communism through round-table negotiations and trust agreements between communists and their contenders, some experienced symbolic or physical violence sooner or later after the fall of the communist regimes; some were closer than others to the demise of the state after the fall of the communism. It takes a weaver, a bunch of entities and a vision towards a common goal, that is what history teaches us. Yet, the evolution depends on the content which is set as foundation, the thread leading to little steps or giant leaps in evolution.

If bridging is to be associated with the idea of competitive edges, we have to define how and why the parts would be willing to keep the bridges up. A competitive edge, as the concept is defined in business settings, describes that situation in which one of the contenders has a clear advantage over the competition in terms of one or more elements valued by potential customers. In other words, an association of interconnected entities, acting inside well defined borders, according to well defined competitive rules, outperforms some rivals to grab a greater share of the available resources. There are two potential perils for this kind of equilibrium: the limited resources are exhausted or competition emerges even between the interconnected entities, while trust fades away. The before mentioned example, the faith of former communist countries in Central and Eastern Europe, is to be used again to prove the fragility of this sort of equilibrium, as the ruling elites were rarely able to share a long term vision in these countries. While European Union and a potential NATO membership kept some bridges up, the development of sustainable competitiveness was a matter of exception and not the ruling principle.

The current point of view is rooted in the belief that mutual trust between the bridging entities is attainable and sustainable if blue ocean strategies[15] are the means of development. The image of a deep blue ocean was used by the proponents of this paradigm to describe the unexplored potential of a market space, value innovation – that is, the creation of innovative value to unlock new demand. When it comes to competitive settings and intelligence, most of the current proposals are rooted in Michael Porter's seminal works: intelligence is tool supporting the means to capturing and redistributing resources in a closed environment, so that one entity's gain is achieved at another entity's loss, through more appropriate strategic positioning and operational actions. On these grounds, one can note that innovation in a blue ocean strategy is directed towards the creation of new markets, as one could not swim if there is no water in the pool. In this context, bridging turns into creating an intelligence market. Yet, it takes diligence to set up a market so that academics, business and governmental professionals will find and later fight for value in this market.

Thus, the Promised land comes as a free intelligence-market, a space that triggers many opportunities for the entities involved, no matter if they are academic, business or governmental institutions. In academic settings any attempt to extend intelligence approaches by learning from various scientific disciplines takes shape only when the intelligence market is available as a testing benchmark. Any theoretical approach on intelligence could not be conceived outside an evolving intelligence realm. Such a realm has both a strategic level and a level of routinely executed operational activities, eventually generating surprises for companies, nation states and the myriad of other forms of organizations. Setting up an intelligence market might lead to the integration of different social, economic and political interests, enforce the interoperability of different public institutions and the development of cultural and identity awareness.

The weaver with its mission as an intelligence market initiator and the various facets of the blue ocean strategy used as a source for value innovation, these are the conditions for a web of trust, aimed at reaching, finally, systemic competitive advantage at the society's level. There are at least three key problems that might endanger the development of the intelligence market, as one can find through analogies with the perspectives in complex social adaptive systems. First, one could note the stone-arch problem. As the quote from Italo Calvino directs us, the market depends not only on the weaver's plan, the arch, but on the way in which the myriad of entities, the stones united through more or less visible threads, act in their daily activities, and generate something beyond their own interests, something like welfare.

The dissipative forces endangering the system, such as monopolistic tendencies, cartel or oligarchic behaviour, stand as a second problem, the payback problem. There is no free market without winners and losers, success and failure. It comes as the weaver's task to define the rules aimed at correcting any anomaly emerging on the free intelligence market. It takes principles and norms laid as the foundation of the market. One should not approach this sort of measures as a threat to competitiveness in its own. Rather, such principles would enforce potential solutions for a third problem: the dilution problem, defining the state in which the lack of proficiency and professionalism becomes the rule and not the exception in the intelligence market. It is thus, all about the content, the set of policies, frameworks, associations that shape methodologies, procedures, regulations, that generate high standards for business and competitive intelligence professional activities, that offer key questions and testing benchmarks to researchers, and that finally empower the national intelligence system. But bear in mind that, when everything is intelligence - nothing is intelligence[16].

Concluding remarks

The development of the intelligence market was considered as the promised land of "bridging", in the sense "bridging" is advanced by the workshop. It is the author's contention that no other development is possible in a society outside of such a special sort of community, with academic, business and governmental dimensions being all involved. There are two key items presented as mandatory for the development of the intelligence market: the need for a blue ocean strategy, emphasizing the benefits the society would have by developing such a market, and the need for high standards of education and professionalism in intelligence, translated to the society and thus to the market. The mystic role of the weaver is a collective role, inherently linked with representatives from all the three segments of the society: academic, business, and governmental. The market development is a task of trust and diligence, which might eventually lead to a web of competitive individuals and organizations.

Acknowledgements: This paper is made and published under the aegis of the Research Institute for Quality of Life, Romanian Academy as a part of programme co-funded by the European Union within the Operational Sectorial Programme for Human Resources Development through the project for Pluri and interdisciplinary in doctoral and post-doctoral programmes Project Code: POSDRU/159/1.5/S/141086

References

[1] Calvino, Italo, *Invisible Cities*, Harcourt Brace & Company, 1978, p. 82.

[2] Krugman, Paul, *Competitivness: a dangerous obsession*, Foreign Affairs, 73(2), 1994, 28-44.

[3] Agrell, Wilhelm, and Gregory F. Treverton. *National Intelligence and Science: Beyond the Great Divide in Analysis and Policy*. Oxford University Press, 2014.

[4] Agrell, Wilhelm, and Gregory Treverton, eds. *National intelligence systems: current research and future prospects*. Cambridge University Press, 2009.

[5] Wark, K. Wesley. „Introduction: the study of espionage: past present, future?", *Intelligence and National Security,* Vol. 8, No. 3 , pp. 1-13.

[6] Geuss, Raymond., *The idea of a critical theory: Habermas and the Frankfurt School*, Cambridge University Press, 1981 si Hegel G. W., *Principiile filosofiei dreptului*, Ed. Academiei Republicii Socialiste România, Bucureşti, 1968.

[7] Gill, Peter, Marring Stephen, and Phythian, Mark, *Intelligence Theory. Key Questions and Debates*, Routledge, 2009.

[8] Marrin, Stephen, „Training and Educating U.S. Intelligence Analysts", *International Journal of Intelligence and Counter Intelligence*, 22: 131–146, 2009.

[9] O'Connel, M. Kevin„Thinking About Intelligence Comparatively", *Brown Journal of World Affairs*, 11(1), pp. 189-199, 2004.

[10] Waters, T. J. *Hyperformance: using competitive intelligence for better strategy and execution*. John Wiley & Sons, 2010, p.18.

[11] Arthur Hulnick, „What's Wrong With The Intelligence Cycle", in Loch K. ed. *Strategic Intelligence: Understanding the Hidden Side of Government*. London: Praeger Security International, 2007.

[12] Clark, Robert M. *Intelligence analysis: a target-centric approach*. CQ press, 2012.

[13] Miller, H. John, and Scott E. Page. *Complex adaptive systems: an introduction to computational models of social life: an introduction to computational models of social life*. Princeton University Press, 2009.

[14] Steele Robert David, "Creating a Smart Nation: Strategy, Policy, Intelligence, and Information", *Government Information Quarterly,* vol. 13(2), 1996, pp. 159-173.

[15] Kim, W. Chan, and Renee Mauborgne. *Blue ocean strategy: How to create uncontested market space and make competition irrelevant*. Harvard Business Press, 2005.

[16] Agrell Wilhelm. "When everything is intelligence - nothing is intelligence", *Occasional Papers,* Vol. 1, No. 4, 2002, The Sherman Kent Center for Intelligence Analysis.

COMMUNITY POLICING AND IDEAL SECURITY OFFICERS IN BEST PRACTICE INTELLIGENCE ORGANIZATIONS

Michael ANDREGG[*]

Abstract

This paper will apply principles learned over 150 years of community policing from Scotland Yard in the United Kingdom to St. Paul, Minnesota, USA to derive best practices for ideal security officers in a modern intelligence agency configured to survive the complex, transnational problems that challenge all guardians of public safety in the 21st century.

Intelligence organizations with vision confront multiple paradigm changes similar to what UK Home Secretary Robert Peel faced when he reformed the London City Police headquartered in Scotland Yard in 1829. Peel introduced the Metropolitan Police Act of 1829 that created a new London Police on 29 Sept. 1829, promoting a rigorous and less discretionary approach to law enforcement in general, with more partnerships. A number of ideal goals were articulated that came to be known as Peel's Principles, some of which will be cited in this paper. After providing some history on those principles and echoes from the extensive Community Police program in St. Paul, we will create a contrast table pairing ideal traits of model officers with the corrupted versions that every profession with a real code of ethics must confront in some way, because people are not perfect even when trying as hard as they can to be. It should be obvious that public safety also involves special pressures of various kinds, and a need (rather a duty) to confront the hardest problems we know. Some attention will be paid to the problem of corruption of governance, because that perennial feature of real political systems is the biggest single problem that many officers with consciences face in their careers.

Keywords: community policing, analysis, collection, operations, tradecraft, ethics, best practices

A Brief History of Community Policing

A British Home Secretary named Robert Peel faced a need to reform the Metropolitan Police of London in 1829. As part of that process he wrote a set of guidelines that became known as Peel's

[*] University of St. Thomas, USA

Principles that became a foundation for what is now known as "Community Policing." His words were meant for citizens as well, so I copy here principles number 7 and 9[1].

7: "The police are the public and the public are the police. The police being only members of the public who are paid to give full-time attention to the duties which are incumbent on every citizen."

9: "Recognize always that the test of police efficiency is the absence of crime and disorder, and not the visible evidence of police action in dealing with them."

Mr. Peel wrote these words (slightly paraphrased) in 1829 when times were chaotic in London, and the army had been used to put down civil disorder. Injustice was common, and the wealthy enjoyed great excess while the poorest starved. In many ways it was much like today. But Robert Peel observed eternal truths that he tried to incorporate into the founding principles of what would become the police of the leading metropolis of its time, better known today as Scotland Yard. The police and the public should be one in purpose, but this cannot occur if the police are set against the ordinary citizen. The ultimate measure of good police work is not how many citizens you can jail, even hardened criminals, but rather how much crime can be prevented by maintaining the proper relationship between society and its guardians.

These concepts are echoed by counterterrorism officer, and professor at *Mihai Viteazul's* National Intelligence Academy Cristian Barna: "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!"[2].

Internal security involves more than simple police work, as practitioners of counterintelligence and counterterrorism emphasize. But the principles of right relationship are eternal and apply to all, including soldiers who protect populations from external enemies and special police whose task is transnational organized crime. If experts are not created, ordinary citizens have to face such dangers alone, without special training, equipment or organization. It was so long ago, and it will be so again if police, soldiers and special security officers forget that they come from the general population whom they must always have as allies if they wish to win. Community policing has been practiced in St. Paul, Minnesota, USA for two generations, so our police are leaders in the USA in practical application of such principles. Words on paper have their place, but if the ideas are not embraced by ordinary officers and troops, if the principles do not live in their own hearts, they will not be expressed in dark corners of the night when danger is close. So turning concepts into actual practice is very important, because the communities that police patrol will know whether their guardians are sincere allies in maintaining public order, or merely an occupying force for power elites. One example now of relevant doctrine.

In St. Paul, Minnesota, USA, unlike most large city police forces, officers were once required to live within the city limits. Thus they were known personally to neighbors, off duty as well as on. They suffered the same laws and social conditions as other citizens did. If crime was rampant, their families were in jeopardy. If schools were failing, their children were held back. If corruption dominated politics (as it sometimes did) the police were poorer like the average citizen was. But also, if solving crimes required information from the neighborhoods, the police had many ears in many places that had gained the trust of many neighbors with common interests. For ideal results it is essential that proactive efforts be made to include all major ethnicities and religions among the regular police force, and for the Chief to make himself available to such groups.

This innovative process ran into stiff opposition from the police union, which pointed out one major problem. They observed that police known to neighbors had a hard time ‘getting away from work,’ getting rest, or time to take proper care of their families, because neighbors brought many problems to them directly at home rather than calling proper channels. A compromise was reached where living in neighborhoods was no longer required, but was encouraged by allowing those who did so to take squad cars home with them. In the same spirit, the state of Minnesota licenses all of its police as “peace officers” rather than “police officers.” This symbolic but important difference is stressed in its POST certification required for employment (Peace Officer’s Standards and Training) for anyone who carries a gun in law enforcement here.

The US Department of Justice has a 12 page handbook of principles that define Community Policing further at: http://www.cops.usdoj.gov/Publications/e030917193-CP-Defined.pdf, and a longer 82 page treatment from 1994 is at www.ncjrs.gov/pdffiles/commp.pdf. These ideas are not popular with all police departments, because they call for more transparency than some desire, and a far more equal relationship between police and the communities they protect. They require an internal culture of partnerships with citizen groups and professionalism within the force instead of strict control by hierarchic authorities. Intelligence organizations are especially allergic to transparency and partnerships so I addressed how these ideas can be combined in real intelligence organizations last year[3].

Other practices that help with community policing involve getting regular police out of cars to walk streets to practice proactive problem solving more and urgent responses to crisis calls less (obviously some of that must continue) and favoring soft uniforms to armored SWAT teams (Special Weapons And Tactics) that look like military units, sometimes necessary for hostage situations and terrorists. Soft uniforms with faces that people come to recognize encourage far better information sharing with citizens than armored SWAT groups ever can. Community Policing spends more time on long term liaisons with non-profit social groups and businesses, as well as with federal and other agencies, and extensive media relations including use of social media like Facebook, Twitter, etc. While most such practices are matters of emphasis (crime remains the common problem and focus) those priorities affect how our police recruit, hire, train, promote, and conduct themselves with polite society in general. Changing cultures is extremely hard, so this process must continue for a long time to be fully realized.

It should be obvious but bears emphasis that all these good community relations practices require some level of goodness and cooperative spirit among the community as well. Police in ethnic war zones, or working where organized crime is entrenched and well-armed, cannot be as soft and friendly as those in low crime, affluent areas. But our goal should be that peaceful state, toward which both police and public move with common purpose and strategic vision.

Ideal Officers Compared to Corrupt Officers

Remember at all times that no human being can be perfect, not your officers nor your citizens, not you and definitely not me. So expecting or demanding perfection is a formula for failure, and can be cruel to people trying their best to do the right things. So the contrast table below is just an abstract tool to help identify ideals one may aspire to, and dangers to avoid. It may help to remember that every profession has a corrupted form. This is one reason formal codes of ethics were created for doctors and lawyers to help teach behaviors that are best for them[4].

Ideal Police (or security officers)	***Corrupted Police (or security officers)***
Protect the citizens who hire and empower them.	Dominate and exploit citizens, except the elites who hire them.
Are loved by their communities.	Are hated by the people they parasitize.
Collect intelligence openly from neighborhoods and ethnic groups to guard the common safety.	Spy on neighborhoods and ethnic groups because they are feared and hated.
Work hard to reduce crime at early stages by attending to schools, jobs, youth, etc.	Count statistics on arrests and convictions as though these were metrics of success.
Engage minority ethnic or religious groups by recruiting, training and hiring them.	Shun minority groups and critics because they are seen as security risks.
Share information with relevant media as openly as can be safe for all.[1]*	Prefer public relations manipulation of media to promote big budgets for HQ.

[1] Of course there are many aspects of investigations that should be kept confidential to protect both the innocent and police who are trying to penetrate organized crime, foreign spy rings, etc. These issues are very well known to police everywhere, so need not be elaborated here. The point of this simple table is highlighting how different the vision of community policing is from the models shown by police-states, where most people hate the police who victimize so many.

Educate their communities about the realities of local crime or other problems to create a common security culture to solve problems.	Prefer secrecy whenever they can sustain it, out of fear that citizens will oppose them, convict them, or reduce their budgets.
Cherish dissent as essential for progress.	Fear or hate even principled dissent, because they are weak leaders.
Prefer "peace officer" to "police officer"	Think "peace officers" are probably sissies.

What applies to ordinary police applies with minor modifications to the special police who focus on hard targets like organized crime, government corruption, espionage by enemies or betrayal by spies within (counterintelligence) and the military services who guard entire nations. "Terrorism" is just a new label for a very ancient problem of ruthless adversaries only vaguely connected to other nation states. Sometimes they are sponsored by nations, but as often they are mere criminals who have managed to create successful organizations by ruthless means.

Why Should Professional Officers and Intelligence Organizations Move in this Direction?

1. It is easier on the individual officer and their families, which are more likely to remain healthy and intact. Family health also responds to the core ethics of each officer.
2. While there are short term, transitional costs to bureaucracies, in the long term they are able to attract better people and to succeed more fully in their missions. As Nitu and Costinel note[5] the supply of "best people" is always limited and may be declining. Empowered employees are also more able to develop professional skills and networks.
3. National security is truly preserved (excepting of course the perennial threat of invasion by foreign enemies) instead of being slowly corroded by security services gone corrupt. If

enemies do come, they will face a stronger nation, because the people, the police, the military and the intelligence services will have built a much stronger common strategic and security culture to face any external danger[6].

4. Resilience for all involved will be enhanced[7]. This is a strength of great importance.

It should be obvious, but bears stating explicitly, that officers who are loved by their communities have healthier lives and usually families than those who are hated by the people. For starters, they are more likely to still <u>have</u> families. The constant lying required by corrupt systems and practices corrodes healthy family relations, a problem that caused America's CIA to have the highest divorce rate of any U.S. government agency long ago. A related problem emerges when the security system forbids agents to talk directly with their own doctor or religious mentors about stresses they endure. Police work, and even more so espionage, involves considerable stress. And the tradecraft used by spies actually induces certain mental illnesses in many practitioners[8]. When officers are not allowed to consult with doctors or priests excepting those hired by their agency, stress can be increased rather than healed since it is obvious to all that agency doctors do not always keep their patient's interests first, and agency priests may not keep consultations confidential. Think "Nazi Doctors" if this is unclear. When officers cannot talk honestly with spouses, who is surprised that some spouses (and children) will not talk honestly with them, or just leave the decaying relationship for their own welfare?

Community policing usually involves transitional costs, and some ongoing costs because all this collaboration with neighborhoods, ethnic groups, non-profits, businesses and keeping enough boots on the street to maintain neighborhood "beats" as well as vehicle born, rapid response forces able to respond to urgent calls requires real money. Budgets are always tight, so someone is likely to question having "community service officers" or others committed to liaison full time. Some may question the value of working with schools on issues of common truancy or other tasks that respond to tiny crimes as the precursors of bigger crimes.

The same argument could be used against vaccination for medical diseases. But wise doctors learned long ago that it is much cheaper to prevent disease than it is to try to cure disease once a patient is sick. Have no doubt that perceptive people recognize when institutions are sick too. Intelligence agencies have struggled to attract the truly best and brightest for generations because smart university graduates have many options to use their talents that do not require the sacrifice and occasional danger of working for intelligence systems, the Army or the regular police.

Perfection is not possible, information is always incomplete, often contradictory and sometimes perfused with propaganda. And threat profiles can shift rapidly as noted by Florian Diaconu[9]. National security in a time of metastasizing, complex, international and interdisciplinary crises calls for the very best intelligence possible at every level[10]. So genuine national security is best served if you keep the guardian agencies as healthy and attractive as possible for those whose internal identity fits the broad mission of protecting your people and communities from harm. This is a sacred mission; do not repel the best by archaic or corrupt practices. Finally, liaison relations with other nations are increasingly important in the networked, global world of problems too complex for any one country to fix, or even to understand. Liaisons with former enemies may be called for, even liaisons with the better elements of enemies today. This is very subtle business fraught with perils for both individuals and the state. But true security is better served by the police philosophy of the future, which is sometimes called Community Policing.

Resistance from the Troops and Why Enlightened Police Cherish Principled Dissent

Theories can be eloquent and wise yet have near zero impact on the behavior of actual troops in the field, or police in daily work.

Long term community relations can be considered mere public affairs activity that Chiefs must attend to, but be rejected by troops as 'not real police or security work.' Respect within a unit can be negative, and assignment to such duties a sign that the officer is not strong enough to handle 'real' police or security work. There is less adventure, visible heroism, and regrettably often less money in preventing crime than in rushing to react after crimes occur. If political leadership is corrupt things are even harder, because they will promote repression of those who don't pay off the politicians, and oppose investigation of criminal groups aligned with the regime of the day. All of these problems make changing primitive security cultures to more enlightened forms very difficult.

Few groups are more traditional than a country's military, and many intelligence groups are functional extensions of the military, if not actively controlled and staffed by them. Military organizations have an almost unique need for hierarchical structure because they train to face the harshest environments ever created. Unity of command is powerful if the commander is competent and wise. Time for dissent vanishes in the heat and confusion of real combat. If one team member shirks their duty, or even delays, everyone may die. Since intelligence agencies were created to provide decision support for commanders under great time and other pressures, the culture of intelligence organizations is at least para-military. Dissent is not traditionally embraced by any of these entities.

But all progress begins with someone dissenting from the common wisdom of their place and time. Every advance of science starts with someone noticing evidence that the dominant paradigm is wrong. Old professors, dogmatic clergy and bone-headed Generals often hate that, but they have been proven wrong a million times in human history. When they are very wrong many people die young. Your teachers claim to desire a "science" of intelligence in the knowledge society. This depends upon embracing principled dissent.

My country was created by "colonists" rebelling against a sclerotic King whose rules had nothing to do with colonial welfare.

He sent his agents to harass us, with global 'writs' to search everyone, and confiscate 'subversive literature' and the presses that printed same. When my ancestors rose against him, he sent the greatest Army of its time to crush us. So we waged war in new and different ways until he was defeated. More recently, we created many of the best 'weapons of mass destruction' before we realized they could destroy us too. We refined corruption of governance to an art form, which caused its own dissent. So our NSA built the best surveillance tool ever invented, and turned it against our citizens as well as "terrorists." Now we decide whether to cherish real freedom, or try to crush dissent at home and thereby die.

The Reverend Dr. Martin Luther King became a world known name by articulating principles of conscientious dissent, or civil disobedience, following the paths of Mahatma Gandhi and others with vision who stood up to other colonial powers. King was then killed by dark forces among our intelligence entities, sent by leaders who were trusted with the safety of the nation.

They had grown old and confused dissent with crime, and peace with subversion[11]. There is not space here to enumerate the principles that distinguish constructive dissent from reckless resistance except that non-violence is high among the distinguishing qualities. When students of Otpor! in your neighbor Serbia sought to get rid of Slobodan Milošević who had started four wars with neighbors and ruined his nation, they got some excellent advice about nonviolent civil disobedience from a student of King's, Gene Sharp, and a US Army Colonel of psychological operations named Robert Helvey[12]. They also got cash, printing materials and intelligence from our CIA. Milošević died in jail, and while things are never perfect there is much more peace in former Yugoslavia today because of wise application of these concepts.

Dissent is the first sign that something may be wrong. Dissent tells us when power gets in bed with crime, and is essential to forestall the growth of corruption which occurs spontaneously in positions of power. Sometimes the power (king, president, or director of internal security ;-) just gets old. Not a crime, but the errors of the elderly who hang on too long should not afflict the young or nations. Dissent is the font of most progress in both science and military affairs.

So wise policemen and intelligence professionals cherish dissent so long as that stays within the prudent boundaries of nonviolence and patient enough to show what must be done to fix things.

It should be acknowledged from the start that "civil disobedience" only works if the government involved has already advanced beyond medieval forms. Genghis Khan slaughtered his dissenters like many tyrants before and since, and thus ruled a vast empire. Until it also fell as all tyrannies do. Tyrannies do not have long terms, because they eat their best and brightest until the children turn on them. Therefore I call your attention to a contemporary case in another attempt to show why enlightened police embrace dissent that primitive or corrupt police repress. North and South Korea were one country just 64 years ago. One went the way of police-states; the other tried to join the modern world. Today the economy of South Korea is about 40 times larger than impoverished North Korea, which imprisons its best, brightest, most creative and free-thinking citizens. So even their police are impoverished, financially but also spiritually, and in basic ways like freedom to travel, to speak, and even to think about the true condition and challenges of their country.

Romania, and most of all Romanian intelligence professionals, should never forget the Securitate and the brutal poverty for everyone that follows when the men and women who should be guardians of their communities become mere thugs for hated dictators. Look toward Ukraine for a more recent example, and look toward Turkey for a nation moving backward now.

A Religious Dimension to this Situation

There is a fifth reason why professional intelligence officers and organizations should move in the direction of Community

Policing. You have a soul, we have a destiny, and you do not want to tarnish either by primitive practices used in dark ages of the past. A wise Romanian General told me that 95% of Romanians belong openly or in their hearts to the Romanian Orthodox Church. So you should understand basic Christian principles. Be that as it may, I write to you now as a microscopic servant of the Creator of us all that transcends all churches and religions.

You have a soul, which can be corroded by the lies and abuse of innocents that comes from corrupt practices. Police must be confident in their work, but hubris is corrosive to all things. Excessive pride (hubris) is often coupled with contempt for others, and contempt for the citizens who ultimately hire and support the police. Such hubris is the beginning of the end of honor for police who wish to meet their maker with a tranquil heart.

We have a destiny, as individuals and as professionals to protect our peoples and civilization. Humankind has a destiny as well, and it is time for humankind to grow up. Endless wars of each against all, or among religions arguing about whose wisdom is the best (none) are a primitive condition that cannot long endure once weapons of mass destruction have been discovered and created. It is the sacred duty of intelligence professionals to recognize such things before the rest, to advise their policy leaders appropriately, and to stimulate change as necessary at the same time we guard the perimeter against dangers known and not.

References

[1] "Policing by Consent," Peel's Principles provided by the Home Office of the UK Government. https://www.gov.uk/government/publications/policing-by-consent.
[2] Barna, Christian. "Re-shaping Intelligence for the Prevention and Countering of Terrorism After 9/11: A Cultural Approach to the 'Need to Share' Paradigm," in Proceedings of the 18th Annual International Conference on Intelligence in the Knowledge Society, *Mihai Viteazul* National Intelligence Academy, Bucharest, Romania, 2013, pp. 181-194.
[3] Andregg, Michael. "All Source Intelligence Tradecraft: A Multidisciplinary Perspective," presented at the 19th International Conference on Intelligence in the Knowledge Society, *Mihai Viteazul* National Intelligence Academy, Bucharest, Romania, 2013, pp. 161-172.
[4] Andregg, Michael. "The Birth of Professional Ethos: Some Comparisons Among Medicine, Law and Intelligence Communities," in the American Intelligence Journal, Vol. 28, No. 1, published by the US National Military Intelligence Association, 2010.
[5] Nitu, Ionel and Anuta Costinel. "Romania in 2030: Future Trends Impacting the Romanian Intelligence Service, in Proceedings of the 18th Annual International Conference on Intelligence in the Knowledge Society, *Mihai Viteazul* National Intelligence Academy, Bucharest, Romania, 2013, pp. 287-302.
[6] Posastiuc, Cristina (General). "Strategic Analysis: Facing the New Challenges" in Proceedings of the 18th Annual International Conference on Intelligence in the Knowledge Society, *Mihai Viteazul* National Intelligence Academy, Bucharest, Romania, 2013, pp. 75-86.
[7] Ivan, Cristina. "Resilience – the X Factor of Organizational Endurance. A Practical Model for Intelligence Services," in Proceedings of the 18th Annual International Conference on Intelligence in the Knowledge Society, *Mihai Viteazul* National Intelligence Academy, Bucharest, Romania, 2013, pp. 161-172.
[8] Andregg, Michael. "Why the Intelligence Community (IC) System Drives you Crazy, and How to Come in from the Cold," in Proceedings of the 12th annual conference on Intelligence Reform sponsored by Open Source Solutions, Washington D.C., April 12, 2004. 22 pages text. http://www.phibetaiota.net/2004/12/2004-andregg-us-why-the-intelligence-community-ic-system-drives-you-crazy-and-how-to-come-in-from-the-cold/
[9] Diaconu, Florian. "Some Major Challenges Academic Intelligence and Intelligence Education and Training are Confronted With," in Proceedings of the 18th Annual International Conference on Intelligence in the Knowledge Society, *Mihai Viteazul* National Intelligence Academy, Bucharest, Romania, 2013, pp. 23-38.
[10] Maior, George Christian, and Sergei Konoplyov, editors. Strategic Knowledge in the Wider Black Sea Area. Bucharest, Romania: Editura RAO, 2011.

[11] Pepper, William. Orders to Kill: The Truth Behind the Murder of Martin Luther King, New York, NY: Carroll & Graf Publishers, September 1995.
[12] Arrow, Ruaridh. "How to Start a Revolution" an 85 minute video documentary on the Otpor! Movement in Serbia, with commentary from Gene Sharp and Col. Robert "Bob" Helvey, produced in Scotland, 18 September, 2011, distributed by TVF International.

ANCIENT GREECE AND ALEXANDER THE GREAT HUMINT NETWORKS: HOW INTELLIGENCE ANALYSTS CAN USE OPEN SOURCES INTELLIGENCE (OSINT) AS A SUPPLEMENTARY TOOL TO INTELLIGENCE REPORTS

John M. NOMIKOS[*]

Abstract

The article focuses on Macedonian Alexander the Great Intelligence Policy during his military operations in the Greek Cities and abroad (Mesopotamia, Persia, India and Afghanistan), how Alexander the Great collected Human Intelligence (HUMINT) and Open Sources Intelligence (OSINT) and what today's intelligence analysts can learn from his Intelligence Methodology.

Keywords: Alexander the Great, HUMINT, OSINT, Fusion Centers, Intelligence Analysis

Human beings have always needed information to secure their livelihood and their safety- the locations of the best fishing stream, the site where firewood might be gathered, when deer herds were likely to appear. In the classical Greece, covert action and clandestine operations were among the most common and yet most vilified methods of statecraft. All states used (Athens and Sparta), but no state wants to admit the fact, and if the operations became public, the world severely disapproved. Greeks used local citizens who served as "proxenos."[1]

The "Proxenos" had to be a citizen of the state in which he served, not of the state he represented. These men ("proxenos") became the equivalent of modern spies or agents as a conduit for

[*] Prof John M Nomikos is Director of the Research Institute for European and American Studies (RIEAS) based in Athens, Greece. He is the Founding Editor of the Journal of Mediterranean and Balkan Intelligence (JMBI).

Open Sources Intelligence (OSINT) and covert activities in the course of normal duties during the Peloponnesian Wars[2].

Furthermore, the historical record suggests that very few societies (especially not Empires) could pass up the opportunity of using Open Sources Intelligence (OSINT) when overt military operations were either impractical or impossible. Nowhere is this clearer than in the case of the ancient Romans[3].

In this sense, the campaigns of Alexander the Great represent for us an opportunity to study and understand how successful the collection of Open Sources Intelligence (OSINT) was during his campaign to Asia (Persia, India, and Afghanistan). And yet, despite this commonality of strategic experience, Alexander's the Great campaigns do seem completely removed from strategy in the modern world. They were based on Human Intelligence (HUMINT) and Open Sources Intelligence (OSINT). Comparing nowadays with the current "information age", we can say that we are constantly bombarded by facts, opinions, speculations, rumours and gossip from every direction. Computers draw us into interactive milieu where e-mails give and expects in return (via satellites), even more rapid exchanges of information in all parts of the world[4]. Today, foreign policy decisions are preceded in most cases by the gathering and interpretations of information by government officials about the costs and benefits that may accrue to their nation from various options. A question that must be asked is: Did Alexander the Great have access to Signal Intelligence (SIGINT) such as satellites, cell phones, email accounts or any other modern technology for his strategy in Asia? The answer is no!

But how Alexander the Great collected and transfer HUMINT to his Generals in order to prepare the tactics and strategy towards modern Iraq (the site of Gaugamela) and Afghanistan (the area of Bactria and Sogdiana)?[5] Much may have change since Alexander the Great led his army through the Persian Empire, but *was has remained a constant feature of man's experience*[6].

Alexander the Great Methods of Transferring HUMINT and OSINT

Alexander the Great was born in July 20th, 356 B.C. in Pella, which was the administrative capital of Madeconia. Alexander the

Great was the son of Philip II and Olympias (one of Philip's seven wives). Alexander the Great was brought up with the belief that he was of divine birth.

In 343 B.C., Alexander the Great father's, Philip II, summoned the Greek Philosopher Aristotle from the Greek island Lesbos to tutor Alexander the Great. For three years, Aristotle instructed Alexander the Great in philosophy, government, military strategy and sciences. Aristotle prepared a shortened edition of the Iliad (collection of epic poetry in history) in which Alexander the Great always kept with him. Aristotle believed in despotic control of Greek enemies, but Alexander the Great believed that the Macedonians should free the barbarians from despotism and offer them Greek protection and care.

Alexander the Great used the following collection methods such as the "Runners", "Loudspeakers" and the "Beacons" to transfer HUMINT information through his military campaigns from the Greek Cities to Afghanista[7]. Nowadays, the "Runners" could be Human Intelligence (HUMINT) and OSINT officers, the "Loudspeakers" could be Signal Intelligence (SIGINT) and the "Beacons" could be Imagery Intelligence (IMINT).

1) "Runners"

Alexander the Great Macedonian Army exchanged fast information without problems during war period. They had trained "runners" to cross 700 km in about an hour in order to transfer HUMINT to their Macedonians Intelligence Officers in the war fields[8].

The most famous "runner" who stayed in history was Pheidippides, who went from Athens to Marathon and back to Athens the message of victory without any stops and died of exhaustion. In the walk long distances, the "runners" had to use horses in order to transfer HUMINT and created stations in order to pass the HUMINT to other "runners" and changed horses[9].

2) "Loudspeakers"

Alexander the Great was the first who conceived the idea that "playback sounds" through the headset telegraph could carry the sounds through the air to remote distances.[10]

3) "The Beacons "

The fire (and the light) was a basic condition to transport the message in short and long distances. Without having access to cell phones or satellites, the use of traffic Imagery Intelligence (IMINT) was mainly used in war to carry the orders of their superior officers.[11]

"OSINT Fusion Centers" in Greek Cities and Abroad

In Alexander the Great era, an Open Sources Intelligence (OSINT) Fusion Centre was defined as a collaborative effort that provides resources, expertise and information with the goal of maximizing the ability to organize his military operations. At the same time, OSINT Fusion Centres have broken ground in their ability to share information from state to state (from Greek Cities and abroad to Alexander the Great headquarter in Pella, Northern Macedonia in Greece) in order to inform military decision making at both the tactical and strategic levels.

Alexander the Great built up "Open Sources Intelligence (OSINT) Fusion Centres" by assigning his intelligence officers to stay in Greek Cities, as well as in foreign states for a long time and learn the languages, customs, study of religion and society as well as marry local women and work as tradesmen. His OSINT officers always had a policy which took into account a range of factors such as politics, economic, social, human security, agriculture and water supplies, as well as administrative information and sources for the region which Alexander the Great wanted to fight and conquer from the Greek Cities all the way to India and Afghanistan.

It is important to be announced that the "OSINT Fusion Centres" consisted on a small number of officers in order to avoid possible leaks among them. The officers submitted reports to Alexander the Great military headquarter in Pella, northern part of Macedonia in Greece. The OSINT reports provided Alexander the Great the necessary information in order to plan his military strategy and tactics for his operations in the Greek Cities and abroad.

It is noted that Alexander the Great was a skilled tactician, but his operations were built upon straightforward, rapid offensive and manoeuvers that overwhelmed the decision-making and will of the enemy.

Concluding Remarks

In the complex world we live today, collective action among the military and intelligence services depended on shared intelligence and common assessment in order to prevent prospective conflicts. Human Intelligence (HUMINT) and Open Sources Intelligence (OSINT) play a strategic role on the efficiency and performance on the intelligence services. With an estimated 80% of required information available for use in an open source for specific information vital for a deep analysis in academic journals, conference proceedings, television transcripts and blogs, Open Sources Intelligence (OSINT) is a necessary tool for analysis in the intelligence services.

In the twenty-first century, surprises and security challenges will require creative and agile information methods; sharing knowledge about specific threats and establishing productive local-to municipality and government interactions about responses that will make the state safe.

Alexander the Great has realized the significance of HUMINT and OSINT for collecting information and sharing intelligence with his generals before planning his military operations in Greek Cities and abroad.

It has frequently been recognized that the information collection and the use of accurate intelligence was of fundamental significance for the success of Alexander the Great military campaigns. No intelligence or tactical decisions can be made by any military commander without advance knowledge of an enemy's location, strength and weakness, as well as his capabilities and the geography of the projected military operation.

It is hoped that Alexander the Great intelligence system has shed some light on the role of intelligence for his strategic and tactical planning. Although failures did occur, few commanders in any era seem to have made better use of military intelligence for making effective strategic and tactical decisions[12]. It appears that Alexander the Great exercised direct supervision over many military intelligence operations himself and seldom if ever delegated this important authority to anyone. Alexander the Great would never commit the safety and well-being of his troops on any military operations without careful preparation. This preparation in turn was based on planning, and the planning on accurate intelligence, although these aspects of the campaigns are generally ignored by the sources[13].

In conclusion, one of the best lessons that intelligence analysts[14] can draw out by studying the intelligence methodology of Alexander the Great is that ***human brain*** is the chief of any analysis in civilian and military intelligence and modern technology (satellites, cell phones, television, and social media) provides only supplementary tool to make analyses productive to the decision-makers and in no way replacing human brain!

References

[1] Gerolymatos, Andre, "Espionage and Treason: A Study of the "Proxenia" in Political and Military Intelligence Gathering in Ancient Greece", (Amsterdam, J.C. Gieben, The Netherlands, 1986).

[2] The Greek historian Thucydides documented the war between Sparta and Athens, which lasted for 27 years between 431 and 404 BC. The war was the largest the Greek world had known of up to this date, and 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", Intelligence and Counterintelligence, Vol. 10, No.3, Fall 1997, pp: 299-300.

[4] Loch K. Johnson, "The Secret Agencies", (Yale University, USA, 1996).

[5] David J. Lonsdale, "Alexander the Great: Lessons in Strategy", (Routledge Publishing Company, Abington, Oxon, UK, 2007), pp: 1-3.

[6] Ibidem.

[7] Christos Lazos, "Τηλεπικοινωνίες στην Αρχαία Ελλάδα" (Telecommunications in Ancient Greece), (Aiolos Publishing Company, Athens, Greece, 1997), pp: 1-179.

[8] Ibidem.

[9] Ibidem.

[10] Ibidem.

[11] Ibidem.

[12] Donald Engels, "Alexander's Intelligence System", The Classical Quarterly, Vol. 30, No. 2, 1980, pp: 327-340.

[13] Ibidem.

[14] Maurice R. Greenberg and Richard Haass, "Making Intelligence Smarter: The Future of U.S. Intelligence", Report of an Independent Task Force, (Council of Foreign Relations, USA, 1996), pp: 1-39.

SECURITY TODAY: NEW DRIVERS, CHALLENGES, AND OPPORTUNITIES

The fast paced development of the human society has made intelligence and security organizations face a whole new set of emerging threats. Therefore, the need to re-conceptualize "the old security paradigm" has become a permanent issue on the international agenda, specific focus being laid on how to efficiently integrate the different dimensions of security at national, regional and international level. The aim of this chapter is to capitalize on both academic and practitioners' expertise in order to envision a shared understanding of existing and potential future threats. This endeavour has become a must if we are to coherently approach the constantly changing security environment. New drivers of change in the social, legal, technological, economic and political fields open up the practice of security organisations towards new skills and instruments which need to be shared and build into a common body of knowledge across disciplines.

CRISIS INDICATORS. PRACTICAL CONSIDERATION

Iuliana UDROIU[*]

Abstract

Building new theories in the field of crisis prevention and management is not an easy nor every time feasible task. Regular failures prove that science is needed to explain why crises form and burst. Yet, since fails to anticipate such incidents. Choosing relevant indicators for preventing national security crisis is a tenuous activity that must work with scientific principles and a solid methodology. The future belongs to those who creatively and foreseeably succeed in identifying the perfect combination between various crisis indicators in order to signal relevant changes in the security environment, timely enough to allow decision makers to adopt necessary measures.

Keywords: crisis, security, indicators, decision

Understanding crisis from an intelligence point of view

Coping with security crises has never been an easy task for decision makers nor security managers and practitioners – no matter where they come from: intelligence, military, law enforcement, state authorities and so on. Because we live in turbulent times, we perceive the security environment as the most unpredictable as ever. In fact, it has always been unpredictable, as a result of progress in human development, technology, warfare etc. The challenges we face now were made all the more difficult by a multitude of changes in the political, administrative, economic, social and, last but not least, media landscape.

[*] PhD, Institutul de Economie Mondială.

From some intelligence structures point of view, such as US Intelligence Community, the indicator & warning perspective may prove useful in reducing some of the unpredictability of the security environment and overcoming the challenges raised by the discrepancy between the theoretical perspective over crisis prevention processes and actual pattern of crisis development.

From, the early effort of Defence Advanced Research Projects Agency/DARPA, such as *Indications and Warning Analysis Management Syst*em/ IWAMS (Clarkson, Krasno, Kidd, 1980), or intelligence practitioners and scholars, such as Cynthia Grabo (2002), to European funded projects such as G-MOSAIC[1] and national confidential programs, the very objective is to assist stakeholders in crisis areas and deliver timely and reliable information about crisis potential and crisis development.

In the intelligence world, for many crises are curses, for some – opportunities. Many times it is associated with failure of protecting national security and has huge effects over the citizens or state assets - the case of terrorist attacks. It implies lots of resources both to prevent and manage them. In different circumstances, crisis may be drivers for changes in current status and bring lots of gain in terms of international profiling and strategic status – as these cases are sensitive, they remain under the veil of national secrecy laws for any state.

Tens of definitions exist in the dedicated literature of crisis and crisis management, coming from social, military, and political field, juggling around the concepts of unbalance, disruption, discontinuity, anomaly, tension etc. They all make sense and are valid in specific contexts. As a working definition, from the intelligence perspective, crisis is a negative change in security environment that may affect national interests or obstruct decision makers from taking necessary measures to maintain internal stability.

In an article signed in 2014, Henry Kissinger stated that the very concept of order that has underpinned the modern era is in crisis. The fact is that world is permanently going through a systemic crisis. Deindustrialization crisis, migration crisis, global governance crisis, and aging crisis – local or national crisis have regional or global effects, not only as a result of globalization. The War on Iraq, for example, raised the price of oil, the Gaza blockade has stirred international reactions (the role of religion and ethnicity can be discussed here).

Most of the crises focus on social and economic/ financial issues in general, while a crises caused by military issues is just an exception: Ebola pandemics seem to raise more fear than the Ukrainian conflict in 2014. Also, the global crisis in 2008 gave rise to more drama than the Russian-Georgian war. But the crisis in Ukraine may be more important that a pandemics for a state that shares a border with Ukraine even if that there are more victims at global level as a result of Ebola.

A lot of money is invested in finding the right solutions to prevent and mitigate crisis. The EU, for example, is financing numerous projects dedicated to specific challenges through Horizon 2020, ASR, FP7 SEC projects etc. These projects are dedicated to cope with challenges such as public awareness and resilience, response, strategic planning, innovation and technical support, situational awareness, cooperation and communication, managing resources, operational support or recovery logistics[2].

Crisis happens even when it has been predicted long ago

Finances, environment, resources, cyberspace – experts from academia, research institutes or dedicated organizations keep on proving that things are going into, the wrong direction but crises still burst, even when measures are taken preventively.

For example, the global crisis followed a pattern experienced not so long ago in Asia (1997) and Latin America (2001). The economic crises that started in 2008 was predicted by American economists Nouriel Roubini, Paul Volker, George Soros, Warren Buffett or Alan Greenspan, but the USA was the very source of the turbulences that still haunt the world. Actually, the American authorities preferred to use the world *turbulence*, coined by Alan Greenspan 20 years ago, instead of crisis, thinking that the last is *too strong* (Vasilescu, 2011, p. 16). Adrian Vasilescu explains why global economic crisis was an event that could have been prevented, but was not: it would have ruined the concept of “American dream” (feeling which actually was felt once the crisis burst) and because of people’s investment in the future (Vasilescu, 2011, p. 46). Also in Romania, he says, the National Bank issued a warning, in 2003, regarding the speed of the spending rate and the large volume of real estate loans, based on the discrepancy between the large consumption and limited internal offer of commodities and services. (Vasilescu, 2011, p. 46).

As for the Ukrainian crisis, Vladimir Putin in person warned about the consequences of any involvement in Kiev’s internal affairs and attempting to run Russia out from its Eastern European space of manoeuver. In a meeting with media representatives on March 4, 2014, Vladimir Putin stated that ‘if we see such uncontrolled crime spreading to the eastern regions of the country, and if the people ask us for help, while we already have the official request from the legitimate President, we retain the right to use all available means to protect those people. We believe this would be absolutely legitimate. (…) Moreover, here is what I would like to say: we have always considered Ukraine not only a neighbour, but also a brotherly neighbouring republic, and will continue to do so’[3].

Russian determination in regaining control over Ukraine may be a relevant milestone in international relations and the inflexion point for a new perspective in crisis management theory, as the military aspects become more relevant in the European area after decades of ‘soft’ crises management. But preaching that the world is more unpredictable than ever in its history may be too bold, as for history is full of crisis, mainly military ones. The same situation may be considered regarding environmental disasters, social or political internal disruptions or pandemics outbreaks. Moreover, we cannot imagine Middle East in a stable security context as it has never been the case.

Truth is that insecurity sources are nowadays more diverse and more complex, constantly and rapidly changing, but so are the mechanisms used to anticipate or mitigate them. In fact, the security environment should be more predictable than ever, due to increased access to communication technologies and instant acknowledge of real time information using UAVs, satellites etc.

Indicators &Warning. Old concepts in new contexts

From a theoretical perspective, indications and warning (I&W) is a generic term usually associated with intelligence activities needed to detect and report time-sensitive knowledge on foreign events that could threaten a country's allies, its citizens abroad, or the country's military, economic, or political interests. Also, indications and warning intelligence refers to information that alerts or warns of an impending course of action by a foreign power that is detrimental to the interests of a country. This information is the product of recognition and correlation of threat indications and the synthesis of a threat posture. As a result, an indications and warning system is considered to be a network of intelligence production facilities with analytical resources capable of contributing to or developing indications and warning intelligence, and disseminating this product within their own command and to other facilities, organizations, or commands (Goldman, 2011).

Indications are generally perishable and demand a high clock speed in order to get ahead of the adversary's planning[4]. Warning is also a time-related process, which requires that informed decision makers take opportune measures in order to avoid a possible damaging situation on national security.

In US military doctrine, Indications and warnings (I&W) is mentioned as one of the 6 intelligence categories, along with Current Intelligence, General Military Intelligence, Target Intelligence, Scientific and Technical Intelligence, and Counterintelligence[5].

Intensive research was made by the US military and intelligence communities in order to identify a system of I&W that can help decision makers to better understand the changes in security environment, not only the sudden ones, but also those signalled long time ago, such as the degradation of the physical environment and the link between the natural disasters and local or regional conflicts, the damaging effects on national security of constant degradation in social living conditions of ethnic marginalized communities. Warning and alerting systems were created for sensitive matters, all practitioners stating that there must be a strong political commitment in order to ensure the success of these initiatives.

After the Arab Spring, the US Intelligence Community tried to emphasise on strategic warning and intimately connected it with Indications and warning process that includes forewarning of enemy actions or intentions, imminent hostilities, insurgencies, attacks on the United States or its forces or allies, hostile reactions to U.S. reconnaissance activities, terrorist attacks and other events.

According to Defence Intelligence Agency (DIA) Deputy Director David R. Shedd, improvement in strategic warning involves standardizing the I&W process into a template that will make it easier to see shifts in trends toward what could be strategic warning issues or significant shifts in existing hotspots. The indications and warning piece is something that will be monitored at a point that the combatant commands, the J2 [Joint Staff Intelligence Directorate] and DIA are all looking at a similar set of indicators, as opposed to each sort of interpreting their own version. With such a template in use among combatant commands, the J2 structure and DIA will better serve DIA customers. DIA's Strategic Plan for 2012-2017 contains four drivers: to prevent strategic surprise and provide a way to manage an emerging crisis; to deepen DIA partnerships with allies and friends in a region or in a country; to optimize DIA performance in defending the nation, and to strengthen DIA core capabilities in intelligence collection and analysis[6].

From a newer perspective, intelligence requires also cyberspace Indications and Warning (I&W) technologies that address the challenge of cyber-attacks, as the security domains are increasingly dependent on cyberspace operations. This way, intelligence agencies seeks to enhance their ability to predict and warn - within operationally relevant timelines - against adversary activity in cyberspace in order to facilitate a proactive network defensive posture and provide for cyberspace resiliency during operations.

This kind of developments requires more research and innovation, in-house and from outsources activity, always keeping in mind the principles of functionality, responsibility to protect, and systemic approach. It implies the newest IT&C technologies and a smart use of human potential.

Intell can't predict an unexpected crisis, but they can warn about it

In this regard, maybe the old fashioned model of indicators & warning used during the Cold War should be reconsidered and updated, should be put in an innovative technological framework and used by the intelligence analysts as a main tool in evaluating and anticipating the trends that may affect the future of the national security. In fact, indicators are essential in early detection of possible crisis, managing them once they burst and check how the situation returns to normality after the crises ends.

They are important in establishing the origin, patterns and trends of crisis. Based on these variables, intelligence is expected to identify, describe, and quantify key vulnerabilities, risks and threats that can result in crisis situations or cause difficulty in addressing security issues.

Using indicator clusters, intelligence analysts can spot trends and patterns, frequency and probability of crisis. Indicators are therefore useful in every stage of a crisis: before a crisis, for planning and preparedness in high-risk areas, during a crisis, for rapid mapping in support of rescue and relief operations, and after a crisis, for post-event damage assessment and reconstruction activities.

Building indicators is a tailored process, as every crisis has its own development and finding the right "recipe" of quantifiable, measurable and replicable indicator systems can make the difference between failure and success in managing national security issues that can develop into severe crisis.

A distinction should be made between warning and predictive indicators. In the latter case, successful foresight based on indicators in only possible, however, if the problem is clearly defined. Subsequently, the threat must be recognized or, at least, recognizable, in the sense that is at least partially known. In fact, to my knowledge, no one can predict something that does not exist, but obvious events or phenomena, based on signs or indicators. This way, we can distinguish between those who really sense the imminence of a crisis and its course and those who just put apparent things into an innovative perspective or analysis grid that argues their point of view.

Existing solutions to avoid or manage a crisis

The new security environment, both volatile and competitive, requires the development of effective and efficient I&W systems fitted to separate signals from the noise. I&W requires a methodology to the strategic and operational levels, analysts applying actively and regularly proper methodologies.

The analyst's toolkit contains quantitative methodologies, such as sentiment analysis in order to analyse the media's tone on specific topics, monitor the posture of the media affiliated with the main actors involved in a controversy or policy that has an impact on national security. One cannot precisely foresee the details of a crisis, but get an advanced warning that the posture of the actor has changed. The change in posture may signal that there is an increased likelihood of possible conflict.

From a qualitative perspective, analysts use radar scanning-type of analysis, strategic, operational, tactical, and trying to bring the main facts and an analysis of each threat and an evaluation of their development in the future, using intelligence gathered through all the sources of the service. Mixed or complex methodologies, such as relevance trees, Scenarios, STEEP, War Gaming.

According to Randolph H. Pherson, three techniques are particularly useful in helping analysts anticipate low probability events, avoid surprise and enhance a better warning analysis: High Impact/Low Probability Analysis, What If? Analysis, and the PreMortem Assessment. The use of these techniques will ensure greater rigor in the analysis and reduce the chances of surprise. Also, The Indicators Validator was developed by Pherson Associates in 2008 to assess the diagnostic power of indicators. Once an analyst has developed a set of alternative scenarios or future worlds, the next step is to generate indicators for each scenario (or world) that would appear if that particular world were beginning to emerge. A critical question that is not often asked is whether a given indicator would appear only in the scenario to which it is assigned or in one or more alternative scenarios as well. Indicators that could appear in several scenarios are not considered diagnostic, suggesting that they are not particularly useful in determining whether a specific scenario is emerging. The ideal indicator is highly consistent for the world it is assigned and highly inconsistent for all other worlds (Pherson, 2013).

A possible roadmap

Based on these theoretical prerequisite, I propose a few solutions that may be easily put together by intelligence in order to prevent if not most of the crises, perhaps the most important ones:

1. Plan for crisis! That means to improve organization and organizational support, allocate enough resources for operational planning, ensure analysts' standard toolkit and tradecraft, acquire& build specialized expertise.
2. Educate customers and stakeholders! Make them understand how intelligence works, what it can deliver and what it’s impossible to do.
3. Improve research form in-house expertise and outsourcing! That means to find the equilibrium between what you can do and what you can find off-the-self – there is so much knowledge in the academia, private research institutes, national and international organizations that can be considered. Don’t waste quality time to do what others can do better.
4. Learn from innovators! - Never stop from searching new methods for finding anomalies that elude baseline scenarios – if they don’t exist, adapt and invent them. Innovators are all around us and not just limited to an elite few.
5. Find and test patterns! Gathering data is not enough, we must drag them from the chaotic universe of information, pet it, grow it and finally transform it into knowledge.

6. Play! Perform crisis exercises using comparative and competitive stories with clear indicators showing when the scenario fails or succeeds.

Conclusion

Even the most performing intelligence may find it almost impossible to successfully perform all these activities and expect to solve any potential or current crisis. After all, a black swan remains just a black swan until we see it.

But even that I&W analysis is not an exact science and predictions can never be issued by analysts without some uncertainty, it is a part of crisis prevention and management, doing what it always does, but in a quicker manner and with more responsibility than ever, as I&W is developed mainly out of intelligence and defence, and with international and national security issues in mind.

Acknowledgements: This paper has been financially supported within the project entitled "Horizon 2020 - Doctoral and Postdoctoral Studies: Promoting the National Interest through Excellence, Competitiveness and Responsibility in the Field of Romanian Fundamental and Applied Scientific Research", contract number POSDRU/159/1.5/S/140106. This project is co-financed by European Social Fund through Sectoral Operational Programme for Human Resources Development 2007-2013. Investing in people!

References

1. Centre for Strategy & Evaluation Services (2011). *Ex-post Evaluation of PASR Activities in the field of Security Interim Evaluation of FP7 Research Activities in the field of Space and Security Crisis Management – Case Study*, http://ec.europa.eu/enterprise/policies/security/files/doc/crisis_management_case_study_cses_en.pdf [30.05.2015].
2. Centre for Strategy & Evaluation Services (2011). *Ex-post Evaluation of the Preparatory Action on Security Research (PASR) Interim Evaluation of FP7 Security Research Final report (Appendices),* http://ec.europa.eu/enterprise/policies/security/files/doc/interim_evaluation_of_fp7_security_ex_post_pasr_appendices_en.pdf [30.05.2015].
3. Clarkson, Albert, Krasno, Laurence, Kidd, Jerry (1980). *Indications and Warn1ing Analysis Management System (IWAMS) Final Report*, Sunnyvale, SUA, A Project Sponsored by Cybernetics Technology Office, Defence Advanced Research Projects Agency.
4. Goldberg, Joe. *How Early Warning and Response Intelligence Applies to Crisis Management*, http://www.slideshare.net/IntelCollab/how-early-warning-and-response-intelligence-applies-to-crisis-management [30.05.2015].
5. Goldman, Jan (2011). *Words of Intelligence: An Intelligence Professional's Lexicon for Domestic and Foreign Th*reats, Plymouth, Great Britain, Scarecrow Press.
6. Grabo, Cynthia M. (2002). *Anticipating Surprise. Analysis for Strategic Warning*, Washington, DC, Joint Military Intelligence College, Centre for Strategic Intelligence Research.
7. **** How the Army Runs: A Senior Leader Reference Handbook, 2005-2006*, Last updated 17 November 2005, http://www.globalsecurity.org/military/library/report/2005/htar2005ch18.pdf, p. 403 [30.05.2015].
8. Morris, CharlesRr. (2009). *Criza economică şi profeţii ei,* Bucureşti, Litera.
9. Pherson, Randolph H. (2013). *The Tradecraft of Warning: Overcoming Cognitive Barriers*, http://www.pherson.org/wp-content/uploads/2013/11/02.-The-Tradecraft-of-Warning-Paper_FINAL.pdf [30.05.2015].
10. Vasilescu, Adrian (2011). *Biletul de ieşire din criză*, Bucureşti, Curtea Veche.
11. **** Vladimir Putin answered journalists' questions on the situation in Ukraine*, March 4, 2014, Novo-Ogaryovo, Moscow Region, http://en.kremlin.ru/events/president/news/20366 [30.05.2015].
12. http://www.defense.gov/news/newsarticle.aspx?id=117160[30.05.2015].
13. http://www.gmes-gmosaic.eu[30.05.2015].
14. http://spaces.icgpartners.com/index2.asp?NGuid=9CF25C12FC6E49BD9FAA7768BD2ACD81[30.05.2015].

[1] http://www.gmes-gmosaic.eu[30.05.2015].

[2] Center for Strategy&Evaluation Services (2011). *Ex-post Evaluation of PASR Activities in the field of Security Interim Evaluation of FP7 Research Activities in the field of Space and Security Crisis Management – Case Study*, http://ec.europa.eu/enterprise/policies/security/files/doc/crisis_management_case_study_cses_en.pdf[30.05.2015]; Center for Strategy&Evaluation Services (2011). *Ex-post Evaluation of the Preparatory Action on Security Research (PASR) Interim Evaluation of FP7 Security Research Final report (Appendices),* http://ec.europa.eu/enterprise/policies/security/files/doc/interim_evaluation_of_fp7_security_ex_post_pasr_appendices_en.pdf [30.05.2015].

[3] *Vladimir Putin answered journalists' questions on the situation in Ukraine*, March 4, 2014, Novo-Ogaryovo, Moscow Region, http://en.kremlin.ru/events/president/news/20366 [30.05.2015].

[4] http://spaces.icgpartners.com/index2.asp?NGuid=9CF25C12FC6E49BD9FAA7768BD2ACD81[30.05.2015].

[5] ****How the Army Runs: A Senior Leader Reference Handbook, 2005-2006*, Last updated 17 November 2005, http://www.globalsecurity.org/military/library/report/2005/htar2005ch18.pdf, p. 403 [30.05.2015].

[6] http://www.defense.gov/news/newsarticle.aspx?id=117160[30.05.2015].

FOOD SECURITY COMPONENT OF THE NATIONAL SECURITY – PROSPECTS AND CHALLENGES IN THE NEXT DECADE

Bogdan BAZGĂ[*]

Abstract

This article presents a series of interesting aspects regarding food security as a component of national security, factors that influence the national and global food security. All these elements put together will analyse the next possible steps for global food security creating possible scenarios of food security prospects and challenges in the next decade. A source of legitimacy of a country is in practice its own ability to provide security, especially to protect and maintain the rights of its citizens and to ensure a secure life, satisfying their needs, ensuring a prosperous and favourable environment. Today, there are a series of rising risk phenomena near Romania and we notice that, a series of global problems affect more and more our security and obviously our food security. Thus, it is highly important to approach food security as a phenomenon that may generate social convulsions.

According to many experts, food security for a nation is the most important field within the national security. A country has food security only when it has enough available food and agricultural products to provide nutrition for all its inhabitants, while ensuring forage for animals and water in case of natural disasters, crises, war, etc. Food insecurity may generate internally social tensions and convulsions can physically and psychologically damage the population, may create economic and political instability, and externally may generate unwanted political, economic and diplomatic tensions that endanger the national security.

Keywords: food security, agriculture potential, price volatility, agriculture, commodities

National security, a factor of social stability. General concepts

A state`s legitimacy lies in its ability to provide security, protect and support its inhabitants` rights and ensure a prosperous

[*] The Institute of National Economy, Bucharest, Romania

environment for satisfying their needs. Today, there is a series of rising risk phenomena near Romania and we notice that a series of global problems affect more and more our security. Thus, it is highly important to approach food security as a phenomenon that may generate social convulsions. Vision of food security has its roots in the definition adopted at the World Food Summit (WFS) in November 1996 on the General Session of Food and Agriculture Organization of the United Nations (UN FAO): "*Food security exists when all people at all times have physical or economic access to sufficient safe and nutritious food to meet their dietary needs and food preferences for an active and healthy life*" (FAO, 1996).

According to many experts, food security is a country`s most important field in national security. A state has food security only when is has enough available food and agricultural products to provide nutrition for all its inhabitants, while ensuring forage for animals and water in case of natural disasters, crises, war, etc. Food insecurity may generate internally social tensions and convulsions which can physically and psychologically damage the population, may create economic and political instability, and externally may generate unwanted political, economic and diplomatic tensions that endanger national security.

In the common sense, the term of "security" (which derives from Latin "securitas(atis)" and signifies "no worry", and from a semantic view, meaning "being protected by any threat or danger") is known as the capacity of "an actor", in a power outlook, to protect the fundamental values and to enhance their impact on the international system. It is correlated with different parts of the social- so, we speak about "economic", "social", "military"," community", " public", "information" security - or about the one of the relations between different entities: international, worldwide, global, continental, regional, local, collective, national.

Traditionally, "the security" concept, which was set at the beginning of The Cold War, had been associated with the defence concept, military structures, power balances, strategies and tactics. Taking into account a range of classical definitions, this concept may indicate the situation of a country protected against the attacks or aggressions, which come from the inside or outside. Observing that, it can be understood that military defence, is just a part of what is being called “security”, a concept which is about to become as elusive as the military issues are less counted. So, it has provided elements to underlie some paradigms as: “collective security”, “multi-dimensional security’, “global security”, etc.

The consistency of the concepts “security” and “national security” are strongly related with the state`s nature. The phrase “national security” is a translation of the English concept “national security”, a counterpart of “state security”, which, obviously, raises multiple ties and bears away of its essence. The state implies, in the same time, an idea, an institution and a physical basis, but it is as well, a complex organizational structure, a collectivity and a policy tool[1].

From this perspective, the state is a device for promoting the security, before it becomes a topic or a referee of the security. It is the body which assures the mediation between the national interest, defined in a unitary way, and the interests of its communities. Therefore, in the study “The people, states and fear- an agenda for international security studies after The Cold War”, Barry Buzan’s emphasis on the one way, that when it comes to security we refer to national security of a state, and on the other way, the dynamic of the security is relational and based on the interaction between states[2]. At the same time with the establishment of nation-states, at the middle of nineteenth century, the problem of national security has been traditionally tackled in terms of “peace” and “power” concepts. Peace has become the central concept of idealists and has ruled over the foreign relations, especially in the inter-war time. The second concept, power, is the nucleus of the analysis of the second and the most important school of international relations, realism, due to the fact that “power is the main factor to create the international order”[3]. The food problem has two basic elements: “the food policy” and “the policy of nurture”. The food problem moves in two plans: one is referring to the supply and the quality of the products, and the other to consumer and its capacity of consuming.

The main guiding ideas on the importance of the food security and agriculture as the main branch of the Romanian economy to ensure vital public resources and arguments, which help us in drawing the essential elements of impact, giving the side of safety on all levels social life: idividual, national, regional and global deserved place among the other similar size, especially in light of EU integration as Romania's national interest.

These changes will have serious effects on the five dimensions of food security:

- Food availability,
- Price volatility,
- Population`s access to food availability,
- Food use,
- Stability of food.

For Romania, agriculture and its sub-branches - growing plants and animals, agri-food industry, are one of the most important resources. This intervention identifies one or more of the next goals:

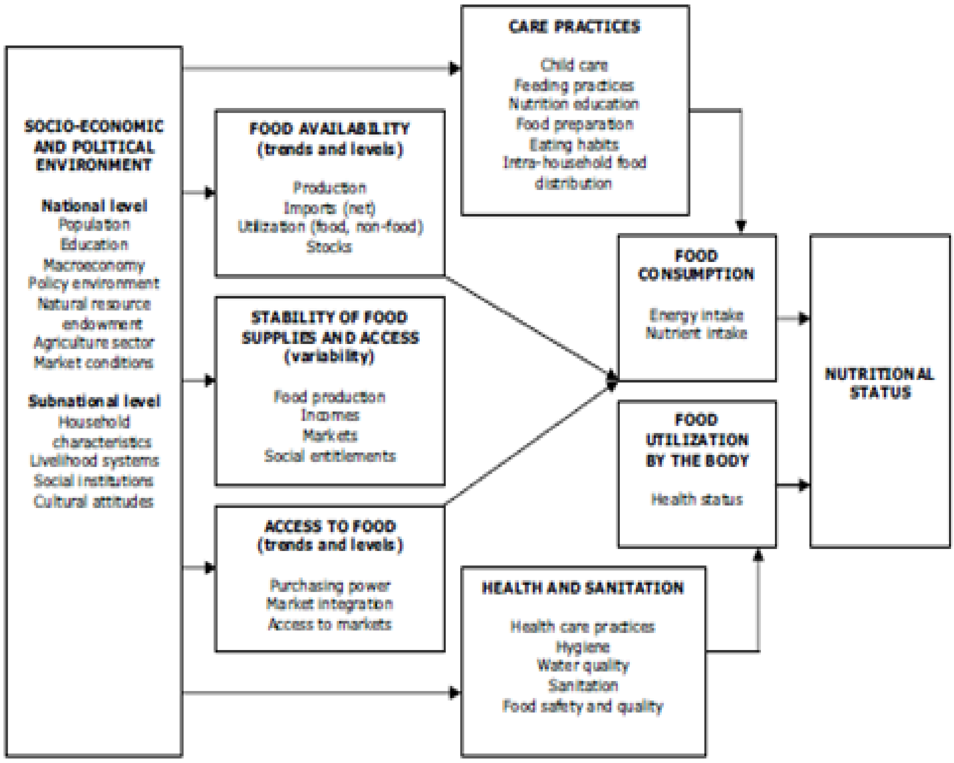
- Setting the food prices, being aware of the international price waves;
- Ensuring a certain nutritional level of the population suffering malnutrition;
- Controlling the food prices;
- Restricting the inflation pressure by controlling the food prices.

Therefore, food policies represent the ensemble of governmental measures, be it legislative, normative, administrative and financial which have foreseen targets, and aims to ensure a balance between the physiological needs for food consumption.

Regarding the statements of many specialists, food security of one country represents the most important dimension of national security. A state has food security when it has enough disposable of agrarian and food products, being able to cover the needs for food for all the inhabitants, from inside its borders and to assure at the same time the necessary stocks of feeds for the animals, and water as well in the time of the natural disasters, wars, crisis, etc. Not ensuring food security may produce inside the state convulsions and social tensions, may damage the physical and mental health of the population, may create economic and political instability, and abroad may interfere with diplomatic, economic and political pressure, having undesirable and pernicious effects for the national security.

In 2008 World Food Security of the Inter-Agency Working Group established the Food Insecurity and Vulnerability Information and Mapping System (FIVIMS) elaborated a conceptual framework that gave operational meaning to this definition (Figure 1). FAO reaffirmed this view in its first published assessment of the implications of climate change for food security, contained in its 2015 to 2030 projections for world agriculture.

Figure 1. Conceptual framework of possible causes of low food consumption and poor nutritional status



Source: FAO, 2000c.

Prospects and challenges to food security in the next decade

One of the great challenges of the next decade at the global and regional level is and will remain the “price volatility” of commodities. This is a serious problem especially for countries of the world which are dependent producers of raw materials. Agricultural commodity price volatility is and will remain as generate factor of national food insecurity. About two billion people, almost one third of the world's population are dependent on the production of primary goods such as grain, sugar, rice, meat, cotton, ferrous and nonferrous metals, copper.

Basic commodity prices are particularly volatile in the short term, sometimes they vary even more than 50% - 60% in one year. Clearly, these grimaces of the economy - lower commodity prices will lead to lower incomes for farmers and workers in rural agro-industry.

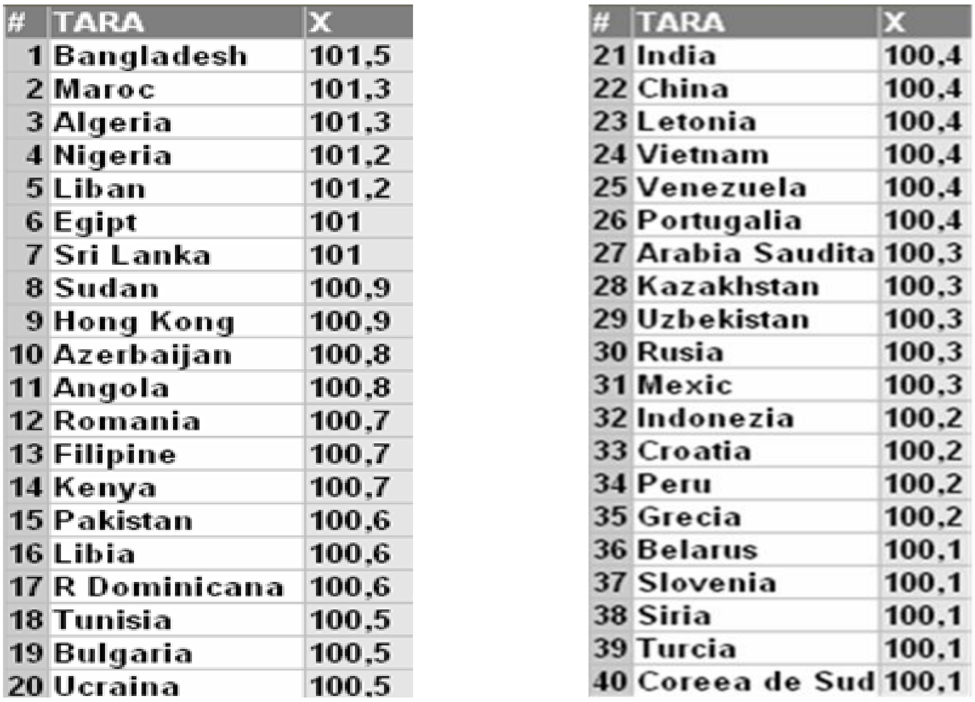
Food insecurity combined with price volatility will induce unstable prices and complicate the whole management and financial planning at local, regional and global level.

For Romania, we do not need to make predictions on the occurrence of a food crisis because, much of the population is affected by this phenomenon. Food security of the more precarious of the Romanian people is not the result of lack of food, yet, but of the decrease in purchasing power generated by at least four factors: salary adjustment, increased VAT and taxation recalculation of pensions and inflation. These factors contribute substantially to reducing consumption, both quantitatively and qualitatively.

After Romania's admission to NATO - as a member with full rights and obligations - politicians with responsibility for the national security plan argued - rightly - given the participation of our troops in several parts of the world, that our country has turned into a security provider for other countries. But it would be "excellent" to make the same assessment about food security. Unfortunately, we are in a plain opposite to that assessment, as at present, Romania is a "net importer" of food and therefore food security. The most favored countries in terms of food security are those with agricultural potential capable of supplying larger quantities of agricultural commodities and food than their national needs. These countries include Romania, which has a rich agricultural potential, which is placed 5th among EU countries, able to cover the food needs of approx. 80 million people. One can appreciate that that's how the country can be - and most of them have - of course food independence. This comparative advantage that Romania has is insufficiently exploited as, in the estimation of experts and national and international institutions in the field, ca.70% of the aggregate demand for food, existing market profile of our country, is covered from imports.

In these conditions, the current state of Romania's independence and food security is unacceptable. Remember the same plan and forecast made by Nomura Bank of Japan, which emphasizes that the problem will worsen food in Romania. According to this, our country ranks 12 in world food in the risk generated - mainly - the volatility (vulnerability) of food prices. (Table no. 1)

Table no. 1



#	TARA	X
1	Bangladesh	101,5
2	Maroc	101,3
3	Algeria	101,3
4	Nigeria	101,2
5	Liban	101,2
6	Egipt	101
7	Sri Lanka	101
8	Sudan	100,9
9	Hong Kong	100,9
10	Azerbaijan	100,8
11	Angola	100,8
12	Romania	100,7
13	Filipine	100,7
14	Kenya	100,7
15	Pakistan	100,6
16	Libia	100,6
17	R Dominicana	100,6
18	Tunisia	100,5
19	Bulgaria	100,5
20	Ucraina	100,5
21	India	100,4
22	China	100,4
23	Letonia	100,4
24	Vietnam	100,4
25	Venezuela	100,4
26	Portugalia	100,4
27	Arabia Saudita	100,3
28	Kazakhstan	100,3
29	Uzbekistan	100,3
30	Rusia	100,3
31	Mexic	100,3
32	Indonezia	100,2
33	Croatia	100,2
34	Peru	100,2
35	Grecia	100,2
36	Belarus	100,1
37	Slovenia	100,1
38	Siria	100,1
39	Turcia	100,1
40	Coreea de Sud	100,1

Source: Business Intelligence no. 5074/2011, p. 33

Price volatility measures the rate at which prices rise or fall in a certain period of time. High volatility in world prices indicates that for farmers, and especially those in Europe, it is difficult to decide on their future production because of uncertainty about future prices. Conflict crises in various regions of the globe directly affect the food security of vulnerable populations whose access to food are reduced by high prices and cannot afford to buy in bulk when prices are low.

Dynamics of prices for agricultural commodities in the charts below is more worrisome, the food production and food in the near future. The FAO Food Price Index is a measure of the monthly change in international prices of a basket of food commodities.
The FAO Food Commodity Price Indices show changes in monthly international prices of major food commodities. (Fig 1. and 2)

Figure no. 1

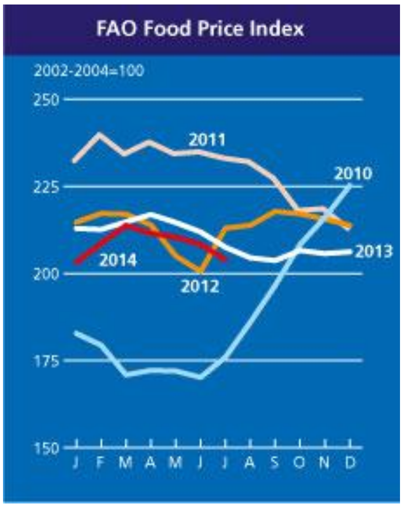
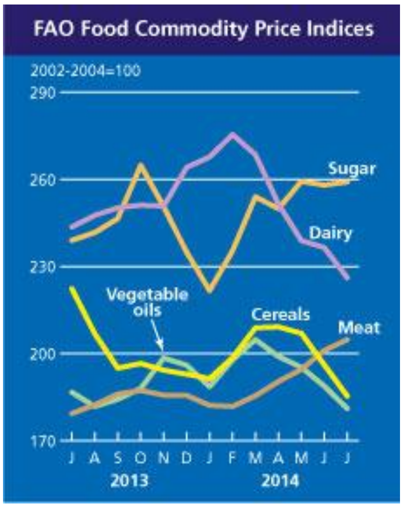
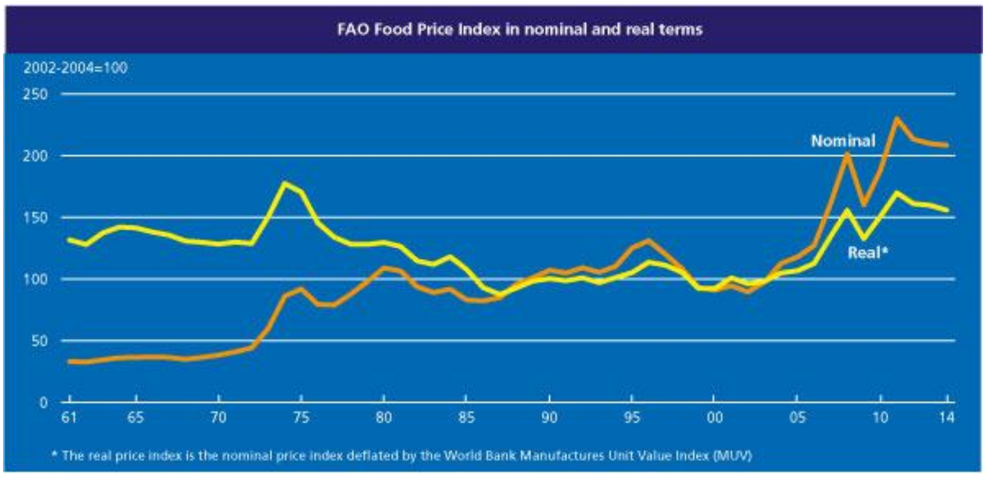


Figure no. 2



Source: www.fao.org; Release date: 09/10/2014

Figure no. 3



Source:www.fao.org; Release date: 09/10/2014

Dynamics of agricultural commodities price indices calculated by FAO clearly indicates a big drop in prices (price volatility) on the first part of the production increases in key commodities. Given this situation of the main agricultural products base amid considerable volatility, the effect of contraction rebounds on global markets.

Lack of national support for agricultural producers is one of the main economic factors underlying the decline of agricultural production, in addition to climate change, natural disasters, large differences of regional development and regional conflicts.

Conclusions

Food security is a complex and multidimensional issue. At times, when food security is threatened by global food price volatility, there is a need for both international and national responses. For example, increased coordination of policies at the international level can ensure effective and rapid responses to food price surges. At the national level, there is a need for comprehensive national food security strategies that take into account the country's specificities and characteristics, and that address both the food supply and access dimensions of food security. Such strategies should include policies that reduce food price volatility and measures that mitigate its impact especially on vulnerable populations, benefiting both consumers and producers. Such strategies should be evidence based, developed and implemented in an inclusive manner with the participation of civil society, farmers' organizations and the private sector.

At the national level, every country, including our country Romania, need information systems to monitor food markets, assess hunger and malnutrition, provide early warning and target assistance effectively. Social safety nets can reduce the impact of food price surges on the most vulnerable consumers.

Food reserves can be linked to such social safety nets but can also be utilized to directly stabilize market prices in national markets. Other policies that can mitigate the impact of food price volatility on producers include market based risk management instruments. Such risk management strategies can also be adopted by countries to stabilize their food import bills.

Food prices are expected to remain high. Growing population and income in emerging and developing countries significantly strengthens the demand for food. By 2050 the world's population is expected to have reached about 9 billion people and the demand for food to have increased by between 70% and 100%. Support policies leading to increased demand for crops by the biofuel sector in developed countries also contribute to strengthening the demand. On the supply side, the rate of growth in agricultural production is expected to fall to 1.5% between now and 2030 and further to 0.9% between 2030 and 2050, as compared with 2.3% per year since 1961. If the rate of growth of agricultural production does not keep pace with demand, there will be upward and continuing pressure on prices. With the supply-demand balance already tight, an external shock can result in significant food price surges and extreme volatility.

Food security is the main component of national security concerns organizational tools and policies used to prevent risks, threats and vulnerabilities and to address any crisis occurring in the food and especially the guarantee of access to food for the population of a state.

Romania, as in fact any country in the world must be independent of any other factor that might influence or unbalance the normal state of food security. The best countries in terms of food security are those with agricultural potential capable of supplying large quantities of agricultural raw materials and food than their national needs

Acknowledgements: *This paper of PhD. Bogdan Bazgă, has been financially supported within the project entitled „SOCERT. Knowledge society, dynamism through research", contract number POSDRU/159/1.5/S/132406. This project is co-financed by European Social Fund through Sectorial Operational Programme for Human Resources Development 2007-2013. Investing in people!"*

Bibliography

1. Bogdan Bazgă, „Food Security, as determinant factor to improve the valorification of the Romanian agriculture potential", PhD Thesis, Bucharest, 2013.
2. Banu, C., Barascu, E., Stoica, Al., Nicolau, A., „Sovereignty, Security and Food Safety ASAB Publishing", Bucharest 2007.
3. Barry Buzan, „People, States and Fear - An Agenda for International Security Studies after the Cold War", Cartier, Chişinău, 2000.
4. Blacioti Stefan, „Food security national interest of Romania in terms of European integration", Economic Tribune Publishing House, Bucharest, 2010.
6. Gabriel Michael, requirements and European standards in agriculture. Influences on National Security (PhD Thesis), National University of Defense Publishing House, Bucharest, 2010.
7. Ionescu Mihai, „After hegemony. Four security scenarios for Eastern Europe in the 90s", Scripta Publishing, 1993.
8. Maior George Cristian, „New Ally. Rethinking defense policy of Romania at the beginning of XXI century", RAO Publishing House, Bucharest, 2009.
9. Niculiţă, P., „Food safety and biotechnology", Edtura Printech, Bucharest, 2006.
10. B. Bazgă, „Prospects for Food Security in Romania". International Conference „Emerging Markets Queries in Finance and Business/EMQFB - 2012", Tîrgu-Mureş, România, Procedia Economics and Finance Volume 3, 2012.
11. ***, Price volatility and food security, 2011. Price volatility and food security, A report of The High Level Panel of Experts on Food Security and Nutrition, Rome, July 2011.

12. www.fao.org, Special Program for Food Security, FAO.
13. www.faostat.fao.org.
14. Bogdan Bazgă, „Securitatea Alimentară de la Concept la Realitate"; Conferinţa Internaţională „The Economic and Ecological Dimension of Development in the Third Millenium", a treia ediţie, din 11 Aprilie 2011 - Bucureşti, România, publicată în „Supplement of - Quality acces to Succes" - Journal Year, Vol 13, S1, Aprilie 2011.

References

[1] Barry Buzan, *op. cit.* pp. 65–66

[2] Idem, p. 22.

[3] George Cristian Maior, New Ally. Rethinking the defense policy of Romania at the beginning of 21st century.

CONSIDERATIONS REGARDING THE IMPACT OF ECONOMIC SECURITY ON NATIONAL SECURITY

Mihai TEODOR[*]

Abstract

The concept of security was studied until 20 years ago only by strictly referring to the military aspects. Changes occurring at the end of the century, in the European environment, led to a redefinition of the concept (security) by considering the threats type such as: economic, social, ecological, etc., in the event of a broad framework of measures against them. The pages that follow capture the steps of analysing the economic impact on National Security from the perspective of the Copenhagen School and also the Army position, in shaping the security features of the new capitalist economic system. Starting from understanding the new concepts, in the future, we will be able to understand the necessary requirements to maintain a realistic control over the national economy in order to ensure security.

Keywords: Copenhagen School, security, people, states, economic security, transition, restructure, managerial revolution

Introduction

"Until "recently", "security"- usually understood as "national security" - meant keeping some military expenses of, as preventive measure considered justified in the past, when such attacks were thought to be the only real threats to national survival. However, today, when the atmosphere is polluted with poisonous substances due to some nuclear and chemical accidents, which spread death and

[*] Romanian Intelligence Service.

disease on large areas of the Earth (e.g. disasters such as Chernobyl in USSR) and when the danger of epidemics (e.g. AIDS) and natural disasters (e.g. the "green house" effect) may endanger human life throughout the entire natural environment on the planet, the perspective of a narrow and restrictive view if the concept of security seems completely anachronistic and unrealistic.

The collapse of the Soviet Union set as an urgent necessity abandoning the traditional way of analysis the concept of security based on military and political studies. "The core problem was that by the time of its fast decline and subsequent implosion, the Soviet Union had at least the second military force that has ever existed in the world. The Soviet security was fatally compromised by the weakness of its socio-economic and institutional policy basis and not by lack of military force. The implications of this fact were that the hierarchy problems in the traditional agenda of security supported by "high level" and "low level" notions ignored, or at least simplified the very complex interaction between socio- economic and national security issues".[1]

Abandoning for good the classical way of analysing on military matters led to the loss of control over the reform process by Gorbachev. Clearly, many theorists and probationers of politics, all very influential, were aware of the internal crisis in the Soviet Union. However, those who criticize the traditional concept of security argue that these crises did not receive the needed attention because of the narrow approach of the security agenda. The (neo)realist paradigm found difficulties in including internal socio- economic matters into its agenda. The argument is that this fact contributed to, and also supported the logic of high "level" and "low level" politics. Security issues were considered of primary importance, and political and military aspects or "high level" politics, were synonymous with security. This way, complex forces which acted in the Soviet Union and which eventually led to its collapse were not included on the security agenda. Consequently, many theorists and practitioners have been disconcerted by the sudden end of the Cold War and the collapse of the Soviet Union.

Adapting to the new challenges

The new way to analyse the concept of security was provided by the so-called “Copenhagen School” which soon became the common name for the entire analysis of the security concept and the fields to which security must be provided. All this literature was generated by some analysts associated to the Copenhagen Centre for peace and conflict research. Certainly, the most influential analysts were Barry Buzan and Ole Waever. Their innovative activity brought great contribution, and in some cases shifted the debate on the nature of security studies.

The Copenhagen School considered the security studies “as being problematic if they are narrowly built around the military dimension of security and excluding other dimensions”[2].

Through publishing of “People, States and Fear”, Barry Buzan has provided the theoretical support to analyse the security concept by including other types of security together with the military one.

The first complex analysis that launched the idea of different ways of security, and that contributed to its inclusion on the agenda of academic perspectives, was made in Barry Buzan’ s book “People, States and Fear”, published in 1983. Due to being published during the first Reagan administration and in the middle of what some people called “the second Cold War”, the book had a real impact. And the second edition published in1991 had a greater impact. Buzan illustrates the international system, states and individuals as objects of reference, and the military, political, economic, societal and environmental landscapes as sources of potential threats to those references. This is a starting point to clearly understand the complexities of the security “problem”. Perhaps the most debated of these dilemmas refers to the extent to which that it is useful to privilege any of the reference objects of security.

The most powerful debate focused on rival claims of states and individuals on the position of primary references of security. This dilemma was stated most clearly by Ken Booth when he asked: “the easiest test refers to the main reference object: states or people? Whose security comes first? ” For Buzan, the answer, at least in *People, States and Fear* is that the main concept of security must be the state”[3]. Barry Buzan believes that “politics should be made only in a state's level in order to ensure security"[4]. Since the "economic security of a company, however, means more than economic security of economic or market agents. The issue is related to the state's role in the economy"[5].

Examining the "extremely difficult idea of economic security", Barry Buzan points out that "the national economy belongs somehow to the physical basis of the state" and "the economic threats are, undoubtedly, the most misleading and difficult to dominate in the national security", therefore, in a market system, there is a huge number and variety of economic threats so that these "economic threats seem like an attack to the state"[6].

The Copenhagen School's thinking has influenced the politics of most member States' in security organizations. In 1991, during the summit in Rome, NATO has decreed – in Copenhagen School's classical language - that security now has five dimensions: military, societal, political, economic and environmental.

The Copenhagen School has not only influenced the way researchers analyse the concept of security, it has also an impact on the community that writes policies. North Atlantic Treaty Organization "provides the forum where consultations take place in any problems and where the member countries make decisions regarding political and military problems which could affect their security. The organization provides necessary structures to make consultations and cooperation among member countries easier regarding political, military and economic areas, such as scientific and outside military areas"[7].

The potential power of a nation "is thought to derive from several sources that should be considered as a unified and balanced system. These sources are: geography, population, economy, national will, leadership"[8]. Some strategic analysts argue that in the next century, which we will reach in a few months, economic competition will be much more important than military competition in order to gain national power. Corresponding to this view, they say that the main emphasis should be on the "economic basis of national security"[9]. In this respect, another author believes that "the economic potential of a state reveals its power"[10].

Economic power, understood as the ability to exploit the economic potential of a country at a certain point, allowed the

Romanian state to support the military reform that aims at "building a modern army, appropriately sized, flexible and mobile, with a credible combat capability regarding its efficiency, able to discourage and deal any external military threat "[11].

Carrying out the transformation process of the Romanian Army “will have as a result the creation of military capabilities characterized by flexibility, high response speed and interoperability”[12]. The transformation process of the Romanian Army is very complex, and getting success in the field depends on the financial, human and material resources required to support it. The main element which determines the size, performances and efficiency of the armed forces are finances.

Carrying the reform process of the armed forces “depends on the country's financial resources, on the institutional possibility of the Ministry of National Defence to implement policies and measures correlating them to policies of economic reform and institutional capacity of other ministries and agencies to meet the time functions they must do. Taking into account these institutional requirements, annual military spending will account for 2,38 % of gross domestic product”[13], an effort that depends on providing a real economic development.

A strong, performant and competitive economy, macro-dynamic and stable in terms of growth, and functional "is an important pillar of security, providing conditions for economic and social security, the interest of the majority to support the basis for democratic institutions and the necessary basis for promoting initiatives aiming at the nation's prosperity and security ”[14].

The effects of the transition process are reflected mainly in the growth of economic competitiveness, as a result of macro stabilization efforts of the state through a series of applied security policies, and as an indirect result of private business activity.

The structural improvement of the Romanian economy is, first of all, the result of the consecration of freedom as a choice of possible solutions from the most profitable and most efficient. Economic nonsense like “planned losses” have definitely become history.

The way of the new security elements of the capitalist economic system will be stored is based on achieving the old goal of rebuilding and renewing the economy, realities demonstrated by a tough export, which performed because of improving the quality of the products, this became a real peak form of our nation' s competition with other nations.

The restructuring of the economy led to the return of small or medium economic units instead of the industrial giants, creating possibilities of accessing better resources and causing a new economic balance. The force of democracy is given by the amount of effective actions of all economic agents, which emphasizes efficiency as a rule for economic security.

Understanding the mechanisms of centralized economy of the communist years and the effects of their economic doctrine is one of the starting points needed to assess developments on the economic security of the entire Romanian society.

Also - in my opinion – it is of real help to be aware of the devastating effects that handling and application of scientifically unfounded theories can have on the life of the entire international community and, in particular, the destinies of nations, in order to forcefully and in an appropriate way address these forgeries which are well hidden under a reason, actually serving the interests of foreign economic security and protection of the entire social construction of democracy.

A realistic understanding of the requirements necessary to maintain control over the economy and to overcome the negative circumstances, offering each time the absolutely necessary solution for economic progress is a huge performance of the technocrat Romanian economic elites, whose role might be better emphasized in the future.

Through effective collaboration with the major international economic institutions, the Romanian technocracy opened the gate to a global economy for the national economy too, allowing for the essentially strategic purpose of the whole process of transition - the modernization of the Romanian nation.

The managerial revolution in Romania is the certain element of achieving a future climate of economic efficiency, being able to guarantee the elimination of disparities to western European economies.

Also, strengthening and improving the business of the market, based on the principle of free competition and social solidarity is a priority. It is "the basis for healthy economic development, capable to ensure effective integration of Romania into the European Union, assuring globalization demands, normal access to resources and international markets, resistance to major economic fluctuations"[15].

Conclusion

The evolution of the concept of security and its great complexity caused a review of the analysis of its problems.

Knowledge of economic realities which was the starting point of transition in Romania in an effort to close the gap to the free world, is one of the keys to understanding the events of our recent history and certainly for understanding developments in the future, too - hopefully - as few years as possible.

Changing the communist type of economic mechanism to the capitalist type resulted in the creation of a new economic environment in which our country can appreciate that there has been a lower extent than the one desired of the technological revolution - and Romania jumped over it in the past, but which was implemented by free economic activity throughout the national economy that has a guaranteed progress through practicing modern management.

References

[1] Frunzeti, Teodor, „Geostrategia", Editura Centrului Tehnic-Editorial al Armatei, Bucureşti, 2009.

[2] Croft, Stuart, „Studii de Securitate", Editura Cavallioti, Bucureşti, 2005.

[3] Buzan, Barry, „Popoarele Statele şi Teama", Editura Cartier, Bucureşti, 2000,

[4] Croft, Stuart, *op.cit.*

[5] Sava, Ionel Nicu, „Studii de Securitate", Editura Centrului Român de Studii Regionale, Bucureşti, 2005,

[6] Barry Buzan, *op. cit.*

[7] *NATO* Manual, Office of Information and Press, NATO 1100 Brussels – Belgium, 2000.

[8] Frunzeti Teodor, *op.cit.*

[9] *Ibidem.*

[10] Creţu Gheorghe, „Riscuri la adresa securităţii naţionale”, Editura Sylvi, Bucureşti, 2006,

[11] Ministerul Apărării Naţionale, „Cartea Albă a Guvernului - Armata României 2010: Reformă şi integrare euroatlantică”, Editura Militară, Bucureşti, 2000.

[12] Ministerul Apărării Naţionale, „Strategia de transformare a Armatei României”, Bucureşti, 2007.

[13] Anghelache Constantin, „România 2006: Starea economică înaintea aderării”, Editura Economică, Bucureşti, 2006.

[14] Parlamentul României, „Strategia de securitate naţională a României”, Bucureşti, 2006.

[15] *Ibidem*.

MAPPING THE CYBER SECURITY DILEMMA SELECTIVE THEORETICAL REMARKS

Iulian F. POPA[*]

Abstract

To date only a few scholars and security studies experts around the world referred explicitly to the cyber security dilemma within their research works. As I generally agree with Nicholas Rueter and Mike McConnell's findings on this topic, I strongly believe the classical security dilemma framework – as defined and conceptualized by Robert Jervis previously, emerges within cyberspace undoubtedly.

In other words, in terms of cyber security, this paper aims to identify and reveal the most likely elements which describe the both cyber security dilemma escalation and de-escalation (referred herein as "ease" or "settlement"). Therefore, I focus my attention on continuing Rueter's work, by stepping forward his theory in terms of factors or behavior leading to the occurrence and escalation of cyber clashes among international "cyber stakeholders". Last but not the least, I describe and review briefly the cyber security dilemma escalation and settlement pattern.

Keywords: national ecurity, cyber security, cyber security dilemma, security dilemma

A Brief Theoretical Overview

As it may have been expected, more than twenty years after the end of Cold War, the security dilemma (SD) is still one of the main concerns for both political and military decision makers and scholars around the world as well.

Theoretically, there is no serious doubt the SD was mainly coined within the framework of both defensive and offensive structural realism international relations theory.

[*] Ph. D. Candidate, International Relations and Security Studies Doctoral School,`Babeş-Bolyai` University, Cluj-Romania

Therefore, from the very beginning one may argue the SD is structurally cross-linked with neorealism and its exponents, who extensively explained that the SD may arise mainly due to the anarchic nature of the world. For example, Mearsheimer suggests the world *comprises independent political units* (e.g. states) *that have no central authority above them*, being *potentially dangerous to each other*[1].

Traditionally, it may be appreciated the states' struggle to survive, to protect their national interests, and to self-maximize their power and security (mainly military) causes an imbalance of power or a situation broadly known as the "security dilemma". In fact, in the view of most neorealist scholars, states are mainly distrustful and uncertain *about the intentions of other states [...], which simply means that states can never be sure that other states do not have offensive intentions to go with their offensive military capabilities*[2].

In particular, to date, even among neorealist scholars there is a significant intellectual dispute regarding the nature and ways to counteract or escape the SD, if indeed avoiding SD or the arms racing context is practically possible. In this regard, it is worth mentioning that states might have the *tendency to defect from cooperative arrangements if they perceive other states' security preparations as threatening (misperception; arms racing)*[3].

But the more a state tries to improve its security, the less safe other states will feel[4]. Widely known as the spiral of insecurity[5], this situation describes quite accurately the international security framework.

In fact, it arises when one state (military) defensive or offensive decisions and maneuvers are understood mainly as national security threats by other states (e.g. adversaries) and continues many a time as an arms racing, rationally or irrationally motivated by national security needs. In this regard, John H. Herz described the security dilemma as *a social constellation in which units of power... find themselves whenever they exist side by side without higher authority that might impose standards of behavior upon them and thus protect them from attacking each other. In such a condition, a feeling of insecurity, deriving from mutual suspicion and mutual fear, compels these units to compete for ever more power in order to* *find more security, an effort which proves self-defeating because complete security remains ultimately unobtainable*[6].

In theory, the both defensive and offensive behavior may be reasonably distinguished in some cases, but things become worrisome when the traditional offense-defense theory becomes practically void. In this regard, it is worth mentioning that some experts previously suggested that the *offense and defense cannot be distinguished since virtually all weapons can be used for both offense and defense*, [and therefore the] *offense-defense theory cannot be implemented*[7].

Nonetheless, according to Robert Jervis, *when defensive weapons differ from offensive ones, it is possible for a state to make itself more secure without making others less secure. And when the defense has the advantage over the offense, a large increase in one state's security only slightly decreases the security of the others, and status quo powers can all enjoy a high level of security and largely escape from the state of nature*[8].

In other words, in the light of the offensive-defensive theory, Robert Jervis splits the security dilemma into four plausible scenarios (as described below) which may encounter practically, using an intensity-based/power approach – well known among international scholars. In fact, Jervis uses this approach to gradually distinguish between various SD stages during its initialization, escalation or settlement (ease) (*please see the tables below and the brief summaries).*

Table no. 1 – SD Scenarios according to Robert Jervis[9]

	SD Behavior	Behavior Type	Advantage	SD Intensity	Environment Type
1	Offensive and Defensive	Not distinguishable	Offense	Very intense	2 X Dangerous Aggressive Arms race
2	Offensive and Defensive	Not distinguishable	Defense	Intense	Probably dangerous
3	Offensive and Defensive	Distinguishable	Offense	Not intense	Less aggressive Probably safe

4	Offensive and Defensive	Distinguishable	Defense	Low intensity/ No intensity	2 X Safe Very little dangerous

Table no. 2 – SD Scenarios relative to good governance

Scenario	1	2	3	4
Good governance	Very unfriendly	Unfriendly	Less friendly	Friendly

Therefore, even though we clearly witness nowadays the states are less willing to join good governance arrangements, I argue the SD may be diminished to a certain extent by good governance, complex interdependencies or "rewards and punish" approaches, even more as I strongly believe the SD is seriously influenced by mistrust in international relations rather than "the anarchy of the world" – if there is an intrinsic one as neo-realists suggest. Indeed, competitive states might have serious national security grounded fears based on the fact that their adversaries might become too powerful, but it might be wiser for global decision makers to also regard SD as *a social structure composed of intersubjective understandings in which states are so distrustful that they make worst-case assumptions about each other's intentions*[10]. At least in cyberspace.

However, bearing in mind virtual space is – even apparently, less physically violent and aggressive compared to the "real world". In the following I will briefly introduce the cyber security dilemma (CSD) and analyze its current pattern.

Therefore, as Nicholas C. Rueter suggested[11], I assume there is a security dilemma within cyberspace also, namely the "cyber security dilemma". Though I do not fully agree with Rueter's arguments on *cooperation over cyber-warfare [...] despite the security dilemma*[12], I suggest the CSD or the "cyber arms race" might be for both state and non-state actors a convenient and less intense/aggressive alternative to the classical security dilemma, due to increased operational flexibility and *reduced entry costs*[13] in cyberspace.

The Cyber Security dilemma

Forrest Hare argues that *the nature of "cyber security" as a national security issue is ambiguous and there is a heightened potential for a security dilemma in the domain*[14].

Indeed, despite some critics, to date there are many hurdles which significantly keep us away from clearly distinguishing between OCEO (offensive cyber effects operations) and DCEO (defensive cyber effects operations). Neither more nor less the "cyber security" concept itself it may be problematic to some extent.

What is cyber security in fact?

For the purpose of this paper, I define the cyber security as being the *complex [set] of legal, organizational, technical and educational*[15] measures and countermeasures put into force both within and outside cyberspace to secure *the cyber environment, organization's and user's [cyber] assets*[16] and actions.

What CSD stands for?

Obviously, the "CSD" acronym stands for the "cyber security dilemma". Therefore, based on Jervis' remarks, I define the CSD as being the feeling or the spiral of cyber insecurity that arises when one competitive actor's (state or non-state) power and security architecture is challenged or threaten by its opponents mostly via non-kinetic offensive and/or defensive operational and/or tactical cyber means, the initial target being compelled to actively and/or passively defend its posture and offset the induced imbalances via offensive and/or defensive cyber means as well.

Such unique situation, known as the CSD initialization (phase A and B), may give rise to serious tensions among the initial attacker and target due to the operational, tactical, and (why not?) strategic power imbalances among them. Not surprisingly, almost in the same time or within a very short period of time the initial attacker might become target as well, escalating significantly the dilemma (phase C to E) – please see the figure no. 1.

How CSD works?

As previously suggested[17], and bearing in mind the context described above, I have identified that CSD looks as a "recursive loop", being invariably a systematic alternation between gradual tension escalation and relief. In fact, the CSD initialization-escalation-settlement pattern looks very similar to a Gaussian conflict escalation curve, excepting the pinnacle – often regarded as collateral (mutually disadvantageous) stalemate or *mutually hurting stalemate,* which in fact might be not fully disadvantageous for parties involved.

Firstly, even though to date the assumption above has only empiric grounds, the benefits of dilemma initialization and escalation might have a serious lucrative logic to some extent (mainly phase D to phase G). Therefore, despite criticism, I strongly believe not only the CSD initialization, but the escalation also is indeed "worth trying" in most cases.

Secondly, as might have been expected, there is no genuine cyber security dilemma when the cyber security based dilemma extends outside cyberspace. In such cases, the security dilemma is in fact a classical one rather than a CSD.

Thirdly, as most of the global relevant non-state cyber actors increase their close cooperation arrangements with various national governments and state actors, it is expected that CSD will shortly emerge among relevant and/or competitive non-state actors, either global or regional, sharing "enough" tactical or strategic interests.

What is CSD struggle?

I define the CSD struggle as the competitive actors' ability to exploit and wisely use all the available cyber techniques, means, and instruments to timely limit and overcome the opponents' operational, tactical and/or strategic advantages.

The CSD pattern explained

In theory, as shown in the image and table below – regardless the time unit, a full CSD cycle comprises 5 specific stages (ST), namely**:**

1 – the initialization (phase A to B);
2 – **the escalation** (phase C to D);
3 – **the peak or the "melting point"** (phase E and F);
4 – **the de-escalation** (phase G to H);
5 – **the settlement** (phase I to J) of CSD.

Please refer to the table and figure below for more detailed information.

Table no. 3 – CSD Stages Explained

ST.	PH.	OCEO vs. DCEO	INTENSITY	COMMENTS
1	**A**	Distinguishable	No intensity	initial target identification and acquisition;
	B	Distinguishable	Low intensity	initialization phase; OCEO and DCEO planning;
2	**C**	Distinguishable	Moderate	constructive or disruptive/ destructive mutual responses; during this phase the CSD may still be reversible via good cyber governance approaches;
	D	Not distinguishable	Intense	the CSD becomes irreversible; the tensions increase;
3	**E**	Not distinguishable	Very intense	the tensions pinnacle is reached; bidirectional clashes have serious effects on the opponents;
	F	Not distinguishable	Very intense	tensions decrease as the melting point was reached; most likely at least one party is or becomes no longer able to offset properly the induced power imbalance by means of efficient offensive and/or defensive behavior;
4	**G**	Not distinguishable	Intense	although the parties start gradually disengage, OCEO and DCEO are still prevalent;
	H	Distinguishable	Moderate	parties initiate constructive approaches; this phase is not mandatory;
5	**I**	Distinguishable	Low intensity	de-escalation consolidation phase; each actor actively contributes to CSD settlement while strengthening the stabilization (not mandatory);
	J	Distinguishable	No intensity	forced or non-forced CSD settlement; the dilemma may be re-initiated at any time again;

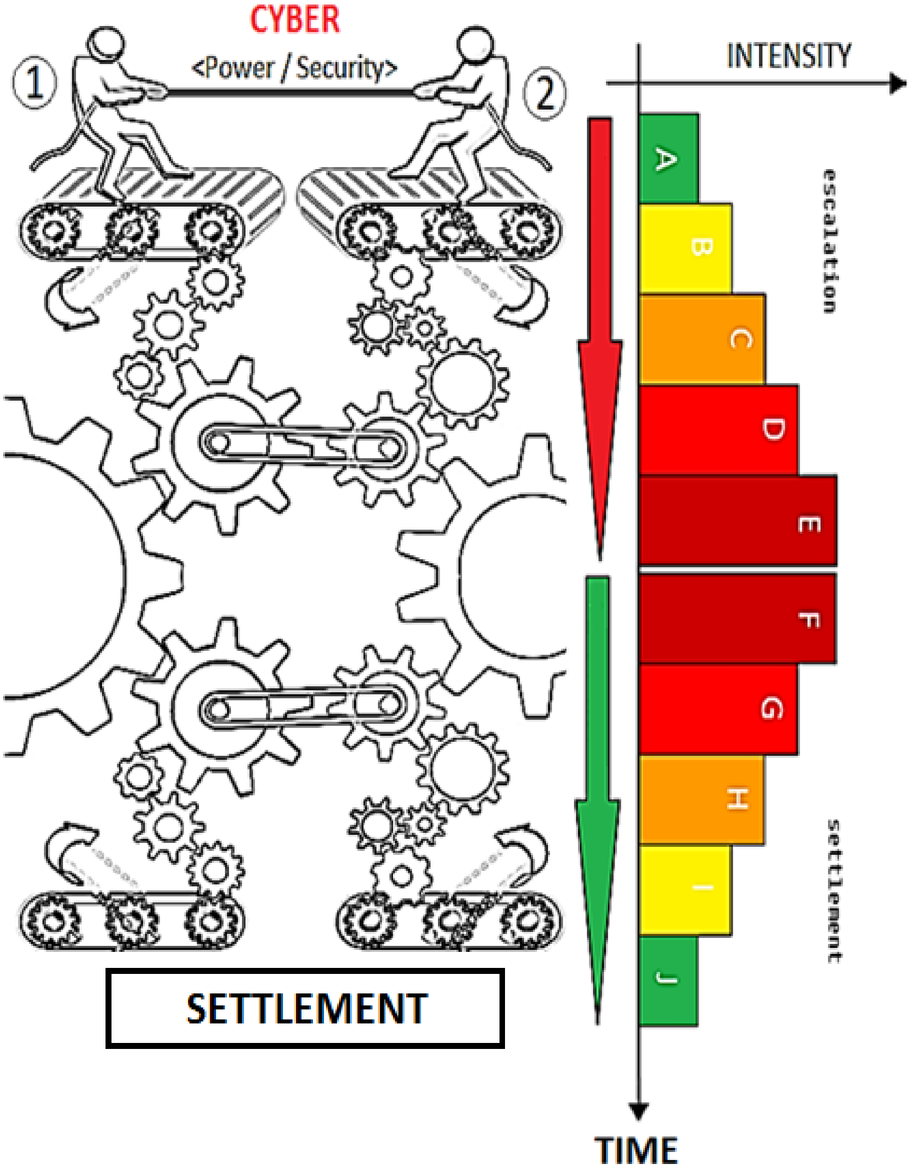


Figure 1 – CSD half loop pattern (in drawings[18])

Conclusion

It seems that, Nicholas C. Reuter as cited above was right. Therefore, most likely, there is a security dilemma within cyberspace, even though, military speaking, no one is able at the moment to clearly assess whether or not there is an arms racing within the "cyber" domain.

Personally, from a neorealist academic approach – which not necessarily I entirely agree with, I strongly believe the CSD emerges within the "virtual battlefield" as well. Nonetheless, the international scientific research on CSD is still at its very beginnings and therefore far from having irrefutable outcomes on this topic.

Generally speaking, the CSD resembles to its classical counterparts, but with some notable exceptions. Briefly – no matter what the theoretical perspective or paradigm (e.g. structural realism, constructivism, etc.) these revolve around the following findings:

- compared to its classical counterparts, the CSD's initialization has serious economic grounds – highly likely the most relevant ones, besides the military purposes; also there are strong clues the CSD may escalate on a "social-engineering" basis, as these techniques and practices progress very swiftly;
- the CSD side effects are mainly of virtual type (non-kinetic), even though cyber security has a significant military dimension and most of the critical infrastructures are highly cyber-dependent;
- the CSD is unlikely to inflict a classical security dilemma at large scale; the vice versa is highly likely as it comes more closer to the nowadays global security environment realities;
- the CSD goes beyond the state-to-state security dilemma framework, as the some competitive non-state actors become nowadays as relevant as some state actors;
- the CSD is less aggressive and violent compared to its classical counterparts;

- while most of the time the classical security dilemma may leads to a stalemate, the CSD might have a serious benefits for the parties involved.

Therefore, I argue the CSD is deeply rooted in the cyberspace security ecosystem. In the future, it has to be assessed whether or not the CSD escalation favors its initiators to bypass the international cyber governance framework and regulations regarding the proper conduct within cyberspace and military operations as well. To the moment, I haven't been able to clearly identify whether or not the international community's past and current (good) cyber governance efforts prevent significantly the CSD's escalation, as its initialization is unavoidable for the moment[19].

Bibliography

1. Bellany, Ian, "Defensive Arms and the Security Dilemma: A Cybernetic Approach" *Journal of Peace Research,* Vol. 33, No. 3 (Aug., 1996), pp. 263-271.
2. Cerny, Philip G., "The New Security Dilemma: divisibility, defection and disorder in the global era" Review of International Studies 26, 2000, 623–646.
3. Glaser, Charles L., "The Security Dilemma Revisited" *World Politics,* Vol. 50, No. 1, Fiftieth Anniversary Special Issue, 1997, pp. 171-201.
4. Geers, Kenneth*, Strategic Cyber Security* (Tallinn, NATO CCD COE, 2011) p. 63.
5. Hare, Forrest, "Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security?" *Cryptology and Information Security Series – Volume 3* (Amsterdam: IOS Press, 2011), p. 89.
6. Herz, John H., *International Politics in the Atomic Age* (New York: Columbia University Press, 1962), p. 231.
7. Higgins, Kelly Jackson, "Aurora Attacks Still Under Way, Investigators Closing In On Malware Creators", accessed August 8, 2014, at http://www.darkreading.com/security/news/222700786.
8. International Telecommunications Union, *Recommendation X.1205 – Overview of cybersecurity,* accessed August 11, 2014, at https://www.itu.int/rec/T-REC-X.1205-200804-I.
9. Jano, Dorian, "Aspects of Security Dilemma – What We Have Learned from the Macedonian Case" *Perceptions,* 2009, available, at http://sam.gov.tr/wp-content/uploads/2012/01/Dorian-Jano.pdf.

10. Jervis, Robert, “Cooperation under the Security Dilemma” *World Politics*, Vol. 30, no. 2, pp. 167-214.
11. Lynn-Jones, Sean M., “Offense-Defense Theory and Its Critics” *Security Studies*, Vol. 4, Summer, 1995, 672-674.
12. Mearsheimer, John, “The False Promise of International Institutions” *International Security*, vol. 19, no. 3, 1994, pp. 9-10.
13. Popa, Iulian F., “Cyberspace Governance. New Governance Approach in Support to International Security” Conference Proceedings, *The Complex and Dynamic Nature of the Security Environment* (Bucharest, The Centre for Defence and Security Strategic Studies - Carol I National Defense University, 2013), pp. 369-379, accessed August 13, 2014, at http://cssas.unap.ro/en/pdf_books/conference_2013.pdf.
14. Rueter, Nicholas C., *The Cybersecurity Dilemma* (Durham, NC, Duke University, 2011), pp. 1-7.
15. Schreier, Fred, “On Cyberwarfare” *DCAF Horizon,* No. 7 (Working Paper), 2005, p. 12, accessed on August 9, 2014, at http://www.dcaf.ch/content/download/67316/1025687/file/OnCyberwarfare-Schreier.pdf.
Starr, Stuart H., “Towards an Evolving Theory of Cyberpower” *Cryptology and Information Security Series*, (Amsterdam: IOS Press, 2011), pp. 18-52.
The Parliament, *Czech Republic – Draft Act on Cyber Security (2014),* p. 2, accessed on August 10, 2014, at http://www.ccdcoe.org/cyber-definitions.html.
Wendt, Alexander, "Constructing International Politics " *International Security,* vol. 20, no. 1, 1995, p. 73.

Acknowledgements: This work was possible due to financial support of the Sectoral Operational Programme for Human Resources Development 2007-2013, co-financed by the European Social Fund, under the project number POSDRU/159/1.5/S/140863, with the title “Competitive Researchers in Europe in the Field of Humanities and Socio-Economic Sciences. A Multi-regional Research Network”.

References

[1] John Mearsheimer, "The False Promise of International Institutions", International Security, vol. 19, no. 3, 1994, pp. 5-49.

[2] Idem, p. 10.

[3] Philip G. Cerny, "The New Security Dilemma: divisibility, defection and disorder in the global era" *Review of International Studies*, vol. 26, 2000, p. 623-646.

[4] Dorian Jano, "Aspects of Security Dilemma – What We Have Learned from the Macedonian Case" *Perceptions,* Spring-Summer, 2009, accessed August 4, 2014, at http://sam.gov.tr/wp-content/uploads/2012/01/Dorian-Jano.pdf.

[5] Charles L. Glaser, "The Security Dilemma Revisited" *World Politics,* Vol. 50, No. 1, Fiftieth Anniversary Special Issue, 1997, pp. 171-201.

[6] John H. Herz, *International Politics in the Atomic Age* (New York: Columbia University Press, 1962), p. 231, *apud* Ian Bellany, "Defensive Arms and the Security Dilemma: A Cybernetic Approach" *Journal of Peace Research,* Vol. 33, No. 3 (Aug., 1996), pp. 263-271.

[7] Cf. Sean M. Lynn-Jones, "Offense-Defense Theory and Its Critics," Security Studies, Vol. 4, Summer 1995, 672-674.

[8] Robert Jervis, "Cooperation Under the Security Dilemma" *World Politics*, Vol. 30, no. 2, pp. 167-214, *apud* Idem.

[9] Idem, pp. 186-214.

[10] Alexander Wendt, "Constructing International Politics " *International Security,* vol. 20, no. 1, 1995, p. 73.

[11] Nicholas C. Rueter, *The Cybersecurity Dilemma* (Durham, NC, Duke University, 2011), pp. 1-7.

[12] Idem, pp. 43-54.

[13] Fred Schreier, "On Cyberwarfare" *DCAF Horizon,* No. 7 (Working Paper), 2005, p. 12, accessed on August 9, 2014, at http://www.dcaf.ch/content/download/67316/1025687/file/OnCyberwarfare-Schreier.pdf.

[14] Forrest Hare, "Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security?"*,* in Christian Czosseck (ed.), Kenneth Geers, *Cryptology and Information Security Series – Volume 3* (Amsterdam: IOS Press, 2011), p. 89.

[15] The Parliament, *Czech Republic – Draft Act on Cyber Security (2014),* p. 2, accessed on August 10, 2014, at http://www.ccdcoe.org/cyber-definitions.html.

[16] International Telecommunications Union, *Recommendation X.1205 – Overview of cybersecurity,* accessed August 11, 2014, at https://www.itu.int/rec/T-REC-X.1205-200804-I.

[17] Charles L. Glaser, *op. cit.*, pp. 171-201.

[18] Edited image. Original image courtesy belongs to *The Association for Conflict Resolution*, accessed on August 9, 2014, at http://www.acrkentucky.org/wp-content/uploads/2013/04/resolving_conflict.jpg.

[19] Iulian F. Popa, "Cyberspace Governance. New Governance Approach in Support to International Security" Conference Proceedings, *The Complex and Dynamic Nature of the Security Environment* (Bucharest, The Centre for Defence and Security Strategic Studies - Carol I National Defense University, 2013), pp. 369-379, accessed August 13, 2014, at http://cssas.unap.ro/en/pdf_books/conference_2013.pdf.

CYBERTERRORISM – SHOULD WE FEAR?

Daniel COSTAN[*]

Abstract

Terrorism became a growing threat of global concern. Terror attacks are real serious threats to any country, and cyberattacks should not be treated any differently. Just because cyberattacks do not use bombs, guns or daggers does not mean that it can be ignored or taken easily. You do not necessarily have to carry a machine gun or a belt stuffed with TNT to spread fear and terror among peoples. Is it in fact possible that, in a time not very far from now, terrorists move their destructive activities from the classic battleground to the virtual world, taking advantage of the modern technology? Of multiple vulnerabilities still existing in IT systems and networks?

May computers revolutionize terrorism in the same manner that they have revolutionized everyday life?

Keywords: terrorism, cyberterrorism, vulnerabilities, fear

What is cyberterrorism?

The Information Age is here. It is a reality. This evolution of technology in daily life, as well as in the educational life style, has allowed rapid global communications and networking to shape modern society. Though the Internet itself has existed since 1969, it was with the invention of the World Wide Web in 1989 by British scientist Tim Berners-Lee, and its introduction in 1991, that the Internet became an easily accessible network.

Let us suppose you woke up this morning eager to start a new day. You are a regular person, so you are used to surf the news on Internet while you drink a nice cup of coffee. Sitting there and opening e-mails or clicking links to read some interesting article about today's weather, you may have just became part of a huge

[*] National Cyberint Center

network of zombie-computers controlled by a terrorist organization, intended to inflict damages on specific state's infrastructures. Is in fact possible?

Certainly this is one of the many unanswered questions. What is cyberterrorism? Most people, governments included, consider it primarily as the premeditated, politically motivated attack against information, computer systems, computer programs, and data by sub national groups or clandestine agents.

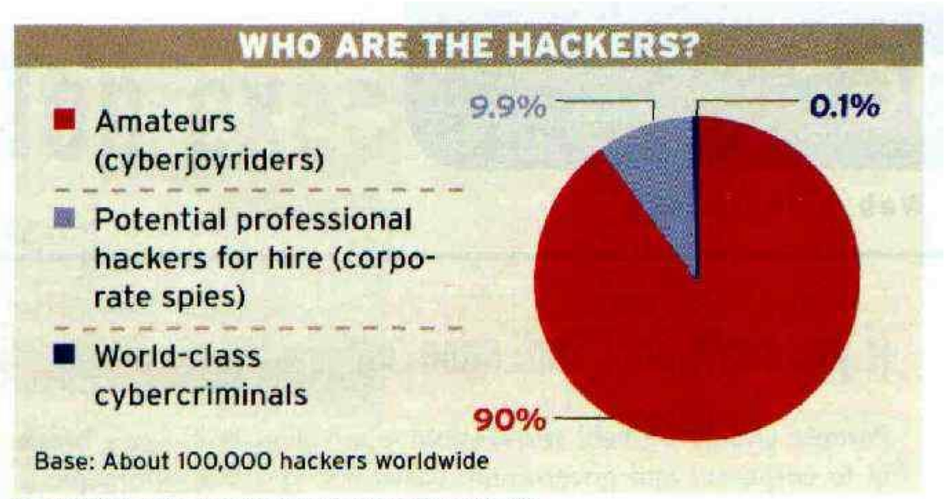
Most notably, Dorothy E. Denning, professor of computer science at Georgetown University, has put forward an admirably unambiguous definition in numerous articles and in her testimony on the subject before the House Armed Services Committee in May 2000[1]: "*Cyberterrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not*".

In fact, how real is the threat of cyberterrorism? Could terrorists cripple critical military, financial, and strategic computer systems? Could they harm infrastructures and spread panic among the people? Do they have the capabilities to inflict such damages? Despite the multitude of scenarios popularized by journalists, politicians and various experts, many of those fears are rather exaggerated: not a single case of cyberterrorism has yet been recorded. Hackers are regularly mistaken for terrorists, and the states cyber infrastructures are commonly robust. Even so, the potential threat is undeniable and seems likely to increase, making it all the more important to address the danger adequately.

Who are those hackers?

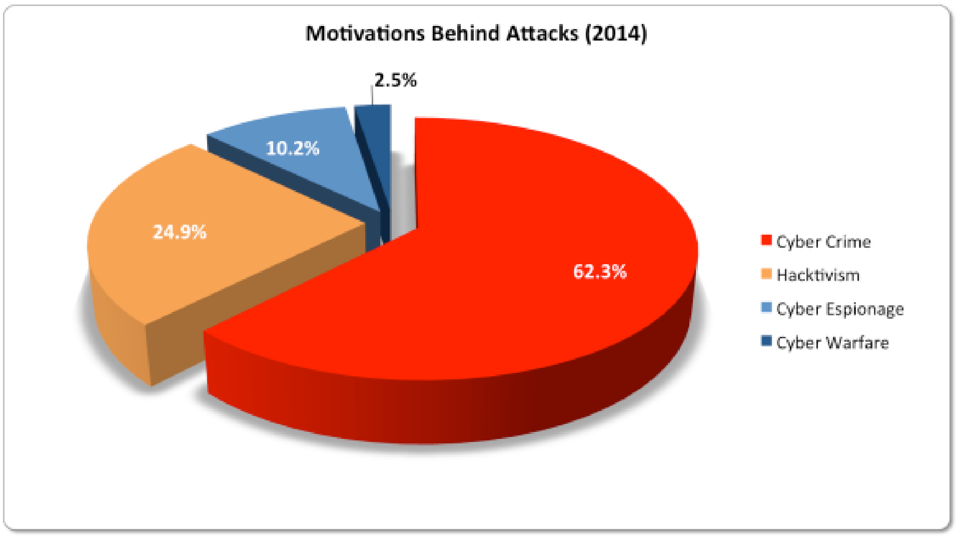
Experts estimate that hackers may number 19 million worldwide. They are responsible for tens of thousands of attacks each day and many of them are „fighting for a cause". State decisions, global decisions or territories occupation are the main reasons for ideologically and politically motivated cyberattacks.

An interesting study conducted by the IBM Global Security Analysis Lab on a base of about 100.000 hackers illustrate that 90% of them are in fact amateurs ... joyriders[2]. This could be good news. Joyriders usually do it for fun, they lack the knowledge of advanced cyberattack techniques and they haven't got enough cyber capabilities to conduct a massive and destructive attack against state critical infrastructures. But let us take a look over the other 10%.
Should we be worried?



Source: IBM Global Security Analysis Lab, Yorktown Heights, N.Y.

According to www.hackmaggedon.com[3], in 2014 cybercrime attacks ranked at number one with 62.3% followed by Hacktivism 24.9% and cyber espionage 10.2%.



Governments and Industries have been the most preferred targets for cyber attackers with similar values (respectively 27.1% and 25.2%), with a substantial growth year-over-year (they were respectively 23% and 22% last year). Targets belonging to Finance rank at number three (15.7%, more than twice in comparison with 2013). Organizations and News come after with respectively 8.3% and 6.6%. If we admit that hackers numbers approximately 19 million worldwide and 10% of them are professional or high-skilled, respectively world-class cybercriminals, we are facing a serious problem: somewhere in the world, there are about 2 million well-hidden hackers, ready to be hired by state or sub-state actors.

Good news

Although there is a large number of hackers and cyber-attacks worldwide, most of them are low-level and conducted by hackers who lack technical expertise. In fact, according to IBM Global Security Analysis Lab, just about 1% of hackers are advanced enough to successfully conduct a disruptive attack against the state's infrastructures.

There are, also, strong barriers to prevent the acquisition of resources to enable the capability to execute a cyberterrorist attack. Simulated cyberattacks, conducted by the United States Naval War in 2002[4] indicated that "attempts to cripple the U.S. telecommunications infrastructure would be unsuccessful because the system redundancy would prevent damage from becoming too widespread. Many observers suggested that evidence from natural disasters shows that many of the critical infrastructure systems, including banking, power, and water and air traffic control would likely recover rapidly from a possible cyberattack".

On the other hand, "it would be possible to inflict some serious damage to the nation's data and physical infrastructure systems, but it would require a syndicate with significant resources, including $200 million, country-level intelligence and five years of preparation time".

Bad news

Cyberterrorism is an attractive option for modern terrorists for several reasons: First, the **variety and number of targets** are enormous. Cyberterrorists could target the computers and computer networks of governments, individuals, public utilities, private airlines, and so forth. The sheer number and complexity of potential targets guarantee that terrorists can always find weaknesses and vulnerabilities to exploit. This is a continuous mouse and mice game, and the criminals are always one step ahead.

Several studies have shown that critical infrastructures, such as electric power grids and emergency services, are in fact vulnerable to a cyberterrorist attack because the infrastructures and the computer systems that run them are highly **complex**, making it effectively impossible to eliminate all weaknesses.

Third, cyberterrorism is more **anonymous** than traditional terrorist methods. Like many Internet surfers, terrorists use online nicknames or log on to a website as an unidentified "guest user," making it very hard for security agencies and police forces to track down their real identity. There are no physical barriers in cyberspace such as checkpoints to navigate, no borders to cross, and no customs agents to outsmart.

Cyberterrorism can be conducted **remotely**, a feature that is especially appealing to terrorists. Cyberterrorism requires less physical training, psychological investment, risk of mortality, and travel than conventional forms of terrorism, making it easier for terrorist organizations to recruit and retain followers.

Case studies

Just before the end of 2014, amid all the noise about the Sony breach, a quiet 2014 report[5] by Germany's Federal Office for Information Security was issued. One of the incidents described was a successful attack that infiltrated the industrial controls at an unnamed German steel mill. The attack caused 'massive' damage by making it impossible to shut down a blast furnace. Wired magazine[6] cited a translation of the report, saying it appeared that "the hackers obtained access via a spear phishing attack" before quickly moving across a "multitude" of sensitive corporate networks. Who the hackers were, how long they were in the system, whether they intended to destroy the furnace and what, if any, other equipment they accessed, and all remains unclear.

A Bloomberg News article[7] on December 10, 2014, highlighted just how destructive digital attacks can be. A recently disclosed 2008 targeted attack on the majority BP-owned Baku-Tbilisi-Ceyhan pipeline in Turkey caused an explosion with flames as high as 150 feet. At the time, Baku-Tbilisi-Ceyhan was thought to be one of the most secure pipelines in the world. Still, attackers infiltrated the pipeline through a wireless network, tampered with the systems, and caused severe physical damage.

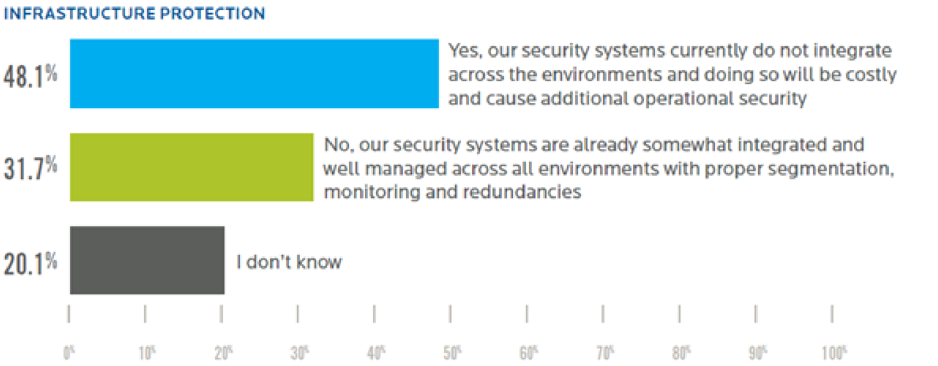
In a November 20, 2014, hearing for the House Intelligence Committee, NSA Director Admiral Michael Rogers said several foreign governments had already hacked into U.S. energy, water and fuel distribution systems, potentially damaging essential services, according to Bloomberg. "This is not theoretical," Rogers said. "This is something real that is impacting our nation and those of our allies and friends every day." In May 2014, the Department of Homeland Security and its Industrial Control Systems Cyber Emergency Response Team issued an ICS-CERT report[8] warning of several known attacks against U.S. utilities in the first quarter of 2014. They cited details of one unnamed utility that had been breached and warned U.S. utilities to be on guard for intrusion activity[9].

Studies

One national study by Newspoll asked Australians how much they would be impacted by a *two-day failure of various critical infrastructures*. The results show that the impact of a major failure of vital services would be significant on a large mass of population:

Electricity supply	84%
Water supply	80%
Banking systems	60%
Mobile phone network	46%
Internet	46%
Public transport network	27%
Capital City Airports	17%

Still – a survey of electric utility representatives in USA showed that 48% of respondents indicated they did not have integrated security systems with the "proper segmentation, monitoring and redundancies" needed for cyber threat protection. Only 32% said they had these protections in place.



Source: Black & Veatch

Respondents were asked if the expanded definition of "infrastructure protection" to include cyber, physical, corporate and control system environments and the increasingly integrated nature of infrastructure protection systems would cause additional operational security risks.

Conclusions

Despite evidence of growing sophistication in terrorists' use of the internet, the threat of a cyberterrorist attack against critical infrastructure has yet to manifest into a core national security issue[10]. Terrorist groups tend to use the internet for organizational and administrative purposes. Currently, the greatest threat that exists from cyberattacks is in the form disruptive (non-destructive) nuisance attacks that have not demonstrated a vital threat. However, the internet continues to offer terror groups wide-ranging opportunities for cyberattacks, which, if combined with the proper expertise, could potentially threaten vital national security targets.

Terror attacks are real serious threats to any country and cyber-attacks should not be treated any differently. Just because cyber-attacks do not use bombs and guns does not mean that it can be ignored or taken easily.

Every proactive step toward protecting critical infrastructure is a move in the right direction and there is no better time than now to begin.

References

[1] http://www.stealth-iss.com/documents/pdf/CYBERTERRORISM.pdf, pp. 1, last accessed 15 March 2015.

[2] To **joyride** is to drive around in a stolen vehicle with no particular goal; a ride taken solely for pleasure.

[3] http://hackmageddon.com/2015/01/13/2014-cyber-attacks-statistics-aggregated/, last accessed 17 March 2015.

[4]https://books.google.ro/books?id=bdZStsXdsikC&pg=PA55&lpg=PA55&dq=war-game+conducted+by+the+United+States+Naval+War+College+cyberterrorism&source=bl&ots=OfPYFonQB1&sig=8YqHIJ4AOu1DUGA81y1Y2SX1KnA&hl=en&sa=X&ei=3swKVYfpDNX1ap7TgNgE&ved=0CCQQ6AEwAQ#v=onepage&q=war-game%20conducted%20by%20the%20United%20States%20Naval%20War%20College%20cyberterrorism&f=false, pp.55, last accessed 19 March 2015.

[5] http://www.wired.com/wp-content/uploads/2015/01/Lagebericht2014.pdf, accessed 19 March 2015.

[6] http://www.wired.com/2015/01/german-steel-mill-hack-destruction/, accessed 19 March 2015.

[7] http://www.bloomberg.com/news/2014-12-10/the-map-that-shows-why-a-pipeline-explosion-in-turkey-matters-to-the-u-s-.html accessed 19 March 2015.

[8] http://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_%20Jan-April2014.pdf, accessed 19 March 2015

[9] http://www.tripwire.com/state-of-security/incident-detection/dhs-confirms-u-s-public-utilitys-control-system-was-hacked/, accessed 19 March 2015

[10] http://www.perspectivesonglobalissues.com/archives/fall-2010-conflict/cyberterrorism-trend-analysis/, accessed 15 March 2015

THE PROCESS OF ISLAMIC RADICALIZATION – GLOBAL THREAT AND NATIONAL DIMENSION

Sorin-Gabriel COZMA

Abstract

Islamic radicalization is one of the most dangerous threats to European security, due to the fact that, through this process, individuals with a moderate understanding of Islam adopt extremist ideology and behaviour, to the point of perpetrating a terrorist attack, on their own decision or on call from a terrorist structure.

The conflicts in the Middle East (Syria, Iraq, North Africa) brought to the forefront some terrorist entities (like Islamic State), very active and efficient in the field of online propaganda, the most important source of radicalization. The aforementioned jihadist theatres also offer a good opportunity for individuals with radical views to put into the practice these options, to continue and develop the radicalization process to the last and the most radical phases. More radicalized, with combat experience, knowledge of terrorist modus operandi, some of these individuals come back to Europe, creating significant terrorist threats.

In Romania, Islamic radicalization is apparent at a small number of peoples in different phases of the process. The radicalization includes lone individuals or small groups, created on the basis of country of origin.

The assessment of Islamic radicalization at national level, taking into consideration the number of affected peoples, the presence and action of the radicalization factors and triggers, sustain the conclusion that this process is in an initial stage and is not a major threat to our national security.

Keywords: radicalization, self-radicalization, Islamic, indicators, violence, propaganda

Introduction

Islamic radicalization represents one of the major threats to the global security environment because through this process people having a moderate approach to Islam can adopt an extremist ideology and attitude, to the point of perpetrating a terrorist attack, of their own will or at the request of a terrorist group.

At the European level, the risks are amplified by the existence of significant Muslim communities in Western and Northern European countries, who are still not integrated in the economic, social and cultural environment of those countries, and whose standards of living are below the majority of the population. Against that background, various radicalization factors can identify fertile action ground there.

Although there haven't been major attacks generated by Islamic radicalism after those that occurred in London in 2005, smaller-scale attacks took place in the UK (Woolwich), France (Toulouse), Denmark (Copenhagen), Sweden (Stockholm), Brussels (Belgium) etc. This phenomenon manifests itself differently all over the continent, but even low-risk countries cannot consider themselves secure islands in a Europe facing the threat of radicalization. This impossibility to isolate themselves from global developments is all the more obvious on the Internet, which by definition does not have limits. For this reason, it became the main source of Islamic radicalization.

Radicalization – concepts, factors and indicators

Considering the current security context, the size and forms of manifestation of terrorist threats, radicalization represents a concept highly discussed by the CT community. Many critics contest the very existence of the phenomenon per se[1], considering the term radicalization as being an arbitrary one, without a unanimously accepted definition and frequently used to negatively describe ideas / precepts that aren't accepted by others[2].

One of the most complex definitions of radicalization was provided by Charles E. Allen, "the process of adopting an extremist belief system, including the willingness to use, support, or facilitate violence, as a method to effect societal change"[3].

This definition focuses on the use of violence as a result of the radicalization process, but many researchers draw a distinction between the cognitive, conceptual (adopting extremist violent concepts) radicalization and violent radicalization (putting them into effect)[4].

Radicalization can appear in relation to certain ideologies: left / right wing, national-separatist, animal rights or one single problem ("single issue extremism"). Due to the fact that Islamic radicalization represents the topic of this review, the next term that has to be discussed is "Islamism".

We believe that one of the best definitions is that provided by Peter Mandaville: “forms of political theory and practice that have as their goal the establishment of an Islamic political order in the sense of a state whose governmental principles, institutions and legal system derive directly from the shari’ah”[5].

Another relevant term for the Islamic radicalization issue is Salafism, considered an Islamic conservative doctrine. Although undoubtedly certain Salafi structures espouse violence, Salafism is mainly an intellectual movement, which cannot be reduced to extremism and violence. A German representative described this situation by saying: “Not all Salafis are terrorists, but all terrorists are Salafis”[6]. Additionally, a study by Marc Sageman indicates that 97% of Jihadists became followers of a form of Salafism during the radicalization process. [7]

Regarding Islamic radicalization, we notice responses obtained from a radical version of Islam, reached not via intense religious studies, but via self-learning and a different manner of understanding religion.

The analysis of the radicalization factors is contested, as well. Few problems have generated as many disputes between experts within the official security, civil and academic circles, as factors that lead a person to radicalization. Some theories stress political factors, marginalization and social cleavages, sometimes seen as fundamental factors (root causes) of radicalization. Others take into consideration personal factors, such as trauma, or the influence of mentors, gurus. Other people believe that radicalization within the Muslim communities in Europe is the result of economic privations and discrimination.

Many analysts view the radicalization process as a passive one, namely that those facing this process were subjects of a brainwashing process and act automatically according to the implemented ideas[8]. In most cases of European Muslims that joined the jihad in the theatre of operations, the radicalization process took place from a bottom-up direction. Studies made by Marc Sageman and other academics emphasized that the image of the recruiting terrorist that creeps into the mosques to draw naïve believers is false[9].

In some cases, radicalization is a purely individual process (self-radicalization), the individual becoming radicalized only through the Internet; however, it usually occurs in small groups. The individuals are introduced to radical circles by friends, relatives, and radicalization takes place while interacting with people having similar views.

We should point out the following features of the radicalization process[10], which also reflect factors that act in it:

- There is no demographic pattern of radicalization; those radicalized have the most diverse economic and social background, come from educated families, but also from middle-class or under-privileged families, with a significant criminal background;
- The radicalization process usually takes place when young people, feeling frustrated because of Western society, start looking for a cause to join jihad, seeking the consolidation of their own identity; thus, they find the necessary answers in various ideologies, among them being radical Islam[11];
- Many of the young people radicalized have only vague knowledge of the Islamic religion, and extremist preachers take advantage of this situation in order to teach them a fundamentalist, extremist approach of Islam;
- The strong relations within the group seem to represent the precursors to radicalization, because the phenomenon appears sometimes in cases of members of tight groups (people frequenting certain mosques, supporters of a football team, neighborhood gangs etc.);
- A sophisticated ideology doesn't necessary represent a precursor to radical action. The psychologists contest the idea that people's behavior automatically and undirectionally derives from a well-researched system of ideas. Many times, the ideas appear after a certain way of action is carried out (they become followers of violent ideologies after already being involved in violent acts). Many people share violent concepts, but they rarely resort to violence / become violent. If all people supporting Jihad on the Internet put their concepts into practice, the world would be full of terrorists.

In conclusion, the factors determining radicalization include identity crises, personal traumas, discrimination, and segregation, and alienation, deception regarding Islam or Western foreign policies.

However, most experts agree that radicalization is a complex and individualized process, sometimes determined by the interaction of structural and personal factors. Thus, there is neither a standard path to radicalization nor a common profile, and each case must be individually analysed.

The last concept that must be approached is the one of **indicators** of the radicalization phenomenon. Although this is also contested, it is unanimously accepted that a person facing a process of radicalization (irrespective of the stage) acts differently regarding oneself before the beginning of the process.

There is a series of changes in the behaviour of the subject facing a radicalization process, which represent indicators of this process; they are not necessarily clear, because one or many indicators don't necessarily lead to the conclusion that the person in question is facing a radicalization process (for example, there are many people with a poor financial situation, with a low level of education, with a background touched by trauma etc., but these factors don't necessarily determine the start of a process of radicalization).

Although the radicalization/self-radicalization process is a cognitive one, its main manifestations occur at the behavioural level, making visible changes in the life of the person that is facing this process.

We emphasize the fact that these indicators of radicalization can individually or cumulatively manifest at various levels and more or less visibly, depending on the individual's background, his personality, temper, his resistance to changes, the event that persuaded him to seek such a radical change etc.

Precarious security situations in proximity to Europe – radicalization sources

The developments near Europe's border provide opportunities for radicalized people to travel to theatres of conflict in order to put into practice their radical ideas, these theatres being areas where the radicalization and indoctrination process continues and develops up to the final phases. Additionally radicalized, with battlefield experience and having knowledge of terrorist MOs, some of these people return to Europe. The *returnees* represent the most significant terrorist threat to the European and Euro-Atlantic security space, and have already conducted the first terrorist attack in Europe (May 2014, Brussels).

The developments in Syria, Iraq or Northern Africa have impelled in the first line terrorist structures that are very attractive to radicalized people in Europe and are present and active online, the Internet being the most important source of radicalization.

The most significant jihadist theatre close to Europe is Syria/Iraq, a transnational area that actually represents the new centre of the jihadist activity in the world, and outclasses theatres of war such as Afghanistan, Pakistan, Yemen, Mali etc. The area of Syria/ Iraq can be compared with Afghanistan in the 1980s, and even outclasses it in regard to the massive presence (thousands of people) of some fighters originating from European countries.

In Syria / Iraq, the terrorist organization which is most visible at the moment (significantly exceeding Al Qaida from this point of view), the Islamic State, operates a newly established terrorist structure, whose roots are in the AQ in Iraq. On June 30, 2014, by means of a video posted online[12], the group proclaimed the establishment of an Islamic caliphate in the territories under its control, changing its name into the Islamic State (IS). Taking advantage of its rapid advancement in Iraq, and the fact that it controls a large territory (approx. equivalent to the surface of Great Britain), the group rapidly became attractive for radicalized people / jihadists worldwide, including from Europe.

The latest assessments[13] indicate that IS might have 20,000-31,500 fighters (more than the 10,000 previously announced), including 2,000 people coming from Europe.

The main arguments IS used to mobilize such a large support and become the main destination (and also source) of radicalized individuals are:

- The proclamation of the Islamic caliphate, the prime objective of any Jihadist, in a central and historical area of Islam and of the first caliphates. The ambition of Caliph Baghdadi is to reunite within this caliphate all territories that are or were Islamic land, including Romania;
- Implementing in the territories under their control (Rakka, Mosul, etc.) the Islamic principles and shari'ah. In Rakka, for example, the actions taken to impose the Islamic law are very drastic: women must wear black clothing, and only their eyes can be visible, the prayer hours must be strictly obeyed, the death penalty is put into practice, including for accusations of "disbelief";
- The extreme violence of the organization. According to the director of BvF, the German Intelligence Service[14], young Muslims are attracted by the violence, radicalism and rigour of IS, features which make the organization appear more "authentic" than AQ. The extreme violence seems to be the main and almost the only doctrinal innovation of IS; by killing people in a medieval manner, IS seems to draw attention to its attempt to resurrect the medieval caliphate[15], considered the golden era of the Muslim world;

- The intense ongoing propaganda of IS and even its leader, Baghdadi, mostly through the Internet. The group knew how to efficiently use Twitter to announce and spread among the Muslim communities in the West its rapid accession in Iraq, and the subsequent blocking of the organization's Twitter accounts had no other result than to redirect the online propaganda to other social platforms (Facebook, Youtube, and Diaspora – a social platform known for respecting the users' privacy)[16]. The beheadings of some Western nationals represent sophisticated, professional "productions", full of symbols, (the orange clothes of the hostage, the British accent of the terrorist etc.)[17], highly effective on the Internet;
- Operational action directions. As opposed to AQ (which mainly targeted the Western enemy – especially the United States), IS has mainly focused on regional targets, more concrete and tangible, trying to remove the governments from its area of operations, and announced the caliphate as soon as it managed to control a transnational area[18].
- The good financial situation, which allows IS to appropriately pay its fighters. Apart from the financial resources obtained after taking control of the banks based in Northern and Western Iraq, as well as exploiting the oil resources, there are suspicions that IS receives funds from Saudi Arabia and Qatar. Thus, the Islamic State is probably the richest terrorist organization in the region.

Radicalization – national dimension

In Romania, Islamic radicalization has not become a phenomenon, but people at various radicalization stages have sometimes been identified. Their number is small, and the radicalization takes place individually or in small groups, usually set up based on their origin.

Due to the fact that the study's topic is Islamic radicalization (but not extremist manifestations generated by left/right wing ideologies), the radicalization cases within the Muslim community in Romania are the only ones of interest here.

This community is comprised of approx. 75,000 individuals, most of them belonging to the Turkish-Tartar community established long ago in Romania. It is well integrated, practices a moderate Islam and radical individuals originating from it are extremely rare. The radicalization cases mainly appear in the foreign Muslim community, people originating from areas facing terrorist risk, and that came in contact with terrorist ideologies.

To a lesser extent, some radicalization cases were in connection to Romanian nationals converted to Islam. In this case, it was noticed that the interest of those people in integrating and manifesting within the new community determines them to adopt a radical view of Islamic concepts, being predisposed to a (self) radicalization process.

Besides the fact that few cases appeared in Romania, other aspects defining radicalization on our national soil are as follows[19]:

- The expression of radical points of view mainly takes place in private, in small circles[20]. Set up on the nationality criterion (area of origin), such groups mainly target discussions about the developments in their areas of origin, and on those occasions they support violent solutions or terrorist organizations;
- Correlated with the first feature, it is stressed that mosques (Islamic centres) have only a small role in the radicalization process; they sometimes play an important role in the West, though, given their facilities (interaction between Muslims, direct contact with people sharing the same values). In Romania, the mosques act as meeting places for the Muslim community's members, but we could notice radicalization factors acting within them only in some isolated cases;
- We noticed radical tendencies especially during tense moments within the community in question. Due to the fact that, at the national level, no factors similar to the Islamic veil in France, the minarets in Switzerland etc. were identified, such triggers have external origin, including crisis situations in their area of origin. Recent cases, identifiable in the public sphere, include the crisis situations in Syria, Iraq, Gaza Strip etc.

The messages are reactive, and thus the absence of some constant radicalization sources on national soil can be noticed;

- In most cases, the tendencies to violent acts remain just verbal declarations and target the situation in the country of origin; we noticed violent tendencies regarding Romania only in a few particular cases, mainly regarding the Romanian troops deployed in the operation theatres in Muslim areas. Such a case of radicalized individuals willing to take action was identified in December 2012, when foreign nationals Muhamad Ramzan and Adel Muhamad carried out preparatory activities in order to conduct terrorist attacks in Romania during the winter holidays[21];

- Similar to the European level, a high level of risk is generated by the self-radicalization cases, when people - that aren't present in circles with radicalization potential and thus aren't monitored by the security structures - can become radicalized through the Internet (propaganda materials). Such a case is the Iraqi national Khzr Karim Friad, resident in Finland, who intended to conduct a terrorist attack targeting a diplomat of a Western embassy in Bucharest, and was identified by security personnel in the vicinity of the embassy. No intelligence was revealed previous to this attempt regarding the terrorist risk posed by this person[22];
- The radicalization process mainly targets young people that came to Romania by means of illegal migration or legal routes (for studies, businesses etc.), having previous contacts or keeping in contact during their stay in Romania with radical elements outside our country, directly or through the Internet;
- The circles where radicalization factors emerge, as well as individuals facing various stages of radicalization, usually include mosques, Islamic nongovernmental organizations, and asylum centres for immigrants, prisons, circles frequented by the converted persons etc.

A short review of some individuals' radicalization process in Romania can better outline the size and ways of manifestation of the phenomenon in our country.

The first case of a Romanian citizen becoming radicalized was Florin Lesch – sentenced to 12 years' imprisonment for terrorism, in November 2007, following his attempt to organize a terrorist attack in Timişoara, by detonating a car where an IED was placed.

Converted to Islam in the late 1990s, he represents a "classic" model: his father died when Lesch was a child, his family faced financial difficulties; he personally had problems with the law (in 1992 he was imprisoned for 6 months for trying to fraudulently cross the state's border), displayed a violent behaviour and was a difficult person etc.

Since the early 1990s, he showed interests in the Islamic religion, but due to the fact that he didn't have solid knowledge in this area, he rapidly adopted extremist views. He changed his name to Aynan Hassan Abger, and was active on a series of forums of Muslims who had fought in Bosnia war. Before leaving to carry out the terrorist attack, Florian Lesch said goodbye to his mother and girlfriend and posted a threatening message on the Internet, which expressed that if the "Islamist brothers are not left alone, we are prepared any moment in Romania[23]".

Other recent cases of foreign citizens with legal residence in Romania are as follows:

- Muhamad Ramzan, a Pakistani citizen, who came to Romania in 2008, as postgraduate within a program financed with EU funds. Apparently well integrated, Muhamad Ramzan learned to speak Romanian very well, and did not arouse any suspicion among his colleagues and teachers from the University in Sibiu. In December 2012, he was declared undesirable for 15 years, because he had helped prepare terrorist attacks on Romanian soil during the winter celebrations, aiding an extremist structure ideologically affiliated to Al Qaeda.
- Ghouila Tarek, of Tunisian origin, came to Romania on a study visa, he didn't try to radicalize people in Romania, but operated as a "lone actor". As a high-ranking member of on-line media influenced by the AQ ideology, Ghouila Tarek promoted terrorist and extremist messages and also recruited people for jihad; he held information on the means and methods of carrying out terrorist attacks, which included outlines and video documentaries on the manufacture of IEDs[24].

Taking into consideration the radicalization cases in Romania, SRI, as the national authority for preventing and countering terrorism, started taking advantage of opportunities offered by the European programs regarding radicalization, emphasizing RAN and CoPPRa.

Starting from the stipulations of the EU Internal Security Strategy ("the empowerment of the communities in order to prevent radicalization and recruitment"), in 2011, EC established the RAN platform, as an umbrella-network for discussions and exchange of good practices for preventing and countering radicalization. The project is developed through eight working groups; SRI participates in the works of some of these groups and is going to participate in a number of projects developed by RAN, with European financing.

CoPPRA (Community Policing Preventing Radicalization), established by Belgium, seeks means to counter radicalization prevent people from reaching the final stage of violent manifestation. SRI actively participated in the *train-the-trainers* activities organized by CoPPRa.

Through these projects, developed in cooperation with other institutions and authorities within the National System for Preventing and Combating Terrorism, we aim to identify as early as possible the individuals who are going through a radicalization process; we aim to take the necessary measures against their radicalization and to prevent their involvement in violent action.

Acknowledgements: This paper is made and published under the aegis of the Research Institute for Quality of Life, Romanian Academy as a part of programme co-funded by the European Union within the Operational Sectorial Programme for Human Resources Development through the project for Pluri and interdisciplinary in doctoral and post-doctoral programmes Project Code: POSDRU/159/1.5/S/141086

References

[1] Mark Sedgwick, "The Concept of Radicalization as a Source of Confusion", *Terrorism and Political Violence*, vol. 22, no. 4 (2010), pp. 479–494.

[2] Moreover, some critics emphasize that the term's essence has changed during the time. For example, at the beginning of the twentieth century, the label was put on the Suffragette organization, which militated in favor of the female right's vote. Moreover, ideas that seem radical for one culture, can be seen as normal by a different one. Lorenzo Vidino, "Jihadist Radicalization in Switzerland", Center for Security Studies (CSS), accessed 5 September 2014 at http://www.css.ethz.ch/publications/pdfs/CH_radicalization_report.pdf.

[3] Charles E. Allen, *Threat of Islamic Radicalization to the Homeland, Testimony before the U.S. Senate Committee on Homeland Security and Government Affairs*, March 14, 2007, p. 4.

[4] The International Centre for the Study of Radicalization and Political Violence (ICSR), *Countering Radicalization in Europe,* 2012, accessed 3 October 2014 at http://iscr.info/wp-content/uploads/2012/12/icsr-report-countering-radicalization-in-Europe.pdf, p. 9

[5] Lorenzo Vidino, op. cit., p. 21

[6] *Ibidem,* p. 22.

[7] Marc Sageman, Understanding Terror Networks, (Philadelphia: University of Pennsylvania Press, 2004), p. 93.

[8] Artis Research & Risk Modeling, *Theoretical Frames on Pathways to Violent Radicalization*, August 2009, accessed 3 October 2014 at http:// www.artisresearch.com/articles/artis_theoretical_frames_August_2009.pdf, p.11

[9] Lorenzo Vidino, op. cit., p. 23.

[10] Artis Research & Risk Modeling, *op. cit.*

[11] Tomas Precht, *Home grown terrorism and Islamist radicalization in Europe,* Research report funded by the Danish Ministry of Justice. December 2007, accessed 17 May 2014 at http://www.justitsministeriet.dk/sites/default/files/media/arbejdsom/raader/forskning/forskningspuljen/2011/2007/Home_grown_terrorism_and_Islamist_radicalization_in_Europe_._an_assesment_of_influencing_factors_2_.pdf.

[12] The Guardian*, Isis announces Islamic caliphate in area straddling Iraq and Syria*, 30 June 2014, accessed 4 September 2014 at http://www.theguardian.com/world/2014/jun/30/isis-announces-islamic-caliphate-iraq-syria

[13] CNN, *How foreign fighters are swelling ISIS ranks in startling numbers*, accessed 7 October 2014 at http://edition.cnn.com/2014/09/12/world/meast/isis-numbers/

[14] First Post, *Top German spy says Islamic State's brutality eclipses al Qaida,* accessed 1 September 2014 at http://www.firstpost.com/world/top-german-spy-says-islamic-states-brutality-eclipses-al-qaeda-1690347.html

[15] The Telegraph*, David Haines murder: miscalculation or desperation?,* accessed 15 September 2014 at http://www.telegraph.co.uk/news/worldnews/middleeast/iraq/11095956/David-Haines-murder-miscalculation-or-desperation.html

[16] BBC News, *Islamic State shifts to new platforms after Twitter block*, accessed 22 September 2014 at http://www.bbc.com/news/world-middle-east-28843350

[17] Robert Kaplan, *Terrorism as a theater*, Stratfor, 27.08.2014, accessed 12.09.2014 at http://www.stratfor.com/weekly/terrorism-theater

[18] Jane's Terrorism and Security Monitor, *Crossing the borders: Campaign conducted by the Islamic State to reconfigurate the borders of Levant*, accessed 20 August 2014 at http://www.janes.com

[19] The main features of the radicalization phenomenon in Romania were obtained from the SRI press releases that emphasize the implementation of measures in the terrorist field (available at http://www.sri.ro/comunicate-de-presa/comunicate-si-declaratii-de-presa.html, accessed 11 October 2014), as well as from other data and reviews available on the Internet.

[20] SRI press release of 6 November 2013, accessed 8 October 2014 at https://www.sri.ro/comunicat-de-presa-09-11-2013-13-18.html

[21] SRI press release of 6 December 2012, accessed 8 October 2014 at http://www.sri.ro/comunicat-de-presa-06-12-2012.html

[22] SRI press release of 5 December 2012, accessed 8 October 2014 at http://www.sri.ro/comunicat-de-presa-12-15-2012.html

[23] Adevărul, *Florin Lesch wanted to punish Romania for its relations with SUA*, accessed 8 October 2014 at adevarul.ro/news/societate/florin-lesch-voia-pedepseasca-romania-relatiile-sua-1_50ac10e07c42d5a66384734c/index.html.

[24] Mediafax, *Tunisian suspected of terrorism, declared undesirable. SRI announces that he recruited followers of jihad*, accessed 8 October 2014 at http://www.mediafax.ro/social/tunisian-suspectat-de-terorism-declarat-indezirabil-sri-anunta-ca-acesta-recruta-adepti-ai-jihadului-11266982

ANOMALY DETECTION: SPOTTING TERRORISTS

Davide BARBIERI[*]

Abstract

Classification is a common task in data mining: it consists in predicting the class of an instance (for example the medical condition of an individual) by means of inductive learning and on the basis of previously collected data. The aim of this paper is to explain how this technique can be applied to the detection of criminal behaviours. The peculiarity of this application lies in the asymmetry of its distribution, where the positive class (criminals) has a much lower frequency than the negative class (non-criminals). This is especially true when dealing with terror-related activities and subjects, whose behaviour is so far from the norm that it is more proper to speak of anomaly detection than basic classification, where all classes have a similar frequency. In anomaly detection, some issues must be faced in order to succeed: (i) the measures to be chosen to assess the performances of a classification model (accuracy may in fact be misleading), and (ii) the methodology and algorithm to be adopted to build a model. These issues will be taken into proper consideration in the present study.

Keywords: intelligence analysis, classification, anomalies, accuracy, hit rate

Introduction

Data mining consists in extracting implicit - but hidden or previously unknown - and actionable information from large data sets (Witten & Frank 2005, p. xxiii), usually in order to support the decision-making process. Data mining is performed by means of machine learning, a sub-field of computer science (and specifically of artificial intelligence). Its aim is to develop algorithms which can "learn" inductively from data that is from empirical evidence, instead of simply applying hard-coded rules deductively, as it can be easily done by computers to perform mathematical calculations.

[*] PhD, University of Ferrara (Italy).

Deduction is a kind of logical inference which starts from general premises in order to come to particular conclusions. It is widely used in intelligence analysis, when, given some general rules, analysts try to identify potential dangers to national security in a specific case. Deduction is a logically necessary inference: conclusions are true if the premises are true. Still, even if the logic is valid, the conclusion may be wrong because the general premises are wrong. For example: "All people who carry weapons are terrorists. John carries a rifle. Then John is a terrorist". Obviously, not all people who carry rifles are terrorists. The premises are a prejudice and John may be a soldier.

Conclusions may be wrong even if the premises are true, if the deduction is not correct. For example: "All terrorists use weapons. John carries a rifle. Then John is a terrorist". A rifle is certainly a weapon, but John may be a hunter. Thus, even if we can rightfully assume that a terrorist is someone who is going to harm us someway by means of any kind of weapon, the conclusion may be wrong because the logic is wrong. The given example describes a common deductive fallacy, which is known as *affirming the consequent* (for a thorough description see Greenland 1998).

The general framework of classic statistical analysis is mainly deductive, since it tries to verify in a sample the accuracy of general hypotheses, and eventually reject or accept them. This *hypothesis-driven* approach is partially limited by the creativity of the analysts and their capability of finding solutions to well defined problems.

Data mining instead is less bound to pre-assumptions, because its approach is *data-driven*. Analysts admit they do not know much about terrorists. They collect as many data as possible in order to learn more about their domain of interest (e.g. national security, counter-terrorism etc.). Then, they try to build hypotheses, i.e. to come to general conclusions from many particular observations. This is how machine learning algorithms work (Witten & Frank 2005, p. 29). Induction is not logically necessary - as deduction - but only likely. Still, if the amount of available evidence is large, predictive accuracy can be significantly high.

The purpose of this paper is to show the possibility of a data-driven approach to intelligence analysis, in particular to the identification of potentially dangerous individuals. This approach bears some resemblance to medical diagnostics, a fact that will be highlighted in the paper. The main prerequisite for its adoption is that the amount of collected data about persons of interest is “large”. In other intelligence tasks (for example, in *early warning*), where it is not feasible to collect large amounts of evidence, other approaches (like Bayesian inference, see Barbieri 2013) can be adopted.

Class imbalance

Classification - a common task in data mining – consists in predicting the *class* of new instances on the basis of previously collected data. For example, in medical diagnostics, doctors may want to predict whether an individual is ill or not given the results of some medical examinations, like blood analysis, x-ray etc. This is a kind of binary classification. In fact, there are only two possible outcomes: positive or negative. Similarly, in order to profile potential terrorists, intelligence analysts need to collect information about suspects and convicted subjects. The classification algorithm will try to build a model - or *classifier* – evaluating the attributes which describe persons of interest. Applying the model to new instances, it will be possible to classify them. For example, cybercrime rates and socio-economic characteristics of the area from which an attempt to access a server comes can be used to classify the request as normal or threat (Kianmehr & Koochakzadeh 2012).

Basic classification is applied to samples in which classes have more or less the same frequency. In many real world applications though, there is a majority class and a minority class. Instances belonging to the majority class have a higher frequency compared to instances belonging to the minority class. Thus, the majority class is better represented, because it was possible to collect a large amount of data about individuals belonging to that class. For example, in diagnostics the healthy - or negative - subjects are well represented, while the positive ones are not (Figure 1), especially if the disease is rare.

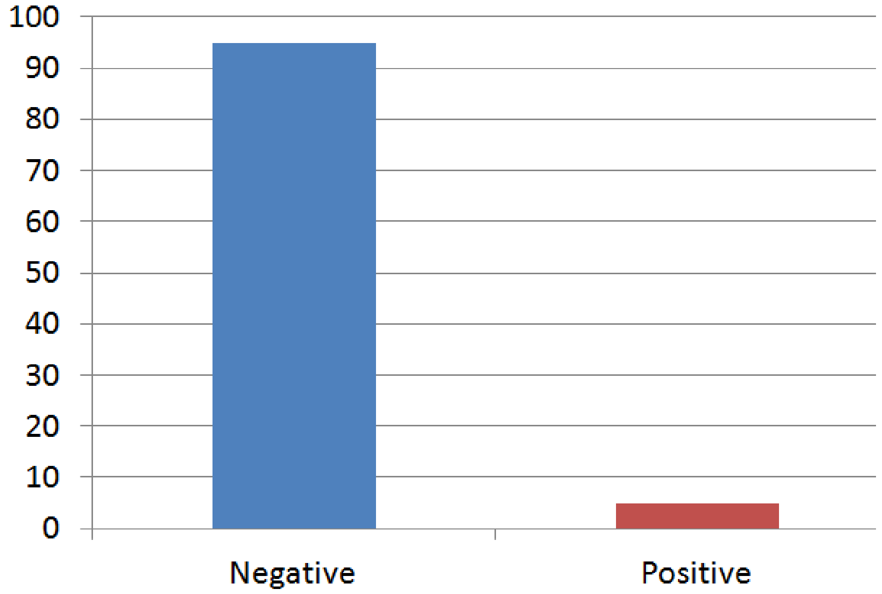


Figure 1. Class imbalance

Something similar may happen in intelligence analysis, since in this activity it is important to correctly recognize the terrorists, those belonging to the positive class. Luckily, terrorists are a small minority compared to the rest of the population: they can be considered exceptions or anomalies, individuals whose behaviour is far from the norm, which in statistics is represented by the majority class, the most frequent, or *mode*. The negative side of this situation is that they are not well represented: no matter how many data have been collected, if class distribution is highly imbalanced, any statistical or data mining method will always have a harder time recognizing individuals belonging to the minority class than those belonging to the majority. Therefore, in such a case, classification becomes *anomaly detection* which has some peculiarities (for a review, see Chandola et al. 2009, Patcha and Park 2007). In particular, one of the main related issues is how to measure the performances of the detection process.

Measuring performances

In binary classification, performances are assessed on the basis of the following “confusion matrix”:

	Actual positive	Actual negative
Predicted positive	TP	FP
Predicted negative	FN	TN

Table 1. Confusion matrix

TP stands for true positives (positive instances correctly classified as such), TN for true negatives (negative instances correctly classified as such), FP for false positives (negative instances misclassified as positive) and FN for false negatives (positive instances misclassified as negative). As it usually happens with imbalanced data sets, classification errors may have different costs. A false alarm (FP), i.e. searching an extra individual at the airport or prescribing an extra medical examination, has a smaller cost than missing a terrorist (FN) or diagnosing as healthy a subject with cancer. One miss may result in loss of human lives.

A basic parameter for the evaluation of a predictive model is *accuracy* (ACC), which is defined as follows:

$$ACC=(TP+TN)/(P+N)$$

where P is the number of positive instances and N is the number of negative instances. In other terms, accuracy is the number of correct predictions divided by the total number of instances (positives and negatives). Though widely adopted in classification as a measure of performance (Rahman & Davis 2013), in anomaly detection it may be misleading. For example, if positive instances are only 1% or less of the total, and we always declare a new instance as negative, accuracy will be 99% or higher: an outstanding performance in predictive analysis. Still, we would be missing all the interesting instances.

Therefore, in case of highly imbalanced data sets, different measures of performances must be chosen, especially if the costs of errors are different and there is one class which is more interesting than the other one. For example, we may use the *hit rate*, or True Positive Rate (TPR), which is defined as follows:

$$TPR=TP/P$$

TPR is the rate of positive instances correctly classified as such. TPR also represents the *sensitivity* of a model. The True Negative Rate (TNR) represents instead the rate of negative instances correctly classified as such, or *specificity*:

$$TNR=TN/N$$

Unfortunately, when TPR increases, the rate of false alarms, or False Positive Rate (FPR), increases. FPR is defined as follows:

$$FPR=FP/N$$

In order to improve the hit rate, the sensitivity of the predictive model is increased, thus increasing FPR and reducing specificity (in fact TNR=1-FPR). A typical “cry wolf” situation may take place, where all subjects are considered to be terrorists. Even if it may have a lower cost than the opposite situation, it is not feasible in practice, because of the limited amount of government resources that intelligence and law enforcement agencies have at their disposal. It would probably require an excessive amount of time. Further, considering all citizens as criminals is not an accepted policy in democratic countries.

So, even if the hit rate is our first choice, in order to measure the effectiveness of a model, a compromise with FPR must be found. Such a trade-off can be represented in *Receiver Operating Characteristic* (ROC) space (for an introduction see Fawcett 2006), which is the accepted standard in assessing anomaly detection (Chawla 2005, Fawcett & Provost 1999), especially in diagnostic systems (Swets 1988). Always predicting negative corresponds to (0,0) in ROC space, which means no false alarms but also no hits, while always predicting positive corresponds to (1,1), which means 100% hit rate, but also 100% FPR. The perfect classifier would be in (0,1), having 0% FPR (x-axis) and 100% TPR (y-axis).

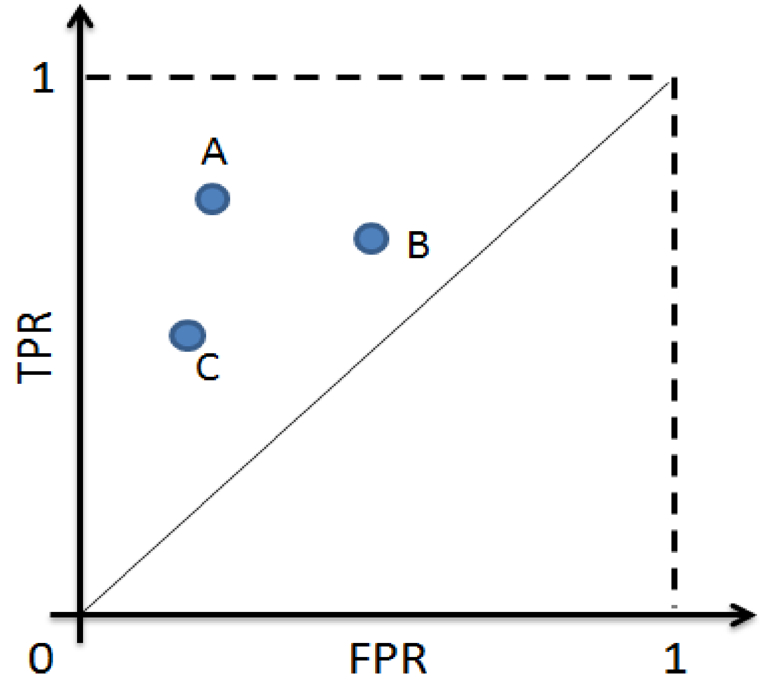


Figure 2. Receiver Operating Characteristic

In practice, classifiers close to the upper left are preferred to classifiers towards the 45° line, which corresponds to random guessing. In Figure 2, classifier A outperforms both B and C, having a higher TPR (hit rate) and a lower FPR (less false alarms) than B, and a higher TPR than C, with a similar FPR. In order to improve the performance of a classifier, i.e. to increase the hit rate (moving up in ROC space) without considerably worsening the rate of false alarms (moving right in ROC space), different methods may be employed.

Methodology

Imbalanced data sets can be managed adopting different strategies. Some algorithms may perceive anomalies as *noise* (like human errors in data entry) and not as suspects, and therefore ignore them. Thus, the choice of the right classifier is particularly important.

We speak of *unsupervised* anomaly detection when the chosen algorithm does not need pre-classified data (i.e. data which have already been labelled as positive or negative). It makes the assumption that the majority of individuals in a sample are to be considered normal. It may then identify the abnormal instances because they are someway "far" from the rest of the sample, according to the principle of strong cohesion within classes and weak coupling between classes. Algorithms of this kind are called *clustering techniques*, rather than classifiers, and many of them are distance-based. In case of anomaly detection, such algorithms identify only two clusters, corresponding to negative (normal) and positive (abnormal) instances. As usual, errors of different kinds and cost, false alarms and false negatives, may be present (Figure 3). Unsupervised approaches are widely used in the detection of suspicious activities (Witten & Frank 2005, p. 357; Elovici et al. 2004), especially in web intelligence (Last et al. 2003).

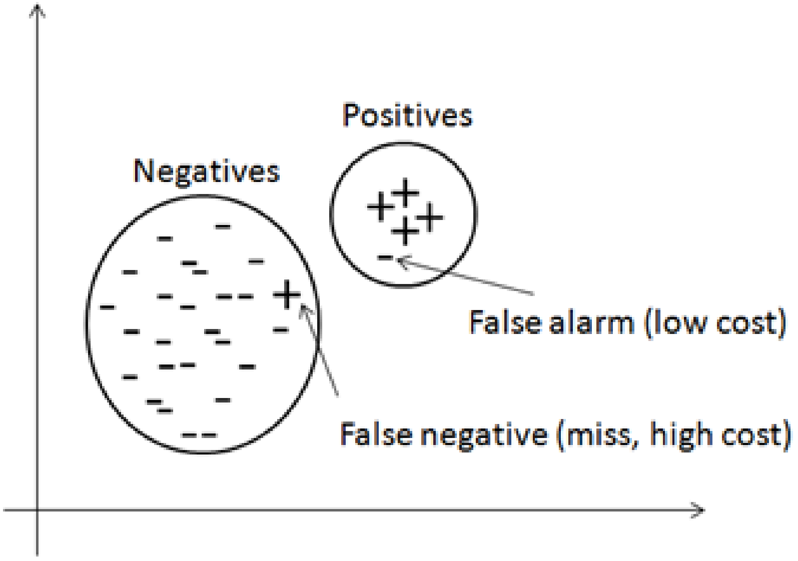


Figure 3. Clustering

Supervised anomaly detection instead needs pre-classified data in order to predict the class of new instances. If only data on the negative/majority class are available, then we speak of *semi-supervised* anomaly detection. This situation may be frequent, since data on the positive class are lacking. With this approach, all new instances which do not fall into the negative class are automatically classified as positive.

Classification is a typical example of supervised learning. A set of collected data, containing several instances of both classes, is divided into training and test (Figure 4). Usually, the test set size is approximately 30% of the given data set. Training data are supplied to the learning algorithm, which produces a model that can distinguish between positive and negative instances on the basis of the attributes (or *features*) of the collected instances. Then, test data are given to the trained model in order to classify them. Since the true class of each instance in the test set is known, it is possible to verify the performances of the model.

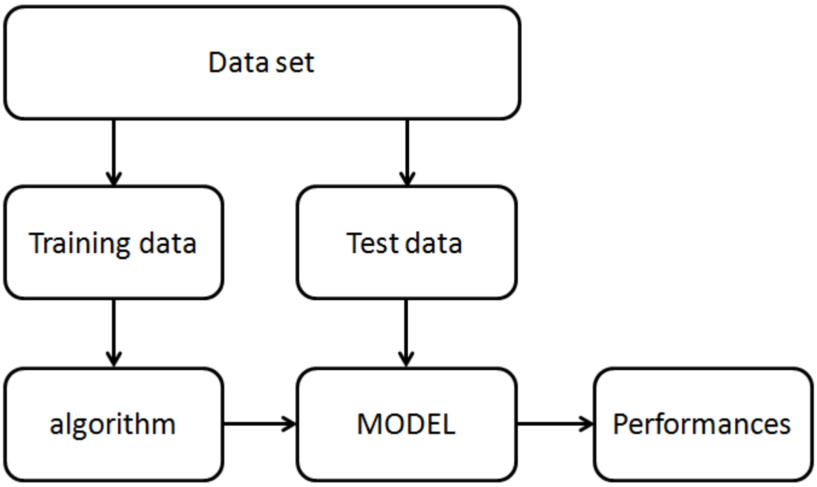


Figure 4. Classification

Nonetheless, analysts must deal with the skewness of data. Two possible re-balancing approaches can be adopted, in order to increase the sensitivity of the algorithm to positive instances. The first and most obvious option is random *under-sampling* of the majority class. Unfortunately, under-sampling reduces the amount of information on the negative class, which usually results in diminished TNR (the capability of identifying negative instances). As specificity decreases, false alarms increase.

The second option is *over-sampling* the minority class, increasing the number of positive examples. This can be done duplicating existing instances. Still, redundant information on positive examples may result in *over fitting*: the model becomes excessively complicated, adapting tightly to past data, and it will not generalize well on new, incoming instances. A possible smart way of over-sampling the minority class is to use the *Synthetic Minority Over-sampling Technique* (SMOTE, Chawla et al. 2002). SMOTE does not simply duplicate positive instances, but creates new examples, similar to existing ones, thus diminishing the risk of over fitting.

For example, sport medical doctors may have collected some anthropometric data like height and weight (h, w) from a large sample of athletes. Some of the individuals are actually champions (i.e. anomalies) of a given sport. The feature vectors associated with two positive instances are A(180 cm, 72 kg) and B(175 cm, 70 kg). A is the starting instance and B its nearest neighbour. The *distance* between the two vectors is computed as δ(A, B)=B-A=(175-180, 70-72)=(-5 cm, -2 kg). Then, the following equation is applied in order to create a new positive instance C (a *virtual champion*):

$$C(h, w)=A+\delta(A, B)\cdot \mathit{Rand}(0\text{-}1)$$

where *Rand*(0-1) is a random number between 0 and 1. In case it is 0.5, the new instance will be described by the feature vector C(h, w)=(180, 72)+(-5, -2)·0,5=(177.5 cm, 71 kg), which is a point on the line connecting A and B (Figure 5). In order to double the number of minority class examples, the procedure described above is replicated for each existing positive instance.

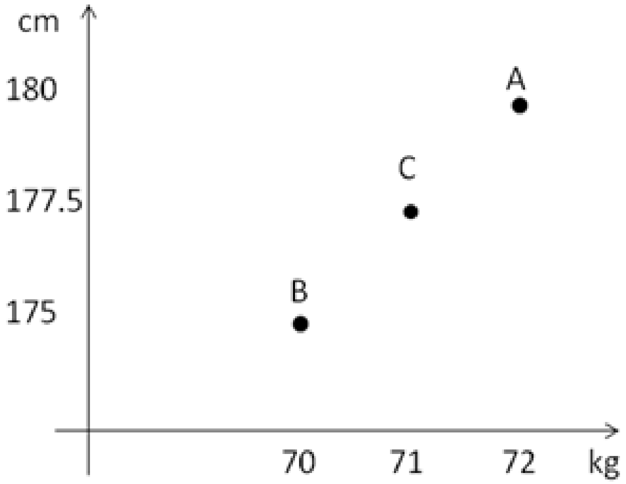


Figure 5. SMOTE: creating positive instances

Anthropometric (i.e. numeric) data may have a role in the identification of sport champions (especially if they have uncommon physical characteristics), but they are of little use in detecting terrorists. Therefore, some nominal attributes (like political inclination, nationality and sex) may be added to profile interesting individuals. In order to deal with nominal values, the following equation (Cost & Salzberg 1993) may be applied to compute distance on the basis of relative frequencies:

$$\delta(V_1, V_2) = \left| \frac{C_{1p}}{C_1} - \frac{C_{2p}}{C_2} \right| + \left| \frac{C_{1n}}{C_1} - \frac{C_{2n}}{C_2} \right|$$

where V_1 and V_2 are the two possible values of a feature. For example, if the chosen feature is political inclination, then V_1 may be “moderate”, while V_2 may be “extremist”. C_1 is the count of feature value V_1 in the given data set (overall amount of moderates), while C_2 is the count of feature value V_2 (overall amount of extremists). C_{1p} is the count of feature value V_1 in the positive class (number of moderates who are terrorists), while C_{2p} is the count of feature value V_2 in the same class (number of extremists who are terrorists). C_{1n} is the count of feature value V_1 in the negative class (number of moderates who are not terrorists), while C_{2n} is the count of feature value V_2 in the same class (number of extremists who are not terrorists).

A combined approach is possible, applying first over-sampling and then under-sampling, in order to minimize the amount of information loss. This approach has produced good results, in terms of both accuracy and hit rate, for instance in medical diagnostics (Barbieri et al. 2014).

Beside re-sampling, the parallel adoption of different classification algorithms - i.e. *meta-learning* - is another approach to supervised anomaly detection which has proved to be successful, especially for fraud detection (Phua et al. 2004).

Conclusions

Classification is a common data mining task which can be adopted in intelligence analysis, particularly in the detection of dangerous individuals, provided that large amounts of information on persons of interests have been previously collected. Prediction may be become increasingly difficult with data skewness. If the positive and usually more interesting class, is extremely under-represented - as it can happen in matters of national security and counter-terrorism - we can speak more properly of anomaly detection.

In this case, accuracy is not a sensible measure of performance. Rather, a compromise between hit rate (i.e. the amount of positive instances correctly classified as such) and false alarms must be taken into consideration. ROC space can be used to identify the best trade-off. It should be noted that errors of different types (i.e. false alarms and false negatives) may have different costs, as it happens in both medical diagnostics and intelligence analysis, when misclassifying positive individuals may cause the loss of human lives.

The choice of the proper classification algorithm to be adopted should take into consideration class imbalance, and the fact that some classifiers may perceive minority class examples as noise. At the same time, re-sampling techniques can be employed to balance the data set and improve the hit rate, without significantly increasing the rate of false alarms or over fitting. Future research should focus on multinomial features, which are commonly used to describe potential threats and suspicious individuals, either improving existing distance-based algorithms or devising new techniques.

References

1. Barbieri D, Sindik J, Matovinović Osvatić M, Ferriani S, „Analyzing growth: A data-driven approach", in *Proceedings of the International Congress of Human Growth and Clinical Auxology*, ISGA XIII, Maribor 17-20 Sept. 2014.

2. Barbieri D, „Bayesian Intelligence Analysis", in *Proceedings of the 19th Conference on Intelligence in the Knowledge Society*, Bucharest, Romania, 18th October 2013.

3. Chandola V, Banerjee A & Kumar V, „Anomaly detection: A survey", *ACM Computing Surveys*, 41, 3, Article 15, July 2009.

4. Chawla NV, Bowyer KW, Hall LO, Kegelmeyer WP, SMOTE: Synthetic Minority Oversampling Technique, „Journal of Artificial Intelligence Research", 16: 321-357, 2002.

5. Chawla NV, Data Mining for Imbalanced Datasets: An Overview, in Maimon O & Rokach L (eds.), *Data Mining and Knowledge Discovery Handbook*, Springer (USA), pp. 853-867, 2005.

6. Cost S & Salzberg S, A Weighted Nearest Neighbor Algorithm for Learning with Symbolic Features, *Machine Learning*, 10(1):57-78, 1993.

7. Elovici Y, Kandel A, Last M, Shapira B & Zaafrany O. Using data mining techniques for detecting terror-related activities on the web. *Journal of Information Warfare*, 3(1), 17-29, 2004.

8. Fawcett T, An introduction to ROC analysis, *Pattern recognition Letters*, 27:861-874, 2006.

9. Fawcett T & Provost F, Activity monitoring: noticing interesting changes in behavior. In *Proceedings of the 5th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*. ACM Press, 53–62, 1999.

10. Greenland S. Induction versus Popper: substance versus semantics. *Int J Epidemiol*. 1998 Aug; 27(4):543-8.

11. Kianmehr K & Koochakzadeh N, Learning from socio-economic characteristics of IP geo-locations for cybercrime prediction, *International Journal of Business Intelligence and Data Mining*, Vol. 7, Nos. 1/2, 2012.

12. Last M, Shapira B, Elovici Y, Zaafrany O, Kandel A, Content-Based Methodology for Anomaly Detection on the Web, in Menasalvas E, Segovia J, Szczepaniak PS (Eds.) *Advances in Web Intelligence*, Springer Berlin, Heidelberg, pp. 113-123, 2003.

13. Patcha A & Park JM, An overview of anomaly detection techniques: existing solutions and latest technological trends, *Journal of Computer Networks*, Vol. 51, No. 12, pp.3448–3470, 2007.

14. Phua C, Alahakoon D & Lee V. Minority report in fraud detection: Classification of skewed data. *SIGKDD Explorer Newsletter 6*, 1, 50–59, 2004.

15. Rahman MM & Davis DN, Addressing the Class Imbalance Problem in Medical Datasets*, International Journal of Machine Learning and Computing*, 3(2):224-228, April 2013.

16. Swets JA, Measuring the accuracy of diagnostic systems, *Science*, 240(4857):1285-93, June 1988.

17. Witten IH & Frank E, *Data Mining: Practical Machine Learning Tools and Techniques*, 2nd ed., Morgan Kaufmann Publishers (Elsevier), San Francisco, CA (USA), 2005.

CHAOS THEORY IN MANAGING COMPLEX SYSTEMS. IMPLICATIONS FOR NATIONAL SECURITY

Maria-Cristina MURARU[*]
Daniela BUNOIU[**]

Abstract

Complexity theory, a recently popularized science, made its way into intelligence analysts' work in the early 1990s, mainly as a result of the global depolarization. This article describes how its main component, complex adaptive systems, also known as systems on the edge of both chaos and order, can be translated into national security mechanisms, such as early warning systems.

Keywords: systems, complexity, chaos, uncertainty, early warning

Theoretical perspectives

Chaos theory

The emergence of crises - whether economic (such as the ones in 1929 and 2007, respectively), social (that represent the result of civil unrest), or food related (Africa) - has been one of the outmost debated issues among scientists and decision makers. Taking into account the unpredictability of crises, scientists tried to design mechanisms and instruments capable of predicting or ensuring a proper response to such situations, such as early warning and response systems.

The evolution of societies triggered an almost exponential growth of risks and threats, which have become more and more diverse. For example, hackers and the way in which they operate were made possible by the progress ensured by the information age.

[*] PhD candidate, "Mihai Viteazul" National Intelligence Academy
[**] OSINT Expert

Also, due to this type of progress, there has been a shift regarding communications among terrorist and organized crime groups.

Also, the time limit in which these risks and threats can occur diminished, so the decision makers are taken by surprise one time too many. The crises that occurred led to chaos, violence, significant human and material losses, regardless of the high number of information sources or the international prevention mechanisms created precisely in order to tackle such situations.

In order to design and implement early warning and response systems, it was necessary to find scientific convergence and, as researchers realized that apparently disorganized social phenomena could be likened to those described by mathematicians, they turned to a niche concept of Mathematics - chaos theory.

For example, mathematical sciences have already proved to be a powerful tool in solving economic issues, which represent one of the core missions in ensuring national security.

Chaos theory has already been applied with a considerable methodological rigor to a wide range of social phenomena, from economics to social sciences, but the need to understand the complexity of social dynamics proved to be a challenge for researchers, that can be explained, at least to some degree, by the inherent non-linearity of social phenomena. In some cases, clear and well-known models (business cycles models, for example) have shown a chaotic behaviour. In these conditions, non-linear time techniques and instruments inspired by chaos theory helped researchers find results.

The 'attraction' of chaos theory finds its roots in management and social organizations theorists' vision according to which organizations are complex, adaptive, non-linear, dynamic systems, which have a similar behaviour to that of natural systems, at different levels of stability and chaos, which basically means that organizations have an unpredictable behaviour, and 'foreseeing' crises in the distant future is impossible. Thus, instead of trying to control a system, a manager should try to take advantage of its complexity.

At the present, chaos theory represents the basis on which early warning systems are designed, no matter their objectives: economic, social, intelligence.

Complexity theory

To some scholars, complexity science is effectively synonymous with chaos theory, or simply an extension of chaos theory. Deterministic chaos is characterized by `sensitivity to initial conditions' and occurs in an infinity of constitutionally simple systems that contain non-linear relationships, but 'it is quite obvious that the world is not chaotic, not completely anyhow'[1].

According to Paul Cilliers, the role of chaos theory in the study of complex systems is still widespread, although the hype of it has abated. Chaos theory could contribute to the study of complexity, but 'it is exactly the robust nature of complex systems, for example their capability to perform in the same way under different conditions, that ensures their survival'[2].

Also, Ruddy Doom and Koen Vlassenroot state that every society is a complex system - in other words open, dynamic and dissipative - and 'chaos and order do not exclude one another, it is just that problems remain in making a distinction between the two zones'[3].

In the last decade, after the pioneering work conducted by the Santa Fe Institute, the scientific world has been the stage of a joint interdisciplinary effort carried out by scientists representing a wide variety of sciences, resulting in a new 'collective' science - Complexity Theory.

> After James Gleick's volume on chaos - ´Chaos: Making a New Science´ -, became a best-seller after being published in 1987, the Santa Fe Institute was created to analyse the self-organization nature of non-linear systems.
>
> The first acknowledged and public-friendly works on complexity were Mitchell Waldrop´s book - ´Complexity: The Emerging Science at the Edge of Order and Chaos´ and Steven Lewin´ volume - ´Complexity: Life at the Edge of Chaos´.

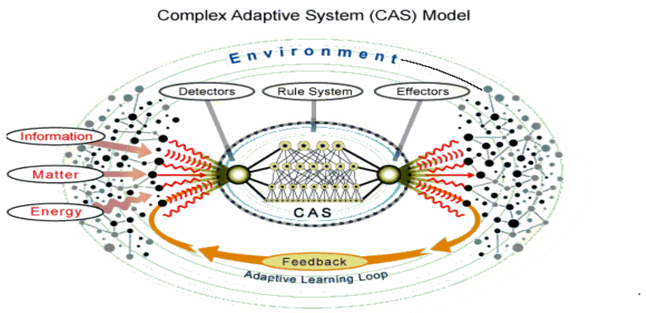
As some scholars argued that the twentieth century science will be known for only three theories: relativity, quantum mechanics, and chaos, Stephen Hawking, perhaps the most renowned scientist of the twenty-first century, postulated in January 2000 that our century belongs to complexity.

Moreover, chaos theory is actually the source of the catch-phrase complex adaptive systems/ CAS, a catch-phrase used by the public as a synonym to neatly organized, almost linear, systems. On the other hand, chaos theory requires removing from thought the concepts of linearity and predictability. In other words, one cannot have both complex adaptive systems and predictability at the same time[4].

The basic principle of Complexity is a result of a series of inter- and intra-relationships, actions and connections of components of a system and between a system and its surrounding environment. According to Professor Murray Gell-Mann of the Santa Fe Institute the term of complexity comes from Latin as the root 'plexus' means entwined and its derived 'complexus' means braided together[5].

Complexity theory scientists have identified three major characteristics common to all CASs[6]:

- Autonomous agents – similar to all sorts of communities, CASs are composed of large numbers of individual actors who make choices, act and react as a result of locally available information processing. All agents act simultaneously, resulting in each one of them influencing and limiting the rest of them.
- Networked structure – the autonomous agents do not take random action, as they all are aware of the common rules. When it comes to human societies, the rules are actually common interests, preferences, ideals or punitive legislation. In other words, the agents are connected via these rules, resulting in a coherent community directed by an objective. The level of connectivity in such a network is moderate, as powerful ties could freeze the evolution of the system and weak ones could lead it into chaos.
- High level of experimentation – systems on the edge of chaos are defined by novelty and experimentation. CASs are also characterized by dynamic stability as they can instantly experience sudden changes of objective. Moreover, this class of evolving systems possesses the abilities of almost instant communication and rapid solution identification.



Source: www.calresco.org

Complex adaptive systems can be applied in a wide range of sciences[7]:

- Life sciences – biological networks and agent-based models;
- Ecology – agent-based/ individual – based models;
- Social sciences – agent-based simulation, Social Network Analysis;
- Physics – smart grid analysis;
- IT – the Internet of Things Analysis.

Similar to chaos theory, the science of Complexity is based on non-linear systems as environments where nothing is predictable, inputs and outputs are the least proportional, and the sum of the subsystems never equals the system. However, despite being unpredictable and uncertain in action, complex systems are ruled by laws of self-organization, requiring out-of-the-box solutions and manner of thinking.

Chaos and Complexity Theory Applications

During the last century the main theoretical scientific progress translated into a shift from the classical, Newtonian point of view towards the more exotic area of chaotic or complex adaptive systems. To sum up, the two new points of view postulate that structures lie within apparently random processes.

Almost twenty years ago, in 1996, a new volume, *Chaos Theory in the Social Sciences – Foundations and Applications* made available to the wide public a series of examples of chaos theory applications in the so-called 'soft-sciences'.

Chaos theory methods have been used to examine and prove the utility of such approach in political science, economics and sociology. A series of applications have been proven to be successful in phenomena such as public opinion, behaviour of states and the evolution of both economic expectations and progress[8].

Also, in order to filter "big data collections" regarding phenomena such as organized crime, financial markets` evolution or terrorism prevention and control, intelligence organizations require a set of ´intelligent' methods and algorithms to compare and scale any set of data to a similar one

Despite the substantially valuable scientific results have so far been obtained in the biological and physical areas, the basic principles are significant resources and seem to offer great utility in studying human social systems.

Taking into consideration that all national security issues revolve around political evolution, economic progress or downfall and sociological aspects such as target groups or communities, one can consider that chaos theory and its CAS derivation can be applied into intelligence studies, the most known example being Early Warning Systems/ EWS.

The inclusion of complexity theory in the intelligence area should not shock anyone as it was previously successfully implemented in economics, biology, weather forecast and corporate management.

Early Warning and Response

Warning analysis is inherently paranoid, as its practitioners have to be more suspicious than most of their colleagues: they operate at the verge of surprise and they tend to be extremely cautious when it comes to their adversaries` actions. This approach is motivated: the history of strategic surprises taught us that when an opinion gets full public support and it becomes an axiom, the risk of a strategic surprise occurring reaches its maximum probability.

Thus, warning analysis constantly avoids focusing on hypotheses: instead of using questions such as “what shall X-entity do next?” it shall leave from “if X-entity wants to attack, how will it behave?” In other words, the starting point of warning analysis is not based on an assumption or on an event’s probability, but on developing a list of indicators, which becomes a key mechanism in the evaluation of potential threats.

No matter the form in which it is organized, present society is still a type of Gestalt system, permanently changing. Approaching such a system should be based on flexibility.

Encompassing both social and exact sciences features, intelligence is the most recent applying domain for chaos theory. As we stated before, nowadays, one of the most important challenges for both theorists and practitioners is identifying, managing or even countering risks and threats, as the world is growing more and more uncertain, on political, social, economic and even cultural level. Moreover, in an ever changing world, the theoretical debates concern identifying an optimal organizational reform in order to ensure intelligence services capable of constantly adapting to these changes.

Crises can be defined through the following features: threat, time pressure, urgency, uncertainty, intensity and surprise and occur as economic turbulences, natural or humanitarian disasters and can be the consequences of preventing or planning failure, critical communications, and wrong perceptions.

Acquiring timely and correct information has proven to be quite a challenge for stakeholders. In these conditions, their mission has changed from (just) actively managing data and events to developing new ways of anticipative thinking and strategic planning.

If early warning is defined as ‘providing timely and efficient information that allow the entities exposed to disasters to act in order to avoid or reduce the risks and prepare an effective response’[9], then an early warning response is based on four stages: identifying risk, monitoring and predicting, disseminating information, reacting. The failure of one of these stages triggers the failure of the entire system.

Monty G. Marshall advanced three types of early warning models:

- Conditional and causal models;

They deal with empirical evidence for causal interference between independent variables and violent conflict/political instability.

A series of causal models is used to explain ethnic rebellion, civil war or state failure (one of these is rebellion motivated by greed[10]).

- Predictive models, which try to forecast the outbreak of violence in a time span of one to five years. These models focus on selected variables. In many cases, they include structural variables, but also process indicators or event-based information.

The most advanced predictive models were developed by Political Instability Task Force/ PITF[11], based on empirical results from a data set in order to explain political instability.

- General risk and capacity models (such as Failed States Index). These are used 'to rank countries from weak to strong, building on the general association between weakness, social problems, political conflict, and poor state performance'[12].

One of the most influential performance ratings, Failed States Index was first published in 2005[13]. The analysis, based on 12 indicators (social, economic and political) ranks countries based on their fragility. It does not rely on an existent data set, but on a monthly review of media reports from national and international sources.

Early warning systems are not seen just as means of warning, but also of response, in order to diminish the risk of another unwanted events occurring, but also to enhance the chances of exploiting potential opportunities.

Basically, no matter the type, all early warning systems definitions encompass several common elements, such as: information-related processes (monitoring, collecting, processing, analysing); anticipative and thorough knowledge of an event or phenomenon dynamics, evolution and possible impact; disseminating early warning to decision makers.

Conclusion

One crucial and in most cases ignored fact is that of the identity of the beneficiary of such systems and their manner of taking things into their own hands. For instance, is there an acknowledged authority that is the first in line when applying early warning systems? Often, the ones at risk are not the first to be informed: the main hypothesis of most early warning systems is that international or regional actors will take it upon themselves to act as protectors as crucial information emerges. In theory all sounds well, it has been too little put into practice. Scholars proposed that efforts should be channeled towards building a warning system or entity right in the core of the conflict as a solution for the constant difference in early warning and the early response.

Bibliography

1. Paul Cilliers*, Complexity and postmodernism*: *understanding complex systems*. Routledge. Conner, D. R. 1998, p.9;
2. Paul Collier; Anke Hoeffler, *Greed and grievance in civil war*, Oxford University Press 2004, available at http://www.econ.nyu.edu/user/debraj/Courses/Readings/CollierHoeffler.pdf, accessed on August 24, 2014;
3. Ruddy Doom, Koen Vlassenroot, *Early warning and conflict prevention: Minerva's Wisdom?*, University of Ghent, Research Group Study of the Third World, 1997, available at http://sites.tufts.edu/jha/archives/113, accessed on August 24, 2014
4. *Transformation Concepts for National Security in the 21st Century,* edited by Williamson Murray, available at http://books.google.ro/books?id=qQkeWFsQhgAC&pg=PA176&lpg=PA176&dq=chaos+theory+in+national+security&source=bl&ots=DKQDd0RQbM&sig=bJWAKIK3uEKUEv4KGJaq_zTwMaM&hl=ro&sa=X&ei=wsDwU7e9IcTIyAPYwYKgBg&ved=0CD0Q6AEwBDgK#v=onepage&q=chaos%20theory%20in%20national%20security&f=false, accessed at August 17, 2014.
5. Murray Gell-Mann, *The Simple and the Complex*, in *Complexity, Global Politics and National Security*, 1997, National Defense University;
6. Douglas Kiel; Euel Elliott; *Chaos Theory in the Social Sciences. Foundations and Applications*, edited by L. Douglas Kiel and Euel Elliott, available at http://muse.jhu.edu/books/9780472022526/, accessed at August 19, 2014.
7. Jacco Van Uden; Kurt A Richardson; Paul Cilliers, *Postmodernism revisited? Complexity science and the study of organisations*, in Tamara: Journal of Critical Postmodern Organization Science, Las Cruces: 2001. vol. 1, issue 3, available online at http://www.peaceaware.com/tamara/issues/volume_1/issue_1_3/PDF%20articles/Van%20Uden_Postmodernism_FT.pdf, accessed at September 20, 2014, p. 8;
8. John Cleveland Innovation Network for Communities, *Complexity Theory. Basic Concepts and Application to Systems Thinking*, 1994, available at http://fr.slideshare.net/johncleveland/complexity-theory-basic-concepts?next_slideshow=1, accessed at August 19, 2014.

References

[1] Jacco Van Uden, Kurt A Richardson, Paul Cilliers, Postmodernism revisited? Complexity science and the study of organisations, in Tamara: Journal of Critical Postmodern Organization Science, Las Cruces: 2001. vol. 1, issue 3, available online at http://www.peaceaware.com/tamara/issues/volume_1/issue_1_3/PDF%20articles/Van%20Uden_Postmodernism_FT.pdf, accessed at September 20, 2014, p. 8.

[2] Paul Cilliers*, Complexity and postmodernism*: understanding complex systems. Routledge. Conner, D. R. 1998, p. ix.

[3] Ruddy Doom, Koen Vlassenroot, Early warning and conflict prevention: Minerva's Wisdom?, University of Ghent, Research Group Study of the Third World, 1997, available at http://sites.tufts.edu/jha/archives/113, accessed on August 24, 2014.

[4] *Transformation Concepts for National Security in the 21st Century,* edited by Williamson Murray, available at http://books.google.ro/books?id=qQkeWFsQhgAC&pg=PA176&lpg=PA176&dq=chaos+theory+in+national+security&source=bl&ots=DKQDd0RQbM&sig=bJWAKIK3uEKUEv4KGJaq_zTwMaM&hl=ro&sa=X&ei=wsDwU7e9IcTIyAPYwYKgBg&ved=0CD0Q6AEwBDgK#v=onepage&q=chaos%20theory%20in%20national%20security&f=false, accessed at August 17, 2014.

[5] *The Simple and the Complex*, in *Complexity, Global Politics and National Security* Prof. Gell-Mann Murray, 1997, National Defense University.

[6] *Complexity Theory. Basic Concepts and Application to Systems Thinking,* John Cleveland Innovation Network for Communities, 1994, available at http://fr.slideshare.net/johncleveland/complexity-theory-basic-concepts?next_slideshow=1 , accessed at August 19, 2014.

[7] According to the 'Complex Adaptive Systems Modeling' edited by Springer.

[8] *Chaos Theory in the Social Sciences. Foundations and Applications*, edited by L. Douglas Kiel and Euel Elliott, available at http://muse.jhu.edu/books/9780472022526/, accessed at August 19, 2014.

[9] International Strategy for Disaster Reduction, United Nations, 2006.

[10] As presented in Paul Collier and Anke Hoeffler, *Greed and grievance in civil war*, Oxford University Press 2004, available at http://www.econ.nyu.edu/user/debraj/Courses/Readings/CollierHoeffler.pdf, accessed on August 24, 2014.

[11] Formerly known as State Failure Task Force, its role is to provide counseling for the American authorities regarding instability in developing countries.

[12] Marshall, Monty G. and Cole, Benjamin R. 2008. *Global Report on Conflict, Governance and State Fragility 2008*. Washington, D.C.: George Mason University, pp. 9-11, *apud* Herbert Wulf, Tobias Debiel, *Conflict Early Warning and Response Mechanisms: Tools for Enhancing the Effectiveness of Regional Organisations? A Comparative Study of the AU, ECOWAS, IGAD, ASEAN/ARF and PIF,* in „Crisis States Working Paper Series", no. 2, Crisis States Research Centre, May 2009, available at http://eprints.lse.ac.uk/28495/1/WP49.2.pdf, accessed on August 25, 2014, p. 5.

[13] http://www.foreignpolicy.com/articles/2005/07/01/the_failed_states_index_2005.

"TIANXIA" AND "GUANXI" FROM COMMUNITY TO FOREIGN POLICY IN CHINA

Mihaela BERBEC[*]

Abstract

The discussion about the Asian international relations theory focuses on cooperation variables which consist in activating socio-cultural norms meant to keep the cohesion and order and to amplify the possibility of institutional political control. In Chinese setting, the effects of phenomena such as guanxi and holistic paradigms such as tianxia are the philosophical source of political governance and a future framework for understanding action in international realm. Already perceived as a leader in international relations, China searched for an appropriate identity that could guide its future decisions in the global environment. Along with the beginning of Hu Jintao's administration in 2002, China defined its growth as "peaceful rise", in an attempt to regain the political reputation from the international community. These trials of defining its identity are part of a greater endeavor, which regards the creation of a new paradigm that could explain contemporary international relations, and diversify the perspectives over the nature and instruments for political governance of societies. The present article will account for guanxi under its thick meaning, and enforce the idea that guanxi should be understood as more than its literal translation as connections or social relations.

Keywords: China, tianxia, quanxi, social relations, community, foreign policy

Introduction to localized perspectives

International relations theory has been dominated in the last decade by the constructivist approach, which solved in part the lacks in social understanding of international political phenomena. Constructivism extracted its explanatory idea from the historical and social experience of the Western world. Identity and interests have as source the basic concepts related to freedom, equality, and belief systems based on Christian morality. Other perspectives, promoted by neorealism and neoliberalism emphasized a narrow view of the world, with nation-states as unique sources of political culture. However, the international realm recently became the frame for dynamic social change, which creates gaps in the prediction of asymmetrical threats and lacks explanatory principles for the behavior and identity of actors.

Lately, the multitude of perspectives resurging from local experiences has transformed the mainstream theories in peripheral ideas. Acharya and Buzan (2010) introduced into the international relations theory the Asian perspective over the international politics. This initiative is responding to the political effects of phenomena with source in the local cultural ideologies. Cultural diversity and deep interconnectivity through social networks affects the interaction of actors in international setting.

The clash of social and cultural norms in international relations is producing effects for the cooperation processes. Moreover, networking at global level brings the need to reassess strategies on a relational rationality in order to access information by constructing bridges with remote social actors. On one hand, social networks theory is assisted by permanent technological advances and innovation in social communication. On the other hand, the integration and use of technology in new cultural settings creates ethical issues with local substance. Hence, there is a conflict between moralities, which appeared along with the effects of networking. The Confucian ethics views the basis for future cooperation in international relations in the harmonization of values and morality.

The discussion about the Asian international relations theory focuses on cooperation variables which consist in activating socio-cultural norms meant to keep the cohesion and order and to amplify the possibility of institutional political control. In Chinese setting, the effects of phenomena such as *guanxi* and holistic paradigms such as *tianxia* are the philosophical source of political governance and a future framework for understanding action in international realm.

Tianxia and the Chinese world view

Already perceived as a leader in international relations, China searched for an appropriate identity that could guide its future decisions in the global environment. Along with the beginning of Hu Jintao's administration in 2002, China defined its growth as "peaceful rise", in an attempt to regain the political reputation from the international community. Later on, the same principle was renamed "peaceful development", in order to project the image of a benevolent power, as understood in the Confucian ethics. These trials of defining its identity are part of a greater endeavor, which regards the creation of a new paradigm that could explain contemporary international relations, and diversify the perspectives over the nature and instruments for political governance of societies.

The concept of *tianxia* (天下) was introduced in the governance literature by Zhao Tingyang, a Chinese contemporary philosopher, as an alternative to the Western paradigms of international relations. His intervention at the 2005 Culture of Knowledge Conference held in Gao, India, marked the beginning of a new line of Chinese scholarship, concerned not only about the national identity and image of China, but also about the need to forge a comprehensive theory that includes actors, structures, and processes currently not accounted by Western theories.

Literally, *tianxia* translates as "all under Heaven" and represents the ethical vision of the world order. Its historical sources are to be found in Shang and Zhou dynasties, on Chinese territory, reborn and redefined in Han dynasty, under the Confucian school of thought, conferring to it a political meaning (Xu, 2014). However, even if *tianxia* appears to be purely Chinese, its principles are recognized throughout East and South-East Asia, under various forms.

In some respects, the proposed worldview of *tianxia* comes against the Western perspectives accepting conflict and competition as natural organization of societies. *Tianxia* accepts harmony reaching as the only natural purpose of humanity, for which selfish, individual purposes should be eliminated. Thus, the Westphalian principle of the sovereignty and equality of states is opposed by the Confucian principle of inclusiveness. This view proposes order and hierarchy as guiding principles for creating a harmonious world, replacing the democratic principles of freedom and equality. As follows, the relation between actors in a society, and in an extended international society would become “unequal, but benign” (Acharya, Buzan, 2010). Yan (2001: 37) contends that benevolent governance (*wangdao* 王道) rather than hegemonic governance (*badao* 霸道) will become the rule in a global system.

The principles of the proposed *tianxia* system are based on geographical, social, and institutional meanings. Firstly, *tianxia* can only include the entire geographical world in its framework, because it represents the humanity as a whole, in which dichotomies should be channeled for a common purpose. As such, differences are part of the same system and should be treated accordingly. Secondly, *tianxia* creates the structure of order between *Tian* 天, the Heaven and the people. The relation between the highest authority and the people is always hierarchical and beneficial for the later. In its early acceptance, the Heaven was represented on land by the Emperor, who was the communication link between Heaven and people. However, *minxin* 民心, the hearts of the people expressed the will of the Heaven, idea concentrated in the Chinese proverb: “He who gains the heart of the people has the right to rule *Tianxia*”. [1] Lastly, *tianxia* is a concentrically imagined structure. The *tianxia* system should account for a center, associated with a certain civilization, from which decisions and influence emanate outward, creating a harmoniously ordered society. These basic principles were later on legitimated by major authors and works of Chinese classical literature, such as Lao Tzu, Chuang Tzu, the Book of Changes, Xun Tzu and Mencius.

All the principles of *tianxia* stand on ethical philosophy extracting its meaning from the Confucian concept of benevolence (*ren* 仁), mostly understood as righteousness. Benevolence is seen as universal, because it helps in building the good society, a society with common rites, culture, language and lifestyle, as argued by Xu (2014: 97).

Chinese scholars are devoted to the necessity of creating a universally valid paradigm, since the Westphalian system became helpless in explaining contemporary socio-political phenomena. Thus, by activating the *tianxia* theory, with its three meanings – geographical, social, and institutional, the redefinition of the world society becomes possible (Callahan, 2008).

Constructivism, the most recent paradigm in international relations, explains the behavior of actors as the result of national interests. In Zhao's critic, along with the *tianxia* system, this view will become obsolete, since the entire world is an inclusive construction based on cooperation and communication.

Consequently, the replacement of the current system should be conceived as a lengthy process of attraction of international actors in the new logic of thought. Most importantly, the concept of order is to become a governing idea and is only complemented by the concept of freedom. *Tianxia* will also valorize elite governance over democracy and ethics over law (Callahan, 2008).

Although, the *tianxia* theory is yet to be extended and researched, it widely reflects the natural organization of the Chinese society and its values. There is a deep connection between socio-cultural norms and the political structure, which is obvious in governmental policies and social institutions (Callahan, 2008).

Tianxia was born in a time where the family unit was central to the Chinese governance system. The ethical principles included in the *tianxia* system were fundamental in promoting the cohesion and stability of the family, of the Chinese society as a whole, and helped in preserving the legitimate political ruling. The inclusiveness perspective appeared natural for the Chinese nation, just as natural as it was for the family organization. Inside the boundaries of the family there was no disagreement, because there was a hierarchical order of decision making and a moral incentive to obeying those decisions. From this perspective, *tianxia* is the greatest family (*jiating fangshi* 家庭方式), an idea extended by Zhao to the entire world, under the phrase the "world as one family" (Xu, 2014).

The *tianxia* system has its critics, one of the most important observations being the practical understanding of inclusiveness. Callahan (2008) noted that although *tianxia* is a universal system, it places the "West" outside its framework. Moreover, the Chinese purpose of governing the world through an ethical approach is quite narrow, relating to previous political processes. Also, the redefinition of the smallest unit in international relations needs to be addressed. In Zhao's perspective, the smallest unit in international relations is the world society in itself, as opposed to the Western system, where the smallest unit to be analyzed is the nation-state. This brings conceptual difficulties in applying the *tianxia* system theory to the current state of affairs.

However, the incentives to develop the *tianxia* perspective come from policy needs, and searches to promote the image of China as a normative soft power (Callahan, 2008).

Guanxi and the Chinese social order

When faced with the endeavor of defining and explaining localized concepts for new phenomena, the social sciences academia distinguishes between the thin and thick types of definitions. The situation with the Chinese social phenomenon entitled *guanxi*关系 (關係) is similar. Most of the Western literature studying the localized processes and phenomena is divided over the acceptance of the literal translation of the word describing the phenomenon, making it a thin concept, or the acceptance of the hidden features of the concept, in essence related to local cultural meanings, accepting it as a thick concept. The applied thinness or thickness of the concept results in creating various views over the meaning and effects of the phenomenon. Hence, the choice is utterly important for the academic research, especially when speaking about localized phenomena.

The present article will account for *guanxi* under its thick meaning, and enforce the idea that *guanxi* should be understood as more than its literal translation as connections or social relations. The thin definition accepts *guanxi* as no more than social capital in Chinese context. However, there are obvious signs that *guanxi* produces different effects in the Chinese society, as compared to the Western world (Hamaguchi, 1985, Sato, 2010, Lin, 2001)

As mainstream academia holds, social capital is the product of using social relations for personal gain. It has an exclusive utilitarian meaning, creating effects in innovation processes. In comparison with the classical definition of social capital, *guanxi* encompasses ethical features, which help in maintaining long-term social cohesion, social dynamics, and promoting social change.

Guanxi is based on the Confucian ethics, built on the ancient principles of wu-lun, the hierarchical organization of the society.

Thus, the Confucian ideology acknowledges for three types of social relations constituting the basis for any social environment and processes necessary to maintain the political unity of the society. The first category is naturally hierarchical, and regards the relation between father and son, the husband and wife, and between older brother and younger brother. It manages the relations inside the family institution, an important dimension for the Chinese social organization. The second category is artificially hierarchical and explains the relation between the emperor and its subjects, managing the political governance of the society. Lastly, the relation between friends, the only horizontal and equal relationship, is creating a large field of inquiry for the application of Granovetter's strong-weak ties theory (1973, 1982).

Conventional Chinese and foreign views perceive *guanxi* as an essential feature of the Chinese social life, starting with familial informal setting and continuing with formal public organization of the society. Firstly observed by outsiders as a pervasive mechanism in business or private affairs, studies have showed that *guanxi* is the mainstream phenomenon governing all areas of activity, such as politics, economy, culture, and social life.

Often assimilated with corruption, *guanxi* is conceived by the political elite as a backward practice, highly detrimental for the national development, since it tags along with legal practices, replacing them frequently. Since the beginning of the ´90s, researches have showed the existence of practices related to *guanxi* not only in Mainland China, but also throughout the Eastern and South-eastern Asian continent, starting with Hong Kong and Taiwan and continuing with Republic of Korea, Japan, Vietnam, Indonesia, Singapore, etc. Moreover, *guanxi* practices are active and stable inside Chinese communities abroad, as sign of cohesion and solidarity.

The application of Granovetter's theory to *guanxi* phenomenon explains part of the research endeavor. Scholars have acknowledged the efficiency of *guanxi* in reducing uncertainty in different information structures, on the basis of social networks theory (Lin, 2009; Chang, 2011). From this point of view, *guanxi* is similar with other types of social networks. However, there is an obvious need to understand *guanxi* not only as embedded in social networks, but also embedded in a particular cultural and historical framework.

From a comparative perspective concerning social networking in different cultural environments, weak ties in Western societies are represented by friends, colleagues, and acquaintances. Weak social networks help furthering innovation, whereas strong social networks are part of the private life, reserved to nuclear family and close relatives. In China and other *guanxi* societies, the dichotomy private-public is non-existent from the sociological point of view. Therefore, the constituency of social networks is not privately or publicly assigned. Strong ties have the capacity to influence social development and cohesion in the same way as weak ties.

Furthermore, traditionally conceived weak ties, initial friends and colleagues have the capacity of transforming in strong ties, by cultivating guanxi. In order for this to happen, there are specific rules and norms that must be satisfied in order to enhance the relationship. Reciprocity, long-term commitment to the relationship, building trust, exchanging favors, permanent indebtedness, preserving and respecting ascribed rituals (including gift giving rituals), and showing genuine emotional attachment and involvement with the members of the guanxi network are mechanisms promoting cohesion and stability. Hence, *guanxi* networks are bound by moral norms, much more than by instrumental purposes. The art of cultivating guanxi, or *guanxixue* (关系学), accepts and encourages instrumentality, but only if it is sustained by a genuine moral and emotional sensibility (*ganqing*感情) towards the participants to the guanxi network.

From Community to Foreign Policy in China

The unity between *guanxi* and *tianxia* is created by the imperative of order. Social organization in Chinese setting is based on norms and rituals that affect social relationships from the smallest unit, the family, to the highest levels of *tianxia,* the governing elite. Recently, the Chinese academic and political elites are searching for an explanatory framework that creates convergence between the current political purposes and the belief systems emanating from deeply rooted Confucian philosophy.

However, there is continuity in respects to the Chinese social values. The political discourse largely admits the adherence to the principles of harmony and order, and is interested in promoting the hierarchical organization of society.

Declarations of Chinese political leaders, Hu Jintao and Xi Jinping show a greater reliance on indigenous concepts in order to promote their foreign policy agenda. Former president Hu proposed in 2002, as soon as he acceded to power, the "harmonious society" concept (Chan, 2010:821), in order to encourage social stability, and continue economic reforms.

– Urban publicity panel, China, Wuhan, June 19, 2014
– Purpose: publicity for LED panels
– Text: Moral benevolent the world (德仁天下)
©Photo copyright of the author

In September 2014, at an international conference in Beijing, commemorating the anniversary of Confucius, President Xi Jinping cites the Chinese philosopher as positive example for a modern nation to follow.[2] Most importantly, with this occasion, political and research elites recognized that Confucianism has a universal vocation and it would be beneficial for other nations as well. According to the members of the gathering, Confucianism has a positive role in socio-economic development and political governance. Xi Jinping emphasized the concern for promoting peace and development, which should be pursued in the traditional frame of Confucian spirit and culture. He added that “the Chinese Communist Party is the successor to and promoter of fine traditional Chinese culture”, a statement which has the potential of explaining the general position of the Communist Party in respects to the effects of Confucian rhetoric for governance.[3]

The increased influence that China has exerted in Asia is due to its soft power foreign policy through which neighbors are reassured about its peaceful development. The fact that countries in Eastern and Southeastern Asia share values of social organization and governance, offers incentives for a strong integration movement, with China at the center.

The deep involvement of China in regional cooperation is showed by its participation at the ASEAN Regional Forum (ARF), ASEAN plus three (ASEAN and China, South Korea and Japan), ASEAN plus One (ASEAN and China), the free trade agreement with ASEAN, the Joint Declaration on Cooperation in the Field of Nontraditional Security Issues, the Joint Declaration on Strategic Partnership for Peace and Prosperity and China’s accession to the ASEAN Treaty of Amity and Cooperation in 2003, and security dialogues related to East Asia. Hence, the image of threatening nation that China had in the past is nowadays returned to be seen as the one of a benevolent power (Li, 2009). Recently, China leads the way for an even more comprehensive dialogue with its neighbors, by sustaining the ASEAN Economic Community (AEC), established in 2015, a free trade zone that seems to concentrate on the social component of economic development and the creation of a regional identity.

Therefore, the Chinese policymakers seem to follow the prescriptions of the proposed tianxia system, in spite of the fact that scholars still need time to transform it into a well-grounded paradigm.

Conclusion

The discussion concerning two of the most important Chinese concepts was meant to open the way for a new approach in international relations theory. The reason for such an endeavor is due to the effects of localized values and processes over the global environment. The relational rationality sustained by the social networks structure affects international politics. Since the positioning of China as a global actor, the effects of deeply rooted social norms, such as guanxi and tianxia have the potential of changing the way we perceive international relations. By the time when the Chinese society will become the source of an Asian theory of international relations, the Western academia and policymakers will be prepared to understand the political evolution of the global system.

Moreover, there is a great opportunity for the intelligence community to refocusing analysis in order to integrate in their prediction frameworks other strategic and tactical objectives, based on the substance of socio-cultural norms and the knowledge produced by contextual specificities.

References

1. Acharya, Amitav, Buzan, Barry (editors), „Why is there no non-Western international relations theory? An Introduction”, in Acharya, Amitav, Buzan, Barry, *Non-Western International Relations Theory: Perspectives on and beyond Asia*, London, New York: Routledge, 2010.

2. Callahan, William A., „Chinese Visions of World Order: Post-Hegemonic or a New Hegemony?”, *International Studies Review*, vol.10, no.4, 2008, (pp.749-761) pp.749-750.

CALLAHAN, William A., „Cultural Governance and Resistance in Pacific Asia”, London, New York: Routledge, 2006, pp.174-176.

3. Chan, Kinman, „Harmonious society” in *International Encyclopedia of Civil Society*, eds. Helmut K.Anheier and Stefan Toeper, NewYork: Springer, 2010.

4. Hamaguchi, Esyun. „A Contextual Model of the Japanese: Toward a Methodological Innovation in Japan Studies.", *Journal of Japanese Studies* 11, no. 2, 1985, pp.289-321.
5. LI, Mingjiang, „Domestic Sources of China's Soft Power Approach", *China Security*, vol.5, no.2, 2009, pp.55-70.
6. Lin, Nan, „Social Capital: A Theory of Social Structure and Action", Cambridge, New York, Melbourne: Cambridge University Press, 2001.
7. Sato, Yoshimichi, „Are Asian Sociologies Possible?: Universalism versus Particularism", Michael BURAWOY, Mau-kuei CHANG, and Michelle Fei-yu HSIEH (editors), *Facing An Unequal World: Challenges for A Global Sociology*, vol. 2: Asia Institute of Sociology, Academia Sinica and Council of National Associations of International Sociological Association, 2010, pp.192-194.
8. Xu, Bijun, „Is Zhao's Tianxia System Misunderstood?", *Tsinghua China Law Review,* vol.6, 2014, pp.95-108.
9. Yan, Xuetong, „The Rise of China in Chinese Eyes", *Journal of Contemporary China*, vol.10, no.26, 2001, pp.33-39.
10. Zhao, Tingyang, YAN, Xin, „The Self and the Other: An Unanswered Question in Confucian Theory", *Frontiers of Philosophy in China*, vol.3, no.2, 2008, pp.163-176.
11. Sun Ye, „Confucius still vibrant at 2565", *China Daily*, September 27, 2014, http://www.chinadaily.com.cn/culture/2014-09/27/content_18671931.htm
12. Jin Kai, „The Chinese Communist Party's Confucian Revival", The Diplomat, September 30, 2014, http://thediplomat.com/2014/09/the-chinese-communist-partys-confucian-revival/

[1] 得民心者得天下(*de minxin zhe de tianxia)* in Xu Bijun, op.cit., 2014, p.97

[2] Sun Ye, "Confucius still vibrant at 2565", *China Daily*, September 27, 2014, http://www.chinadaily.com.cn/culture/2014-09/27/content_18671931.htm

[3] Jin Kai, "The Chinese Communist Party's Confucian Revival", The Diplomat, September 30, 2014, http://thediplomat.com/2014/09/the-chinese-communist-partys-confucian-revival/

CAN EU AND NATO BUILD A „SECURITY COMMUNITY” IN THE WESTERN BALKANS?

Miruna TRONCOTA[*]

Abstract

After the violent dissolution of Yugoslavia, the newly formed states had to start reconstructing their relations and cooperate peacefully on their road towards EU and NATO membership. Regional cooperation has been promoted by the international community as the most important tool for stabilizing the Western Balkans. The goal of this norm of "good neighbourly relations" was to motivate through non-coercive measures the former "enemies" to cooperate and peacefully engage in a regional project together, under the EU and NATO "umbrella". In constructivist terms, this process can be considered as a form of gradually building a so-called „security community", based on shared values and a common trajectory in the international arena. The paper will thus focus on regional cooperation which was used as both a norm in the relationships between these countries, as well as a de facto condition of EU and NATO accession. The main purpose of this article is to assess whether EU and NATO policies in the last 10 years have built a successful or at least a partial security community in the Western Balkans. As such, the theoretical part will focus on defining the concept of "security community" as theorized by Karl Deutsch (1957) and more recently by Emmanuel Adler and Michael Barnett (1998). The empirical part will try to identify concrete examples and arguments in order to assess whether the post-conflict reconstruction policies applied by EU and NATO in the ex-Yugoslav republics match the concept of building a „security community" with its own distinct identity, objectives, and security patterns. The conclusions will focus on the relevance of this geopolitical space and the lessons learnt that could be useful for the recent security shifts in Europe.

Keywords: NATO, EU, security community, Western Balkans, post-conflict reconstruction

[*] Postdoctoral researcher, Department of International Relations and European Integration, SNSPA

Introduction

The EU and NATO's security agenda is heavily overloaded for the moment. The year 2014 brought a series of major turning points which directly affected this security agenda: the conflict between Russia and Ukraine presents a serious challenge to the pan-European security order; the EU is in the process of re-formulating its Eastern Neighbourhood Policy as well as its approach to the Black Sea region which is of vital strategic importance to it; protracted conflicts, closed borders and strategic rivalries have weakened institutions of governance and allowed the democratic rule of law to deteriorate. In these conditions NATO's Wales Summit from September 2014 had the difficult task of defining a new strategy to tackle these challenges. Both scholars and policy makers are for the moment concerned with investigating the best and worst case scenarios for the extended Black Sea region and the way these events can impact regional security. There is a need to re-conceptualise EU and NATO's post-conflict engagement in the Western Balkans in the light of recent developments and the new security threats in the Eastern neighbourhood. The present article contributes to this pressing security debate by reflecting on the present security outcomes achieved by the EU and NATO in promoting regional cooperation in the Western Balkans. This area is extremely relevant because it is a post –conflict region situated in the immediate vicinity of the Black Sea, which represented one of the biggest tests for EU and NATO cooperation in conflict management in the last 10 years. The main research question to be raised in this context is the following: *What are the concrete results in EU and NATO's attempts to transform the security regime in the Western Balkan region from a conflict – driven one towards a security community?* The scope is thus to analyse the emerging institutions and identities that will shape WB's future and eventual membership in the EU and NATO from the perspective of building a security community. The explanatory model will focus on „the narrative of exceptionality" and „the narrative of failure" as dominating discourses that have influenced policy making both on the side of the EU/NATO and on the side of local elites.

As such, the theoretical part will focus on defining the concept of "security community" as theorized by Karl Deutsch (1957) and more recently by Emmanuel Adler and Michael Barnett (1998) connecting it with the concept of "normative power" and its application on security matters and post-conflict settlement. Based on this theoretical background, a series of main characteristics will be identified as suitable for identifying the emergence of a security community in the WB. The empirical part will bring concrete examples and arguments in order to assess whether the post-conflict reconstruction policies applied by EU and NATO in the ex-Yugoslav republics match the concept of building a „security community" with its own distinct identity, objectives, and security patterns. The conclusions will focus on the relevance that this geopolitical space has for the recent security shifts in Europe and the lessons that can be learnt from this area and applied in the present ethnic conflicts in the extended Black Sea region.

What is a "security community" and how can we recognize it?

"If the whole world was integrated into a security community, wars would be automatically excluded."
(Karl Deutsch, *Political Community and the North Atlantic Area,* 1957, p 5)

By promoting the development of shared definitions of security, proper domestic and international action and regional boundaries, social learning encourages political actors to see each other as trustworthy.
And it also leads people to identify with those who were once on the other side of cognitive divides."
(Adler and Barnett, *Security communities,* 1998, p 45)

The theory of international relations can offer useful analytic tools and concepts for tackling the major challenges in the evolution of contemporary intelligence and security studies. The present article is an attempt to bridge the two fields and to show how concepts could help policy analysis in an interdisciplinary approach. As such, the first step will be therefore to describe the main theoretical assumptions of the analysis and to integrate them in the overall conceptual framework that shall be employed further.

The '90s brought paradoxical political events in Europe – on one hand the democratization of former communist countries, on the other violent war in the former Yugoslav space. After the secessionist wars that have erupted in 1991 and lasted until 1999, regional cooperation has been promoted by the international community as the most important tool for the stabilization of the Western Balkans. The delayed intervention of peace keeping missions in Bosnia was justified by the fact that the violent dissolution of Yugoslavia has taken the Western allies "by surprise". As such, the conflict could not be stabilized without the US intervention. After the end of violence, the goal was that the newly formed states have to start „rebooting" their relations and cooperate peacefully on their road towards EU and NATO membership. In constructivist terms, this process can be considered as a form of gradually building a so-called „security community", based on shared values and a common trajectory in the international arena. The concept of "security community", which will be discussed below in a constructivist understanding, refers to the development of trust, shared values, and peaceful resolution of conflict among states that interact regularly, come to identify with one another, and consider violent interaction to be unthinkable The main scholars who wrote on the topic also emphasized that the formation of a security community includes the emergence of trust, belongingness, and reconciliation, along with internalizing the notion of resolving conflicts in a peaceful manner[1]. A shared identity, the sense of sympathy, loyalty and the "we-feeling" are the main values that guide such a community of interests. This makes it easier to predict each other's behaviour, and cooperate accordingly. These are the main indicators that can validate the existence or the absence of a security community between certain states. This process is of a neo-liberal inspiration because it is based on the view on interdependence between actors in the international arena.

Therefore, the following definition of "security communities" employed in this analysis is based on the main indicators as prescribed theoretically by Deutsch and subsequently by Adler and Barnett. Based on their view, a security community is formed when there is a shared sense of identity and purpose among the citizenry and among political elites from various countries which decide to coordinate their foreign actions that leads to expectations of peaceful change. The overarching goal of a security community is to maintain peace. Practically, countries that form a security community will not start an aggression against each other and they will try to solve their disputes in peaceful ways. Consequently, this is the idealist tone of the theory, because it considers that when such a community is established, violence is no longer a viable option for the resolution of conflict[2]. Based on such an understanding of the concept, two or more independent units connect into a common and broader unit based on interests and values. Symbolic rather than material incentives keep the countries under the same 'foreign policy umbrella'. As an illustration of this idea, several socio-constructivist scholars have argued that contemporary Europe emerged as a result of the process of "socialization" between like-minded actors, gathered around the European Union (EU) and the North Atlantic Alliance (NATO)[3]. As such, many authors argued that this post-conflict mechanism of building sustainable security communities proved successful, so it needs to be further on implemented by the EU and NATO themselves, who become on their own drivers of other security communities in their surroundings. As an illustration for such a strategy there are always mentioned the changes that occurred in Central and Eastern Europe after the Cold War, and especially the constitution of the Visegrad Group also called the V4 as it is constituted by the Czech Republic, Slovakia, Hungary and Poland. The positive reforms and the common identity in foreign policy that constituted into a small but strong security community were driven both by the countries themselves and by the EU, NATO or the OSCE. The role of international organizations (IOs) was from the beginning recognized as being very important in the process. Following this logic, some authors believe that the EU and NATO could play a similar role in the creation of a security community in the Balkans.

The main idea that needs to be stressed at this point of theoretical introduction is that all these authors have stressed the fact that there are multiple layers of security community building. Adler and Barnett state that security communities should be built gradually: an emerging community corresponds with the basic needs of peaceful change, while a mature security community is characterized by the collective security mechanisms, as well as by supranational and transnational elements[4]. The process goes through different phases and it involves a complex web of actors, mentalities, and in the end it reaches a distinct status, by acting unitary as a single community. That is actually the main criterion to recognize a security community in the international arena – it acts, talks, thinks as a unitary actor and its policy is coherent in time and respected by all members. The analytic consequences of such a definition is that any case study that aims at identifying the indicators that point to the emergence of a security community needs a chronological approach in order to follow the subsequent phases and to properly contextualize its features. Practically, the most important indicator of such an analysis is the recognition of commonality and enhanced partnership among the governments of a post-conflict region that would fit the model of a security community. As it was mentioned, the process of forming a security community is directly connected with the process of regional cooperation and a certain level of regionalization of foreign policy. Looking at the main evolution of the discursive patterns that characterized the policy narratives of ex-Yugoslav countries and the international community regarding their future aspirations is the proposed method for investigation in the next section.

EU and NATO post-conflict reconstruction policies in the WB

Both the EU and NATO have evolved in parallel with the challenges brought by the security threats in the former Yugoslav space. Both organisations assumed a security stabilizing role in Europe and as such they have had a special focus on the Western Balkans (WB hereafter)[5], taking into consideration that throughout the 90's, the violent conflicts that devastated the region urged the transformation process of NATO, as well as the development of Common Foreign and Security Policy (CFSP) and the birth of European Security and Defence Policy (ESDP). Moreover, after 2000, all the countries of the region have expressed a desire to join European institutions and become a part of the Euro-Atlantic community. Let us have a brief view on the status of the region in their relation with EU and NATO.

After the military interventions in 1995 and 1999, NATO assumed peacekeeping missions in Bosnia and Herzegovina (BiH hereafter) (IFOR, subsequently SFOR) and Kosovo[6] (KFOR). The peacekeeping mission in BiH was considered a success, given that ever since the Dayton Peace Agreement was signed and NATO forces deployed, there was no single armed conflict or casualty of combat operations. This mission left BiH in 2004, after which it was replaced by EUFOR which is still present in the country, but with a reduced contingency. The NATO mission in Kosovo was met with a far more complicated situation, with many more armed attacks against the Serb population, also including attacks and large-scale ethnic cleansing in March 2004, which KFOR managed to bring under control only with great effort and a significant number of casualties. All Western Balkans countries, at this moment, have an institutionalized relationship with NATO, either through the Membership Action Plan (MAP), or just through the participation in the Partnership for Peace programme and Euro-Atlantic Partnership Council. In addition to Slovenia – which was the only former Yugoslav republic to become a member of both the EU and NATO – Croatia and Albania became NATO members in 2009, whilst Macedonia, Montenegro and Bosnia and Herzegovina have been included in the Membership Action Plan (MAP). The only exception is Serbia, which declared neutrality; although it is a member of NATO's Partnership for Peace (PfP) programme, an associate member of NATO's Parliamentary Assembly and is very active in military cooperation with its neighbours. It is important to mention another attempt of enforcing a security community by NATO with the Adriatic Charter, which was signed in 2005, which enabled the creation of the Adriatic Group, gathering Croatia, Albania and Macedonia as a sort of regional alliance within NATO.

At the same time, making use of its normative "soft power" and specific instruments, the EU began systematic efforts in the same direction within the frame of the so-called "regional approach to the Western Balkans". Also, after NATO's military intervention against the former Federal Republic of Yugoslavia in 1999, the Stability Pact in South-East Europe was established at the EU summit in Cologne. The common stand taken at European summits in Zagreb (2000) and Thessaloniki (2003) was that all WB countries could be admitted into the EU if they fulfilled the required conditions. Since the enlargement of May 1st, 2004, the EU and the WB have become even closer neighbours, and so the situation in the region, their progress on the road to European integration and their present and future relations with the EU really are of immediate concern to the EU itself. EU's perspective can be easily resumed to the following ideas: many of the challenges facing the WB countries are not only common to them but also have a cross-border dimension, which involves their regional neighbours. In this context, regional cooperation is therefore a cornerstone of the EU's policy framework for the western Balkans — the stabilisation and association process, which offers to the countries of the region the possibility of eventual EU membership. The concept of 'regional cooperation' is a specific requirement under the SAAs.

Based on these criteria the most advanced country in the region is Croatia, which became an EU member state in 2013 and next is Serbia which started its membership negotiation process in January 2014, after it started its process of normalization of relations with Kosovo. As a consequence, all of the states' security and defence policies are almost completely harmonised (at least on paper), expressing the symbolic message that they are fully engaged to become a member of the EU. As such they are all candidate countries, with the exception of Bosnia and Kosovo, which are still potential candidate countries. Most of them already participate in EU missions within the Common Security and Defence Policy (CSDP), albeit quite modestly. In addition to that, all Western Balkan states are in the PfP program and are either members of NATO or seek to become one in the near future (except Serbia, which declared military neutrality in 2007). Since 2009 and 2010, Western Balkan nationals can also travel freely without visas within the region and to the European Union, with the sole exception of Kosovo.

It is also relevant to underline the fact that the impact of the EU and particularly of NATO in the WB has also faced competition from power-seeking regional actors, some of whom are strongly opposed to further Euro-Atlantic integration of the Balkans such as Russia. Turkey is another powerful actor in the region (especially in the case of Bosnia and the activities of the Muslim Brotherhood).

Balkan Paradoxes – Strengthening regional cooperation, but failing to work together

As we have seen, NATO and EU were very active in the region in their attempts to foster a security community and to determine countries to act together. At the institutional level they have tried a complex set of instruments and policy formats to boost cooperation among Balkan countries. But the results were limited and we are faced at this point with a sort of Balkan paradox and the reality on paper does not match with the reality on the ground. Even though there are multiple policies and actions that have stressed the existence of regional cooperation, in the most vital aspects the WB countries fail to work together and end up in a continuous "zero sum" game. It is often stressed that one consequence of the dissolution of, and war in, the former Yugoslavia was the fragmentation of the region and the creation of new states which have remained burdened by the consequences of war and the disintegration of the former common state. This set of ideas, which are dominant in the literature on the topic of both Western and local analysts, creates premises for two other narratives which I believe are fundamental for understanding the enactment or the failure of a security community in the WB – the narratives of exceptionality and the narrative of failure, which are interlinked.

A series of previous scholars have studied in the recent years the roles of the EU and NATO in potentially fostering a regional security community in the WB[7]. Building or facilitating the manifestation of a security community in the Western Balkans is a crucial process for creating a lasting peace in the region and in the European neighbourhood. The early phases of regional security community development in the Western Balkans over the past decade have been thoroughly assessed by previous researchers[8]. As such we can find a great number of both negative and positive drivers of regional cooperation as well as diverging points referring to pros and cons on the issue of the countries in the WB forming a security community. I organised the main views in two main categories that dominate the debate - „the narrative of exceptionality" and „the narrative of failure" as dominating discourses that have influenced policy making both on the side of the EU/NATO and on the side of local elites. I was guided in the analysis by the fact that the definition of security community points to non-material factors, such as trust, sense of belonging and feelings of reconciliation as the main elements of a designated narrative that point to the formation of such a community. I tried to identify whether these indicators match with the dominating narratives in the studied texts.

Narratives of exceptionality state mainly that the WB represents a region of special concern for the Euro-Atlantic community. There are many arguments for such a stance, but what these narrative simply in the area of policy making is that EU and NATO have a sort of 'duty to intervene' to stabilize this region marked by its own, specific problems. The emphasis is usually put inside this discourse on "special" leading to the necessity of making exceptions to the rule and highlighting the "exceptionality" of the region. The policy consequences of such a narrative is that whatever worked in other cases would not work in our case. Moreover, rules need to be applied differently in the Balkans according to this view, taking into account local sensitivities, the ones which are considered "exceptions" to the rule.

The other major discourse is usually marked by a dominating feature of negativity – the narrative of failure. This entails that no matter the strategy applied in the last 10 years, any action from outside is "doomed to fail" in the case of WB because of the complicated web on interconnected problems that continue to define the area and the numerous unresolved issues. The picture drawn by this narrative is very pessimistic and its impact on the policy level is destructive as it tries to argue that no solution would ever bring positive results in the century long ethnic hatred dominated area. Such a narrative is tributary to what Maria Todorova already in 1997 in her pioneering book "Imagining the Balkans" named as "orientalist" perspectives that negatively stigmatize the Balkans by perpetuating Western negative and colonial stereotypes about backwardness in Eastern Europe.

In short, this narrative argues that both local actors and international community feel that democratization and peace building were not yet reached in the region, with the exception of Slovenia and Croatia. Having a "bad record" of the past conflict, and keeping alive all substantial causes that provoked atrocities throughout the 90s, the WB is described as being still a considerably fragile area. As such, it is being stressed that a regional identity (that would help the creation of a security community) is still strongly influenced by negative stereotypes, the legacy of war and the logic of "Balkanization." Though absence of war and large-scale outbreak of violence is evident, the WB is still regarded inside this narrative as a "powder keg". A related phenomenon is also the negative concept of Balkanization assimilated to fragmentation and ethnic conflict. There are already many analysts who have considered this project of crisis management in the Balkans a failure and even if these countries have still a lot in common (in terms of size, population, multi-ethnic diversity, history and culture) they still do not form a „security community" as defined by the theoretical model. Such a discourse argues that all the basic causes that have provoked wars and clashes in the recent past are still present beneath the surface, nurturing mutual mistrust and un-reconciled ethnic and religious tensions. An extended collection of negative connotations for the recent events in the area are being used as examples by this narrative, pointing to the idea of failed states/ failed policies by the EU and NATO. A special focus here is given to the Dayton Agreement that still organizes ethnic politics in Bosnia and the contested independence of Kosovo as illustrations of this interventionist "failure".

EU's strategy of introducing regional cooperation as part of EU conditionality to guide the integration process is directly connected with the process of security community building in the area. The rationale behind this accelerated security community building attempts was following a neo-liberal costs and benefits logic, focused on the mechanism of interdependence. As such regional cooperation is the concept that dominates EU narratives in relation to the WB countries. All the programmatic documents referring to the region use this term. It became the "mantra" of both its foreign policy component and of its enlargement strategy that has included the countries in the Stabilization and Association process. The EU policy of "stabilization and association" has two main instruments: a regional approach and a policy of conditionality. The regional approach to the countries of the WB aims to build a regional economic and security community, whilst conditioning means that these countries now have the opportunity to become members of the EU and NATO. The condition for that is a process of "socialization", which would make them more compatible with the values, goals and practices underlying the European and Euro-Atlantic community. The view that the improvement of relations and regional cooperation in the WB is a precondition for successful integration of these countries into the EU has become the official policy of the EU in relations with all of them.

There are some evident proofs that political consensus and mutual trust are being built up in the WB. In recent years, a series of highly symbolic manifestations of reconciliation and regional cooperation took place. Gestures of forgiveness after war crimes and of historic apology have mattered a lot for overcoming the pervasive animosities between those countries. But the process has worked mostly on paper and during public festivities especially when you look at a football match between Serbia and Albania as it happened recently, or to the fact that BiH has two national holidays, one for each entity, each celebrating different events and contesting each other. The discourse is thus marked at the symbolic level by the *Us versus Them* debate. However, the progress in relations between Serbia, Croatia and Slovenia has not been followed with adequate progress in Kosovo, BiH and some other areas of the WB, where the situation remains unchanged or has even deteriorated. As such, an important observation to be made here is that an obstacle for security community to fully develop in the region is the fact that there is an unequal involvement of the countries in this process and there are disjoint actions in achieving this "publically acclaimed "common" goal. This is a possible explanation for the persistence of asymmetric results in the process which prevent the creation of a solid security community, independent on Western influence. The ruling elites and public opinion remain divided over the recent past, as well as over the causes and consequences of the civil war in the former Yugoslavia. The interpretation of recent history in the WB is still fundamentally different. This hinders the normalization of relations between the WB countries and the development of regional economic, political and security cooperation. Serbia and Croatia are most important players in the region. the success of the security community depends heavily on their involvement and their bilateral relations. Very relevant are also the weakest actors in the region which are Bosnia and Kosovo. Their willingness to implement required reforms and diminish ethno-nationalists politics in favour of more integrative actions is crucial for the coherence of this security project. I would underline the fact that the interactions between these particular four states are essential for assessing whether EU and NATO managed to build a lasting security community in the WB.

Clearly, as it has been described in the theoretical part, these features do not fit the preconditions of an incumbent security community in the WB, but rather confirm the persistence of Churchill's observation that "the Balkans produce more history than they can consume." These examples are a proof that there are more discursive strategies of maintaining more focus on fragmentation strategies than on building a shared identity.

Conclusions

In the end, the analysis aims to assess whether there are possible lessons to be learnt from this security community building experience in the Balkans that can be transferred to other post-conflict region. The countries from the WB had to overcome a period marked by the symbolic and material consequences of the war, when they were concentrated on emphasising their mutual differences and hostility. This is not the proper setting for developing a security community, which should be characterized by opposite features such as trust, mutual interest and cooperation. After the year 2000 we witnessed a renewal of regional cooperation in the Balkans for which EU and NATO were responsible. But fragmentation is the main obstacle for a successful security community building. Attempts at restoring regional ties ended up with creating competition between Balkan countries which brought more tension and perpetuated the discourse of ethnic hatred more than of defining common goals and a shared identity. The commitment of all of these countries to join the EU and NATO does not automatically imply their willingness to restore mutual relations and create regional institutions. This worked as a destabilizing factor for building a security community.

The external intervention strategy seemed intuitive in the '90s– in order to prepare the WB post-conflict countries to adapt to a larger security community as the EU, they should first reach a smaller community of the same kind between themselves. They needed a previous training for fitting into a larger security community. This should help them overcome bilateral issues faster so that they would not export insecurity in the EU once they gain membership. But this logic created unexpected consequences, as it did not take all factors into consideration. For a security community to be consolidated in the Balkans there is a need for a synergy between the main decision makers, meaning that all countries need active, EU-oriented and reformist parties. This is not yet the case. In order to conclude, building a security community needs local ownership more than external imposition. It is based on the principles of multilateral cooperation and political integration that have defined both EU and

NATO as security communities themselves. External actors have been important drivers in advancing regional cooperation, through EU and NATO conditionality but they cannot replace local ownership. Building a security community means shifting the power game in a certain region from a zero sum game to a win-win situation. Based on the examples and arguments discussed so far, the analysis showed that there are more reasons for observing the lack of a security community than for its existence.

Acknowledgement: This paper was possible with the financial support of the Sectorial Operational Programme for Human Resources Development 2007-2013, co-financed by the European Social Fund, under the project number POSDRU/159/1.5/S/134650 with the title "Doctoral and Postdoctoral Fellowships for young researchers in the fields of Political, Administrative and Communication Sciences and Sociology".

References

[1] Emmanuel Adler and Michael Barnett, eds., *Security Communities,* (Cambridge: Cambridge University Press), 1998.

[2] Karl Deutsch, *Political Community and the North Atlantic Area*. Princeton: Princeton University Press, 1957; Adler and Barnett, op. cit., 1998; Grillot, Suzette R., Rebecca J. Cruise and Valerie J. D'Erman, "Developing Security Community in the Western Balkans: The Role of the EU and NATO," International Politics, 2010, 47 (1): 62–90.

[3] Alexandra Gheciu, *NATO in the 'New Europe': The Politics of International Socialization After the Cold War,* (California: Stanford University Press), 2005

[4] Adler and Barnnett, *op. cit.,* p 45-47

[5] The name "Western Balkans" refers to the Former Yugoslavia plus Albania and minus Slovenia. This is the concept launched by the Austrian Presidency of the European Council in 1999 and its not a concept assumed by or proposed by representatives of the region itself. This shows at the symbolic level the importance of 3rd party players in the region.

[6] According to the UN Resolution 1244. The term "Kosovo" does not make a reference to the status.

[7] Tom Gallagher, *The Balkans in the New Millenium: In the Shadow of War and Peace* (New York: Routledge), 2005; Dimitar Bechev, "Carrots, Sticks and Norms: the EU and Regional Cooperation in Southeastern Europe," *Journal of Southern Europe and the Balkans*, No 8/2006, pp 27–43; Roberto Belloni, "European Integration and the Western Balkans: Lessons, Prospects and Obstacles," *Journal of Balkan and Near Eastern Studies*, No 11, 2009, pp. 313–331;

[8] Filip Ejdus, 2011, "Towards a Western BLkan Security Community, accessed at http://www.bezbednost.org/All-publications/4164/Towards-the-Western-Balkans-Security-Community.shtml accessed on 12.10.2014; Rebecca Cruise and Suzette R. Grillot, "Regional Security Community in the Western Balkans: A Cross-Comparative Analysis", *Journal of Regional Security*, 2013, 8:1, 7–24, available at http://regionalsecurityjournal.com/index.php/JRS/article/viewFile/17/14 accessed on 12.10.2014.

RUSSIAN POLICY IN UKRAINE AND EASTERN EUROPE AND THE RECONSIDERATION OF NATO'S SECURITY IMPERATIVES

Mihaela TEODOR[*]
Bogdan-Alexandru TEODOR[**]

Abstract

The crisis in Ukraine has exposed longer-standing tensions among NATO members regarding the alliance's strategic focus. According to General Philip M. Breedlove, NATO Supreme Allied Commander in Europe, the threat of Islamic extremism and the situation in Ukraine continue to top the list of concerns for the North Atlantic Alliance. After the annexation of Crimea, NATO seeks to reassure Eastern members by strengthening the alliance's periphery. The dilemma is, rather, finding new ways of fulfilling the security objectives established by member countries: collective defence and cooperative security.

Since the crisis in Ukraine will continue to test the durability of NATO and Transatlantic relations, a question – that is, at the same time, the working assumption of current research paper – becomes mandatory: Is NATO prepared to counter non-conventional warfare used by Russia in Ukraine and Eastern Europe? It is possible to find an answer by focusing on the decisions taken at NATO Wales summit of heads of state and government, which took place on September 3-5th, 2014. The main objective of this study is to analyse the final documents adopted at the Wales Summit in order to highlight changes that occurred in setting NATO's security imperatives.

Keywords: NATO future, Ukrainian crisis, cooperative security, collective defence, Wales's summit

Introduction

For the last decade NATO has evolved from an exclusive focus on territorial defence and deterrence in Europe to overseeing a range of military and crises management operations across the globe. This

[*] National Institute for Intelligence Studies, Mihai Viteazul` National Intelligence Academy

[**] `Mihai Viteazul` National Intelligence Academy

transformation was predicated largely on the perception that Russia no longer posed a security threat to NATO and on a conviction that the primary security challenges facing the allies emanated from beyond the Euro-Atlantic region.

Since the crisis in Ukraine tested and continue to test the durability of NATO and Trans-Atlantic relations, a question – that is at the same time the working assumption of this research paper – becomes mandatory: *Is NATO prepared to counter hybrid warfare used by Russian in Ukraine and Eastern Europe?*

It is possible to find an answer to this question by focusing on the decisions taken in Wales NATO Summit (September 3-5th, 2014). In this respect, the main objective of our research is to analyse the final document adopted in Newport, in order to highlight changes occurred in setting NATO's security imperatives.

Russian policy in Ukraine and Eastern Europe

`Russia's military actions in Ukraine came as a strategic surprise for the West` as it was considered by Christian Nünlist and Martin Zapfe in their security policy analyses[1]. Russia's annexation of Crimea on March 18th, 2014 and its continuing intervention in Eastern Ukraine have created a new and destabilizing strategic reality for NATO and EU witch present new challenges for the Alliance. War in the middle of Europe, waged by Russia – a country which was viewed with concern but still treated as a strategic partner – has severely damaged faith in the inviolability of European security.

Moreover, in Ukraine, both conventional military power and *hybrid warfare*[2], a mix of conventional weapons, irregular tactics, terrorism, and criminal behaviour, together with a sophisticated propaganda campaign and political or economic intimidation have been used. The Russian hybrid approach to conflicts has become even more prominent with an extensive use of their special operations forces, `little green men` security forces and intelligence agencies, as well as Russian-speaking minorities, as tools. NATO must plan and exercise for scenarios of hybrid war, starting with the most difficult bit – reaching political consensus. The conflict may go through several stages before reaching the threshold of military action and Article 5. The prospect of hybrid warfare, where internal vulnerabilities come to the fore, adds urgency to inter-agency collaboration at home and inter-institutional cooperation at the international level.

Russia's current aim seems to be the re-building of its sphere of influence. The principal foreign policy goal of Russia is to maintain Eastern Europe in Russia's sphere of influence by stopping, or at least hampering, the political aspirations of Georgia, Moldova and Ukraine to strengthen their ties with both the European Union (EU) and the North Atlantic Treaty Organization (NATO). Russia's new military doctrine, published at the end of 2014, stated that it considered NATO and US efforts in Central and Eastern Europe to be a direct threat.

On the other hand, NATO Secretary General Anders Fogh Rasmussen described the Russian aggression as a `wake-up call` for NATO members and European states[3]. The Russo-Ukrainian conflict created a pivotal moment for the European security architecture changing it inevitable. The security conditions in Central and Eastern Europe have considerably worsened. The region's more exposed frontline countries like the Baltic States, Poland and Romania viewed the crisis in Ukraine, and in general the Russian policy, as a direct and immediate threat.

Russia's annexation of Crimea and the enunciation of a new Putin doctrine that assigns Moscow the right and responsibility to defend Russian speakers everywhere[4], has highlighted the continuing importance of collective defence, one of the founding pillars of the Alliance. Five NATO member countries bordering Russia, two of which, Latvia and Estonia have significant Russian-speaking populations. In this respect, ensuring the defence of all NATO countries has to be the top priority of the Alliance.

The reconsideration of NATO's security imperatives

Some analysts portrayed the Wales Summit as an opportunity to consider a possible strategic shift for NATO, away from the `out of area` focus toward a more narrow focus on territorial defence and deterrence, largely in response to a resurgent Russia.

The reaffirmation of collective defence is the most important moment[5]. The summit's main outcome was assurance of enduring credibility. NATO sent a powerful message which guarantees the collective security of 28 members and Euro Atlantic partnership. Bolstering deterrence against any attack on NATO territory, and reassuring its European allies, became the main topic of discussion. The US Deputy Secretary-General of the North Atlantic Treaty Alexander Vershbow thought that NATO had to "go back to basics" and that it was time to reemphasize the original purpose of the Western military alliance:

> `In response to Russia's actions, we are going «back to basics». We won't abandon our current missions or our core tasks – there are still many threats and challenges out there besides Russia that NATO must be ready for. But we will focus more than before on collective defence`[6].

Fears of further Russian incursions have prompted alliance leaders to reassess NATO's defences in Europe, particularly in the East. The Wales Summit Declaration aims to reassure its Eastern European members, which were Warsaw Pact members until 1991, that they remain safe even after Russia's annexation of Crimea and the increasingly overt military invasion of Ukraine's eastern territories.

The Summit resulted in a large number of political and military measures that aim to foster the outward appearance of closed ranks. Gen. Breedlove urged a strategic re-evaluation of the NATO Response Force, the alliance's rapid deployment force, and said that permanently positioning troops in Eastern Europe should not be ruled out. While Poland has requested a permanent NATO presence on its territory, the Czech Republic opposes the basing of troops. The United States has shored up NATO's air presence over Poland and the Baltic states, and other allies, including Britain, Germany, and Denmark, are looking to provide reinforcements as well.

The Alliance's global ambitions: The withdrawal from Afghanistan at the end of 2014, which marks a tentative end of the alliance's global ambitions, was long announced. The mutual assistance guarantee under Article V, rather than global operations or democratic expansion, has been reconfirmed in Wales as the bedrock of the alliance; and, as the Summit Declaration makes clear, that guarantee is mainly directed against Russia[7]. However, as the Deputy Secretary-General of the North Atlantic Treaty Alexander Vershbow declared in Wales `NATO will remain a multi-purpose Alliance that‘s ready for all contingencies, that looks outwards with a global perspective`[8].

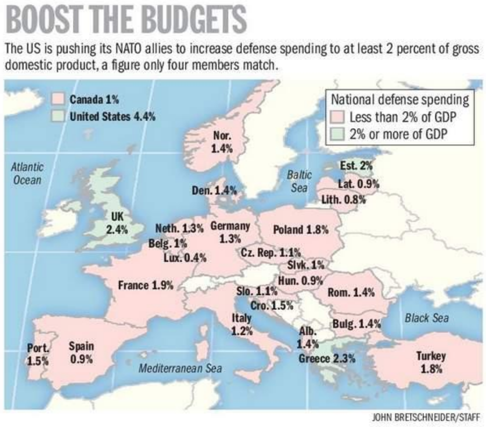
Partnership and Open door policy: Since the end of the Cold War, NATO's membership has expanded from sixteen members to twenty-eight. This open door policy has been an engine of progress towards a Europe whole and free and has contributed much to the collective security of Alliance members. Further enlargement has been under consideration in the western Balkans and with respect to Georgia and Ukraine.

The crisis in Ukraine is also raising questions as to whether NATO should speed the process of adding new members. At the Wales Summit NATO leaders try to convey a strong and convincing message on enlargement. Alexander Vershbow declared that `the Open Door is really still open` and that the process remains merit-based; and that it's taken only in consultations between the Allies and the aspirant countries involved – no third party having a veto[9]. Regarding the partnership, in Wales, NATO announced plans for closer cooperation with Sweden, Finland, Georgia, Jordan, and Australia.

The joint Statement of the NATO-Ukraine Commission, published on 4 September 2014 reiterates NATO members `firm commitment to further develop the Distinctive Partnership between NATO and Ukraine which will contribute to building a stable, peaceful and undivided Europe`[10]. But as a non-member, Ukraine remains outside of NATO's defence perimeter, and there are clear limits on how far it can be brought into institutional structures. Ukrainian Foreign Minister Pavlo Klimkin and NATO General-Secretary Jens Stoltenberg during a meeting on first of October discussed key priorities of the further cooperation[11]. NATO is helping to reform and modernize the Ukrainian armed forces, Rasmussen said, but that doesn't mean NATO is ready to join a shooting war[12].

Europeans need to consider rearmament: In the past two decades, most NATO members have decreased defence spending to historic lows, leaving the United States to foot the bill. The primary limiting factor hindering military transformation has been the lack of European defence spending and investment. Only six of twenty-six European Allies spend 2 percent or more of GDP on these purposes; only about a dozen have met goals for making military forces deployable and sustainable.

From 1990 to 1994, the European members of NATO spent an average of 2.5 percent of their gross domestic product (GDP) on defence. By 2013 that number had plummeted to 1.6 percent, below NATO's 2 percent guidance.[13] The U.S. share of NATO defence spending was 70 percent, and only four NATO allies—the United States, the United Kingdom, Greece, and Estonia – hit the agreed defence spending target of at least 2 percent of GDP.[14]



Source: http://www.defensenews.com

On May 2nd, 2014, US Defence Secretary Chuck Hagel was calling on NATO members to invest more on defence in the face of Russian aggression.[15] Earlier in April, US Vice President Joe Biden, speaking at a conference at the Atlantic Council, said he hopes to see that `by Wales all NATO members will have increased their commitments to NATO, to NATO's reassurance efforts and to their own defence budgets`.[16]

To bolster deterrence, NATO must develop the mechanisms, capabilities and political will for effective action on its eastern flank. To achieve this, European members of the Alliance must fulfil their pledge to reach 2% of GDP in annual defence spending by 2025.[17]After Wales, Lithuania, Romania and Sweden have all announced plans to boost spending. Only Estonia, among European Allies, will meet the 2% of GDP target in 2015, while the rest of the member states more or less gave up on this "benchmark". Defence expenditure did increase in Poland, Latvia, Lithuania, the Netherlands, Norway and Romania – the leading responders to the Russian threat. In contrast, Canada, the United Kingdom, Italy and – most importantly – Germany, significantly reduced their military budgets.[18] The latter trend is also apparent in Central Europe, particularly in Hungary and Bulgaria, creating a negative balance overall within NATO and raising further doubts in the United States about Europe's willingness to defend itself.

How to deal with Russia or cooperative security: The NATO-Russia partnership was conceived as a means for fostering security in the Euro-Atlantic region; in 2010, the Alliance remains dedicated to that goal the Strategic Concept reaffirming NATO's desire to help build a cooperative Euro-Atlantic security order which includes security cooperation with Russia.[19] After Moscow's annexation of the Crimea, its ongoing destabilization efforts in Eastern and Southern Ukraine, and public pronouncements that it is willing to `protect` Russian minorities anywhere in the world, including in NATO member states, it is almost impossible **to talk about Russia as a partner anymore**. In this respect, Alexander Vershbow declared in May 2014: `Russia seems to have chosen confrontation over cooperation, and to view NATO as a strategic rival. As a result, we cannot ignore the reality of Russia's present course and we must review our relationship`[20].

In April 2014, NATO suspended cooperation with Russia over Moscow's alleged role in the Ukrainian crisis, a claim Russia has repeatedly denied. Gen. Breedlove, NATO's top military commander, said in May 2014 that the Alliance needs to prepare for a future in which Moscow can no longer be viewed as a partner.[21] While NATO has suspended practical cooperation with Russia, it has `kept the chance for political contact open`[22].

The US deputy Alexander Vershbow declared on 5th September: `We will await a time when more enlightened leadership in Moscow allows us to rebuild the true strategic partnership with Russia that we desire`[23]. NATO's new Secretary General Jens Stoltenberg said on first of October 2014 that the Alliance was ready to consider a proposal to convene the Russia-NATO council if it gets such a request.

Unlike his predecessor, Anders Fogh Rasmussen, Stoltenberg has a more flexible approach toward Russia. In what concerns the approach of hybrid warfare the Alliance has to speed up its adaptation to the new strategic environment.

Conclusions

Russia's illegal annexation of Crimea and destabilization of Ukraine give NATO renewed purpose. Essentially, the debate in Wales was over the future role Russia should play within the European security architecture. The Alliance diverge significantly, especially concerning the question of how to deal with Russia, while solidarity persists on maintaining sanctions against Russia. The Western community is ready to impose additional sanctions if further destabilization occurs, but serious questions remain as to whether the same principle also applies to the deployment and development of defence capabilities.

Wales Summit constituted a turning point in the history of NATO. In September 2014, NATO leaders agreed a number of concrete measures aimed at strengthening collective defence and deterrence. At the Wales summit, NATO leaders agreed to increase the Alliance's military presence in Central and Eastern Europe (CEE). In so doing, the Allies responded to the concerns of Poland, the Baltic States and Romania - NATO members who feel directly threatened by Russia's actions in Ukraine. However the real significance of the Wales Summit will be judged by the level of effective implementation of the decisions made by the Alliance, as well as, by the effects they will have on strengthening transatlantic security.

The NATO summit in Wales ended on 5 September 2014 with a symbolic gesture. In 2016, the heads of state and government of the 28 allied countries will assemble in Warsaw for the first time – in the city where the Warsaw Pact was founded in 1955. In this way, NATO aims to reassure its Eastern European members, which were Warsaw Pact members until 1991, that they remain safe even after Russia's annexation of Crimea and the increasingly overt military invasion of Ukraine's Eastern territories.

References

[1] Christian Nünlist, Martin Zapfe, *NATO after Wales: Dealing with Russia*, Center for Security Studies (CSS), Analyses in Security Policy, Issue no. 161, October 2014, Zurich, p. 2, accessed on June 11, 2015 at http://www.css.ethz.ch/publications/pdfs/CSSAnalyse161-EN.pdf.

[2] Julio Miranda Calha, *Hybrid Warfare: NATO's New Strategic Challenge?*, General report draft for NATO Parliamentary Assembly Defense and Security Committee, April 7, 2015, p. 2, accessed on June 15th, 2015 at http://www.nato-pa.int/default.asp: `Hybrid warfare exploits domestic weaknesses via non-military means (such as political, informational, and economic intimidation and manipulation), but is backed by the threat of conventional military means. While the concept of hybrid warfare is not new, its application by Russia against NATO member states' interests present new challenges to the Alliance`.

[3] *NATO Secretary General speaking after a meeting of NATO's defense ministers in Brussels*, 3 June 2014, accessed on June 2014 at http://www.bbc.com/news/world-europe-27690320 and http://www.washingtonpost.com/world/national-security/russias-moves-in-ukraine-are-wake-up-call-natos-rasmussen-says-in-speech/2014/03/19/80560d7c-af88-11e3-9627-c65021d6d572_story.html.

[4] *Concept of the Foreign Policy of the Russian Federation*, Approved by President of the Russian Federation V. Putin on 12 February 2013, art. 4. g) `ensuring comprehensive protection of rights and legitimate interests of Russian citizens and compatriots residing abroad, and promoting, in various international formats, *Russia's approach to human rights issues*`, unofficial translation of the document, accessed on June 2014 at http://www.mid.ru/bdomp/nsosndoc.nsf/1e5f0de28fe77fdcc32575d900298676/869c9d2b87ad8014c32575d9002b1c38!

[5] Wales Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, accessed on June 2015 http://www.nato.int/cps/en/natohq/official_texts_112964.htm

[6] Remarks by NATO Deputy Secretary General Ambassador Alexander Vershbow at the Atlantic Council of the United States Conference, *Toward a Europe whole and free*, Washington DC, May 1st, 2014, accessed on June 2015 at http://www.nato.int/cps/en/natohq/opinions_109419.htm?selectedLocale=en.

[7] *Wales Summit Declaration* issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, accessed on June 2015 http://www.nato.int/cps/en/natohq/official_texts_112964.htm

[8] http://www.nato.int/cps/en/natohq/opinions_112977.htm

[9] Remarks by NATO Deputy Secretary General Ambassador Alexander Vershbow at the NATO Future Leaders Summit, Cardiff – 5 September 2014, accessed on June 2015 at http://www.nato.int/cps/en/natohq/opinions_112977.htm

[10] Joint Statement of the NATO-Ukraine Commission, Published 4 September 2014, accessed on October 2014 at https://www.gov.uk/government/publications/nato-summit-2014-joint-statement-of-the-nato-ukraine commission/joint-statement-of-the-nato-ukraine-commission

[11]Ukrainian Foreign Ministry declarations on October 8, accessed on June 2015 at http://en.ria.ru/military_news/20141008/193827028/Ukraine-NATO-Agree-Cooperation-Program-for-2014-2015-Kiev.html

[12] Joint Statement of the NATO-Ukraine Commission, Published 4 September 2014, accessed on October 2014 at https://www.gov.uk/government/publications/nato-summit-2014-joint-statement-of-the-nato-ukraine-commission/joint-statement-of-the-nato-ukraine-commission

[13] Zachary Fryer Biggs, *US Pushes NATO Allies To Boost Defense Spending*, May 3, 2014, accessed on June 2015 at http://www.defensenews.com/article/20140503/DEFREG01/305030021/US-Pushes-NATO-Allies-Boost-Defense-Spending

[14] Ibid.

[15] Marcus Weisgerber, *Hagel Calls for Large NATO Countries to Step up Defense Spending*, Defense News, May 2nd, 2014, accessed on June 2015 at http://archive.defensenews.com/article/20140502/DEFREG02/305020023/Hagel-Calls-Large-NATO-Countries-Step-up-Defense-Spending

[16] Ibid.

[17] Dániel Bartha, Jakub Kufčák, Marian Majer, Mário Nicolini, *From Wales to Warsaw: NATO's radically adapted posture – or lost in between?* In Security and Defense policy briefs, June 10, 2015, accessed on June 2015 at http://www.cepolicy.org/publications/wales-warsaw-natos-radically-adapted-posture-or-lost-between

[18] Ibid.

[19] The 2010 Strategic Concept for the Defense and Security of the Members of the North Atlantic Treaty Organization, adopted by Heads of State and Government in Lisbon., accessed on June 2015 at http://www.nato.int/cps/en/natohq/topics_82705.htm

[20] Remarks by NATO Deputy Secretary General Ambassador Alexander Vershbow at the Atlantic Council of the United States Conference, *Toward a Europe whole and free*, Washington DC, May 1st, 2014 accessed on June 2015 at http://www.nato.int/cps/en/natohq/opinions_109419.htm?selectedLocale=en

[21] Marcus Weisgerber, Hagel Calls for Large NATO Countries to Step up Defense Spending, Defense News, May 2nd, 2014, accessed on June 2015 at http://archive.defensenews.com/article/20140502/DEFREG02/305020023/Hagel-Calls-Large-NATO-Countries-Step-up-Defense-Spending

[22] Ibid.

[23] Remarks by NATO Deputy Secretary General Ambassador Alexander Vershbow at the Atlantic Council of the United States Conference, *Toward a Europe whole and free*, Washington DC, May 1st, 2014 accessed on June 2015 at http://www.nato.int/cps/en/natohq/opinions_109419.htm?selectedLocale=en

THE BLACK SEA SECURITY ENVIRONMENT IN THE CONTEXT OF RUSSIA'S AGGRESSIVE INVOLVEMENT IN UKRAINE, AND THE INFLUENCE ON ROMANIAN-POLISH RELATIONS [1]

Şerban Filip CIOCULESCU

Abstract

By militarily intervening in Ukraine and illegally changing the borders, Russia showed its revisionist aims and the tendency to stop the possible EU-NATO expansion and power projection, by controling the key-areas of the Wider Black Sea area. Contemporary Poland and Romania are closely connected countries, both being members in the EU and NATO and situated on the eastern flank of the Euro-Atlantic world. They are clearly disturbed by Russia's territorial revisionism and would like to see a coherent West protecting the Helsinki status quo. Romania and Poland want to develop the political, economic, security and cultural cooperation but they must overcome some bureaucratic, mentality and material obstacles. After the NATO Wales summit in September 2014, these states are part of NATO's defensive strategy to deter Russia from a possible new aggression, this time against a member state.

Keywords: diplomacy, strategic partnership, cooperation, security, aggression, revisionism, Euro-Atlantic, Black Sea

Şerban F. Cioculescu (PhD in political science) is a guest lecturer at the University of Bucharest, Department of Political Science, International Relations and Security Studies, a lecturer with the National Defense College of Romania and also a senior scientific researcher with the Institute for Political Studies of Defense and Military History from Bucharest. He is specialized in Euro-Asian strategic studies, security studies, international organizations and international relations theory.

Both Russia and Ukraine are Black Sea littoral states and the recent "drama" of Crimea occurred in that specific area. First, we have to define the Greater Black Sea region using the membership within the Black Sea Economic Cooperation organization – the riparian/littoral states – Bulgaria, Georgia, Romania, Russia, Turkey and Ukraine – and possibly also other adjacent countries which, from a security point of view, belong to the same area – Albania, Armenia, Azerbaijan, Greece and Moldova.

The Black Sea area after the Cold War has been seen as a possible area of cooperation between the West and Russia, but if one looks at the actual crisis between Russia, Ukraine and the EU/NATO states, this could be called a failed opportunity. The classical narrative states that Moscow and Brussels strive to attract the riparian states with their own areas of influence and institutional structures: the Eurasian Economic Union (former Custom Union Russia-Belarus-Kazakhstan)[2] vs. the EU's common market, Eastern Partnership – European Neighbourhood Policy (ENP) and NATO's Partnership for Peace (PfP) and special associative frameworks (like the "commissions" with Georgia and Ukraine). On the other side, many EU states – Greece, Italy, Hungary, Austria a.s.o. (which depend on gas and other economic benefits from Russia) – are very sensitive to avoid any action or stance which could exacerbate Russia's anger and reluctantly agreed to the economic sanctions decided by the EU against Moscow.

During the Cold War, the GBSR was a stalemate between NATO (through Turkey, a geopolitical key-member) and the Warsaw Pact (USSR plus Romania and Bulgaria as riparian states). The failed attempt by Soviet leader Joseph V. Stalin to allow the USSR to establish military bases and free entrance into the Straits immediately after the end of the Second World War was the signal for the US and their allies that the Communist/Soviet block had to be contained. The disintegration of the USSR led to the emergence of the newly independent states which chose to become members of the Commonwealth of Independent States (therefore accepting to be in Russia's sphere of interest) but also, after some years, signed the Partnership for Peace and EAPC framework with NATO, plus the Partnership and Cooperation Agreements with the EU. Being a member in Russia's organization and in the West's cooperative structures was possible on the condition that Moscow, Brussels and Washington perceive their relation as "non-zero sum game" and privilege cooperation over rivalry. This has been basically the case between 1991 and 1998 (before the Kosovo war), but this is not the case nowadays.

On the other side, the legal status of the Black Sea Straits is still stipulated by the "old" Montreux Convention (1936) which gives Turkey the right to check the traffic of civil and military vessels and keeps the Black Sea closed to other foreign powers. Both USA and Russia are worried about Ankara's interpretation of this legal document, meaning the effective time that the foreign vessels could stay in that sea.

The Black Sea after Crimea and the fate of Ukraine

Even before the Crimea crisis, it was known that Moscow and Kyiv had some long-lasting conflicts over a wide range of issues: the sharing of the Black Sea Fleet, the division of former Soviet property, acquisition of energy, international debt repayments, the functioning of the CIS and the ownership of nuclear weapons.[3] In Crimea, from a population of 2.5 million there were 1.7 million ethnic Russians, 600,000 Ukrainians and 280,000 Tartars. Apparently, the fate of the Black Sea Fleet was settled with the signing of the Friendship Treaty on 30 May 1997, but the Russian tolerance towards Ukraine was indeed dependent on Kyiv accepting to stay within Moscow's sphere of influence. When activists in the Maidan Nezalezhnosti (Independence Square) managed to hunt down president Yanukovich and his associates, making them abandon power, flee to Russia and replacing them with opposition leaders, which were known for their anti-Russian stance, Moscow decided to implement the plan of tacking back Crimea and then to destabilize the Donbas area, in order to prevent Ukraine getting closer to EU/NATO. Of course, Ukraine depends almost totally on Russian gas and oil, but Russia also exports 80% of its gas for the EU states via Ukraine, thus the frequent "gas wars" between Moscow and Kyiv, which also affected some EU states. Only 30% of the natural gas used by Ukraine is produced internally and 25% of the oil.[4]

Of course, Russia got Crimea and significantly improved its power position with the Black Sea. But Crimea was not such a radical departure from the status quo ante, as one could think. The August 2008 war between Russia and Georgia was the first major change of territorial status quo, producing two separatist republics recognized only by Russia and some Latin-American states, thus obviously the so-called “Medvedev Doctrine” plays against the sovereignty of Russia‘s small neighbours. This doctrine was formulated by Dmitri Medvedev, the prime minister of Russia and former president, and refers to so-called right of Russia to help Russian minorities abroad, including by using the force. The Crimea and later Donbas battles brought the idea of “hybrid” warfare in the eyes of the public opinion.

So, in the end, after a likely years-long planning, Russia changed the southern Ukrainian borders by military force, setting up a dangerous precedent. Incorporating Crimea brought the strategic advantage of controlling the major lines of transport and military advantage over other riparian states. Crimea means 27.000 sqm and 2500 kms of new borders – having a terrestrial connection with Ukraine by the Isthmus of Perekop, but it lacks the terrestrial contact with Russia, as long as a bridge over Kerch strait will not be built. The issue of Tatars is a very sensitive one: once Moscow got Crimea, the Tatars proceeded to forced immigration, relocation in western Ukraine, or they were forced to accept Russian rules, abuses, violence committed by state officials. It is certain that Russian authorities in Crimea try to eradicate the Ukrainian language, culture and education and punish Tatar leaders for their pro-Ukraine preferences. Turkey is heavily irritated about the fate of Tatars but does not want to further deteriorate the relations with Russia (Ankara is dependent on gas from Russia and hopes for new pipelines).[5] Anyway, this situation did not bring an end of Russian-Turkish “entente” in the Black Sea.

Moscow now suggests that the West carried most of the guilt since it refused giving a chance to Russian vision on new European security architecture. In fact, during the summer 2008 and again in 2009, through the voice of then-President D. Medvedev, Russia proposed a pan-European security treaty based on the idea of “multipolarity” in international relations and the implicit recognition of the legitimate spheres of interests for the great powers. Several European countries, especially France, Germany, Italy, have shown interest in the idea, however others, particularly those in North and East, have expressed scepticism and distrust. In November 2009, Russia formally presented a draft of the so-called “European Security Treaty” to all OSCE member states but it also addressed NATO and EU states. The main points were the not-resorting to force for aggressive aims, non-interference in domestic affairs of other states (including the commitment not to help states which actually infringes on other ones' security) and reasserts the role of the UN Security Council as the sole legitimate instance to deal with military conflicts. One could also find trust building measures among states: mutual consultations and dialogue, the right of member states to receive information from other states which take military measures that could affect their security. If one state is attacked the other could provide it with support until UN Security Council would take the necessary measures for defence. According to article 10 of the draft, the eligible members for this new organization will be all the states "between Vancouver and Vladivostok", but also regional organizations like EU, NATO, OSCE, CIS, CSTO.[6]

The draft treaty alarmed some of the western states because it asked the members that previous obligations should not contradict the new treaty. Thus, in case of a possible aggression against a NATO member, the Alliance could not intervene because the Washington Treaty is no more valid in face of the new pan-European and Eurasian organization![7] The collective defence and self-defence risked to be undermined by the new structure, thus enhancing the vulnerability of some small states which are confronted with powerful neighbours.[8]

I think that in the current situation, Russia cannot unilaterally put an end to the escalating crisis with the West, for psychological and material reasons. It could in the end even deploy nuclear weapons in Crimea and Kaliningrad if the West would heavily arm Ukraine, if Russia would be totally excluded from the NATO missile shield in Europe, if it felt threatened and under heavy economic burden (otherwise Vladimir Putin fears losing political power to domestic opposition and a diminished prestige at home).

On the other side, Ukraine and Moldova are facing the possibility of increased ethnic conflict and secessionist tendencies: Ukraine remains a weak state (lacking a single national identity, heterogeneous ethno-religious landscape, with a poor economy and bad governance), while Moldova is also a weak state with ethnic problems (the Russian and the Gagauts minorities are striving for more independence), thus without foreign support they could become in the end failed states. The issue of Ukrainian refugees is also a very hot one – there are hundreds of thousands who fled to Russia, Poland, the Baltic states, Romania and even Turkey but also many internally displaced persons etc. The humanitarian and economic issue of the refugees goes together with the risk that some of these people will form guerrillas for vengeance or will commit terrorists attacks.

From a geopolitical point of view, the "Novorossiya" concept, referring to the entire territorial belt from East to Southern Ukraine (from Donbas to Budjak) illustrates the Russian old imperial dream – Moscow could in theory try to conquer all eastern and southern Ukraine, but this would completely marginalize it and destroy its already feeble economy. Russian president V. Putin said many times that he does not consider Ukrainians a different nation from the Russians, indeed "one nation" in "Eastern and Western Rus".[9] He refers to the fact that the origins of the Ukrainians as a nation are entangled with those of the Russians, going down to the medieval state Kievan Rus. In the field, Russia seems to prefer to make Donbass another Transnistria, meaning a long standing frozen conflict, rather than conquering "Novorossiya" and assuming the costs for that.

Generally speaking, Russia sees its competition with the EU for their common neighbourhood as a "zero sum game". It is an existential rivalry, since the EU is seen as a competing imperial project, a continuation of the Western hegemony. One should remember that even since the 19th century, the Russian "Narodnis" and "Panslavists" had in their doctrines the idea of isolating the country from the Western influence, considered to be nefarious for the Russian soul and political life. On the other side, obviously the West is not able and willing to stop Russia's aggression in Ukraine because of the risk of war and because of the lack of a single voice in the foreign policy. The West uses the economic tools (the sanctions) to gravely hit Russian economy – the flight of capital, the devaluation of the Rubble, the food scarcity, oil price diminution are the most visible consequences.

What about Ukraine? Is it an artificial state? Indeed, it was created as a territorial entity by the Russian empire and later Soviet Union. In a certain way, it could be like that. But we should remember that there are no "natural" states, only some of them are older and more homogenous than the others. Why should we see Belgium as a more “natural” state than Ukraine? Only because it is about 200 years old while Ukraine only 24 years old? Both are multi-ethnic and multi-religious countries, with secessionist trends. If Ukraine will eventually split, its Centre-West will certainly try to become an EU and NATO member, while the East will be kept as a buffer state by Russia (an independent state) or even become Russian territory in an extreme scenario. Also, remaining at the level of imaginary scenarios, the West of Ukraine could be hypothetically incorporated into Poland, Romania, Slovakia and Hungary or stay as an independent country. But is the West ready to accept Ukraine and even Republic of Moldova into NATO and EU in the near future? This does not look plausible, at least at the moment of writing this study. Or could Ukraine and perhaps Moldova become part of a defence pact with Poland, Romania and the Baltic states? We cannot preclude such a scenario, but in this case NATO would not count any more or would have ceased to exist, so its eastern members would find other defence structure to cope with Russian threats.

On the other hand, is a geopolitical agreement between EU and the Eurasian Economic Union possible in the end? In economic terms, it doesn’t seem possible, since there are different markets with different rules and foreign tariffs, but to save peace one can imagine some clever engineering solution for cooperation between the two “unions”.

Poland and Romania as a counterbalance to Russian destabilization on NATO’s eastern flank

Historically, the diplomatic bilateral relations were established in January 1919, at the level of „legation” and later in 1938 at the level of embassy. [10] In the interwar period, the two states had a mutual defence treaty and they cooperated against the advances of Communist Russia.

During the communist regimes both countries were part of the Soviet sphere of influence and participated in the Warsaw Pact Organization.

Romania and Poland signed the Treaty on friendly relations and cooperation on January 25th 1993 in Bucharest, by Polish

Minister of Foreign Affairs Krzysztof Skubiszewski and his Romanian counterpart, Teodor Meleşcanu. The treaty became valid in December the same year. The main issues were the common pledge for a stronger EU and the membership of both states with it, the need to deal with international and regional conflicts and the protection of human rights.

More than that, the two states have a **Strategic Partnership** (SP) since October 7, 2009, when the two presidents signed the Common Statement and then on October 26, 2010, they agreed on the **Action plan**, during the Polish president's visit in Romania.

Geographically, there is a close connection via the Baltic Sea-Black Sea axis. Now, Romania and Poland share the EU and NATO external borders and are aware of the transnational risks and threats related to the "border country"/frontline state position. Anyway, despite Russia's aggressiveness, the situation nowadays is incredibly good, even better than in the interwar era, when Poland and Romania had a defensive convention of alliance from 1921 but were caught between two geopolitical "monsters": Nazi Germany and Soviet Union. The two countries did their best to survive, they went over foreign occupation and permanent lost of some territories, they faced the killing of many of their citizens by foreign states, the destructions of the war, then the horrors of the communism. Now, both are among the "big countries": Poland is the sixth place and Romania the seventh one in terms of population, with the EU.

NATO and the EU as privileged place for cooperation

Of course, **the future of the European Union** is the main focus for both Romania and Poland. First, the EU must have a more coherent CFSP and second, a more effective management of its neighbourhoods. There is a need to relaunch the European Neighbourhood Policy which had a relatively low profile because of the different strategic and geographic focus of the EU's main powers, the western ones, to their former spheres of influence (the Southern flank). In 2008-2009, Poland and Sweden launched the Eastern Partnership initiative and made it soon a part of EU's ENP. Romania eventually understood that it has to be part in this process, as a state located on the EU's eastern flank and overcame the initial hesitations, supporting the EaP and trying to develop a national expertise in this field.

Within the EU, Poland and Romania want to enhance the process of the European integration; they want to support EU's neighbours via the European Neighbourhood Policy (ENP) and the Eastern Partnership (EaP).

Within the EU, Romania and Poland generally have similar views on the Common Security and Defence Policy (CSDP) and eventually converged on the ENP-Eastern Partnership's main issues. They agree that Europe must rely on a strong and coherent diplomacy, backed by a common strategic culture and by much more military strength. Diplomacy by itself is not necessarily effective and credible without the military deterrent. Situations of crisis and civil war like in Libya, Syria or Yemen cold become frequent in the southern belt – the Middle East-Northern Africa (MENA), as the "Arab Spring" tends to evolve into violent ethnic, socio-economic and religious clashes and civil wars.

In the CFSP-CSDP realm, Romania and Poland could work together to come with proposals for revisiting the European Security Strategy. They must support the pooling and sharing method and support an enforcement of the European Defence Agency's role. They must work within the European External Action Service and provide the High Representative for CFSP with relevant information concerning the Baltic-Black Sea flank. They must ask for an increased use of the EU Battle groups and profoundly reflect on the proposal of the European Commission's president H. Junker concerning a real European army, thus an enhanced EU-NATO harmonization.

Both countries want a strong Euro-Atlantic Alliance with the USA keeping its preponderant systemic power and Germany, France, Great Britain playing a leading role in Europe, from a military perspective. They fear the dissolution of the Alliance and the diminishing of the relevance of article V (i.e. collective defence) of the Washington Treaty. They also want contingency planning for all the flanks and to "keep an eye" on Russia. Nowadays, **NATO** is still the best security provider and guarantor for the two states, but they must ensure that it would be effective and fast in case of a threat evolving in a crisis or a conflict. There is a question of solidarity and cohesion among the 28 member states: they must see together which are the main risks and define in a similar way the challenges and the potential aggressors. The member states should also invest much more in their common defence and the European members should not avoid paying more for their collective defence while hoping that the USA would always do the main tasks.

The two states must think also at he possibility to reshape article 5 from the Washington Treaty in order to make it more committing in case of an armed attack against a member state must be studied. Article 5 planning must be developed by NATO strategic headquarters[11], while diplomatically explaining to eastern non-NATO states that the Alliance is a strictly defensive one with no aggressive intentions.

Within NATO, Romania and Poland could buy together military equipment's using the "smart defence" concept (or the EU's "pooling and sharing" doctrine), or at least use together military planes, helicopters, drones etc. The maintenance for the F16s could be a good beginning in this process. Of course, the permanent exchange of opinions and technical cooperation is a must.

The relations with the USA

Both states have PSs with Washington and acknowledge US undisputed role of supporting most of the defence economic burden with NATO, also having most of the rapid reaction units for enhancing the eastern flank. Poland and Romania will have on their territory **elements of the US anti-missile shield (NMD)** and will be part of the US grand strategy to keep a strong West and a predictable strategic environment. Poland hosts a battery of Patriot 3 missiles but it is developing also its own defensive missile system (Warsaw planned to spend maximum US$400 million on the creation of its own missile defence system, after in March 2013 Washington announced the plan to cancel the installing of the last generation of interceptors SM-3 Block IIB in Poland. Anyway, Poland will have Block IIA installed in the third phase. Up to now, Romania did not take into account the likelihood to buy and install some anti-missile elements on its own, but nothing is impossible and the Polish experience must not be neglected. In 2009, US President Barack

Obama had decided to change the anti-missile shield plan inherited from George W. Bush Jr., giving up the locations from Czech Republic and instead preferring Poland, Romania and Turkey for placing interceptors and radars. Obama later cancelled an earlier interceptor intended for Poland and the radar in the Czech Republic, replacing the high-speed interceptors with slower ones in order to counter Iran's medium-range missiles. The missile defence technology will be deployed in 2015 in Romania and in 2018 in Poland.[12]

From a different angle, the Polish and Romanian citizens still need visas to travel in USA, which is not the case for the older EU states and the two governments should put a bigger pressure on the US government to give up visa requirements for all EU states. They already have the support of the European Commission and Parliament. In strategic terms, both Poland and Romania are key-players in the defensive game of deterring Russia from changing borders and the balance of power in the Black Sea area.

Defence cooperation

In the field of **armaments defence cooperation**, possible areas of cooperation regard the Collaborative Database (CODABA) and the Armaments Co-Operation with the European Defence Agency (EDA), with programs such as transport helicopters, cyber security, air strategic transport capabilities, intelligence, reconnaissance etc.

In 2012 a regular strategic dialog started between Poland and Romania, with the participation of Ministries of Foreign Affairs, Ministries of National Defence and the General Staffs of the armies.

Regarding the **Visegrad Group** (V4 – Poland, Czech Republic, Slovakia, Hungary) - in the past, Romania did not manage to become a member in this group, being rejected in 1992 for its so-called lack of a real central-European identity and its democratic deficit.

I personally consider Poland as being the “natural” leader of V4, being the biggest member, with the strongest economy and the most powerful army. Between July 2012-June 2013, Poland had the V4 presidency and pushed towards a more assertive role for this group. It is likely that the V4 Battle Group will be ready and reach the stand by phases in 2016 - the Polish V4 presidency stated that "There will be a need for V4 consultations on NATO Russian relations, a V4 common position on Missile Defence and on the Russian response, on NATO cooperation with Ukraine and Georgia, consultations on CFE and force deployment in the region, consultations, in the broader format of V4+ Baltic states + Romania and Bulgaria, on common security issues, and with regard to cyber security and energy security. I think Romania could eventually be associated with such regional initiatives as V4 Battle Group (to be ready in 2016) but only on the condition that its legitimate interests are taken into account by the member states. At the same time, this has to help us building a foreign policy identity.

Under the huge pressure of Russia's annexation of Crimea and illegal involvement in the Donbass conflict, eventually it seems that Polish-Romanian **military cooperation** will enhance. Romanian minister of National Defence, Mircea Duşa, met his Polish counterpart Tomasz Siemoniak, on 21 March 2014, and they discussed about the need for coordination and more NATO involvement in the context of the Ukrainian crisis, also about the preparation of NATO summit in September.[13] Among the other topics discussed, one should mention the cooperation agreement between Romania and Poland, especially between their air forces, the stage of the US missile defence system implementation and issues of maritime security in the greater Black Sea region.[14] Romania committed to grow its military budget to about 2% of the GDP in 2016-2020, while Poland announced an increase of 40 billion USD in ten years!

Both Poland and Romania claim a much stronger military presence of NATO forces on the eastern flank of the Alliance, being border-countries for NATO and EU. Poland asked that two heavy brigades be deployed in the Polish-Baltic space, but Germany and Netherlands were opposed to this plan. Bringing more troops and weapons here is considered by Germany, France and other states as against the provisions of the Treaty on conventional armed forces in Europe (CFE treaty). But since Russia stopped its commitment to the CFE in 2007 and the western states also gave up in 2011 –it would be illogical to ask NATO states to unilaterally respect this treaty now. We saw Russia deploying forces and capabilities near the eastern border of Ukraine and in Crimea, even possible nuclear missiles in Crimea.[15] It is true that, in 1997, NATO committed itself to abstain from deploying large number of troops and military assets near Russia's borders, but since Russia also violated the guarantee agreement over Ukraine (signed in 1994 by Russia, USA and Great Britain), this commitment should be interpreted in a more relaxed way.

Of course, the CFE was useful and must be replaced by a similar treaty or a wider regional arrangement, but there should be a negotiated one and the West is not expected to put itself in a situation of vulnerability on its eastern border when Russia begins to enlarge by force its territory.[16]

Romania would also like to receive more Polish support for the Black Sea Synergy and the Black Sea Strategy (both being EU initiatives) and seek bigger involvement with the Eastern Partnership. Bucharest wants Poland to get more involved in the Black Sea area, this seems to be the idea behind the launching of the **Romania-Poland-Turkey "triangle**" in 2012. Turkey and Poland are pivotal states, thus having an added-value for the Romanian foreign policy. Poland and Romania must try to reassure Turkey against any Russian actions or threats and avoid the trend towards a too close relation between Ankara and Moscow, which would be detrimental to NATO coherence.

During the last months, USA became more firm in ensuring the flank deterrence - moving troops in Poland, Romania, the Baltic states on a rotation basis, in spite of president Barack Obama being limited by the opposition congressmen who prefer not to risk a war with Russia. Now 300 US troops are training Ukrainian soldiers from National Guard, this is a good beginning for more commitment.

At NATO's summit in Wales (September 2014), the allied leaders decided to create five "trust funds" —defence cooperative programs funded by NATO member countries that are meant to help Ukraine reform and modernize its defence capabilities. — including one for cyber defence to help Ukraine's military. Romania, a member of NATO's cyber coalition exercises, decided to lead the Ukraine Cyber Defence Trust Fund — and selected the state-owned Rasirom Company.

Energy, economic and defence issues for cooperation

Romania and Poland share the common interest that the EU as a whole must be less dependent on the **energy resources** imported from Russia, thus seeking diversification of the supply corridors and developing alternative less polluting resources. Among the EU members, they are among those favouring the research and exploitation of the shale gas, the diversification of transport corridors. The Strategic partnership stands that Romania and Poland have the European energy security as a priority goal for cooperation. In March-April 2014, following the Ukrainian crisis' aggravation, Poland proposed a European Union of Energy, in order to create a joint mechanism for energy procurement at the EU level and a mechanism for negotiation with foreign suppliers (like Russia) in a coherent and unitary way. Of course, Romania openly supports this project which was endorsed also by other EU states, but it is possible that Bucharest will be strongly influenced by Germany's position on this issue.

Poland proposed in 2014 a **European Energy Union** – mechanisms for solidarity and common approach to third states, EU as a common front and avoiding separate deals with energy sellers. Romania must be able to support this project.

Recent developments: on 2 March 2015 the two presidents met in Warsaw and signed a common statement – preparing for NATO 2016 Warsaw Summit. They asked for common positions and common ideas to enhance NATO eastern flank. The Polish president Mr. Komorowski wanted to organize in Poland a meeting of the three presidents – Poland, Ukraine, Romania, on a regular basis. He warned that we should have a plan in case Russia does not respect the Minsk II agreement (the non-compliance scenario). Romanian president Mr. Klaus Iohannis spoke about the need to assess and consolidate the NATO eastern flank, provide support to Ukraine and Moldova and organize a meeting of the chiefs of states of NATO states in Bucharest, this autumn. He called **the bilateral relation with Poland a strategic priority.**

Facing the Russian geopolitical revisionism

The Russian military conquest of Crimeea, using hybrid warfare tactics - paramilitaries without official signs, called „self-defence forces", propaganda, cyberwar - and the implicit threat that all Eastern and Southern Ukraine (what Russia's leader V. Putin calls „Novorossya", following the Russian imperial tradition) could end by becoming part of Russia again, or a satellite state controlled by it, pushed Poland and the Baltic states to ask for a more detailed contingency planning and more US troops on the eastern flank. Eventually, after the NATO Wales summit in September 2014, the Romanian president announced the fact that Romania will benefit from an allied contingency planning on its eastern border - **which is still pending approval.**

Romania and Poland contribute to the economic "embargo" against Russia, they also must think ways to reduce their dependency on Russian gas. They are among the states which were invited by the Rada of Ukraine (lower house of Parliament) to take part in military exercises with the Ukrainian troops, to increase their effectiveness and operability.

After the Russian annexation of Crimea and revelations that Moscow likely supports Hungary in its revisionist claims (see the Viktor Orban' statement from 10 May about ethnic Hungarians from neighbouring states, including Ukraine, having the right to autonomy and dual citizenship[17] and also revelations about extremist Jobbik Party being materially supported by Russia), Polish prime minister D. Tusk warned Hungary not to try to destabilize its neighbours and said the Orban's statement was "unfortunate and disturbing".[18]

More than that, they need stable and prosperous neighbours to be protected from trans-border risks and also for access to markets and resources. Romania and Poland need security guarantees in case of a war against Russia, in case NATO as such would be involved or only some of the neighbours will experience real troubles. As long as the EU does not still have a unitary foreign and security policy, Poland and Romania (the biggest members in the East) are legitimate to claim their right to shape EU's behaviour towards the Eastern flank. By cooperating, the two states benefit more than if they were alone.

These were mainly the reasons for Romania to search for a more intensive relations with Poland: to have a greater size in the EU's CFSP, to counter Russian perceived aggressiveness and to protect the EU's Eastern neighbours, to make the USA remain committed to the missile shield plan.

In the end, both states could try enhancing military cooperation by organizing common military exercises, a permanent dialogue between the two MoDs or even a common structure for coordination with the MFAs and MoDs (a permanent cell), building a common regional mechanism to support the Helsinki order and avoid territorial changes by force and even setting a common Polish-Romanian battalion and participation in a common EU battle group plus cooperation in the field of "drones" (military and civilian ones) and missile defence systems. They could create a mechanism for jointly supporting the Republic of Moldova and Ukraine (a quadrilateral forum instead of two trilateral ones): for supporting their economic and administrative domestic reforms and for shaping their foreign policies in ways favourable to EU plans[19]. By supporting a common energy market with the EU (the European Energy Union) by new regional mechanisms, supporting the diversification of oil and gas pipelines etc.

* This study reflects only the personal point of view of the author and does not involve the Ministry of National Defence

References

[1] Part of this study was published by the author in the *Monitor Strategic* review, no. 3-4/2014, pp. 13-32, under the title "The main national and regional security issues with the Romanian-Polish contemporary relations".

[2] Anton Barbashin, "The Eurasian Illusion", https://www.foreignaffairs.com/articles/russian-federation/2015-01-15/eurasian-illusion, January 15, 2015.

[3] See J. Morrison, 'Pereyaslav and after: the Russian-Ukrainian relationship', *International Affairs*, vol. 69, no. 4, 1993, p. 677.

[4] Geir Flikke (ed.), Einar Wigen, Helge Blakkisrud and Pål Kolstø, "The Shifting Geopolitics of the Black Sea Region", Norwegian Institute of International Affairs, www.nupi.no, 2011.

[5] ***, "Russia Carries on With Turkish Stream Pipeline", www.stratfor.com, 22 May 2015.

[6] Richard Weitz, "Eurasian Security after Astana", 22.12.2010, http://www.cacianalyst.org/?q=node/5467.

[7] Idem.

[8] Some of these ideas were published by Serban F Cioculescu within the article "The Black Sea Between the Trans-Atlantic and the Eurasian Strategic Trends", South African Review, 2012.

[9]Alexander J. Motyl, "Deconstructing Putin on Ukraine", http://www.worldaffairsjournal.org/blog/alexander-j-motyl/deconstructing-putin-ukrainem, accessed on September 20, 2015. According to Motyl, Putin stated**:** "You know, regardless of what happens and where Ukraine goes, we will still meet sometime and somewhere. Why? Because we are one people." .... "You know, no matter what happens, and wherever Ukraine goes, anyway we shall meet sometime and somewhere. **Why? Because we are one nation**." (the author's underlining) Also "Putin explicitly says "people" (*narod*), and not "nation" (*natsia*). As an ex-KGB officer well-schooled in Leninist dialectics and Stalinist nationality policy, he knows that the Russian and Ukrainian nations cannot constitute a nation. But they might constitute a "people," a lower-level, ethno-cultural agglomeration that doesn't have all the objective characteristics of a nation as defined by Stalin in 1913. Back in Soviet days, Russians, Ukrainians, and all the other nations were supposed to be "drawing together" to form a "new community of people"—the "Soviet people." Motyl continues by saying: "Since the language and culture of the Soviet people were essentially Russian, non-Russian dissident critics of Soviet policy argued, not incorrectly, that the Soviet people was just a smokescreen for a policy practiced by the czars—Russification." According to political analyst Nicu Popescu (Chaillot Paper no. 132, Sept. 2014), in the Russian language this discussion takes the form of a debate on whether to use 'v Ukraine' or 'na Ukraine' to mean 'in Ukraine'. 'V' is used when referring to all countries in the world ('v Germanii'/'in Germany', for example), whereas 'na' is used for regions of countries ('na Dalmem Vostoke'/'in the Far-East', 'na granitse'/'in the borderlands'

[10] *Republica Polonă – Relatii bilaterale* (Republic of Poland – Bilateral relations), http://www.mae.ro/bilateral-relations/1730#832, accessed on December 2, 2013.

[11] Idem, p. 5.

[12] Łukasz Kulesa, Agnes Nicolescu, Stanislav Secrieru, Anita Sobják, "Pushing the Turbo Button: What Next for the Polish–Romanian Strategic Partnership?", PISM Policy Paper, No. 30 (78), November 2013, https://www.pism.pl/files/?id_plik=15355

[13] Bilateral meeting, http://english.mapn.ro/cpresa/4069_Bilateral-Meeting-between-the-Defence-Ministers-of-Poland-and-Romania, accesses on March 24, 2014.

[14] Bilateral Meeting between the MODs of Romania and Poland, http://www.nationaljournal.com/library/129070, accessed on March 5, 2014.

[15] One must mention that in May 1996, the CFE treaty was amended by the so-called "flank agreement", which in fact relaxed the restrictions for Russia and

Ukraine in the flank region as defined in Article V, subparagraph 1(A) of the treaty. But the current situation exceeds what was accepted then.

[16] Elisabeth Brocking, "Remember the CFE Treaty?", http://nationalinterest.org/ commentary/remember-the-cfe-treaty-10203), accessed on April 8, 2014.

[17] "Hungary will stand up for its rights within the European Union and wants autonomy for ethnic Hungarians living beyond its borders in central Europe, including Ukraine" - http://uk.reuters.com/article/2014/05/10/uk-hungary-orban-idUKKBN0DQ0BH20140510, accessed on May 12, 2014.

[18] "Tusk about Viktor Orban's statement: unfortunate and disturbing", 14 May 2014, http://www.warsawvoice.pl/WVpage/pages/article.php/28248/news One must know that the two leaders do not have an adversarial relation. On May 6, Orban, during a visit to Warsaw, had expressed full support for the Polish project of the European energy union.

[19] "Going beyond the EU's internal design, the Polish-Romanian tandem should also aim at upgrading the EU's commitment towards the Eastern Neighborhood, from a strictly institutional design into one with more political significance, difficult as this may be in the current context. Bilateral coordination of political support for Moldova and Ukraine's European association requires long-term strategic vision, but has clear mutual benefits. The increasingly coordinated approaches of Bucharest and Warsaw towards Moldova and Ukraine's pro-European path will have long-term benefits for these two, provided that the present political engagement in the two eastern partners continues, irrespective of developments at the Vilnius summit." - Łukasz Kulesa, Agnes Nicolescu, Stanislav Secrieru, Anita Sobják, "Pushing the Turbo Button: What Next for the Polish–Romanian Strategic Partnership?", PISM Policy Paper, No. 30 (78), November 2013, https://www.pism.pl/files/?id_plik=15355.

"SEPTEMBER 11" AND THE PARADIGM SHIFT AT THE TURN OF THE MILLENNIUM

Cristina IVAN[*]

Abstract

This study is aimed to complement the perspective on identity and otherness, by adding to it the essential component of violence enforced to either preserve the boundaries of the self or to dissolve the threat posed by the other. With this aim in mind, the study will be focused on understanding the inter-textual communication established between public discourse, political doctrine and fictional productions. Looking at violence as a product of the conflict driven neo-realist paradigm that governs current state of affairs in global politics, my aim is to demonstrate that September 11 and the following war on terror produced a significant shift of perceptions and culminated with the implosion of cosmopolitanism and multiculturalism alike. Nevertheless, as I aim to demonstrate, towards the second half of the decade, this new dangerously simplistic "us vs. them" context was gradually compromised. As a result, interest of the public steered away towards those writers and discourses that could, through their manifold allegiances, internalize public negotiations of conflicting identities and provide authentic solutions for a way out.

Keywords: conflicting identities, inter-textual communication, violence, September 11

Motto: *"And therefore never send to know for whom/
the bell tolls; it tolls for thee"*
John Donne, *No man is an island*

For a contextualization of violence at the turn of the Millennium

Undoubtedly the most significant mind-shaping, paradigm-braking event of the first decade of the new Millennium has been the 9/11 terrorist attack. Looking back at the "geographies of anger"

[*] National Institute for Intelligence Studies, Romania

(term coined by Arjun Appadurai in the title of his famous “Fear of small numbers. An Essay on the Geography of Anger”), that it seemed to catalyse, we can very well see that the world is far from overcoming it. Conflicts across the Middle-East, the civil wars, suppressed popular movements, the rise of new terrorist organizations, as the self-proclaimed Islamic State of Iraq, just as well as the hesitant, ineffectual and sometimes violence replicating involvement of international powers have changed perceptions and understandings to the point that we seem more and more to live in a world governed by pure, chaotic, conflict driven neo-realism.

At first there was “the war on terror” which cut the world once again in friends and enemies of democracy. That in turn allowed mystification of the alien other as a malefic opponent and public discourse fell quickly under the spell of its “civilizing” and comforting familiarity. Then, a state of emergency seemed to take hold of public opinion. The old imperial us vs. them paradigm alive again, there was no time to observe the other and decipher his motivations. President Bush’s first address to the American nation, after the terrorist attacks on New York and Washington set the tone for a narrative based on the perception that terrorist attacks were directed specifically against the Western way of living and more importantly, against freedom, as a core value of the nation: “America was targeted for attack because we’re the brightest beacon for freedom and opportunity in the world. And no one will keep that light from shining”. (Bush, 2001) The U.S. ‘us’, defenders of universal values of freedom and opportunity versus an insufficiently specified ‘them’, forces of evil, the very worst of human nature was thus established, while the American nation and the empathic West were dragged into a war mode paradoxically set to demonstrate what President Bush called “our resolve for justice and peace”(idem). The polarized world vision embraced by public discourse deepened in the so called “Bush Doctrine of Pre-Emptive Strikes”, of the National Security Strategy, published by the White House in September 2002, in which the United States, their allies and friends were set in opposition to rogue states and terrorists who could not be allowed “to strike first”: Freedom is the non-negotiable demand of human dignity; the birth right of every person—in every civilization. Throughout history, freedom has been threatened by war and terror; it has been challenged by the clashing wills of powerful states and the evil designs of tyrants; and it has been tested by widespread poverty and disease. Today, humanity holds in its hands the opportunity to further freedom's triumph over all these foes. The United States welcomes our responsibility to lead in this great mission. (Government, United States)

The strategy echoes a mode of thinking set by, among others, the famous Samuel Huntington's article and later book entitled "The Clash of Civilisations", which prophetically announced that, as the world was becoming a smaller place, and civilizations as cultural constructs came to interact more closely to each other, "the most important conflicts of the future (were to occur) along the cultural fault lines separating these civilizations from one another." (Huntington, 1993)

The 'us vs. them' paradigm of coherent, perfectly contained cultures, civilizations and nations, that entered a state of conflict among competing ideas and styles of life, was further complicated by the resurgence of an imperial and hegemonic approach to power relations. In a world of little uncertainty, public discourse, in the American space at least, also focused on an a neo-realist view of the world, in which nations and peoples were naturally functioning in a state of conflict, in which one nation/culture/civilization had to maintain supremacy and lead global affairs. And that state of mind is far from being put down. As late as 2011, Mitt Romney, the republican presidential candidate to be in the elections of 2012, was declaring in another public discourse, held at the military Academy The Citadel, in South Carolina, that: "This century must be an American century. (...) In an American century, America leads the free world and the free world leads the entire world. (...) America is not destined to be one of several equally balanced global powers. America must lead the world, or someone else will." (Romney, 2011) An exceptional country with a unique destiny, America, in this hard-core republican view, is bearer of two contradicting functions and mental frameworks: that of hegemonic power in an imperial quest to dominate the world, and that of champion of universal human rights. In the war mode of thinking, to preserve imperial hegemony and the centrality of American power, are given predominance, while the universal values of freedom and peace get to be overshadowed by the state of emergency to which the nation state is exposed. A paradoxical logic makes way for a form of thinking in which, in order to preserve freedom and peace at home, champions of democracy are allowed to indiscriminately enforce violence upon nations out there. More than a decade after the 9/11 terrorist attacks, America seems to have remained in a state of emergency, in which, as the "Top Secret America" series of *Washington Post* revealed in 2010, the government has expanded the US domestic and foreign security apparatus, with 263 new agencies being created and a total of 1,271 government organizations and 854,000 people involved in fighting against terrorism, thus raising fears of the U.S. becoming a police state: "The top-secret world the government created in response to the terrorist attacks of Sept. 11, 2001, has become so large, so unwieldy and so secretive that no one knows how much money it costs, how many people it employs, how many programs exist within it or exactly how many agencies do the same work." (Top Secret America, 2010)

Thus at the end of the decade, the effects of this mode of thinking promoted by the official discourse are far from the imagined cohesiveness they invoked. Civil society and media increasingly got to question its reality. And, what's more important, at the end of the decade, it became clear, at least in alternative narratives of the media and the public, that the 'us vs. them' paradigm of an endless history of terror which had to be fought by the 'heralds of democracy', was in fact turning into "an alternative geography of the United States, a Top Secret America hidden from public view and lacking in thorough oversight" (idem), an insider questionable weapon that could potentially threaten the very democracy it claimed to protect.

The war mode of thinking instated with the "Pre-emptive Strike National Security Strategy" in the US quickly wiped off Europe as well, with friends and partners of America declaring their rightful solidarity, and also, later on, support to "the war on terror". Paul Gilroy offered a very exact description of the state of the art in the aftermath of 9/11, both in the US and Europe: "Civilizations are now closed or finished cultures that need to be preserved. The individual agents who are their bearers and affiliates come ready-stamped with iconic badges of relative rank. The languages of "race" and absolute ethnicity ensure that this natural hierarchy, which is also social and cultural, cannot be renegotiated. Today, that ranking increasingly conforms to the dictates of the West's reborn imperial power." (After Empire 65)

The UK in particular, and Tony Blair's cabinet at the time, was quick to assert solidarity and later on support to military actions in Iraq and Afghanistan. In the aftermath of 9/11, BBC news noted that Blair described the bombardment of the World Trade Centre in New York as "the worst terrorist attack there has been on British citizens since the Second World War" (BBC News, Britain 'at war with terrorism').

And one of the first direct consequences of the new state of facts was the implosion of cosmopolitanism and multiculturalism. The state of war created a state of emergency, and the state of emergency created a global lack of time and availability to consider the other. The nation state became in the process the fundamental unit of measure of comfort and security. Back to the fundamental conceptual framework that gave birth to the modern state, public discourse in the West as a whole and in Britain in particular moved fast into a neo-realist paradigm in which conflict was the sole regulator and preferred mode of transaction of power and capital. As Paul Gilroy rightfully noted, when the New York towers fell, (...) Blair's belligerent, sanctified, and resolutely Churchillian Britain was aligned politically with the worst and most backward features of the latest U.S. imperial adventure. (...) A new set of issues had emerged to prompt the remaking of the nation's relationship with its imperial past and to feed the hope that its buried and disavowed colonial history might become useful at last as a guide to the evasive, multicultural future prefigured everywhere in the ordinary experiences of contact, cooperation, and conflict across the supposedly impermeable boundaries of race, culture, identity, and ethnicity. (After Empire 9)

British home-grown terrorism and the other within

Furthermore, another major development that shaped understanding of violence came forth just a few years later in the form of home-grown terrorism. The London underground bombings of July 7, 2005, conducted by four separate Islamist extremist suicide bombers, killing 56 people and injuring 700, the subsequent 2007 Glasgow International Airport attack, perpetrated by Islamist extremists or the 2008 Exeter attempted bombing, in which only the

Islamist perpetrator was injured, show the level of threat increased and deepened as terrorists born and raised within European borders in general and within British borders in particular, created another profound shift of paradigm.

With this shift, the 'us vs. them' paradigm was proven unviable, as 'the other', conservatively cast outside the known borders, increasingly showed to live within an 'us' that defined both Western civilization and the nation and that proved ethnic definitions of the nation state increasingly out-dated. And that was where chaos made its way and conflict got to rule... but not alone. Fear of the other produced anxieties and racial outrage. It also produced a fascination with the alien inside, a need to know why and to understand responsibility and agency. This quest however was far from being met by public discourse on both sides of the Atlantic. It did nothing more than to widen the gap between spectral representations of alterity and to inculcate a feeling of vulnerability of the sovereign state in the face of the unknown. In a compelling book, entitled *The Rhetoric of Terror: Reflections on 9/11 and the War on Terror*, Mark Redfield very well observes that "the declaration of war on terror is the exemplary postmodern sovereign speech act: it unleashes war as terror and terror as war, while remaining a crazed, even in a certain sense fictional performative utterance". (17)

Yet, as we have come to learn, performative utterances shape cultural modes and cultural modes in their turn regulate ethic positions and frame our understanding of ongoing facts. It is also worth noting, with Judith Butler, that the frames through which we apprehend or, indeed, fail to apprehend the lives of others as lost or injured (lose-able or injurable) are politically saturated. They are themselves operations of power. They do not unilaterally decide the conditions of appearance but their aim is nevertheless to delimit the sphere of appearance itself (Frames of War 1)

As a clear instance of how politically saturated frames imposed by a significant segment of public discourse was after September 11 back in the America and across the Atlantic, we can refer to the inter-textual communication created between camps and discourses. Ulrich Fichtner, in an article entitled "The Terrorist Next Door", written September 2011, attracted attention that "America's Muslims have become the country's internal enemy" (Fichtner, 2013) and pinpointed to a narrative created and proliferated by hard core conservative thinkers and promoters, like for instance the colourful media figure, Brigitte Gabriel, whose statements are a clear indication of the profound change of perspective which affected America and the West. Fichtner notes that Brigitte Gabriel's first book, *Because they hate us*, produced a very simplistic view on Islamist fanaticism. Such perspectives have increasingly populated the public and media discourse in the first decade of the 21st century. Fortunately, they were not the only type of discourse, and if a powerful alternative is to be looked for in search of counter narratives, cultural productions must be noted, as they took their place on the market of intellectual ideas.

Writer Mohsin Hamid, living and writing in the UK at the time, offered a powerful response to such narratives in his fiction productions, but also in his journalistic articles. One such article is entitled in a very evocative and inter-textual manner – how else? - "Why do they hate us?". In this article, dated July 22, 2007, Hamid draws attention to how this interrogation and "a pose of wounded innocence" come in direct contradiction with imperialist claims. As the writer notes, a generalization of 'they', as dangerously simplistic as we might perceive it to be, is also ingrained with a perplexity of thought that obviously doesn't keep track with "the accreted residue of many years of US foreign policies", and the numerous times America intervened "to shape the destinies of other countries, and then, as a nation walked away" from consequences (Why do they hate us?). The interest of the public for such responses, on both sides of the Atlantic, reflects a mode of thinking that steers away from the 'us vs. them' narrative and the belief in the clash of closed and finished civilizations and cultures. Towards what the interest steers is yet another issue to be further explored in part 3 of the current study.

However, at this point, it is worth mentioning that writers with manifold ethnic and ethic allegiances did generate fascination and interest from the public precisely because they had no other choice than to internalize public negotiations of conflicting identities and explore the other not outside but within the borders of their own identity. And that created, for at least part of their audience, an enhanced legitimacy. Theirs was a testimonial of yet to be discovered synergies and yet to be overcome obstacles towards a new paradigm of thinking of both state and individual conflict management and resolution. That can be framed as well in a larger context, in which, as Mark Redfield suggests, “the idea of a war on terror relays the complex, spectral afterlife of sovereignty in an era of bio power, global capital, and telecommunication” (7), in other words in an era in which the individual citizen is increasingly exposed to a sense of loss and ineffectiveness of sovereignty as we know it.

In this context, Mohsin Hamid’s legitimacy in building an alternative discourse has come from his simultaneous identification with both ‘*us*’ and ‘*them*’. Born in Pakistan, he was raised from 3 to 9 years old in the US, then he returned to Pakistan, got educated at Princeton and Harvard. Today, Hamid shares his work between London and Lahore. Therefore, Hamid has the perfect profile of someone set to resolve the dilemma of the other within. But he is not the only one and, as we shall see, most of the writers and critical thinkers that have managed to create ontological explanations of identity conflict and violence at the turn of the Millennium share the same type of hybrid, multicultural framework that Hamid was born and raised in.

References

Abu-Lughod, L., 1991. Writing against Culture. In: R. G. Fox, ed. *Recapturing Anthropology: Working in the Present*. Santa Fe: NM: School of American Research Press.

Ali, M., 2004. *Brick Lane*. s.l.:Black Swan.

Anderson, B., 1991. *Imagined Communities*. London: Verso.

Anon., 2006. *Cricklewood*. [Online] Available at: http://www.foreignaffairs.com/articles/48950/samuel-p-huntington/the-clash-of-civilizations

Anon., n.d. [Online].

Anon., n.d. *Multiculturalism*. [Online] Available at: http://www.oxforddictionaries.com/definition/english/multicultural[Accessed 5 08 2014].

Anon., n.d. *The Clash of Civilisations?*. [Online].

Anon., n.d. *World History Timeline*. [Online] Available at: http://www.fsmitha.com/time/1989.html

Appadurai, A., 2006. *Fear of Small Numbers, An essay on the geography of anger*. s.l.:s.n.

Appiah, A. K., 2005. *The Ethics of Identity*. New Jersey: Princeton University Press.

Aslam, N., 2006. *Maps for Lost Lovers*. London: Faber and Faber.

Aslam, N., 2009. *An Interview with Nadeem Aslam.* [Online] Available at: https://www.bookbrowse.com/author_interviews/full/index.cfm/author_number /1149/nadeem-aslam,[Accessed 15 March 2015].

Aslam, N., 2009. *The Wasted Vigil.* Croydon: Faber and Faber.

Aslam, N., 2014. *The Blind Man's Garden.* New York: Vintage International.

Bauman, Z., 2000. *Liquid Modernity.* Cambridge: Polity Press.

Beck, U., 2002. The Cosmopolitan Society and its Enemies. *Theory, Culture and Society,* 19(1/2), pp. 17-45.

Benjamin, W., n.d. Critique of Violence. In: *Reflections, Essays, Aphorisms, Autobiographical Writings.* New York: Schocken Books, pp. 277-300.

Bermann, S., 2005. Introduction. In: *Nation, Language and the Ethics of Translation.* Princeton: Princeton University Press.

Bernardi, D. et al., 2012. *Narrative Landmines.* London: Rutgers University Press.

Borradori, G., 2003. *Philosophy in a time of terror, Dialogues with Jurgen Habermas and Jacques Derrida.* Chicago: Chicago University Press.

Brace, M., 2004. *Nadeem Aslam: A question of honour.* [Online] Available at: http://www.independent.co.uk/arts-entertainment/books/features/nadeem-aslam-a-question-of-honour-6167858.html[Accessed 12 March 2015].

Brewin, K., 2011. *Other, Embracing Difference in a Fractured World.* London: Hodder.

Bush, G., 2001. *Statement by the President in His Address to the Nation.* [Online] Available at: http://georgewbush-whitehouse.archives.gov/news/releases/ 2001/09/20010911-16.html[Accessed 23 June 2015].

Butler, J., 2006. Critique, Coercion, and Sacred Life in Benjamin's "Critique of Violence". In: H. d. V. a. L. E. Sullivan, ed. *Political Theologies, Public Religions in a Post-Saecular World.* New York: Fordham University Press.

Butler, J., 2009. *Frames of War, When is live grievable.* London: Verso.

Butt, N., 2008. Between Orthodoxy and Modernity: Mapping the Transcultural Predicaments of Pakistani Immigrants in Multi-Ethnic Britain in Nadeem Aslam's Maps for Lost Lovers.. In: *Multi-Ethnic Britain 2000+ , New Perspectives in Literature, Film and the Arts.* New York: Rodopi.

Cavendish, R., 1998. *History today.* [Online] Available at: http://www.historytoday.com/richard-cavendish/arrival-ss-empire-windrush

Chakrabarty, D., 2000. *Provincializing Europe, Postcolonial thought and historical difference.* New Jersey: Princeton University Press.

Childs, P. & Green, J., 2013. *Aesthetics and Ethics in Twenty-First Century British Novels.* London: Bloomsbury.

Chomski, N., 2003. *Hegemony or Survival, America's Quest for Global Dominance.* New York: Holt Paperbacks .

Cities, C. W. U., 1999. London, New York: Routledge & The Open University,.

De Lilo, D., 2001. *In the Ruins of the Future.* [Online] Available at: http://harpers.org/archive/2001/12/in-the-ruins-of-the-future [Accessed 12 December 2014].

De Vries, H. & Weber, S., 1997. *Violence, Identity and Self Determination.* Stanford: Stanford University Press.

Dehaene, M. & Cauter, L. D., 2008. *Heterotopia and the City Public Space in a Postcivil Society*. London: Routledge.

Douzinas, C., 2007. *Human Rights and Empire, The political philosophy of cosmopolitanism*. Cavendish: Routledge.

Eads, M. G., 2010. *Imagining America: Mohsin Hamid's The Reluctant Fundamentalist*. [Online] Available at: http://thecresset.org/2010/Advent/Eads_A10.html[Accessed 12 June 2015].

Eatwell, R. G. M. J. ed., 2010. *The New Extremism in 21st century Britain*. Oxon: Routledge.

Fichtner, U., 2013. *The Terrorist Next Door*. [Online] Available at: http://www.spiegel.de/international/world/the-terrorist-next-door-american-muslims-face-growing-prejudice-a-785836.html,

Fine, R., 2007. *Cosmopolitanism, Key Ideas*. London: Routledge.

Fiona, M., 2012. *Cosmopolitanism in Contemporary British Fiction*. London: Palgrave Mc Millan.

Floyd Mair, E., 2013. *Author Caryl Philips explores issues of Multiculturalism*. [Online] Available at: http://www.timesunion.com/living/article/Discomfort-zone-1459716.php[Accessed 23 February 2013].

Foreign Policy, 2007. Interview with Mohsin Hamid on National Identity, Globalization and Muslim Immigrants. In: *The Reluctant Fundamentalist*. s.l.:Diesterweg, pp. 241-245..

Foucault, M., 1984. Of Other Spaces. *Architecture /Mouvement/ Continuité* , October.

Freud, S. a. W. S., 1997. Thoughts for the time on war and death. In: H. W. S. De Vries, ed. *Violence, Identity and Self Determination*. Stanford(USA): Stanford University Press.

Fukuyama, F., 1992. *The End of History and the Last Man*. Hardmondsworh: Penguin Books.

Gehring, P., n.d. *Force and the "Mystical Foundation" of Law: How Jacques Derrida addresses legal discourse*. [Online] Available at: https://www.germanlawjournal.com/pdfs/Vol06No01/PDF_Vol_06_No_01_151-169_SI_Gehring.pdf

Geoffrey, P., 2010. *Alter-Globalization, Becoming Actors in the Global Age*. Malden: Polity Press.

Gilroy, P., 2000. *Between Camps, Nations, Cultures and the Allure of Race*. London: Penguin Books.

Gilroy, P., 2004. *After Empire, Melancholia or convivial culture?*. London: Routledge.

Gilroy, P., 2004. *After Empire, Melancholia or Convivial Culture?*. Oxofordshire: Routledge.

Government of the United Kingdom, n.d. *The National Archives*. [Online] Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/267913/britnatsummary.pdf [Accessed 14 August 2014].

Government, U. S., 2002. *The National Security Strategy of the United States of America*. [Online] Available at: http://www.state.gov/documents/organization/63562.pdf

Gray, R., 2011. *After the Fall: American Literature Since 9/11*. Chichester: Wiley-Blackwell.

Gunning, D., 2010. *Race and Antiracism in Black Brisitsh and British Asian Literature*. Liverpool: Liverpool University Press.

Halverson R. Jefffrey, G. H. J. C. S. R., 2011. *Master Narratives of Islamist Extremism*. New York: Palgrave McMillan.

Hamid, M., 2007. *Critical Outakes: Mohsin Hamid on Camus, Immigration, and Love*. [Online] Available at: http://bookcritics.org/blog/archive/critical_outakes_mohsin_hamid_on_camus_immigration_and_love
[Accessed 23 June 2015].

Hamid, M., 2007. *NPR Fresh Air interview with Mohsin Hamid* [Interview] (03 04 2007).

Hamid, M., 2007. *Why do they hate us?*. [Online] Available at: http://www.washingtonpost.com/wp-dyn/content/article/2007/07/20/AR2007072001806.html[Accessed 9 September 2014].

Hamid, M., 2012. *The Reluctant Fundamentalist*. Braunschweig: Diesterweg.

Hamid, M., 2013. *Harvard Law Bulletin profile on Moth Smoke and law school.* [Online]
Available at: http://today.law.harvard.edu/bulletin/issue/

Hardt, M. N. A., 2004. *Multitude. War and Democracy in the age of the Empire.* New York : Penguin Press.

Harvey, D., 2009. *Cosmopolitanism and the geographies of freedom.* New York: Columbia University Press,.

Head, D., 2002. *The Cambridge Introduction to Modern British Fiction (1950-2000).* Cambridge: Cambridge University Press.

Head, D., 2008. *The State of the Novel: Britain and Beyond.* Sussex: Wiley-Blackwell.

Heckmann, F., 1993. Multiculturalism defined seven ways. *The Social Contract,* Summer.pp. 245-246.

Hong, T., 2013. *An interview with Nadeem Aslam.* [Online] Available at: http://www.bookslut.com/features/2013_07_020162.php [Accessed 23 February 2015].

Huntington, S. P., 1993. *The Clash of Civilisations.* [Online] Available at: https://www.foreignaffairs.com/articles/united-states/1993-06-01/clash-civilizations[Accessed 23 05 2015].

Jivraj Stephen and Simpson, L., ed., 2015. *Ethnic identity and inequalities in Britain. The Dynamics of Diversity*.. Bristol: Polity Press.

Kapur, A., 2005. *'Maps for Lost Lovers': Little Murders,.* [Online] Available at: http://www.nytimes.com/2005/05/22/books/review/22KAPURL.html?_r=0, retrieved March 2015.[Accessed 8 June 20014].

Lacan, J., 2013. On the names of the father. *Interstitial Journal.*

Lehman, S., 2015. *Reading The Times with Mohsin Hamid.* [Online] Available at: http://www.nytimes.com/times-insider/2015/03/26/reading-the-times-with-mohsin-hamid/?_r=1[Accessed 4 May 2015].

Lemke, C., 2008. Racism in the Diaspora: Nadeem Aslam's Maps for Lost Lovers. In: *Multi-Ethnic Britain in Nadeem Aslam's Maps for Lost Lovers (2004), in Multi-Ethnic Britain 2000+ , New Perspectives in Literature, Film and the Arts.* New York: Rodopi.

Lewis, J., 2005. *Language, The role of media and culture in global terror and political violence wars.* London: Pluto Press.

Littau, P. K. a. K., n.d. *A companion to tranlsation studies.* s.l.:s.n.

Malouf, A., 2000. *On identity.* Haberville: Panther.

Massey, D., 2008. In: A. J. S. P. Massey Doreen, ed. *Human Geography Today.* Cambridge: Polity Press.

Mc Cullogh, F., 2012. *Cosmpolitanism in Contemporary British Fiction, Imagined identities.* London: Palgrave McMillan.

McLeod, J., 2004. *Post-Colonial London, Rewriting the metropolis.* London: Routledge, London.

Mythography.com, n.d. *Casiope.* [Online] Available at: http://www.mythography.com/myth/welcome-to-mythography/greek-heroes/greek-heroes-1/cassiopeia/[Accessed 14 05 2015].

News, B., 2001. *Britain 'at war with terrorism'.* [Online] Available at: http://news.bbc.co.uk/2/hi/uk_news/politics/1545411.stm

Ogilvie, B. S. D. W. F. O. ed., 2010. *Vivre en Europe, Philosophie, politique et science aujourd'hui.* Paris: L'Harmattan.

Parekh, B., 2000. Defining British National Identity,. *The Political Quarterly,* January, 71(1), pp. 4-14.

Philips, A., 2007. *Multiculturalism without Culture.* Princeton: Princeton University Press.

Philips, C., 2000. *'Mixed and Matched', review of White Teeth.* [Online] Available at: http://www.theguardian.com/books/2000/jan/09/fiction.zadiesmith

Philips, C., 2001. *A new world order.* s.l.:s.n.

Philips, C., 2005. *A distant shore.* New York: Vinatge International.

Philips, C., 2011. *"The Narrative Is Not Written in Stone".* [Online] Available at: http://smallaxe.net/wordpress3/interviews/2011/12/16/"the-narrative-is-not-written-in-stone"/,[Accessed 23 February 2015].

Philips, C., 2011. *Color me English, Reflections on Migration and Belonging.* New York: The New York Press.

Philips, M. q. i. D. D. D. F. a. E. B., 2004. Milennial Currents. In: *Postcolonial London, Rewriting the Metropolis.* London: Routledge.

Pile, S., 1999. What is a city?. In: D. A. J. P. S. Massey, ed. *City Worlds, Understanding Cities* . London, New York: Routledge & The Open University, pp. 3-51.

Procter, J., 2009. *British Council Literature.* [Online] Available at: http://literature.britishcouncil.org/mohsin-hamid

Rahim, S., 2012. *The Satanic Verses and me.* [Online] Available at: http://www.telegraph.co.uk/culture/books/9523983/The-Satanic-Verses-and-me.html[Accessed 7 December 2014].

Redfield, M., 2009. *The Rhetoric of Terror: Reflections on 9/11 and the War on Terror.* [Online] Available at: <https://muse.jhu.edu/>.[Accessed 9 October 2014].

Rennison, N., 2005. *Contemporary British Novelists.* Oxfordshire: Routledge.

Ricoeur, P., 2006. *On Tranlation, Thinking in Action.* London: Routledge.

Ricouer, P., 1992. *Oneself as Other.* Chicago: University of Chicago Press.

Robertson, R., 1992. *Globalization:Social Theory and Global Culture.* London: Sage Publications.

Romney, M., 2011. *The Wall Street Journal.* [Online] Available at: http://blogs.wsj.com/washwire/2011/10/07/text-of-mitt-romneys-speech-on-foreign-policy-at-the-citadel/
[Accessed 3 May 2015].

Rushdie, S., 1991. *Imaginary Homelands.* London: Granta Books.

Said, E. W., 1997. *Coverimng Islam, How the media and the experts determine how we see the rest of the world.* New York: Vintage Books, .

Scanlan, M., 2012. Migrating from terror: The postcolonial novel after September 11. In: S. M. A. V. a. R. S. Fiona Tolan, ed. *Literature, Migration and the War on Terror.* London, New York: Routledge, pp. 22-35.

Sen, A., 2006. *Identity and Violence, The Illusion of Destiny, , 2006, p.157.* London: Penguin Books.

Shivani, A., 2013. *I Don't Believe in Reality: An Interview with Mohsin Hamid.* [Online] Available at: https://lareviewofbooks.org/interview/i-dont-believe-in-reality-an-interview-with-mohsin-hamid[Accessed 3 October 2014].

Smith, S. J., 1999. The CulturaL Politics of Difference. In: A. J. S. P. Massey Doreen, ed. *Human Geography Today.* Cambridge: Polity Press, pp. 129-151.

Smith, Z., 2000. *White Teeth.* London: Penguin Books.

Smith, Z., n.d. *Zadie Smith, Quotes.* [Online] Available at: http://www.goodreads.com/author/quotes/2522.Zadie_Smith[Accessed 24 04 2014].

Sohn, H., 2008. Heterotopia: anamnesis of a medical term . In: M. D. C. L. Dehaene, ed. *Heterotopia and the City Public Space in a Postcivil Society.* London: Routledge.

Soja, E., 1998. In: D. A. J. S. P. Massey, ed. *Human Geography Today.* Cambridge: Polity Press.

Spivak, G. C., 2005. Translating into English. In: S. &. W. M. Bermann, ed. *Nation, Language and Ethics of Translation.* New Jersey: Princeton University Press.

Tew, P. &. M. R. ed., 2006. *British Fiction Today.* London: Continuum.

Todorova, M., 1997. *Imagining the Balkans.* Oxfordshire: Oxford University Press.

Tolan, F., 2010. *New Directions, Writing post 1990.* London: York Press.

Top Secret America, A. W. P. I., 2010. *Washington Post.* [Online] Available at: http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control/, Trousdale, R., 2010. *Nabokov, Rushdie and the Transnational Imagination. Novels of Exile and Alternate Worlds*. US: Palgrave, McMillan.

Upstone, S., 2009. Spatial Politics in the Postcolonial Novel. In: Farnham (Surrey): Ashgate.

Versluys, K., 2009. *Out of the Blue, September 11 and the Novel*. New York: Columbia University Press.

Walkowitz, R. L., 2006. The Location of Literature: The Transnational Book and the Migrant Writer. *Contemporary Literature,* Winter .47(4).

Wetherell, M., ed., 2009. *Identity in the 21st century, New Trends in Changing Time*. Houndmills: Palgrave, Macmillan.

Zizek, S., 2002. *Welcome to the Desert of the Real, Five Essays on September 11 and Related Dates*. Lpndon, New York: Verso.

Zizek, S., 2008. *For They Know Not What They Do: Enjoyment s a Political Factor*. London, New York: Verso.

Zizek, S., 2008. *In defense of lost causes*. London, New York: Verso.