USING SOCIAL NETWORK ANALYSIS IN INTELLIGENCE: THE COMPLEX AND COMPLETE PROBLEM

Dan MAZARE[*]

Abstract:
Using social network analysis in intelligence activities is a complex and complete problem, as an analogy with the computational complexity theory suggests. Complexity emerges as one connects a scientific approach with intelligence, and the civil and military realms, the national security strategy with a corresponding doctrine and develops a training program for the personnel. Solving this problem leads to one finding the key to other complex problems, such as the development and deployment of early warning systems, simulation and modeling systems, human terrain systems. The problem is complete and solving it is a keen organizational learning process. When reached, the promise a land of a solution adds value to the intelligence organization, processes and products.
Keywords: *social networks, intelligence, science, action, value* ***Intelligence, knowledge and action***

As a product of the emotional echoes related with the event that was labeled "9/11", the "social network" keyword gained ubiquity. Its presence is visible not only in the media but also there where the Academia crosses borders with the institutionalized community defending national security. On the one hand there are academics, on the other hand security professionals, both public and private workers, enrolled in universities of all sorts, in police, army, intelligence agencies, and in private security companies.

Beyond the core of the perpetual security problem itself – the use of knowledge to support action and the use of action to support knowledge[1], – the meeting point between academics and professionals is where the need for financial support and research funding meets the need for effective and efficient institutional action. Since emotions are always called as explanatory

[*] National Intelligence Academy „Mihai Viteazul"
[1] A formula rooted in the OODA Cycle – Observe, Orient, Decide, Act

variables, leading us to a particular understanding of the evolution of political, social or economic processes, of the public opinion, one would expect that emotions affect at a lesser extent the rationality of scientific probity, or bureaucracies (positive meaning) specific to public institutions. That is not the case, as shown by the hype that followed 9/11, visible through the number of academic approaches on topics such as "terrorism" and "social networks supporting terrorism". Not only representatives of the social sciences, especially sociologists, but also computer scientists and mathematicians alike, they all went on the trails of terrorist organizations, using their abstract arsenal, academic specific tools and methods. As a response to requests from the institutional environment, academics sought the Scientific Truth but also funding, not necessarily in this order. Leaving aside the flourishing academic literature on the matter, one could think about the success of these research activities as secret documents were revealed to the public, through unauthorized means, describing hypothetical information systems operated by some of the US intelligence agencies, systems employing social network analysis. The systems, the documents reveal, use graphs and networks for representation purposes, dealing with "metadata" gathered from a plethora of sources (*The Guardian*, November 2013). While one could still cast doubt on this, it is more likely to have covered definitions for terms such as Human Terrain System or Human Aspects of the Operational Environment, to find that for the current armed conflicts, knowledge of social dynamics is a prerequisite. Thus, when learning about the social dynamics, defined as a "combination of social, cultural and behavioral relationships and activities that characterize a population of a theater of operations", one would have "to identify social networks, interpersonal interaction information, organizational, economic, describing the networks of trust, dependence, and sustainability, including tribal communities, institutions or community-level government" (Lamb et al., 2013, pp. 7-8).

The current article is the result of the author's efforts to identify a controllable environment for the interaction between academics and representatives of the national security system, using social network analysis as a means of dialogue between these two communities. In order to focus the discourse, the article reduces the generic "security related activity" to the "intelligence activity" – intelligence, in different variants thereof: intelligence that supports law enforcement and policing, military intelligence supporting counterinsurgency operations with knowledge of human terrain, economic intelligence supporting political and strategic interests. Distinct in details, such activities keep at the definition and principle levels a common

denominator, which allows for the existence of the national intelligence community in most countries of the Euro-Atlantic political space. Such a community, a goal in itself, depends upon the national security intelligence doctrine, supporting institutional interoperability but not enforcing the effectiveness of the community.

By the controllable environment, we mean a research and development environment (applied research), with feedback loops (Spink, 1997), meaning that academic researchers have access to empirical knowledge acquired by security practitioners and vice versa, practitioners employ working tools drawn from the theoretical-academic activities but showing utility to security or defense activities. The belief that such an environment exists and can be defined is maintained by those examples in which a representative of academia has contributed to a security problem, in the settings of the type mentioned above, describing the interactions with the institutional environment in a book or journal (Morselli, 2009; Klerks, 2001, pp. 53-65).

An exercise for thought

We are going to start the exercise by making an analogy, using as reference point the computational complexity theory (Goldreich, 2008, pp. 1-7). This theory makes a distinction between decision problems (accept „yes/no" solutions) which can be solved in short time (the time needed to reach a solution with a specific algorithm can be computed by using a polynomial function that takes as parameter the input data) and decision problems that take much longer to be solved, when an algorithm is known – labeled as complex problems (the time needed to reach a solution with a specific algorithm can be computed by using an exponential function that takes as parameter the input data). We say that the use of social network analysis to support intelligence activities is a complex problem.

It is definitely not an easy task to understand and plan the way in which one could use scientific results to define a methodology to be employed by national security institutions, either using it as it is or by translating it into institutional rules and procedures. Going further with the analogy we have to note that the computational complexity theory identifies a series of special complex problems. Not only that these problems are hard, but they are also complete. As the mentioned theory goes, if one finds a solution for a complete problem, a special fast (polynomial) algorithm, many other related complex

problems can be solved. Thus, when solving a complete problem, one finds the way to address a series of complex problems.

The current article is aimed at providing a framework to understand this analogy, so that if we find the settings for using social network analysis to enrich the intelligence activity, then we are in the position of addressing and solving problems of similar complexity. To name just a few of these problems: the development and use of an early warning system, of a center for modeling and simulation of security related scenarios or of a system for strategic analysis. Without entering in the details that emerge when comparing these problems, we have to establish at least the axes of similarity.

First, one has to note that these problems are part of a debate which search for solutions to reintegrate science in a relationship with the national intelligence culture (Agrell & Treverton, 2014, pp.1-31)[2]. This is an initiative emphasizing developments such as those of Reginald V. Jones or Harrold Lasswell, promoters of scientific intelligence (Clark, Studies in Intelligence, 19-1)[3] and, respectively, policy science – an interdisciplinary domain aimed at using social sciences to support governmental action .

Second, one has to notice that these problems are specific to the civil-military relations. At the end of the Second World War, the civil-military relations were analyzed by trying to establish the conceptual limits of the interactions between the military culture and the liberal – democratic values. Nowadays, such a theme continues to trigger questions yet from additional viewpoints: as an example, the topic of defining a contract between military and civilian entities (for defense services, technological development, research, etc.) received more and more attention. The subject recurrently

---

[2] One should also take into account the way in which such a theme gained visibility in the USA, simply by comparing the Camelot project (aimed at studying counterinsurgency and started by the US Army 1964) and the Minerva Initiative project (aimed at financing academic research without passing through the National Science Foundation, project started by the US Army in 2008).

[3] Clark, Robert M. analyzes the evolution of scientific and technologic intelligence during the Cold War, starting with the definition Reginald V. Jones offered for these intelligence approaches during the Second World War. Clark asserted at that time that scientific intelligence was to be conceived as a support for the economic warfare and not only as a means of supporting the arms race. Concerning Lasswell, Harold in M.S. McDougal, H.D. Lasswell, W.M. Reisman, „The Intelligence Function and World Public Order", Temple Law Quarterly, 46(3), 1973, 365-449 he defines intelligence as a means of identifying and solving social problems, useful in developing policy alternatives and not just in setting objectives, emphasizing trends and establishing policy development conditions.

emerges both in the operational environments of recent wars and during consultancy activities conducted by think tanks and NGO-s[4].

Third, the similarity of these problems is also visible when one draws connections between the national security strategy, the national defense strategy, the military and intelligence doctrines and the training programs developed for security professionals. The use of social network analysis by the intelligence practitioners should come as a result of special training programs developed by taking into account the latest developments of the doctrine and strategy, in an adaptive manner. Without entering into the dynamics of the relationship between the grand national strategy – the national security strategy – the military and intelligence doctrines, we have to note that this relationship leads to the continuous adaptation of the training programs and thus to the development of particular profiles for the human capital[5].

For each of these three remarks, young democracies stand as special cases, as the literature reveals. Regarding the link between science and society, the general framework in which we place the relationship between science and the intelligence culture, young democracies have to manage the use of new means to redefine the concept of value and the notion of property, for tangible and intangible goods. Such a situation leads to civil - military relations that tend to degenerate, with military institutions interfering in politics, beyond those limits imposed by the constitution and the legal settings of the liberal democracies, and with a political class that lacks knowledge and coherence[6]. In the absence of an effective political administration of the state, militarized institutions enter the arena of governance through ways and means that are not necessarily as obvious as the coups in Latin America or

---

[4] From the debate that emerged around two classic viewpoints, Huntington (The Soldier and the State, 1957) – Janowitz (The Professional Soldier, 1960) to Finer's (The Man on Horseback: The Role of the Military in Politics, 1988) attempt in finding the meaning of civil-military relations as the strong military institutions could distort the liberal democratic settings, from strategies that could potential mingle citizenship and patriotism in democratic settings to the privatization of the army, Camacho, Paul. "A Forum on Privatization With Comments on the Relevant Literature Found in Armed Forces & Society", Armed Forces & Society, Vol. 36, No. 4, 2010.

[5] The activity of national military centers in correlating the doctrine with the training programs seems to be more or less intensive, function of that state's role in setting military global trends, as member of NATO if we limit the argument to the Euro-Atlantic space.

[6] As in S. Finer, The Man on Horseback: The Role of the Military in Politics, Boulder, Colorado: Westview Press., 1988, which takes into account a series of „classic" military regimes, or as in the vast literature the political science and the media have dedicated to the subject of lustration in former communist countries, in Central and Eastern Europe, Romania being a particular case.

Africa. Depending on the level of political culture and the geopolitical space, such situations can lead to de facto or de jure militarized regimes, for shorter or longer periods of time. Inherently, these situations ask for different ways of describing the relationship between the national strategy, the political space and the policies it generates: defining profiles for security professionals becomes even more difficult, given that such professionals assume forms of political responsibility, in an environment with a developing political culture.

Change management in the intelligence organization

Social network analysis, imagined as a support for the intelligence activity is a complex and complete problem, in the sense that it depends on the way in which the relationship between science and security is understood in a society, on the civil-military relations, and on the way in which a society defines and periodically reviews the profiles of the security professionals. In terms of human resources, before being regulated as a labor market, with occupational standards as the venue of interaction between education providers and producers of goods and services, security is a market defined by state owned institutions, through documents promoted by these institutions, strategies and doctrines, through dedicated training programs for its security professionals. Without ignoring the transformations of the security environment (intelligence, defense and law enforcement alike), in terms of the entities involved, the state continues to hold the monopoly of the legitimate use of physical force, in the Weberian sense.

The goal of defining social networking analysis as a support for the intelligence work, with its definition as a complex and complete problem projected on all three listed dimensions, lies in the need for highlighting the ways in which an organization engaged in intelligence activity learns and adapts to the environment.

The intelligence literature of the last decade proposed topics addressing this issue but placed the analysis on a meta-level: existing studies present the way in which intelligence developed as a topic of interest for the academics in social sciences, as a two faceted domain, with academic and professional dimensions, and as a theory or theorization (Mazare, 2011, pp. 21-33). Such approaches are essential in a time when the security dynamics provide new contexts for interpretation, previously less visible, leading to subjects such as "social sciences and human behavior, support for improving analysis of information", "learning from other disciplines - intelligence and medicine, intelligence and policy analysis", "intelligence analyst as knowledge

workers (knowledge worker)". Praiseworthy and edifying in highlighting the relevance of this issue, these approaches do not provide guidelines, or a code of good practice for intelligence organizations, forced to adapt to the changes of the security environment. Such approaches do not provide even a brief formula that links the theoretical knowledge and the organizational action. In the author's view, such a guide should emphasize a number of general principles, policies and mechanisms, methodologies and procedures through which institutional action might gain consistency and coherence.

In terms of organizational change, as a mandatory process, when adapting to the security environment, the state owned institutions have sought alternatives, trying to outsource activities to entities such as private security companies and various non-governmental organizations, thus searching for capabilities that are not present at the institutional level. The typology of these outsourced activities are diverse, ranging from risk assessment to intelligence analysis, from recruitment and training of personnel to physical protection of objectives, from the public policies development to targeted scientific research.

Ethical and legal problems are inherent in this form of indirect transfer of responsibility, as those situations where the context of the outsourced activities is of extreme intensity tellingly reveal[7]. An example for this state of affairs is the development of the Human Terrain System project. Run by the US Army the project was aimed at joining the teams of the US military forces with representatives of social sciences, with a mission to provide support in understanding human communities in theaters of operations[8].

The development of the project that employed both representatives of social sciences and former military professionals, its adaptation and the

[7] The theatre of operations is one of those contexts with extreme conditions, as long as the loss of human lives continues to be considered an extreme situation, no matter the side on which death might occur.

[8] The literature around this subject is pretty vast and polarized, with at least two opposing sides, of those who support the idea (most of them part of the project) and of those who oppose the program, the contesters. Many examples could be named: the critical literature offers more journalistic stances, like Jon Stanton's, US Army Human Terrain System. 2008 – 2013. The Program from Hell, 2013; in the supporting literature of the HTS one could note the work of the anthropologist Montgomery McFate, e.g "Anthropology and counterinsurgency: The strange story of their curious relationship", Military Review, 2005, 85.2: 24-38. For a more balanced approached, unanimously appreciated see Lamb, Christopher J., James Douglas Orton, Michael C. Davies, T. Pikulsky Theodore, and LTG Michael T. Flynn. "Human Terrain Teams: An Organizational Innovation for Sociocultural Knowledge in Irregular Warfare." 2013.

organizational changes which have been taking place for more than 7 years, the debate emerging in the American society as a whole, the polarization of contesters around the arguments brought by the critical voice of the American Anthropological Association, the way in which the idea was received and transferred to other countries of the Euro-Atlantic space, all these subjects stand as a useful example in understanding the issue of outsourcing some of the institutional activities.

One of the fundamental aspects defining the relationship that emerged between the state-owned institutions and the contractors is related to the assessment of the outsourcing's effectiveness and efficiency. Thus, the state has to imagine the means to measure the performance of contractors in carrying out the contracts they gain, especially when the outcome of their work remains in the category of intangible goods and services. In the case of Human Terrain System, the teams deployed in theater of operations supported the armed forces with analysis reports, covering the social aspects of the environment. According to the principles on which the program was based, the social scientists' support was meant to interfere only with the planning of military activities and not with the military action per se, as arising from the counterinsurgency doctrine in place ("seek and destroy" missions). Such a distinction increases the difficulty of the performance assessment. A balance between qualitative and quantitative assessment is absolutely necessary while the adoption of methodologies that integrate and ponder the relevance of various criteria is also mandatory.

As it was previously emphasized, the evaluation of such programs depends upon the institutional availability for change and environmental adaptation. The main critique this paper addresses to the before mentioned meta-level analyses of the intelligence transformations builds on the missing topic: the identification of the feedback cycles needed to change the organization, in terms of systems theory.

From this point of view, the current article advances the idea that an approach based on action science and double-loop learning, as these concepts were introduced by Chris Argyris, could lead to solutions supporting complex processes of institutional change and adaptation[9].

---

[9] There is a vast amount of literature generated by the themes launched by Chris Argyris, going beyond the borders of academia, being contextualized and adapted to various professional settings. The current paper uses the concepts developed by Argyris, Chris, Schon Donald A, Organizational Learning: A Theory of Action Perspective, Addison-Wesley, 1978.

Such an approach makes a distinction between the theory in use and espoused theory, both being presented as theories of action. The difference lies in the fact that the theory in use is the engine that really moves the organization daily (values, beliefs, norms, strategies – hypotheses on which the behavior of people and the management practice in organizational processes is based on), while the espoused theory is the same amalgam of elements, but in the form officially presented to the others, a declarative version of truth.

It is this difference of the mechanism that starts to enlarge a gap between the models of communication and control that are used and those that are explicitly declared, between resources allocation strategies, personnel selection practices and norms, staff rewarding alternatives and so on. Due to these two perspectives, naturally present in any organization, the double loop learning brings an extension to the classical feedback learning mechanisms – present in technical and biological systems. The double loop learning asks for a reevaluation of the theory in use, in other words it calls for an introspective activity, a self – awareness that goes beyond declarative stances.

This sort of reevaluation is based on a methodology that questions the theory in use by creating the appropriate contexts, so that the norms, the hypotheses and the strategies on which the action is based in the organization are examined. According to this approach, an organization learns while the people inside the organization, particularly the managers, learn to falsify and challenge their assumptions, in individual and collective activities. Using a literary pencil, one would write that the organizational learning emerges when the "double-think" is understood and addressed.

Approaching social network analysis in this article we go beyond those elementary but useful exercises that identify practical scenarios in which the domain of social network analysis is used to represent and study social and technical structures (Wheaton & Melonie). The use of social network analysis in an intelligence organization is conceived as a complex and complete problem, so that approaching it one could hope for the inception of a double-loop learning process in the organization, enforcing change mechanisms and supporting other organizational topics. In the next section of the article we propose an assessment framework, based on which one could evaluate the use of social network analysis in the intelligence organization.

Adding value to intelligence

The exercise of searching for structural patterns and for the specificity of an ensemble of entities (human, organizational, institutional), interacting in

their attempt to reach goals, individually and collectively, is not a recent research endeavor. Such activities are not new, neither in theory, as academic literature proves it, nor in practice, as the institutions endowed with the responsibility of defending state security and citizen safety have used such approaches in a controllable manner since the Second World War at least. Yet, in the last two decades, we can speak of an effervescence in the use of relational representations for those political, social or economic processes interfering with the security context: processes generated by the changes of the global context at the end of the Cold War, by the spread of liberal democracy in geopolitical spaces previously closed, inaccessible areas in terms of movement of people, goods, services and information as such (Mazare, 2011, pp. 21-33).

Technology has only supported, nurtured, these processes, favoring the emergence of "social networks mediated by technological networks" (the cellular telephone networks, the Internet etc.).

Social network analysis, a phrase used to label any attempt to employ graphs for the conceptual and empiric representation of phenomena of all kinds, became an important research area (both fundamental and applied research) when it comes to security issues. Among the factors which supported such developments, one could list the new permeability of political borders and the migration per se, the impact of terrorist threats, the economic and financial crisis requiring new forms of organization and optimization of production and consumption processes, the evolutions in information and communication technology that shaped a new framework of trust and security. Yet, the difficulty one encounters when joining social network analysis as an applied research area lies precisely in the way of amalgamation of the aforementioned factors. In most of the cases, the networked individuals imagine and use both economic and technological processes to support terrorist and criminal activities, thus claiming political goals or just interfering with the law.

These changes of the security environment have required the adaptation of the intelligence analysis so that it can be adjusted to much faster information flows, to information sources that got richer in content, to scenarios dealing with both open and secret information. The purpose of the intelligence analysis remained the same, to support decision making in competitive environments, but intelligence as an organization, process (of which intelligence analysis is part of) and product changed. Change management always requires measurement: it is an appeal to building indicators and controlling the adjustment of previous well defined processes

and working groups, currently unable to support the organizational needs. From this point of view but also taking into account the budgetary constraints that prevailed in the last decade, the intelligence adaptation on all its three dimensions (organization, process and product) required better approaches on measuring the value added by the acquisition of new IT systems (Bouthillier și Shearer, 2003), and by the development of new training programs for the human resources, aimed at enriching the organizational portfolio of capabilities with new analytic methods.

When talking about the value of goods and services we make by default a comparison between two states, one placed before and one placed after the event through which we got to hold the goods or to operate the services. The two states are identifiable not only in those scenarios in which the economists talk of an exchange value - transactional value, equated with the purchasing power of goods or services, but also in those scenarios when one can establish the impact of the goods or services on developing activities, thus computing the value in use for the goods or services. In both cases, one has to quantify the transition between an initial state and a final state, thus assessing the value added, in terms of a specific financial framework or just in terms of a symbolic framework, for example related with the vision and the mission undertaken by the organization.

Using these benchmarks, we define and then map the dimensions needed to establish the value added to the intelligence activity when the social network analysis is inserted into the organizational portfolio of capabilities. The figure below synthetically shows the mentioned benchmarks, highlighting the triple valence of the term intelligence (organization, process, and product) and the dual nature of value (value in use and exchange value). It follows that there are six cases (A to ..., F), dimensions on which one can quantify the value added by social network analysis.

Social network analysis – not just a catchy keyword

Social network analysis is defined as a body of theoretic elements, procedures, dedicated software tools, an assembly of elements used in various disciplines when a representation of a set of entities and their relationships is needed, as a means to identify the development patterns of the parts and of the whole.

As a reaction to the effervescence in the use of terms such as "social networking" and "social network analysis", equally in a variety of disciplines (sociology, political science, anthropology, economics, computer science,

mathematics, criminology etc.) and the media, a group of researchers laid the foundations of what was called "network science". The promoters of this project define network science as "the study of the collection, management, analysis, interpretation and presentation of relational data." (Brandes, 2013, pp. 1-15)

Taking into the account this definition, one can establish certain analogies with the intelligence process, as collection, analysis, and presentation activities are also part of the so called intelligence cycle. It is this simple observation a first step in justifying the usefulness of any attempt to determine the value added by social network analysis to the intelligence process.

This assumption is further enforced as long as one compares intelligence activities with puzzle solving. The puzzle is made of pieces/entities and the relationships between this pieces / entities. Social network analysis, as a scientific method, offers to the analyst a procedural support in approaching puzzles – structures. It stands as body of methods which, when applied rigorously, could add knowledge and thus value, yet in a scientific manner that allows auditing measures to be defined and promoted.

A. Social network analysis - value in use for the intelligence organization

Social network analysis evolved as an activity which employs software tools and requires trained human resources, able to deal with theory and applications: first, one has to conceptualize and abstract the phenomena of interest in terms of entities and relationships between entities; second, there must be developed a corresponding network representation and data collected accordingly; third, a series of network indicators have to be computed and interpreted by taking into account the peculiar context of the phenomenon under scrutiny, thus revealing useful knowledge about the parts and the whole.

We have previously come across two factors that shaped the evolution of the intelligence organization in the last two decades: the technological progress and the increased pressure placed on the available human resources towards updating the portfolio of available analytics. In such a context, trying to determine the value in use added to the intelligence organization by the social network analysis availability at portfolio level, one enters a recurrent problem in a particular way: how the value added to an organization by training and any other form of knowledge transfer is to be computed.

This problem has a long career in the academic literature addressing the management of human resources. Precisely, it leads to finding the right indicators that could measure the performance of the organizational investments in specialization and training programs. This generic problem reveals that, in order to add value by using new goods and services in the organization, one has to follow a well-defined strategy and abide by the declared vision and mission of the organization (Fitz-Enz, 2010).

From this point of view, adding social network analysis to the organizational body of knowledge is in line with changes that have occurred in defining the functioning principles and policies of the intelligence organizations: the insertion of scientific method for the improved environmental scanning. Equally, such a decision could make of social network analysis a transmission belt between the operational levels on the one hand and the tactical and strategic levels on the other hand, serving as a means to deal with issues that start from data collection and resource allocation in intelligence operations up to issues specific to strategic decision making. It is appropriate to note that the value in use, that is the value added to the intelligence organization when the social network analysis becomes part of the organizational body of knowledge and practice, is first to be conceived in symbolic terms and not through its financial benefits.

As knowledge management is another hot topic for the intelligence organizations, somewhere between these two extremes, between the symbolic and financial benefits, we can also place the benefits that emerge when social network analysis is used as a means to define an archive of those phenomena of relational nature.

B. Social network analysis - exchange value for the intelligence organization

Beyond the necessity to adapt to technological change and to enrich the internalized analytical body of knowledge and practices, intelligence organizations have become entities in an ecosystem whose diversity has increased significantly: there are public or private organizations, endowed with social responsibility or not, state-owned institutions, corporations and nonprofit organizations, military academies and civilian universities, all addressing issues specific to the intelligence community and thus supporting decision-making chains or developing education and research projects. Communication on intelligence matters between these entities is the result of communication protocols defined in policies of organizational transparency. In terms of its exchange value, social network analysis can be approached

from the perspective of its role as a subject of communication between the various organizations of the before described ecosystem.

By its nature, social network analysis has evolved as a tool used by several academic disciplines, from those which are to be classified as social sciences (political science, sociology, anthropology) to economics, computer science or mathematics. Whatever the topic of interest, the social network analysis employs an analytical recipe, as mentioned above: data collection, processing, analysis, dissemination. Each disciplinary approach claims the ownership of some particular topics: a psychologist is interested in representing the human entities that are connected through trust based relations, the sociologist looks at the structure defined by these relationships, the anthropologist aims at approaching a particular entity of the network in a particular cultural context, and thus favors the so called ego-networks, the mathematician develops abstract reasoning about representation and numerical alternatives, the economist insists on the transactions and flows that emerge in the network. While for each of these specialists the network is an object of scientific research, for an intelligence organization having a particular role in defending a security framework, the network is an object of practice, a form of organization supporting competitive purposes in a competitive environment.

Given these observations, the current paper asserts that the exchange value brought by social network analysis to an intelligence organization derives precisely from the possibility of transforming it into an element of partnership with academia. The moment seems to be appropriate for such partnerships, to the extent that the identification of conceptual meeting points between the social sciences and intelligence studies is an evolving process. The young network science can also be enriched by connecting it with the intelligence studies, regardless of the perspective endorsed in such studies: theories/theorizations that substantiate the conceptual basis (Gill et al., 2008), developments of the analytical culture through scientific methods used in intelligence practice (Marrin, 2008, pp. 131-146), comparative studies of the intelligence communities in various cultural spaces (O'Connell, 2004, pp. 189-199).

What must be emphasized is that all these conceptual approaches migrated during the last two decades from a military to a civilian and academic interpretive framework, helping to define an intelligence culture in a given society. It is this migration the foundation on which an intelligence organization could seek to define the exchange value for social network analysis.

C. Social network analysis – value in use for the intelligence process

The information overload coupled with failures that affected some of the most prepared intelligence agencies challenged the previously undeniable validity of the so called intelligence cycle. The cyclic approach on the intelligence process (starts when a decision-maker issues a Request for Intelligence, continues with data collection and processing, leads to analysis and intelligence product development, ends when the intelligence report is delivered to the decision maker) was subject of various debates, without a final resolution of the issue. In order to emphasize the value in use brought to the intelligence process by the social network analysis, the current paper assumes, with no argumentative loses, that the intelligence process follows its classic description.

While previously we have defined social network analysis as a potential source for the enrichment of the organizational body of knowledge and practices (A), and as a means of conceptual exchanges in the intelligence ecosystem (B), on the current dimension (C) we place the value in use at the level of practice in the intelligence process.

The role social network analysis could play for intelligence analysis gets more visible as we focus on the analytic stage (thus leaving aside relational data collection and processing): there are at least two ways that show how value could be added to the intelligence analysis. First, social network analysis helps in defining and computing a series of indicators that measure the properties of the structural traits of the network or the flows manifested in the network (with tangible – (e.g. material goods) and intangible (e.g. influence, trust) assets flowing from one entity to another. Among the many existing indicators and their corresponding computation algorithms, those indicators defining central nodes in the network got more visible as they are able to reveal the so called key players of the network (nodes that connect or coordinate parts of the network, monopolizing particular relationship types) (Cross et al., 2003).

A special scenario of social network analysis is aimed at researching the alternative development patterns for a network that has to reconfigure after some particular nodes are removed. This scenario corresponds to those contexts in which law enforcement security institutions target and act upon a criminal network by imprisoning particular members (Carley, 2007, pp. 169-187). The Global War on Terrorism and all the other subsequent transformations that followed 9/11 and redefined the global security

environment placed social network analysis in a privileged role, with a plethora of disciplinary approaches on the subject. Unfortunately, in most of the case, the academics, sociologists or mathematicians, economists or computer scientists, approached the „terrorist network" as if they could have restrained it to only those characteristics accessible to their particular scientific tools. Such an approach is definitely not suitable to adding value to intelligence analysis, a process aimed at integrating evidences and ways of reasoning so that any cognitive bias is carefully avoided. The only academic domain that seems not to follow this recipe, criminology, offers an integrative viewpoint on such matters: the relevance of any network based reasoning can be established only by referring it to the practical support it would bring to the criminologist. Criminology is the domain that could offer examples for imagining use case scenarios in which social network analysis adds value to the intelligence process: the effective and efficient allocation of intelligence officers in missions targeting networks and the efficient deployment of surveillance equipment's are examples of open problems of this kind (Morselli, 2009 şi Klerks, 2001).

D. Social network analysis – exchange value for the intelligence process

The intelligence process is an integrative activity, asking for human resources in all the intelligence organization's departments, for collection and data processing, analysis and dissemination. Defined by so many transactions at departmental and interdepartmental levels, organizational and inter-organizational levels, the intelligence process is influenced by the intelligence community's way of addressing information and knowledge sharing.

Thinking about a security context in relational terms and subsequently representing the context as a network of interacting entities are activities specific to the intelligence process, as previously showed. The exchange value of social network analysis rests in defining the network as the key element for a successful dialog between the various actors / roles involved in the intelligence process.

The actors, collectors, analysts and decision makers exchange, at least different viewpoints having in mind a common representation of the phenomenon under investigation: the collectors have access to a detailed image of the network, analysts are able to advance particular hypotheses on the potential transformations of the network, and decision makers keep an eye on the central nodes – the key players. The exchange of information between such actors was proved to be favored by the existence of a visual

layer of the available information, so that knowledge fusion is better supported (Thomas et al., 2005).

E. Social network analysis – value in use for the intelligence product

While not supportive in integrative terms, the different disciplinary approaches on relational structures emphasized specific procedures for the management of network complexity: zooming in and out, hiding particular nodes while increasing the visibility of others, changing the point of view without losing relevance. Based on such assumptions one could draw a link to the way in which the intelligence report has to be conceived, as structure and content.

Yet, we have to note the limits of using a graphic network representation in an intelligence report. Such a report is most of the times particularly set up, avoiding any terms that might lead to misunderstandings. Social network analysis is a scientific approach so that its usefulness in offering the final touch on some intelligence report aimed at supporting decision makers could be questioned. From this point of view, when dealing with reports that are addressing issues under time and various other constraints pressure, the value in use brought by the social network analysis to the intelligence product has to be carefully considered.

F. Social network analysis – exchange value for the intelligence product

Information technology has shaped not only the way in which intelligence collection, processing and analysis take place but also the alternatives for the dissemination of the intelligence report (Few, 2005).

Most of the software tools aimed at supporting the intelligence process offer functionalities for the customization and scheduling of the intelligence reports delivery, by taking into account organizational roles and profiles, generic security policies or well defined access control settings. The decision maker receives a hypertext based report; he or she can interact with the report by using custom annotations, labels or further delivery options, thus acting like a reactive participant in the intelligence process.

Such software functionalities are aimed at supporting the collaborative work in intelligence teams, so that reports integrate from basic graphic elements to maps and interactive network widgets. Social network analysis is able to define and enhance particular visual representations thus adding value

for all those exchanges taking place during collaborative work, based on sharing intelligence products.

Concluding remarks

The current article has first defined social network analysis as a complex and complete problem. Using an analogy directing towards computational complexity theory, complexity comes out on three dimensions. Thus, the insertion of social network analysis into the intelligence analyst's bag of knowledge and practices depends upon the following three relationships: science – intelligence, civil – military relations, strategy – doctrine – training. The completeness of this problem (the insertion of) resides in the similarities that could be established with problems like the development and deployment of an early warning system, or the modeling and simulation of phenomena specific to the security environment. After carefully asserting that solutions to this complex and complete problem exist and are not unique, and directing the reader to this sort of projects – solutions, the article makes an appeal to the organizational change and learning framework laid down by Chris Argyris. It then goes further to identify those dimensions on which one should project the value added by the social network analysis to the organizational analytic portfolio.

„Social network analysis" is, first of all, a catchy phrase, well represented in the current discourse of the media and of the security professionals, in various contexts and scenarios, both in business and state-owned institutions. Such an increased visibility and ubiquity can be interpreted as a reaction to the political, economic and social transformations that led to the development of communication networks, supporting social decentralized and ad-hoc organization (the Internet and cellular phone networks being two examples of this kind). Yet, beyond discursive stances, „social network analysis" is an assembly of concepts and methods having scientific roots, attracting researchers in many domains while promising to offer ways of accessing the relational nature of the social, political and economic life. The promised land of the relational nature of things was laid at the base of the new network science, aimed at offering an integrative viewpoint, crossing the disciplinary divide.

In order to determine the potential value, added to the intelligence domain through the employment of the social network analysis, the article followed an argumentative schema based on segmentations of both intelligence (as an organization, process and product) and value (value in use

and exchange value). The resulting six points of intersection between these dimensions were then explicitly described, not approaching any financial quantification of the value under scrutiny. Social network analysis was proved to generate value for the intelligence domain in those use cases in which its strengths and limits were simultaneously taken into account.

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

References:

1. Agrell, Wilhelm, Gregory F. Treverton. (2014) National Intelligence and Science: Beyond the Great Divide in Analysis and Policy. Oxford University Press.
2. Argyris, Chris, Schon Donald A. (1978) Organizational Learning: A Theory of Action Perspective, Addison-Wesley.
3. Brandes, Ulrik, Robins, Garry, Mccranie Ann, and Stanley, Wasserman. (2013) What is Network Science, Network Science, Volume 1 / Issue 01 / April 2013, pp 1 – 15.
4. Bouthillier, France, Shearer, Kathleen. (2003) Assessing Competitive Intelligence Software: A Guide to Evaluating CI Technology, Information Today, Inc.
5. Camacho, Paul. (2010). A Forum on Privatization with Comments on the Relevant Literature Found in Armed Forces & Society, Armed Forces & Society, Vol. 36, No. 4.
6. Carley, M. Kathleen. (2007). Dynamic Network Analysis in Counterterrorism Research, in Weidman S., ed., Proceedings of a Workshop on Statistics on Networks, Committee on Applied and Theoretical Studies, National Research Council, pp. 169-187.
7. Clark, Robert M., Scientific and Technical Intelligence, Studies in Intelligence, 19 (1).
8. Cross, Rob, Parker, Andrew, Lisa, Sasson. (2003). Networks in the Knowledge Economy, Oxford University Press.
9. Few, Stephen. (2005). Information Dashboard Design. The Effective Visual Communication of Data, O' Reilly.
10. Finer, S. (1988). The Man on Horseback: The Role of the Military in Politics, Boulder, Colorado: Westview Press.
11. Fitz-Enz, Jac. (2010). The New HR Analytics: Predicting the Economic Value of Your Company's Human Capital Investments, Amacom Books.
12. Gill Peter, Stephen Marrin, and Mark Phythian. (2009) Intelligence Theory. Key Questions and Debates, Routledge.
13. Goldreich, Oded. (2008). Computational Complexity: A Conceptual Perspective, Cambridge University Press, 1 ed.
14. Huntington, Samuel P. (1957). The soldier and the state: The theory and politics of civil-military relations, Harvard University Press, 1957.

15. Janowitz, Morris, (1976). Military Institutions and Citizenship in Western Societies, Armed Forces & Society, vol. 2: pp. 185–204.
16. Klerks, Peter. (2001). The Network Paradigm Applied to Criminal Organizations: Theoretical nitpicking or a relevant doctrine for investigators? Recent developments in the Netherlands, Connections 24, 3(2001): pp. 53-65.
17. Lamb, Christopher J., Douglas Orton James, Davies Michael C., Pikulsky Theodore, and Ltg Flynn, Michael T. (2013). Human Terrain Teams: An Organizational Innovation for Sociocultural Knowledge in Irregular Warfare.
18. Marrin, Stephen. (2009) „Training and Educating U.S. Intelligence Analysts", International Journal of Intelligence and CounterIntelligence, 22: pp. 131–146.
19. Mazare, DAN. (2011). Ştiinţa politică românească şi studiile de intelligence, Analele Universitatii Bucuresti. Stiinte Politice, Anul XIII, 2(2011), pp. 21-33.
20. Mcdougal M.S, Lasswell H.D, Reisman W. M. (1973). The Intelligence Function and World Public Order, Temple Law Quarterly, 46(3), pp. 365-449.
21. Montgomery Mcfate, (2005). *Anthropology and counterinsurgency: The strange story of their curious relationship*, in Military Review, 2005, 85.2: 24-38.
22. Morselli, Carlo. (2009), Inside Criminal Networks, Springer.
23. O'Connell, Kevin. (2004). Thinking About Intelligence Comparatively, Brown Journal of World Affairs, 11(1), pp. 189-199.
24. Spink, Amanda. (1997). Information science: a third feedback framework, Journal of the American Society for Information Science, 48 (8), pp. 728-740.
25. Stanton Jon. (2013). *US Army Human Terrain System. 2008 – 2013. The Program from Hell,* Create Space Independent Publishing Platform.
26. The Guardian, NSA Prism program slides, accessed 26-04 -2015. http://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document
27. Thomas, J. James and Cook A., Kristin. (2005) Illuminating the Path. The Research and Development Agenda for Visual Analytics. No. PNNL-SA-45230. Pacific Northwest National Laboratory (PNNL), Richland, WA (US).
28. Wheaton Kristan, Richey Melonie, The Potential of Social Network Analysis in Intelligence, accessed 26-04-2015 http://sourcesandmethods.blogspot.ro/2014/01/the-potential-of-social-network.html
29. Wheaton Kristan, Critiques of the Cycle: Which Intelligence Cycle? (Let's Kill the Intelligence Cycle), last accessed 25-04-2015 http://sourcesandmethods.blogspot.ro/2011/05/part-5-critiques-of-cycle-which.html.