



THE 21ST EDITION OF THE INTERNATIONAL CONFERENCE EUROPEAN INTEGRATION REALITIES AND PERSPECTIVES

International Relations in the Contemporary World. Geopolitics and Diplomacy

The Multidisciplinary Character of Intelligence Domain

Mircea Mocanu¹

Abstract: In its defining nature, the intelligence domain reflects the quest for any situation or development that might cause harm to national security or military operation. That exposes the observer to a multitude of phenomena pertaining to numerous scientific domains. Recently, this feature became more important two ways: the security environment complexity increased, and the sciences established and developed sophisticated branches meant to cover these dynamics and to produce knowledge necessary to governments for mastering the new complex security environment. This paper approaches the intelligence exposure to various scientific domains from two points of view: scientific fields from which intelligence can be examined; and scientific domains which overlap with intelligence disciplines in the quest for truth to be delivered to power. Previous research addressed such issues, but hardly all together. The findings show that scientific branches able to offer a valuable perspective on intelligence, and which are addressed in this paper are the system theory, military sciences, of course, as well as law, the complexity theory, and education. Implications of this multidisciplinary approach lead to opportunities for significant progress in improving the management of intelligence and its interconnection with other governance branches.

Keywords: System theory; complexity theory; military science; international law; non-formal education

1. Introduction

The diversity of the fields covered by the intelligence activity, as well as the disciplinary angles through which the study of the intelligence domain can be approached, also cause overlaps in the presentation of the multi-disciplinary dimension of the subject, for example in the dichotomy of systems theory/complexity theory. Intelligence structures and the security environment interact through the decision-making system of the security macro-system, which itself has a complex character. The interaction of the components produces properties of the system that are not found at the level of the individual components. This is easy to exemplify in the case of the international security environment, especially considering the effects of globalization and the increasing relevance of non-state actors and

¹ Associate Professor, PhD, Danubius International University, Romania, Address: 3 Galati Blvd., Galați 800654, Romania, Corresponding author: mirceamocanu@univ-danubius.ro.



Copyright: © 2026 by the authors.
Open access publication under the terms and conditions of the
Creative Commons Attribution-NonCommercial (CC BY NC) license
(<https://creativecommons.org/licenses/by-nc/4.0/>)

emerging factors with relevance in the field of security. Through the effect and diversity of the exchanges of information and energy flows meant to regulate the control of Clausewitzian friction in favor of the part served by the intelligence structure, intelligence support is the subject of *complexity theory* and offers casuistry and theoretical developments in this scientific field.

2. The Intelligence Field, an Open System within the Management Macrosystem

The above arguments indicate the dimension of intelligence support in relation to the concepts of *systems theory*, a system being defined, in short, as a “set of interacting entities”. Among these concepts, the intelligence process is analyzed in these pages in relation to the functioning of the intelligence subsystem within the macro-system of governance/risk management/military planning and command. The equilibria and dynamics of this system are marked by the persistence of Clausewitzian uncertainty, information flows and the increase of entropy in international security developments. Such realities underline the complexity of the current security environment (and to which we will return in these lines). The intelligence domain serves the control of the conflict through the intelligence support provided to decision-making, so it operates fully with the complexity of the macro-system, be it the military system or the government/foreign policy system. “Combat is, by its nature, a complex activity... A number of interacting units, behaving under small numbers of rules or algorithms, can generate extremely complex behavior, corresponding to an extremely large number of accessible states or a wide variety configuration, in Cybernetic terms.” (Moffat. 2004, p. 46). Thus, through the activity that involves tracking, understanding and predicting the possible states of a complex system, the intelligence process permanently operates with information flows that reflect the dynamics of a complex system, with all the dovetailing arising from this macro-social phenomenon. More precisely, the intelligence domain is part of the macro-system that must control the military system in armed combat, and “the control system itself... has to be complex” (Moffat. 2004, p. 46).

It can be argued that the limits of the application of systems theory in the field of intelligence are related to the limited possibility of constructing an *objective function*, which mathematically integrates the functioning of the system and allows intervention through corrections and adjustments to achieve the optimization of the system functions. This limitation is generated precisely by the character of an open system, because the success of the intelligence process is subsumed to the success of the macro management system that the intelligence subsystem serves. In principle, for the epistemic component, an objective function can be constructed, having at its disposal objective parameters and variables measurable or estimable on a reasonable scale, then operating with the tools of information theory. But the purpose of the intelligence field is *to provide the truth to power*, and this type of success is not objectively measured before the end of the intelligence process by capitalizing on information in decisions and action. Unfortunately, during the Valorization stage of the intelligence cycle, the information is subject to deontic variables, suffering the intervention of *psychological* (affective) considerations. On the other hand, complications also arise of a deterministic nature, such as measurable components in the category of logistics, own resources (human and material), as well as resources added through cooperation (allied militaries, trading partners). Therefore, given the diversity and number of variables faced by the deontic field (governance, operational command, strategic management – in a general sense) there can no longer be the question of building an objective function with reliable possibilities to provide mathematical optimization. “It is vitally important that the military domain be considered as a *complex system* that is connected and interacts (in “coevolution”) with the surrounding socio-economic environment/context.” (Moffat. 2004, p. xiii) (We will return to the approach as a

complex system below). So, compared to technical systems and even macro-systems, social macro-systems, such as the national defense system, or the national security system, seem to lack the prospects of developing objectively mathematical functions. In the absence of this direction of effort, the assessment of global risks is done through methods in the field of sociology, such as the Delphi method (expert survey). The same is done in the evaluation of systemic success, and it is reevaluated on historical coordinates, with the addition or change of some value criteria and following the realization of the long-term consequences.

3. The Intelligence Process from the Perspective of Information Theory and Military Sciences, Sociology and Ethics

Information theory. Obviously, the raw material of the intelligence domain is information, which is also the core of the study of systems, an element underlined by the criticality of entropy and uncertainty as defining quantities for the systemic approach to the subject. In this respect, all intelligence activities are related to *information theory*, including cybernetics, through the methodologies of selection, grouping by categories (with the generation of metadata and the distinct analysis of extrinsic information from the intrinsic information that accompanies the transmission of a message), evaluation (with the attribution of value to information, even instinctively, at the subconscious level), analysis, processing, search in data libraries/big data, encryption, transmission **Information theory.** Obviously, the raw material of the intelligence domain is information, which is also the core of the study of systems, an element underlined by the criticality of entropy and uncertainty as defining quantities for the systemic approach to the subject. In this respect, all intelligence activities are related to *information theory*, including cybernetics, through the methodologies, storage, generation of added value in new information products, as well as optimizations of courses of action or security information protection procedures.

Obviously, the possibility of mathematizing processes according to systems theory decreases as the level of macrosystems increases on the scale of the social phenomenon under consideration. It is possible that developments in Artificial Intelligence (AI) will bring considerable improvements in the intelligence process, on favorable segments, but the limits of principle remain. However, from the point of view of systems theory, the problem of constructing an objective function for the epistemic sub-domain of the intelligence process, i.e. until Dissemination, stands out as a direction of interest for scientific research in the theory of the intelligence domain.

Military science. Also, the isomorphism that characterizes the working mentality and the specificity of operating with secret/protected information define both the internal mechanisms of the intelligence structures and the interactions with external systems (macro-system of the beneficiaries' deontic authorities, macro-system of the security environment). This specificity of the operation with secret/classified information even indicates the specific difference of the *intelligence domain as a branch of military science*, as a definition classification. Military science studies the space-time-armed combat correlation, obviously a manifestation of the correlations described in *the complexity theory*, and perspectives of this nature appeared evident in the conditions of Network Centric Warfare (NCW), which highlighted the complexity of interactions in an environment with intense dynamics (rapid evolution of equilibria). That is why this scientific branch has undergone a remarkable continuous development, generating a rich bibliography, but the aspect being both ample and obvious, it is not the subject of development in these pages.

Sociology. By the fact that the informative-operative activity (intelligence) has as its object the security and/or military activities, the intelligence domain is probably subsumed, not the least, to *sociology*, both

being subjects of the social sciences. And even in the case of war, military intelligence is described very well in sociological terms. It is obvious that the object of security information is the population and social interactions, from the individual level, as human sources of information of informative or operative interest, to communities (minorities, parties, non-governmental organizations, trade unions, ideological currents, criminal or occult groups), and, especially, at the state level, with all governmental manifestations of interest in terms of security.

Ethics. Through the subtleties and professional interactions, especially in relation to other governmental structures, in a multinational environment, but also towards fellow citizens, the intelligence activity involves aspects distinct from the field of *ethics*. The general domain of morality in intelligence is associated with the *theory of just war* and involves two levels of attention: the level of practitioners, covering the concrete activities of individuals, “without contesting decisions at the strategic level”, respectively the institutional level, “on the limits of actions in the service of the employing state” (Stoian, 2024, p. 9). These issues raise aspects of loyalty, principles, morality and deontology, in the context in which members of intelligence structures also carry out clandestine activities, in theaters of operations or on the territory of other states.

4. The Interaction of Intelligence Domain with Law and Diplomacy

Legal domain. A pragmatic projection of ethics is the judicial field. Therefore, by studying and determining the action on the security environment, the intelligence domain has inherent connections with *law*, from several points of view, including *international law*, through international treaties with military and security references, as well as through *diplomacy*. Through national security-related activity, counter-intelligence operates under civilian supervision under *constitutional law* and under the limitations imposed by *human rights*. Also, through the activity abroad, foreign intelligence operates under the constraints of criminal law, with the complications arising from the fact that it is the criminal law of other states. Military intelligence active in crisis and conflict areas is subject to international law and *humanitarian law*, even having “special treatment” under the Geneva Conventions.

It can also be added that the evolution of intelligence collection requirements towards the need for criminal prosecution of terrorists or other categories of organized crime has led to the emergence of the sub-domain of *judicial intelligence*. This new branch develops the specific aspects of investigations aimed at obtaining *evidence* bearing the legal value necessary for the criminal prosecution of the perpetrators.

Diplomacy. It is in the framework of international law where the relations among governments occur, and diplomacy is the domain of interest in that respect. In the international manifestation of countries, the possession and use of sensitive information in the field of security are essential components. The obvious role of embassies or other types of external representations of states includes informing capitals about developments of interest in the states of accreditation. Here, the limit of the legality of obtaining information has always been a thin line, even a gray area somewhat tolerated by the host state, given the interest of maintaining diplomatic relations, as well as the aspect of reciprocity, which is not negligible. It should be noticed that among the procedures for collecting intelligence in an approximately legal way is *elicitation*, which involves obtaining information directly from people who actually understand what is happening. A concrete application of information support in diplomacy is *Strategic Communication* (*StratCom*), which includes messages generated including with the support of intelligence structures,

but shaped and refined for public distribution (*public diplomacy*), so as to achieve effects of political magnitude as per communicator's interest.

5. Intelligence as a Form of Non-formal Education

The educational function of Intelligence support. In the military field, commanders are equipped through professional training with all the necessary knowledge regarding the role of military intelligence that is provided for the purpose of military decision-making. In the political field, however, raising the competence of the beneficiary becomes, in this way, a requirement to increase the efficiency of Intelligence support, because many political decision-makers have little or no experience in making use of Intelligence support, even if they are graduates of defense colleges or intelligence colleges. Thus, intelligence structures must find the best methods "to 'instruct' political decision-makers, in the most pertinent and not at all offensive sense of the word, on how to request the intelligence product, how to use it and how to follow, over time, how this product has been capitalized" (Medar, 2006, p. 14). Moreover, for special categories of intelligence products, the form of training even has a special name, being called 'indoctrination' for the understanding and use of those products, to ensure the protection of the sensitive capabilities of intelligence structures.

Intelligence as a form of non-formal education. As a form of development, information support is presented as a *non-formal education activity*, because it takes place within the institutional framework of the military or national security system, but **outside the education system**. Of course, the intelligence services also carry out formal education activities, within the curricula of higher or post-graduate education institutions, but these pages aim to highlight only the educational function of intelligence support, i.e. the one carried out in a non-formal way, during the activity that has a primary objective other than education.

On the other hand, it can be noted that the educational side of intelligence activity, whether formal or non-formal, grows into a new form of education, security education. The establishment of this category of "new education" responds to the increasingly obvious need to build an *intelligence culture*, not only among decision-makers, but also for the general public, within the broader framework of the security culture.

Specifically, in the case of military intelligence, learning takes place during real operations, by identifying lessons and determining how to apply them; after operations, through post-mission analysis and application of lessons in future operations (Knowledge Management Section, 2008, pp. 3-8), through the concept and practice of "*lessons learned*".

6. Intelligence and Complexity Theory

6.1. Security Systems Are Complex Systems

The researches aimed at framing the Intelligence support processes in objective parameters associate the concept of '*complex system*' to security systems, the approach being similarly operative for the security environment, in general (Mocanu, 2014, pp. 39 – 52). These types of systems are called 'complex systems' because "their general behavior cannot be reduced to a sum of properties characteristic of the individual components" (Moffat, 2004, p. xi). Moreover, "complex systems cannot be studied independently of their surroundings" ... which may "be represented by one type or another of 'noise'" (Moffat, 2004, p. xiii), and these 'engines' or 'noises' are equally crucial to the understanding of the system as is the analysis of

the system itself (Moffat, 2004, p. xiii). Therefore, complex systems are *sensitive to disturbances* even of relatively small magnitude and cannot be studied by ignoring the relationship with the external environment. The application of constraints, disturbances from the outside prevent the system from reaching a *balance* (Moffat, 2004, p.5). It must be said that, in the case of military/security systems, states of equilibrium cannot be described in deterministic terms, as in physical systems, but behave like biological systems, where equilibria are subject to the subjective factors of actors with free will. That is why the intelligence domain does not operate with the analysis of balances that can be mathematically determined, yet it operates with *levels of acceptability* on the part of the actors/parts of the system in interaction.

Also, the security systems studied by the intelligence scholars show *correlations* between distant components of the system, they can have *adaptive* capacities, intelligent structures display even *learning capacities* (Moffat, 2004, pp. 7 - 43). Thus, the terrorist attacks of September 11, 2001 are of crucial importance more for their effects than for their concrete punctual scale, as they triggered the paradigm shift of strategic deterrence at global level. This historical transition manifests multidimensional components, mainly in the military and security fields, as well as lasting consequences, which the whole of humanity still perceives and tries to face. Similarly, the collapse of real estate loans in the US (the credit crash of 2008) highlighted dysfunctions in the global financial system that led to the economic and financial crisis of the end of the first decade. That crisis affected the entire world and seems to be prolonged, through manifestations aggravated by the Covid-19 pandemic and recent geopolitical developments (the armed conflicts in Ukraine and the Middle East/West Asia). The rapid action of these disturbances is favored by the manifestation of the characteristics of the Information Age and is present in various fields, but intensely involves the decision-making levels at the national level and in intergovernmental organizations.

The action of external *constraints* to a system (in the general sense) implies energy flows in both directions (Moffat, 2004, p. 5), and for the intelligence domain these flows are expressed through the generation and transfer of information, in which case the equilibria are also described by entropy. By considering the intelligence process as an open system, systems theory shows that the tendency of entropy growth increases through contact with another system, characterized by another equilibrium. Through the communication gateways with the management system, the phenomenon of *equifinality can also be reached*, i.e. the achievement of similar states of separate systems, through negative injections of entropy due to the metabolism of the superior system (von Bertalanffy, 1968, pp. 39-41). In the intelligence domain, such an effect is achieved by similarly directing similar intelligence systems, which is observed in the case of multinational structures managed in the same managerial vision (similar policies, values). Such interactions between systems highlight the similarity of information transfer to energy transfers that are more evident in other types of systems. In the case of intelligence systems, the essential role of information is obvious, and the tendency to increase entropy, expressed by the second principle of thermodynamics, produces the same effects as energy (von Bertalanffy, 1968, pp. 41-44).

In the military field, Effects-Based Operations (EBO) have been approached (Ho, 2003, pp. 9 – 13) from several perspectives, including the application of the concept of Network Centric Warfare (NCW) (Mocanu, 2018, pp. 77-109), to ensure synergy in an extended and efficient format, by exploiting self-synchronization and distributed capabilities. On the other hand, the intelligence domain, par excellence informational, also presents the reality of the manifestations of other systemic phenomena specific to the *anthropological* field. For example, intelligence activity displays directivity, goal-orientation, goal-seeking, adaptiveness (von Bertalanffy, 1968, pp. 44-46). These concepts, developed in the specialized

literature, highlight the usefulness of operating with the parameters of systems theory in elucidating the problems of the military domain, in general, and the intelligence field, in particular.

The latter approach treats the enemy faced in conflict or crisis also as a complex and adaptive system, and conflict as a clash between such systems that evolve and adapt to the environment in a non-linear way, which makes them very difficult to predict (Smith, 2002, p. 26).

6.2. Concepts from Complexity Theory Applied in Intelligence

The way in which mathematical concepts can be applied to complex systems has been examined by the British researcher James Moffat, who lists the laws of nonlinear physics, *chaos theory* and notions such as *the equilibrium state*, *external perturbations*, *correlation of events*. Studies in this regard (Moffat, 2004, pp 3-8) show that the relationship between complexity and information-based conflict is less deterministic than in the situation of Industrial Age conflicts, it is focused less on physics and more on behavior, less on physical objects and more on relationships, which underlines the importance of human intervention in security phenomena. Thus, in the Information Age, command and control (C2) emphasize speed, information distribution and decentralization, exactly the essential characteristics of NCW. On the other hand, the decisive contribution to the intervention mechanisms in the decision-making process of a decision-maker or of the masses that make up the public opinion or the electorate, sends the action of intelligence specialists into the essence of '*cognitive warfare*'.

To study future events in a complex system, the analogy with physical, economic, or biological systems is useful. It has been found that *open systems*, which respond to *external stimuli/disturbances* with behavioral changes, manifest *dissipative reactions*, suffer *breaks of internal symmetry*, can develop *different modes of behavior* to stimuli (including *self-organization*), *internal emergent groups (fractals)* in time and space, as well as *correlations between responses to disturbances* (Moffat, 2004, pp. 3-8). In principle, in the field of intelligence, analysts look for *anomalies* in the behavior of geopolitical or military actors, in the internal and external interactions of the studied security systems, therefore *breaks in symmetry* with the current activity and events that can reveal *injections of energy* in terms specific to the theory of complexity, on the part of actors acting to alter *the state of equilibrium* of that system. The interactions of the actors in order to restore the state of equilibrium *qvo antes* reflect *the self-organizing capacity* of the respective security system, which is a specific property of *complex adaptive systems*.

As the difficulties of applying the EBO concept in the military domain have been noted, the over-mathematization of security phenomena presents the danger of choking the system and the collapse of the whole risk management activity. As we have previously argued, this effect may be the consequence of exceeding the ability to track too many variables in a timely manner, due to the unpredictability introduced by the human factor. However, the mathematical approach retains its theoretical value and can still provide certain clarifications, solutions and valuable tools for increasing the efficiency of risk management in security systems or military staff planning.

The usefulness of mathematical tools for modeling complexity is manifested in the study of the (nonlinear) behavior of open systems that can absorb *energy injections*, in the study of *information flows* transferred between open systems, as well as in the field of knowledge representation. For long-term forecasting, the study of knowledge processes highlights the mechanisms of identifying correlations within high entropy systems, such as the international security environment. The identification and study of this type of quantities is favored under the perspective offered by the evolution of phenomena over a longer period of time, in foresight studies. Such evolutions cannot emerge in the time sequences studied in *current intelligence*, or even in *estimative intelligence*. Thus, the methods of studying the future use

procedures based on the patterns identified in the behavior of the studied systems and on the consideration of all the disturbing factors imaginable to influence the evolution of reality. One example in this regard is the ‘*shock test*’ applied by NATO’s Allied Command for Transformation during the Multiple Future Project (Mocanu & Botoș, 2011, pp. 33-46).

6.3. The Functions of Intelligence Support in Terms of Complexity

A brief examination of how the concepts of complexity theory correspond to the system of the international security environment must begin with the simplest situation, namely *the state of normality*. In the language of complexity, this corresponds to the ‘*equilibrium state*’ towards which complex systems tend, through the tendency to establish ‘symptotically stable’ relationships, with the clarifications made earlier, regarding *levels of acceptability* with regard to the equilibrium state described as ‘normal’. The intelligence field serves this trend through *Intelligence support*, more precisely through *the construction of information superiority*. This functional category of Intelligence support (Mocanu, 2015) makes it possible to understand the developments and ‘correlations’ in the security environment and to substantiate the possibilities of favourable diplomatic resolution of tense situations or conflicts before they degenerate. The efforts to asymptotic stabilize the security environment are carried out through ‘information flows’ and ‘energy flows’, mentioned above, the energy side being represented by another functional category that we have called *warning*. The action of intelligence structures takes place in the cognitive domain of NCW, and the decisions taken as a result of Intelligence support (and other informational contributions) contain elements that are called ‘control parameters’ in complexity theory. These parameters define *spaces of the possibilities* of own action for *the response options* in military planning, going down to firing solutions for the tactical field of armed combat. They also serve to adjust the variables of the security situation/operational situation in order to reach a minimum of the ‘loss function’ defined in risk management, i.e. the difference between the and the desired situation. These aspects are studied in military sciences within *the framework of the correlation between forces and means*.

These intertwinings between intelligence, as part of military sciences, and systems theory, in conjunction with complexity theory, gain insights from the nature of *information theory* and *operational research* through the impact brought by NCW concepts, as already mentioned. The new paradigm is the interconnection of *networks of networks*, not only between information networks, but also in networks of military capabilities. In this context, the macro-decision-making system of the enemy manifests *capacities of self-organization*, and the moment of decision/various levels decisions, can be estimated according to the sufficient level of decrease in the entropy of the system. These elements are the basis of the new command exercises (*wargames*), in which the response times of commanders are calculated/estimated as a function of the assumptions of network behavior. A working process is to inject human decisions into a structured environment, in order to generate and study the open system behavior of the military command (Moffat, 2004, pp. 93, 94, 96, 136). Such tested decisions constitute flows of energy/information injected from outside the system, which moves into self-organization and generates response options to move the system towards a new equilibrium, with other internal parameters and other external exposure.

Looking at the process in the mirror, the intelligence structure follows *the control parameters* used by the adversary, seeking to extrapolate the values of the following such parameters. In order not to leave any possibility uncovered, intelligence structures group these parameters, in the logic of their effects, into sets of *indicators* that correspond to *the courses of action* considered as possible. In complexity

theory, these variants of parameter sets correspond to the '*modes of behavior*' proper to complex systems. As mentioned above, given that the security environment and security systems are subject to human intervention (their own decisions or those of the enemy's actions), their '*state function*' is non-linear in nature, and its representation through an *objective function* that is intended to be optimized (through the procedures of systems theory) is very problematic and, probably, impossible to apply consistently. This path is also complicated by the fact that the wargames test military decision-making systems without memory, Markov-type, so the decision cycles are independent of the results of the previous cycle. On the other hand, the subjective, irrational, non-linear character of human decision injections or intelligence product injections tends to increase with the level of decision, from tactical to operational (and especially at the strategic level). It remains to be seen to what extent Artificial Intelligence (AI) can compensate for these limitations of mathematical modeling of command cycles and responses of self-organizing systems.

Through the adjustments made thanks to the Intelligence support, the intelligence domain contributes to the manifestation of the characteristic called 'self-organization' specific to the 'emerging complex behavior' of the international security environment. This means the self-organization of one's own (institutional) system, not the analysis of the interactions that constitute the self-organization of the systems being studied, which was mentioned earlier.

Through the warning efforts, the Intelligence support identifies 'critical points' that manifest themselves in time and space, in the security environment. Through the 'anomaly indications' sought, intelligence analysts identify possible 'symmetry breaks' defined in complex systems. In open systems, 'energy injections' from the outside can constitute 'imbalance constraints' which, in the field of security, translates into generating *political tensions* or *threats when hostile intentions are manifested*. The critical points in complex systems lead to the emergence of 'turbulences' that security systems must absorb through crisis management measures, just as, in open complex systems, "the imbalance requires the system to transform part of the energy communicated from the external environment into an ordered behavior of a new type: the 'dissipative structure'" (Moffat, 2004, p. 8). Obviously, in the case of any country's security system, intelligence is the first line of defense, the first element that contributes to the dissipation of energy applied from outside through political pressure or military threat. Thus, crisis management is an activity specific to a 'dissipative system'. The analysis can be continued by identifying the correspondences of the 'trajectory of the phase space' of the adversary's policy. This can be considered as a historical evolution, but also as a probable evolution, and by assimilating the regime called 'attractor' in the theory of complexity, as the general conduct characteristic of a certain international actor.

However, considering the hostile posture manifested by various actors in the security environment, *Surprise* as an element of Clausewitzian friction It is of particular interest in terms of complexity theory, because it is precisely the element that can trigger a decisive evolution for the state of the security environment. Recent studies have highlighted the idea that surprise will remain a factor in the friction of conflict in the future, because, "if the roots of surprise lie in aspects of human perception..., then it is difficult to understand why this source of friction would diminish the magnitude of its estimated effects in the perspective of future war" (Watts, 2004, p. 42). Thus, the complex character of surprise as an element of Clausewitzian friction is underlined by the intervention of the human component, and this becomes all the more unpredictable the greater the stress of the unexpected situation. In fact, it was stated that "surprise is a feature of complexity, not only of uncertainty" (Bracken et al, 2008, p. 23) which supports the interest in this research direction.

In the light of the complexity theory, the interpretation that the term surprise acquires starts from the idea that the surprise is meant to amplify to the maximum the Clausewitzian friction perceived by the adversary, by generating non-linear developments that are as difficult as possible for the surprised party to control. In complexity theory, *symmetry breaks* and *turbulences*, which can be assimilated with tactical maneuvers and rhythm breaks, or during periods of tension/crisis, can generate rapid successions of seemingly incoherent cascading events, called '*clusters*'. Through the property of *adaptation*, specific to complex adaptive systems, the '*clusters*' and avalanches of events constantly created by more or less local interactions „are dissolved within the entire system" (Moffat, 2011, p. 26) or absorbed in the sense of constructing an *order in disequilibrium*. "Such emergent order arises in open systems in which energy and/or information can cross the boundaries of the system" (Moffat, 2011, p. 26). If, however, these '*clusters*' exceed the response capacity of the opposing party or are overwhelmingly chained, they cause the effect of major surprise, which can play a decisive role in the success of the operation or political confrontation. Actions with surprise value overwhelm the ability of the surprised party to manage the chaos of the confrontation, and its reactions in turn acquire a chaotic character, without continuity with previous actions and without covering logical areas and lead to a radical change of the previous state. In complexity theory, such emergent developments are those referred to as 'fractals' or 'fractal evolutions' and can be exemplified by the unpredictable consequences of natural phenomena from the simplest ones, such as the germination of a seed or a lightning, to the consequences of natural cataclysms or historical revolutions.

The concept of 'surprise' in the field of security can be associated with the concept of 'emergence' in complexity theory, based on the decisive nature of the effects of the surprise event on the state of the system. The dimensions and severity of the impact of the strategic surprise determine the radical change of the political or operational situation, with the development of non-linear developments that go beyond the logic of previous events and can lead to the emergence of unpredictable states that manifest balances and composition different from those prior to the shocks.

Interpreting the idea of Clausewitzian friction control, exposed above, it can be argued that the intelligence domain contributes decisively to the efforts to achieve control over complexity on directions of action corresponding to the three functional categories proposed for Intelligence support (Mocanu, 2015):

- during periods of reduced Clausewitzian friction, information support is manifested through the functional category of *the construction of information superiority*, and intelligence structures contribute to substantiating the possibilities for the security system to generate clusters/turbulences unfavorable to the adversary or even decisive fractal evolutions, in order to impose its own will;
- then, as the Clausewitzian friction increases, the Intelligence support aims to avoid surprise through the functional category of *warning*. Concretely, the intelligence structure contributes to the protection of its own system by acting as a dissipative system. By providing warning, intelligence diminishes or eliminates the possibility that the security system served is subject to suffer symmetry breakings by turbulences or fractal evolutions, which could exceed the control capacities of the system. Also through warning, intelligence structures identify the adversary's vulnerabilities and favorable situational conditions as opportunities in the sense of surprising the adversary, therefore planning turbulence or triggering fractal developments that the adversary is unable to manage;
- during periods of maximum Clausewitzian friction, intelligence structures, operating in close liaison with operational planners and decision-makers, provide 'actionable intelligence' that is immediately

integrated into action to help directly control turbulences or emerging developments, and establish an acceptable new equilibrium.

Thus, after interpreting the role of the intelligence domain in the Clausewitzian friction transfer, the incursion into complexity theory allows the formulation of the role of Intelligence support in relation to current theoretical concepts.

7. Other Scientific Domains Used in Intelligence

In order to conclude the scrutiny of the scientific fields associated with the intelligence activity, apart from the fields that offer advantages to the general approach of the intelligence domain, as well as for analysis, we can add the sciences that are functionally closely linked to the disciplines of intelligence collection: *linguistics* for intelligence from human sources (HUMINT) and for analysis; *electronics* for SIGnals INTelligence (SIGINT) with the COMmunication INTelligence (COMINT) and ELectronic INTelligence (ELINT) branches, *physics* for Measurement And Signature INTelligence (MASINT).

Both at the level of collecting intelligence from human sources (HUMINT) and in the situation of Intelligence support offered to decision-makers (during the Valorization phase of the Intelligence Cycle), the field of intelligence is closely related to *psychology*. Psychological considerations are important both in direct and clandestine contact with persons of interest in the hostile external environment, in direct contact with the enemy (military or other hostile categories, such as terrorists), as well as in one's own, national environment, through the relationship with the beneficiaries of intelligence products, where Intelligence support must take the most appropriate forms for success in achieving national security objectives or military operations objectives.

8. Conclusions

All scientific branches discussed above benefit from ample literature, but one goal of this paper is only to display the diversity of areas of knowledge needed for developments in intelligence, not to exhaust their specifics. These areas of knowledge are necessary for developments in intelligence organisations, human resources, education curricula, not only in the very phases of the intelligence activity proper (Direction, Collection, and Analysis).

Exploring the diversity of fields associated with intelligence activity highlights the complexity of operational requirements when dealing with the unknown, given that the 'must have' unknown is even firmly protected against unauthorized access. These difficulties are expanding in the context of globalization and the increasing complexity of the security environment by associating new scientific fields with the existential requirement of national security.

Moreover, compared to scientific research where conclusions can only be confidently formulated after all possibilities of empirical proof have been exhausted, in the case of Intelligence support, the provision of critically important assessments is often urgently demanded, before the analyst is fully sure of his conclusions, given the limitation and fragmentation of the available information. That is why intelligence is probably among the few domains where the encyclopedic spirit is not outdated, but imperatively necessary. Thus, by projecting the professional requirements into creative altitudes, the multidisciplinary aspect of the intelligence field is one of the arguments of the dilemma of considering this activity both under the rigors of science and under the aura of art. Obviously, this points to the need of multidisciplinary approach plus state-of-the-art information for all research in intelligence.

References

- Bracken, P., Remmer, I., & Gordon, D. (Eds.). (2008). *Managing strategic surprise: Lessons from risk management and risk assessment*. Cambridge University Press.
- Headquarters, Department of the Army. (2008). *FM 6-01.1 knowledge management section*.
- Ho, J. (2003). *The advent of a new way of war: Theory and practice of effects-based operations*. Institute for Defence and Strategic Studies, Singapore. <http://www.rsis.edu.sg/publications/WorkingPapers/WP57.pdf>
- Medar, S. (2006). *Military intelligence in the current security context [Informațiile militare în contextul de securitate actual]*. Military Technical-Publishing Center.
- Mocanu, M. (2014). *Intelligence and the theory of complexity*. “Carol I” National Defense University.
- Mocanu, M. (2015). *Functionality of intelligence support to command and control*. Command and Control Research and Technology International Symposium, Department of Defense. <http://www.dodccrp-test.org>
- Mocanu, M. (2018). *Intelligence in 21st-century military operations*. “Carol I” National Defense University.
- Mocanu, M., & Botoș, I. (2011). *Long-term analysis and the concept of multiple futures [Analiza pe termen lung și conceptul de viitor multiplu]* (Vol. 2, pp. 33–46). Center for Defense and Security Strategic Studies, “Carol I” National Defense University. https://cssas.unap.ro/ro/pdf_carti/sesiune_2011_vol2.pdf
- Moffat, J. (2004). *Complexity theory and network-centric warfare*. CCRP, Department of Defense.
- Moffat, J. (2011). *Adapting modeling and simulation for network-enabled operations*. CCRP, Department of Defense.
- Smith, E., Jr. (2002). *Effects-based operations: Applying network-centric warfare in peace, crisis, and war*. CCRP Series, Department of Defense.
- Stoian, V. (2024). *Intelligence activity: Moral limits and deontology*. European Institute.
- von Bertalanffy, L. (1968). *General system theory: Foundations, development, applications*. George Braziller.
- Watts, B. (2004). *Clausewitzian friction and future war* (McNair Paper No. 68). NDU Press, Institute for National Strategic Studies, National Defense University.