20th ICCRTS

I - 099

Title: **Intelligence and Complexity Theory**

Topics: primary: Topic 1: Concepts, Theory, and Policy
alternate: Topic 2: Organizational Concepts and Approaches
alternate: Topic 4: Experimentation, Metrics, and Analysis

Name of Author: Mircea MOCANU, PhD
Author's affiliation: none, retired, former military intelligence officer.
Author's complete address: Bucureşti, Str. Conţeşti nr 6, bl P-83, sc 1, ap 19, sector 5, ROMANIA.
POC Name: **Mircea MOCANU**
POC Organization: none, retired.
POC Complete Address: Bucureşti, Str. Conţeşti nr 6, bl P-83, sc 1, ap 19, sector 5, ROMANIA
POC Telephone: + 40 734 690 176
POC E-mail Address: **mirceamocanu@yahoo.com**

Summary: The present security environment displays a wide variety of challanges and sofisticated risks and threats relevant in the field of global security. In Clausewitzian view, these features underline the uncertainty of the security environment and an increase in intensity for the risk management activities, where the intelligence domain contributes significantly. This contribution reveals the open system characteristics of intelligence, which allows this activity to be approached from the perspective of system theory.

In this context, the whole risk management problem can also be considered in terms of the complexity theory, and several concepts of this scientific discipline are relevant for understanding the role of intelligence and for improving intelligence support in risk management. Among these, the concept of «surprise» stands out because of its consequences upon stability and security at both global and national level.

Key words: intelligence, complexity theory, fractal, surprise, warning, open system, risk management, operational planning.

I - 099

Intelligence and Complexity Theory [*]

COL. (RET) Mircea Mocanu, PhD [**]

1. The increased complexity of the present security environment[1]

Comparing with the Cold War times, when the security environment was conveniently described by the posture of the force structures maintained by the nations, the present and the future display an eclectic content of the international security, including diverse components (economic-financial, cultural-religious, sanitary-epidemiologic, environmental, informational). The economic and financial crisis triggered in 2008 and agravated in Europe by the case of Greece, starting with 2011, is already a strong argument for this change.

Among the above mentioned components, the economy stands out as the most relevant for its impact on the security environment. In that respect, Stephen Flanagan notices that "the potential of economic globalization to wreak great turmoil rapidly is becoming more evident"[2], and Richard Kugler states that "the coming era likely will be one in which economics and security share center stage in determining how the World evolves"[3].

An example proving the value of considering points of view pertaining to areas non-specific to security is the annual study published each January by the

---

[*] This paper elaborates on sections of Mircea Mocanu, *A Novel Vision on the Intelligence Cycle in the Conditions of the Network Centric Warfare*, PhD thesis defended at National Defence University "Carol I", Bucharest, June 6, 2013.

[**] Col (ret) Mircea Mocanu, BE, PhD, has worked as head of Analysis, Military Intelligence, Ministry of National Defence of Romania, and head Production Branch, IMS INT Division, NATO HQ, Bruxelles, Belgium.

[1] This section uses parts of Mircea Mocanu and Ilie Botoş, *Long Term Analysis and the Multiple Future Concept*, presented at "Power Balance and Security Environment" conference, Centre for Strategic, Defence and Security Studies, National Defence University Publishing House, Bucharest, November 17-18, 2011, vol II, pp. 33 - 46.

[2] Stephen Flanagan, *Meeting the Challenges of the Global Century*, in Richard L. Kugler and Ellen L. Frost (coord.), *The Global Century: Globalization and National Security*, Institute for National Strategic Studies / National Defense University, Washington, DC, 2001, p. 11.

[3] Richard L. Kugler, *Controlling Chaos: New Axial Strategic Principles*, in Richard Kugler and Ellen Frost, *Op.cit.*, p. 75.

World Economic Forum in Geneva (WEF)[4]. In the 2011 issue, WEF identifies 35 risk factors inflicting upon the World economy and discusses their likelihood and economic impact. In the 2012 Global Risks Report, WEF presents the evolving perception of these risks, which indicates the growth in the likelihood and impact of the financial-economic risks. The 2013 Report points out to the dynamics of the risks compared to 2012, which adds value to the estimate. In 2014, the WEF Report underlines the systemic and interdependent nature of the main 31 global risks. Global conflicts are rated as having among the most severe economic impacts, along with financial crises and climate change. However, they have a rather low likelihood, compared to many other risks, among which failure of global governance, organized crime, terrorism, corruption, migration, and failed states have a significant impact upon the security environment. In the 2015 Report though, interstate conflicts are considered instead of global conflicts, probably due to the crisis in Ukraine. In January 2015, conflicts are assessed very high in both probability and impact, followed closely by water crises, failure of adaptation to climate change, and unemployment.

Consequently, there is a growing entropy in international security developments, which underlines the complexity of today's security environment, considering complexity in its most general meaning. An increase in the complexity of the very security structures can also be noticed, since "complexity is not just in the problem - looking for terrorists or WMD in Iraq - but in the organization doing the looking" [5].

[4] * * * World Economic Forum, *Global Risks Report 2011*, p. 3, accessed at 14.10 2011; *Global Risks Report 2012*, 22.01.2012, pp. 4 - 6, accessed at 27.01.2012; *Global Risks Report 2013*, 07.01.2013, pp. 4 - 5, 45 - 54, accessed at 17.01.2013; *Global Risks Report 2014*, 16.01.2014, pp. 9 - 10, accessed at 19.01.2014; and, *Global Risks Report 2015*, p. 3, accessed at 30.01 2015; all published at www.weforum.org/reports.

[5] Paul Bracken, *How to Build A Warning System*, in Paul Bracken, Ian Bremmer and David Gordon, *Managing Strategic Surprise. Lessons from Risk Management and Risk Assessment*, Cambridge University Press, Cambridge, UK, 2008, p. 23.

2. Intelligence system as open system [6]

The main meaning of intelligence support to military decisionmakers places military intelligence as a sub-system of the superior / wider system, the decision-making realm, which includes the commanding officer, his staff, the upper bodies of the national Defence Ministry / Department or other organizations of the Defence, Law Enforcement and national Security System. So, intelligence support acts inside another function of security / military, namely the function of *risk management* or *operational planning*, respectively: "it is crucial to recognize that warning [as a function of intelligence] is one piece of a larger risk management system"[7]. In the same time, the integration of «actionable» intelligence into decision and concrete action (as the practical destination of intelligence products) casts more light upon the relations between intelligence activities and the realities of the security environment, military organization or operational situation.

Between the decisionmaking system, performing risk management, and the intelligence sub-system, transfers of all systemic components are conducted: resource transfers (material, energy, personell), information transfers and suprastructure transfers (rules, directions, performance reports). The major interest interaction - the information exchange - belongs to the general information flow represented by the classic model of the intelligence cycle, which includes the phases of Direction - Collection - Analysis - Dissemination.

The interaction between the intelligence structure (J2) and Command and Control (C2) / the decision-making domain of the security or military system is basically conducted through two points of the intelligence cycle. One is the point allowing the transfer of intelligence requirement and beneficiary feed-back

---

[6] This section uses parts of Mircea Mocanu, *Military Intelligence as Open System*, presented at the interntional scientific conference Strategies XXI: "The Complexity and Dynamism of the Security Environment", Centre for Strategic, Defence and Security Studies, National Defence University Publishing House, Bucharest, November 21-22, 2013, vol II, pp. 276 - 285.

[7] Paul Bracken, *Op.cit.*, *How to Build A Warning System*, in Paul Bracken, Ian Bremmer and David Gordon, *Op. cit.*, p. 42.

towards J2. The second point is dissemination itself, which marks the delivery of the intelligence product from J2 to the decisionmakers. These two moments of the intelligence work are considered to be the most tricky precisely on the grounds that these «gates» are the very contact points between the intelligence subsystem and the C2 system, they are not internal links inside one system.

The two «gates» of the intelligence cycle marking the point of entry for the intelligence requirements and the point of exit for the intelligence products from the intelligence structures materialize the fact that *the intelligence structure is an open system*. So, the conceptual model named intelligence cycle, which describes the intelligence activity, defines the intelligence flow which crosses both the intelligence structures and compartments of the beneficiary, which do not belong to intelligence organisations. Consequently, the beneficiary - actor of the decisionmaking / C2 system, not belonging to J2 - is, however, integral part of the intelligence cycle.

The two communication gates towards the C2 / risk management superior system also clarify two other relations between those systems:

- on one hand, they reveal the mechanism of transfering the Clausewitzian friction within the operational environment or - writ large - within the security environment[8]. Thus, the intelligence support provided by J2 as open system sets the core role of intelligence as an important tool in the attempt to control the Clausewitzian friction of the conflict, even in the phase previous to military engagement, which is outside a Clausewitzian conflict.

- on the other hand, the communication theory allows us to see a significant feature of dissemination, the *energy transfer*, in psychological terms. This transfer operates in the volitve domain, and activates the motivation to start action by the decision based on the intelligence products.

[8] Barry Watts argues the persistance of Clausewitzian uncertainty in the conditions of the Information Age in his paper *Clausewitzian Friction and Future War*, McNair Papers nr. 68, NDU Press, Institute for National Strategic Studies, National Defense University, Washington DC, 2004.

It is clear that the intelligence structures have more «windows» to interact with the exterior environment, along the links of the intelligence cycle, such as:

- Firstly, during the phase of Direction, the intelligence activities are conducted under the authority of the head of the respective structure. However, the authority of responsible staffs at different levels is also relevant in the process, and even the authority of individuals with various responsibilities at lower echelons of the organization. In the reverse sense, the intelligence structures report to higher authorities on their activity and make suggestions for organisation development.

- Secondly, during the Collection phase of the intelligence cycle, the intelligence structure interacts directly with reality, with the security / operational environment, from where it obtains the necessary data and information through activities pertaining to the intelligence collection disciplines. These interactions are specific to the intelligence system and rarely privy to the upper C2 / decisionmaking system. From a systemic and chaos theory point of view, they are *injections* of information. These injections generate intelligence products elaborated according to J2 objectives and procedures, and destined for the decisionmaking system.

Besides their clandestine nature, the complexity and sensitivity of intelligence collection activities can be explained by the complications entailed by the transfer of information between two different systems: one of them is the intelligence system, active in collection, while the other is the international environment - the operational / security system, having a high level of entropy.

Thus, the points of contact with the environment outside the intelligence structures are shown in the model of the intelligence cycle presented in Figure 1. They underline the *open system characteristic* of the intelligence structure, which has significant implications on the research of the intelligence support.

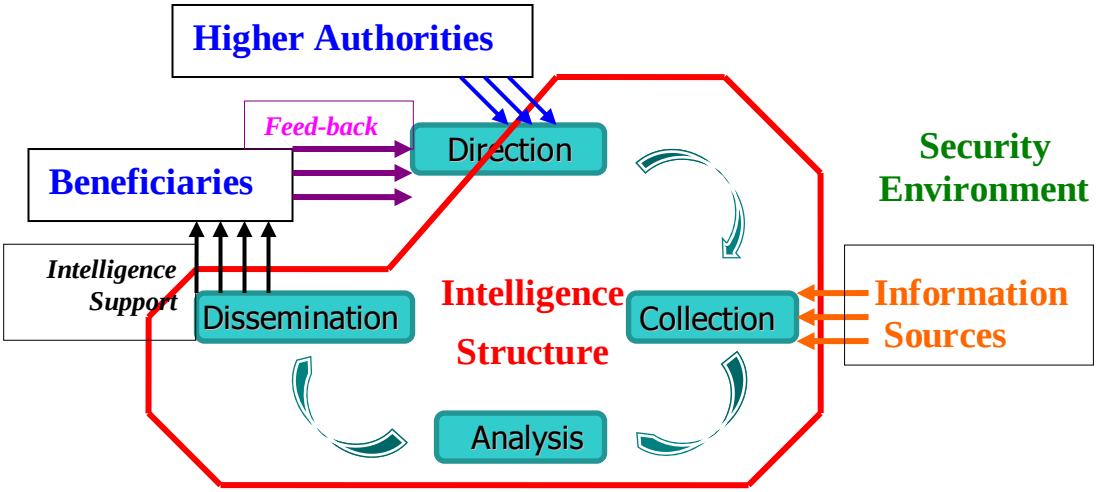

Fig. 1. Communication gates between the intelligence structure and the security environment

Practically, J2 / any intelligence structure and the security environment interact both directly and through the decisionmaking system of the security macro-system, exchanging information and energy flows meant to contribute to the control of the Clausewitzian friction in favour of the party served by the intelligence structure. It is difficult to consider practical measures for the control of the Clausewitzian friction. However, any subject / actor in the security environment has its own perception of the Clausewitzian friction, based on its satisfaction regarding the understanding of the security environment or regarding its success in risk management.

3. Intelligence support seen through complexity theory

The open system features allow intelligence activities to be framed in concepts which reflect open system transfers and provide the opportunity to study intelligence support using the tools of complexity theory. Recent research intended to support the intelligence processes with objective parameters associate security systems to the concept of «*complex system*». This approach is operational, in a similar manner, to the security environment, in general. These kinds of systems are called *complex systems* because "their general behaviour

cannot be limited to a sum of features specific to individual components"[9] of the system. The interaction of system components generate system features which do not reflect features of any individual component, and the system response to stimuli is not always linear. This is simple to verify for the international security environment, especially considering the effects of globalization and the growth in the relevance of non-state actors.

More exactly, the information flows and the capacity to absorb external shocks, along with complex feed-back loops and emerging behaviour, define the security environment and (to a lesser extend) the intelligence organization as complex *adaptive* systems. In such systems, the link between cause and effect is less obvious, due to the complex interactions leading to the emerging behaviour. For example, one cannot say the the Arab spring was caused by the suicidal protester in Tunisia, even if that event was a clear referrence moment in the developments which cover the whole Arab World and are still ongoing. However, that event triggered a reaction, a chain of events which can be described as disproportionate, since they had obviously far more complex causes.

This example prove that complex systems are *sensitive to perturbations*, even limited, they cannot be studied in isolation, ignoring the relationing with the external environment. Complex systems also show *correlations* among distant and distinct components of the system and can display *adaptation* capabilities, the intelligent systems can display even *learning capabilities*[10]. For example, the terrorist attacks of 11 September 2001 are of utmost importance mainly due to their dovetailed effects rather than their immediate impact, because they triggered a paradigm change in strategic deterrence, a historical transition that mankind is still living and coping with. Similarly, the colapse of the real estate financial market in the US revealed malfunctions of the global financial system which led to the economic-financial crisis triggered last decade,

[9] Henrik Jeldtoft Jensen, *Foreword* to James Moffat, *Complexity Theory and Network Centric Warfare*, CCRP Series, Department of Defense, Washington DC, 2004, p. xi - xiii.
[10] James Moffat, *Op.cit.*, *Complexity Theory and Network Centric Warfare*, pp. 7 - 43.

and still inflicting the whole World, while showing only slight signs of recovery. The quick impacts of these perturbations were facilitated by the specifics of the Information Age, are present in multiple fields, and deeply involve the decision level at the national level, as well as within intergovernmental organizations.

In the military, the efforts to achieve operational effects[11] has dealt with[12] from the following perspectives:

a. Integrated planning strategy, implying speed and continuity;

b. Optimized targeting to serve the intended higher effect;

c. Gaining supremacy (in various domains and engagement spaces) with speed, to enforce the decisive feature of the effect;

d. Sinergy of power elements in comprehensive approach;

e. Interaction and cooperation at all levels with all relevant actors, in order to overcome the uncertainty generated by a complex and adaptive opponent; and,

f. Utilization of the Network Centric Warfare (NCW) concept, to secure the operational sinergy in a wider and more effective format, by exploiting self-sincronization and distribution of capacities.

This approach sees the enemy also as a complex adaptive system and the conflict as a relation between such systems, acting and adapting to environment in a non-linear manner, which gives these systems very low predictibility[13]. However, the role of intelligence is still to illuminate the future in the behaviour of the international security environment as a low predictibility complex system.

This approach also allows the most important concepts of complexity theory to be interpreted with significant benefits in terms of intelligence, and, this way, they contribute to improvements in the J2 / intelligence structure activity, especially in the conditions of today's conflicts and NCW requirements.

---

[11] Even if the Effects Based Operations (EBO) concept has been discarded as a practical operational approach, the building bricks of the concepts are quite valuable for the study of the military complex adaptive systems.

[12] Joshua Ho, *The Advent of A New Way of War: Theory and Practice of Effects-based Operations*, Institute for Defence and Strategic Studies Singapore, December 2003, pp. 9 – 13, accessed at 09.05.2012 at http://www.rsis.edu.sg/publications/WorkingPapers/WP57.pdf.

[13] Edward A. Smith Jr., *Effects Based Operations: Applying Network Centric Warfare in Peace, Crisis, and War*, CCRP Series, Department of Defense, Washington DC, 2002, p. 26.

4. Relevant concepts from complexity theory

The way mathematics can be applied to complex systems has been examined by James Moffat, who takes into consideration the laws of *non-linear physics*, *chaos theory*, and terms like *state of equilibrum, external constraints*, and *event correlation*. Research in the complexity theory approach shows that the information-based conflict, in the Information Age, is less deterministic than the conflict specific to the Industrial Age. The information-based conflict is less driven by physics and direct cause-effect relation, and more driven by complex relations and fuzzy interactions among a plethora of relevant actors. This underlines the importance of human involvement in security phenomena. Thus, in the Information Age, C2 highlight the speed of decision and action, information distribution and decentralization, which are core features of NCW.

The forecast of future developments in complex systems requires analogies with physical, economic or biologic systems (this is why they are also called *ecosystems*), starting with the Brownian movement, the quite simple model of random dynamics. In such cases, *open systems (or ecosystems)*, which respond to *external stimuli* / *constraints* with *behaviour changes* show: *dissipative reactions*; undergo internal *symmetry breakings;* can develop various *modes of behaviour to stimuli* (including *self-organisation*), can show internal *emergent groupings* in time and space; as well as, provide *corellations among responses to perturbations*[14].

In the military, for example,the over-mathematization of security phenomena, in the case of implementing the concept of Effects Based Operations (EBO), raises the danger of blocking the system response and can lead to the collapse of planning. This happens when the analyst capability to track a large number of variables quickly enough is overwhelmed, especially considering the unpredictibility of human factor. However, in the absence of any pressure to prematurely implement EBO in real operations, the mathematic

[14] James Moffat, *Op.cit., Complexity Theory and Network Centric Warfare*, pp. 3 – 8.

approach maintains its theoretic value and can provide explanations, solutions, and valuable tools to increase the risk management effectiveness in security systems or military planning.

The value of mathematic tools in modeling complexity appears in research of issues like the (non-linear) behaviour of open systems which can absorb *energy injections, information flows* between open systems; as well as, representation, development and use of *knowledge*. For long term prognosis in intelligence, the research of knowledge highlights the mechanisms of *corellation* identification in *high entropy systems*, such as the international security environment. These investigation methods for the future use procedures based on the patterns identified in the system behaviour, and on the consideration of all imaginable perturbation factors capable to alter the evolution of reality. A good example is the *shock test* applied by NATO researchers during the Multiple Future Project conducted by the Allied Command Transformation (ACT) to generate a projection of the Future Security Environment. The shock test demonstrated the necessity to improve practical procedures for a better understanding of the complex adaptive systems, and to explore the emergent behaviour by various plausible scenarios.

A quick scrutiny of the way that complexity theory concepts match the international security system should start with the simplest situation, i.e., the *state of normality* or, in military terms *peacetime.*

In complexity theory language, this corresponds to *state of equilibrum* to which complex systems tend to evoluate, by their tendency to establish *assymptotically stable* rapports. Intelligence serves this trend by its function of intelligence support, more exactly by the *construction of intelligence superiority*[15]. This functional category of intelligence support allows both the understanding of evolutions and correlations within the security environment,

[15] Three functional categories have been proposed by Mircea Mocanu in *Op.cit. A Novel Vision on the Intelligence Cycle in the Conditions of the Network Centric Warfare* (2013), pp. 109 - 125: construction of intelligence superiority, warning, and integration into action.

and the support for diplomatic options to solve the tense situations of forestall conflicts before they degenerate. As mentioned before, the efforts to assymptotically stabilize the security environment are conducted by applying *information flows* and *energy flows*. Different from thermodynamics, where energy transfer supposes heat, in intelligence, the energy transfer operates in the psychological domain and is represented by the functional category called *warning.*

The action of intelligence structures occurs inside the *cognitive domain* of NCW, and the decisions taken as a result of intelligence support (and other informational contributions) contain elements called *control parameters* in the complexity theory. These parameters define *spaces of possibilities* for action (corresponding to *courses of action* in military planning), and serve to adjust the security / operational situation variables in order to reach a minimum of the *loss function* defined in risk management, i.e., a minimum of the difference between the real situation and the desired situation.

Looking at the process in the mirror, the intelligence structure tracks the *control parameters* used by the adversary, looking to extrapolate their values when producing prognoses and predictions. In the attempt to leave no possibility uncovered, the intelligence structures group these control parameters according to their effects, in sets of *indicators* which correspond to *thresholds* or stages of the *courses of action* considered as possible to occur. In the complexity theory, these sets of parameters correspond to the *modes of behaviour* specific to complex systems. Given that the security environment and the security systems are subject to human intervention, their *state function* is non-linear. Therefore, its representation by an «*objective function*» to be optimised by system theory methods is very complicated and, I dare say, impossible to apply consistently. More generally, this point underlines that the representation of the international security environment as a complex adaptive system is a wicked problem in mathematical sense, and requires numerous assumptions, caveats, and limitations, when imagining representation models and research algorithms.

5. Functional intelligence issues in complexity theory terms

The adjustments that risk management conducts based on intelligence support allow the intelligence structures to contribute to the realisation of *self-organisation* within the security system as a response to the *emergent complex behaviour* of the international security environment.

By *Warning*, J2 identifies points of *criticality* which manifest in time and space within the security environment / operational situation, including in the enemy ranks. By the «*anomaly indications*» they seek, intelligence analysts identify possible *symmetry breakings* as defined in complex systems. For open systems, the *energy injections* from outside may act as *nonequilibrum constraints* which, in security terms, means *political tensions* or *military threats,* when *hostile intentions* are present.

Criticality points defined in complex systems lead to «*turbulences*» which security systems need to absorb by mitigation measures taken in the risk management activity. This reaction by the security systems reflect that, in open complex systems, "the nonequilibrum enables the system to transform part of the energy communicated from the environment into an ordered behaviour of a new type: the «*dissipative structure*»"[16]. Obviously, in the case of the security system of any country, the intelligence activity is the first responder contributing to the dissipation of energy applied from outside by political pressure or military threat. Therefore, risk management is an activity specific to a «dissipative system». Analysis is continued in the *evaluation of the probable evolution* corresponding to the «*trajectory of phase space*» specific to the adversary's policy. In a historic perspective, that is seen as the dynamics of the most probable actions.

Similarly, the regime / state called «*attractor*» in complexity theory, can be associated to the characteristic behaviour / general trend of a certain international actor, with its trend to pursue and achieve its national interests, or,

[16] James Moffat, *Op/cit. Complexity Theory and Network Centric Warfare*, p. 8.

for the operational domain, its specific *military doctrine*, its traditional way to wage war. Military intelligence needs to track adversary's actions considering its attractor, yet always be ready to take into account any action apparently opposite to this attractor, in order to be able to avoid *surprise*.

Considering the hostile posture manifested by various actors in the security environment, *surprise*, as an element of the Clausewitzian friction, presents a special interest from the point of view of complexity theory, because is exactly the element capable of triggering a decisive evolution for the state of the security environment. Recent studies pointed out that surprise will remain a factor of conflict friction in the future because, "if the roots of surprise lie in aspects of human perceptions and uncertainties too basic for technological advances to affect, much less eliminate, then it is difficult to see why this source of friction would diminish in the magnitude of its prospective effects on future war"[17]. So, the complex character of surprise as an element of Clausewitzian friction is underlined by the intervention of the human component. The greater the stress level of the unexpected situation is, the more unpredictible surprise becomes. It has been stated, however, that "surprise is a feature of complexity, not only one of the uncertainty"[18].

The interpretation I suggest for *surprise* in terms of complexity theory is based on the idea that surprise is meant to maximize the Clausewitzian friction perceived by the adversary, by generating non-linear evolutions which are as difficult as possible to control by the surprised party. *Simmetry breakings* and *turbulences* in complex adaptive systems correspond to the *manoeuvres* and *rhythm breakings* terms used in tactics, or in situations of political tensions / crises. They can generate a series of quick cascaded events, which are apparently incoherent, known as *clusters* in complexity theory. "These clusters or avalanches of local interaction are constantly being created and dissolved

[17] Barry D. Watts, *Clausewitzian Friction and Future War*, McNair Papers nr. 68, NDU Press, Institute for National Strategic Studies, National Defense University, Washington DC, 2004, p. 42.
[18] Paul Bracken, *Op.cit., How to Build ...*, în Paul Bracken *et.al., Op.cit., Managing Strategic Surprise...*, p. 23.

accross the system"[19] by the effect of *adaptation*, specific to adaptive complex systems. The system works to dissolve / absorbe the clusters in the process of building an *order in nonequilibrum* which corresponds to the *measures taken in crisis management*. "Such *emergent order* rises in open systems where energy and/or information are allowed to flow accross the boundaries of the system"[20].

If, however, these clusters overcome the response capability of an actor, or they concatenate overwhelmingly and generate the psychological effect of a major surprise, which can impact decisively on the success of the military operation or of a political confrontation. So, the actions with surprise value overwhelm the surprised party's assumptions and its capability to control the Clausewitzian chaos of the confrontation. Therefore, adversary's actions become chaotic, in their turn, with no continuity with previous actions, no coherence, and failing to cover logical zones, thus leading to a *radical change* of the previous situation or course of events, like a catastrophic event. In complexity theory, such catastrophic and low predictibility evolutions are called *fractals* or *fractal evolutions*, and examples of them range from the simplistic: like the breaking of a cofee cup, the rise of a grass blade or the thunder; to the most complicated: like natural cataclisms, the world wars, or historic revolutions.

I propose the association of the concept of surprise, from the military or security domain, with the concept of catastrophic event or fractal / fractal evolution from the complexity theory, on the ground of the chaotic, unmanageable feature, and of the decisive nature of surprise events upon the state of the system, at the level such events occur. The dimensions and gravity of the strategic surprise impact causes the radical change of the political or operational situation, panic following non-linear evolutions, apparently disproportionate, which break the previous events' logic chain. Concrete examples can be, in the military domain: the *breaking of the front, panicked withdrawal*, the *loss of troop control*, leading

[19] James Moffat, *Adapting Modeling and Simulation for Network Enabled Operations*, CCRP Series, Department of Defense, Washington DC, 2011, p. 26.
[20] *Idem*.

to *capitulation;* or, in the political realm: the *dissolution of central institutions*, *anarchy*, *fall of the government*, *monarch's abdication* or *president's resignation*, or the *loss of national sovreignty*.

In aiming to control the Clausewitzian friction, intelligence support, as part of the risk management, significantly contributes to the system's efforts to control the complexity of the security / operational environment. This action is conducted along the lines of the three functional categories proposed for the intelligence support to decisionmaking:

- firstly, during the periods of low Clausewitzian friction, corresponding to the *state of normality* of the complex adaptive system, intelligence support contributes to building informational dominance by the functional category I termed *construction of intelligence superiority*. Thus, intelligence structures contribute to *situation awareness* and to secure the base for security system's option to generate, when necessary, *turbulences* or *clusters* opposing adversay's interests, or even decisive *fractal evolutions* to *surprise* the adversary in order to bend his will;
- secondly, as the Clausewitzian friction increases, when a *threat* is identified or a *risk* escalates, intelligence support assures *avoiding surprise* by the functional category called *warning*. Practically, the intelligence structure contributes to own security system protection by diminishing or eliminating the possibility that the system be subject to *turbulences* or *fractal evolutions* which might overcome system's control capcitity. Also by warning, the intelligence structures identify *vulnerabilities* of the opponent and *favourable conditions* able to be exploited in a certain situation as *opportunities* for decisions aiming to surprise the adversary by planning turbulences or events which can trigger fractals beyond adversary's capabilities to control; and,
- thirdly, during maximum Clausewitzian friction periods, for example during *major international political crises* or *armed conflicts*, the

intelligence structures, operating closely or even integrated with the other operational planners in C2, deliver products at high pace, and containing «actionable» intelligence. Such valuable contents *integrates immediately into action* to contribute to the control of the turbulences or fractal evolutions that the own system faces. This way, intelligence contributes to the construction of an *order in non-equilibrum,* i.e., contributes to *crisis management*, respectively to *operational planning* and *military action*.

Conclusions

Following the interpretation of intelligence role in the transfer of Clausewitzian friction to the adversary and the argumentation for the open system feature of the intelligence structures, the research into complexity theory allows rephrasing intelligence's role using today's thoretical concepts of wide generality.

The natural interpretation of the complexity theory concepts in terms of intelligence activities facilitates the development of theoretic constructions and conceptually proves useful for improving the crisis management efforts or intelligence support for military decision.

Therefore, the research of the intelligence domain through the complexity theory framework is worthy of being followed by the study and interpretation of C2 / crisis management / operational planning from the same complexity theory perspective.

Bibliography

* * * the World Economic Forum reports: *Global Risks Report 2011, Global Risks Report 2012, Global Risks Report 2013 Global Risks Report 2014,* and *Global Risks Report 2015,* published at www.weforum.org/reports.

BRACKEN, Paul; BREMMER, Ian şi GORDON, David, *Managing Strategic Surprise. Lessons from Risk Management and Risk Assessment*, Cambridge University Press, Cambridge, UK, 2008.

HO, Joshua, *The Advent of A New Way of War: Theory and Practice of Effects-based Operations*, Institute for Defence and Strategic Studies Singapore, december 2003, published at http://www.rsis.edu.sg/publications/WorkingPapers/WP57.pdf.

KUGLER, Richard L. and FROST, Ellen L. (coord.), *The Global Century: Globalization and National Security*, Institute for National Strategic Studies / National Defense University, Washington, DC, 2001.

MOCANU, Mircea, *A Novel Vision on the Intelligence Cycle in the Conditions of the Network Centric Warfare*, PhD thesis defended at National Defence University "Carol I", Bucharest, July 6, 2013.

MOCANU, Mircea, *Military Intelligence as Open System*, presented at the interntional scientific conference Strategies XXI: "The Complexity and Dynamism of the Security Environment", Centre for Strategic, Defence and Security Studies, National Defence University Publishing House, Bucharest, November 21-22, 2013, vol II, pp. 276 - 285.

MOCANU, Mircea and BOTOŞ, Ilie, PhD, *Long Term Analysis and the Multiple Future Concept*, presented at "Power Balance and Security Environment" conference, Centre for Strategic, Defence and Security Studies, National Defence University Publishing House, Bucharest, November 17-18, 2011, vol II, pp. 33 - 46.

MOFFAT, James, *Adapting Modeling and Simulation for Network Enabled Operations*, CCRP Series, Department of Defense, Washington, 2011.

MOFFAT, James, *Complexity Theory and Network Centric Warfare*, CCRP Series, Department of Defense, Washington DC, 2004.

SMITH Jr., Edward A., *Effects Based Operations: Applying Network Centric Warfare in Peace, Crisis, and War,* CCRP Series, Department of Defense, Washington DC, 2002.

WATTS, Barry D., *Clausewitzian Friction and Future War,* McNair Papers nr. 68, NDU Press, Institute for National Strategic Studies, National Defense University, Washington DC, 2004.