CONSIDERATIONS REGARDING THE 21st CENTURY's HIGH QUALITY SECURITY CONCEPT

Colonel (ret.) Professor eng. Eugen SITEANU, PhD*

***Abstract**: The present paper is devoted to qualitative security which today has to become a topic issue of world security. The opinions regarding the 21st century's security concept are contradictory since people have different understandings and perceptions of security, respectively insecurity, and do not agree to analyze the security concept as a function of the system. Our take is that implementation of some new security concepts should aim an analysis and understanding of security in an integrating view, in order to make the most comprehensive security environment possible. Therefore, we do believe that it is necessary to define the concept of high quality security, which is translated in our current paper.*

***Keywords**: high quality security, qualitative security, insecurity, integrating character, parameter, process, action capability.*

If we have to compare this century with the previous one, the threats, the dangers, the vulnerabilities and, obviously, the risks have been amplified, and people do not have the same feeling of being safeguarded under the security umbrella. This is the reality of the nowadays security environment in which the security technology and the risks (and also the threats and vulnerabilities) culture have developed and spread at a global scale, on the same scientific grounds. The security technology has assured a fast growing development of integrated security systems and mechanisms

* Professor, PhD, Member of the Academy of Romanian Scientists, E-mail: esiteanu@yahoo.com

for an efficient and effective countering of organized cross-border criminality, crises, catastrophes and disasters. There have been created new concepts and technologies of national risk management, of social security management and of the specific processes for building high quality security environments (which are implemented on the basis of the high quality security concepts).

Following the publishing of some high level scientific papers, the economy security strategy has been developed and for this strategy the security processes have been structured. Thus, some concepts of quality security have been substantiated and implemented (opportune, certain, durable, obligatory, total, sufficient, complete, lasting, maximal, absolute, vital, optimal/optimum, minimum/minimal and qualitative security). The new qualitative security concept emphasizes *„the integrating and multidimensional character of security, and also the possibility of confronting rationally and effectively the hazard of threats and disasters"* [1].

Simultaneously, security is: a dynamic state of any process and system, necessary for their own existence; a main quality parameter (component) of any organization (including here the state, the group of states, etc.) and any system; a cyber-process having the goal of assuring the stability, safety, protection, trust, availability and viability of the systems (organizations) and an action capability (an action element) of the process/system/organization *„of preserving the functional characteristics under the action of some destroying factors or some factors able to cause such mutations which are dangerous for the natural environment or for people's health (including life) which are located in their action range, causing material, information or moral damage"*[2].

At the same time, the qualitative *„security of systems and processes is a state or a result of coherence and consistency of all elements and actions that happen within them and presupposes the existence of a dynamic equilibrium between threats (challenges, defiance, dangers etc.) and*

[1] Gheorghe Ilie, Tiberiu Urdăreanu, *Securitatea deplină*, Editura UTI, Bucureşti, 2001, p. 9, vezi şi Gheorghe Ilie, *Risc şi securitate – articole, comunicări şi prelegeri* – vol I, Editura UTI Press, Bucureşti, 2015, p. 11.

[2] Gheorghe Ilie, Tiberiu Urdăreanu, *op. cit*., p. 13; vezi şi Eugen Siteanu, Bedros Naianu şi Gheorghe Ilie, *Fiabilitatea produselor tehnice,* Editura AISTEDA, Bucureşti, 2000, pp. 133-134.

vulnerabilities to threats. This dynamics is the very essence of what we call safety or security, an essence that can be found, like a sine qua non *condition, in the appropriate functioning of all systems and processes as well as of the whole universe"*[3].

The qualitative security, as a cyber-process, has the above-mentioned goal (of stability), a specific technological support and an appropriate legislation based on some norms, methodologies, strategies, security technologies, actions, processes and law enforcement institutions that provide protection, safety, surveillance and trust services and safe conditions for viability (including reliability and maintenance) and availability of systems/organizations and people.

Concomitantly, the security process (or of the security systems) consumes huge resources, including the financial ones, but also assures reliability, viability, remodeling/adaptability resources of the processes. On the other hand, security assures, through a kind of „tuning", the amplification of functional stability of the systems/organizations, respectively the guidance/limitation to some reasonable values of actions/processes of re-adaptation/re-organization.[4]

Consequently, in accordance with the first part of the previous definition, security represents, first of all, the quality parameter of a system/organization, that is adaptability and stability, which assures the efficiency and effectiveness of the security processes.

Nowadays research done on theory of security/insecurity combines the scientific ideas of peace, crisis and war analysis/studies with sociology, political science, management, international relations, economics, mathematics, psihology, defence, national and international law. Each of these sciences/disciplines approaches the theory of security/insecurity from its particular theoretical insight from the perspective of various/diverse states in the world.

[3] Eugen Siteanu, *Metasecurity – a concept of intempestive geometry*, Annals series on military sciences, volume 9, issue 1/2017, Academy of Romanian Scientists Publishing House, Bucharest, p. 43.

[4] Siteanu Eugen, Bedros Naianu, Ilie Gheorghe, *Fiabilitatea produselor tehnice*, Editura AISTEDA, Bucureşti, 2000, p. 132.

The way of assuring security may be depicted in a schematic way by the connections established between insecurity drawing actions/acts and the protection of the system/organization and people (Figure no. 1).

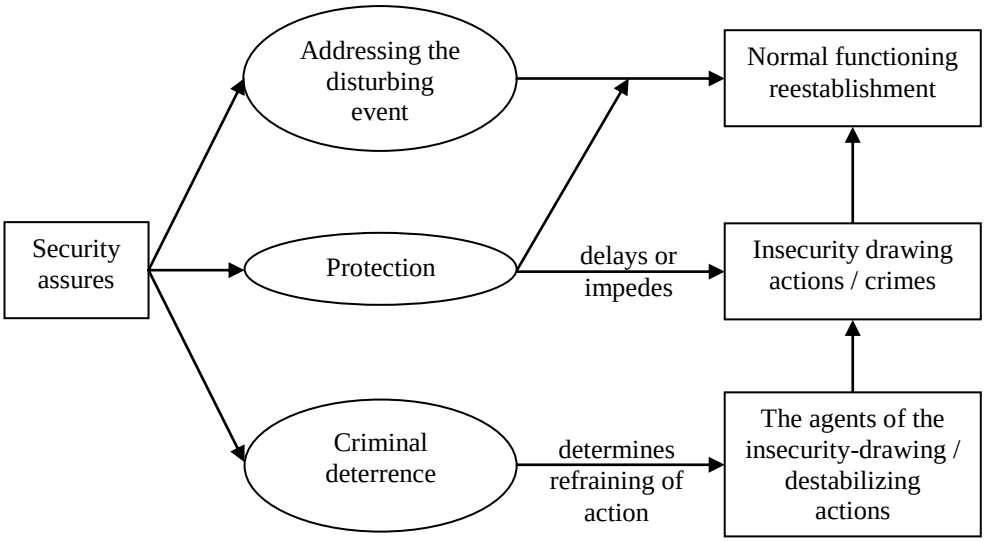

Fig. no. 1. The process of assuring qualitative security

Protection represents the system/organization's capacity of ensuring the prevention or the delay of occurrence of a disturbing/insecurity-drawing event, and at the same time, resuming the functioning/activity after the occurrence of the event that had affected the security. Deterrence refers to the system/organization's capacity of influencing the agents of the insecurity-drawing/destabilizing actions in order to not execute those attacks. Deterrence can be of psychological nature if the security measures are made public/communicated or a factual one (i.e. the effective security mechanisms endowment). Addressing the insecurity-drawing event means to label and ensure some specific conditions of resuming the activity/functionality after the occurrence of the event.

By being a main quality component of the organizations/ systems/processes, security requests efficiency, effectiveness and opportunity as elements that assure those strictly necessary traits to the security concept. The bigger the risks, the lower the security level and

depending on the expenses/costs, the security levels are portrayed as in figure no. 2.

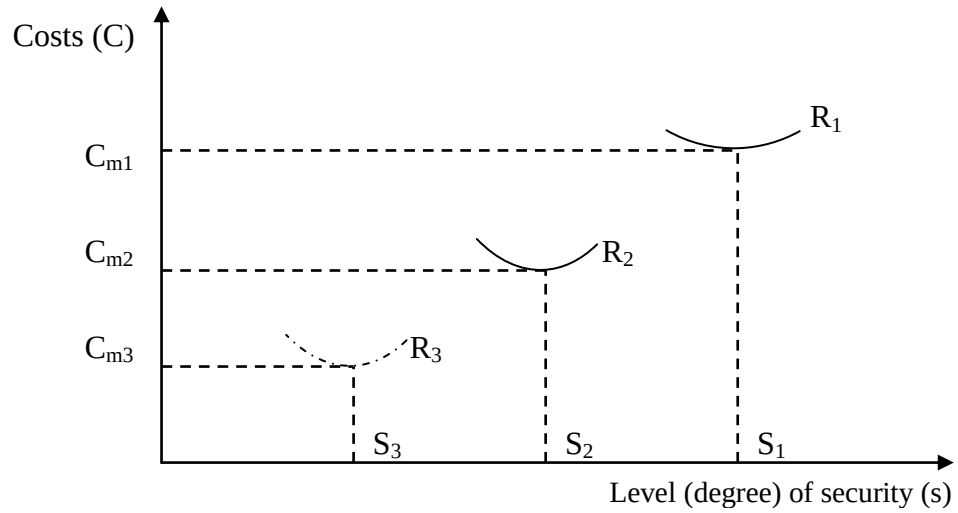

Fig. no. 2. Levels of security depending on the assumed risks and costs

Note:

For risks $R_1<R_2<R_3$, levels of security are $S_1>S_2>S_3$ and C_m=minimal costs.

Security has different dimensions: economic, political, military, social, judicial, scientific, information/cyber, organizational, physical, ecologic, national, regional, international, collective, global etc.

The security of a system (or of an organization) is *„its capacity of preserving its functional characteristics under the action of some destroying factors or some factors able to provoke such mutations which are dangerous for the natural environment or for the health or even life of people who are serving it or are being served (including those living in a so-called risky area) by it or to provoke material, information or moral damage"*[5].

Practice proves that the security measures/plans and mechanisms are perishable (in time, they are lose their efficiency and effectiveness) since

[5] Siteanu Eugen, Bedros Naianu, Ilie Gheorghe, *Fiabilitatea produselor tehnice*, Editura AISTEDA, Bucureşti, 2000, p. 133.

they are facing wearing out and obsolescence (technical/technological and moral) as well as cognitive pressure coming from insecurity-drawing agents. *"On that account, any „frozen" security mechanism is, in fact, compromised; its compromising just being a matter of time, study and money for the adversary".*[6] Security has an integrating character since it has the ability to integrate in its own manifestation both reliability, and vulnerability; as a direct consequence, any large system is safe only if it is concomitantly reliable and viable because the systems are composed/formed by technical and information products/elements and people. This is the reason why the big systems can no longer be analyzed/approached separately, that is from a technical or organizational perspective, but jointly, from both technical and organizational perspectives. Due to its integrating character, security must be approached based on the concept of tolerance to errors (and of concept of error). Error represents an admitted deviation of any system function from its status of normal (stable) function. It is an outcome size/value of the system, being in fact a manifestation of system quality.

All mistakes, flaws, exceptions and crimes are considered errors in the theory of tolerance to errors. *„The theory of errors discovering and measurement is applied in the efficiency, automatic testing and reliability domains".* Tolerance to malfunctions allows the system functioning despite any flaws taking place during its running/operating process since they are addressed in an automatic way. *„In a realistic acceptance, tolerance to errors must be understood as a selective rational behavior of the system in optimal conditions of efficiency, in accordance with a functional, relational and informational risk strategy, consciously assumed".*[7]

UTI GROUP has developed the concept of overall/fully security which *„confers security the ability of conceptual comprising of all judicial, scientific, organizational, procedural, informational, physical and personnel-related aspects, in superior quality environments. To do this, there is a need of opportune, viable, adaptive and perfectible mechanisms, able to handle a large spectrum of attacks, attempts and accidents addressed in a predictable way, during their occurrence or after their*

[6] Ibidem, p. 137.
[7] Ibidem, p. 153.

ending, consciously taking a rational operational risk, in the margins of some bearable necessary costs"[8].

For analyzing security, security itself can be approached from different perspectives: political, military, economic & financial, social, cultural, philosophical, environmental/ecological, demographic etc. In the specialized publications in the field, these are called security dimensions or security components.[9]

Moreover, from a geopolitical point of view, security can be analyzed on few levels: the national, the regional/zonal and the global/international ones.

The word security has a Latin etymology and used to be known as „securitas/securitatis" which had meant normality or lack of worries. In dictionaries, the meaning of security is *„being protected against any danger; the safety feeling perceived by somebody in the absence of any danger; safety"*[10]. The majority of the contemporary authors of the studies/papers concerning security domain do believe that security, or the security concept, must be approached from a multi-domain perspective.

However, the definitions of security are different for each country and there are no chances to predict that in this century a unanimously accepted definition is going to be developed. Canada (National Defense College) appreciates that *„National security is translated into maintaining an acceptable way of life for your own people which is compatible with the legitimate needs and aspirations of the others. It includes the lack of armed assaults and attacks, the lack of coercion, the lack of domestic subversion, and the lack of erosion of political, economic and social fields, which are essential for life quality"*[11].

The state of security, in other authors' opinion[12], is *„on the one hand, the balance established between the internal or external risks, dangers,*

[8] Ilie Gheorghe, *op. cit.*, p. 13.
[9] Eugen Bădălan, Vasile Bogdan, *Organizaţii şi structuri de securitate*, Editura CTEA, Bucureşti, 2016, pp. 32, 36.
[10] *Mic dicţionar enciclopedic*, Ediţia a II-a, Editura ştiinţifică şi enciclopedică, Bucureşti, 1978, p. 874.
[11] Eugen Bădălan, Vasile Bogdan, *op. cit.*, pp. 25-29.
[12] Ibidem, p. 30.

threats and aggressions against a state and, on the other hand, the capacity to counteract them".

The risks, dangers, threats, aggressions and vulnerabilities represent factors of destabilization, and among their countering measures there are: policies, strategies, plans, procedures, measures and actions.

Crisis is a concept expressed through a diversity of definitions. For example: *„the violent manifestation of (economic, political, social, military etc.) contradictions."*[13], or: *„phase from the evolution of a society marked by big (economic, political, social etc.) difficulties; period of tension, of disorder, of trials (often decisive) which are manifested in society"*[14]. Crisis is *„the direct follow-up of an imbalance, disorder materialized in the security status, conceived as normality"*[15].

Crises can have diverse typologies (categories) such as the economic, financial, ecological, food-based, moral, politico-military etc. ones and are manifested under diverse forms: violence, conflict of low, medium or big intensity, terrorism, war, revolution and other forms of conflict (nuclear war, border-related war, civil war, terrorist/anti-terrorist war, actions under UN, OSCE, NATO mandate). By analyzing the evolution of crises, it can be learned that it is disputes that emerge at the beginning (as disharmony/animosity or disagreements noticed in the relationships between different state or non-state actors), disputes that can afterwards escalate into crises and afterwards into wars (armed conflicts).

The stages of a crisis are as follows: pre-crisis, escalation, de-escalation and impact or: the dispute, pre-crisis, escalation, war, truce, peace negotiations and agreement.

„Behind these crises there are the interests of the great finances, and their extraordinary capacity of producing situations that generate crises and conflicts. The interests are some manifestations of the appetite for power, considered as being the capacity of imposing to the enemy your own will or a specific way of conduct"[16].

---

[13] *Mic dicţionar enciclopedic*, Ediţia a II-a, Editura ştiinţifică şi enciclopedică, Bucureşti, 1978, p. 253.

[14] Academia Română, *DEX - Dicţionarul Explicativ al Limbii Române*, Editura Univers Enciclopedic, Bucureşti, 2009, p. 251.

[15] Eugen Bădălan, Vasile Bogdan, *op. cit.*, p. 43.

[16] Ibidem, p. 73.

Even though in the past mankind faced crises which had escalated to violence, wars (including civil wars), revolutions, low intensity conflicts, terrorism and world war, nowadays, in this century, the manifesting forms of crises have been diversified, as follows: nuclear war, border-issue-related war, niche war, military action triggered by a UN, OSCE, EU, NATO mandate and anti-terrorist war.

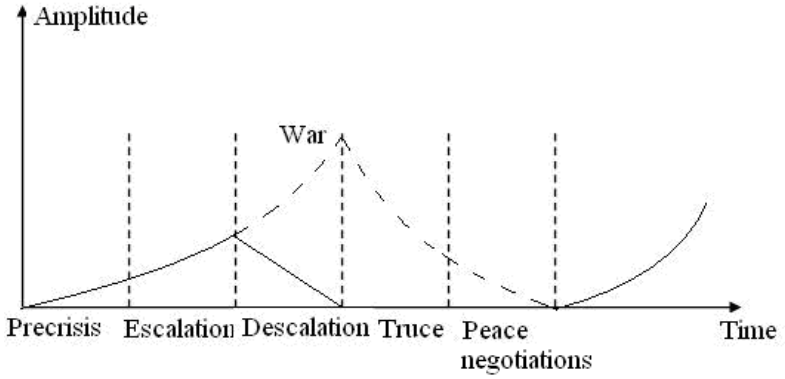

Fig. no. 3. The stages of a crisis/war

Security has three subsystems in its structure[17]: 1) preservation/remodeling (Cv), through avoidance, diminishing or remodeling; 2) functional re-adaptation (fRa) and 3) safe functioning (Si), according to figure no. 4:

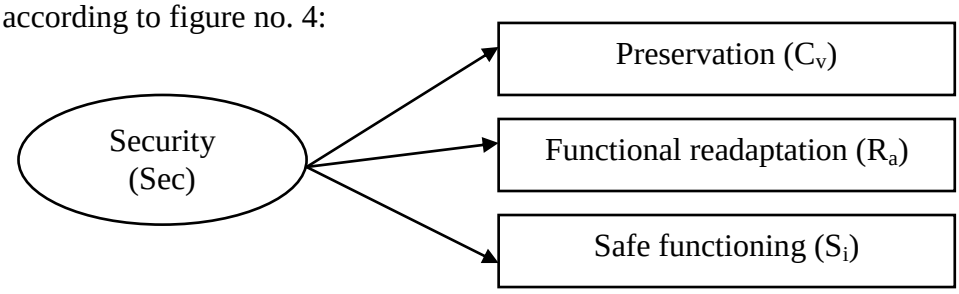

Fig. no. 4. The components of the security system

[17] Ilie Gheorghe, *op. cit.*, p. 23.

By having these three components, security (Sec.) can be mathematically expressed as follows[18]:

$$Sec = Cv + Ra + Si$$

Hence, the security quality of a system/organization or the guarantee of its safe functioning depends on: the level of safe functioning, the possibility of preserving/remodeling the functioning parameters and the capacity of functional re-adaptation of the system/organization (of not becoming dangerous by functioning or consequences). These impose a high reliability and an appropriate viability, as well as facilitating the transparency or diminishing the negative influences of the destroying/destabilizing agents, but also remodeling or functional blockage in case of any imminent threats/dangers. *„In a similar way to reliability and viability, security depends on costs and by this it can be given an optimal value, but the criterion is no longer a simple one, since it represents a correlation, a relation between cost and risk"*[19].

By adopting these letters for identification: p – likelihood of producing the crime which destabilizes the system, Cp – the cost of security system, and W – system wastes following the system destabilization, the parameters of security system can be calculated by using Bayes Theorem *„by reverse unfolding of the events probability tree, in case the value of probability of accomplishing the security function (or of the transfer function of security) can be calculated"* and the following formula can be obtained:

$$\frac{d(Cp^*)}{dp} = w$$, where p* is the optimal value.[20]

Overall/full security of systems is based on *„the paradigm of casual determinism (cause is first, effect is afterwards) and, therefore, proposes the system assessment by error, as a quality manifestation at their output, in close correlation with a level of risk, a determined causality and an adjusting strategy, within the margins of some affordable costs"*[21].

[18] Ibidem, p. 23.
[19] Ibidem, p. 22.
[20] Ibidem, pp. 24-25.
[21] Ibidem, p. 29; see also Eugen SITEANU, Bedros Naianu, Gheorghe Ilie, *op. cit.*, p. 141.

Taking into consideration the above-mentioned elements and the fact that for any system or organization, *„functionality cannot be detached from its main characteristics, the security manifestation, and also from the integrating character associated to security, the association of quality-security becomes an objective one. Consequently, we emphasize the association of the quality categories – security levels or operational risk, which determines a more profound analysis even in this domain. Starting from the association of quality-security, Ilie Gheorghe determined the cyber-model of the optimal security, overall/full security, taking into consideration its structure and the flow of transforming flaws into exceptions and crimes into errors.*"[22] It is crystal clear that the subject of security, national and international security, is/are of great importance for our country, and for the European states. This is why the member states of European Union are fundamentally interested in developing with all states in the world good and stable relations of cooperation and friendship.

"It is true that under the current circumstances no state of the world may assure its security on its own, through isolation, neutrality, lack of interference in some other states' affairs etc., because the level of global insecurity has reached such a high level, that even the great nuclear powers can no longer be certain of their security, no matter how many means they might have or how strong they may be. The asymmetric means, the great finances, the trans-national groups, corporations, and all the other kinds of structures and networks have become so numerous, so powerful and sophisticated, that they may cause huge surprises at both tactical and strategic levels. The terrorist attacks on September 11, 2001 and the following ones are the first such instances, but the financial crisis that burst out in 2008-2009, the surprising re-opening of the strategic ridge Black Sea – Baltic Sea, the war in Syria and especially the emergence and impetuous, aggressive, and extremely rapid development of the Islamic State are powerful arguments of a type of global endogenous insecurity which may culminate with a devastating confrontation to everything mankind has created so far. The huge proportions, the dynamism and the network, the new technology and the capacity of the media to produce cognitive and information insecurity with a speed so far unknown are only a few of the pro

[22] Ibidem, p. 29.

„meta" arguments, both in the security and especially in the insecurity domains, even if the two domains are actually just one, situated on one side and the other of X and Y axes (0x and 0y)."[23]

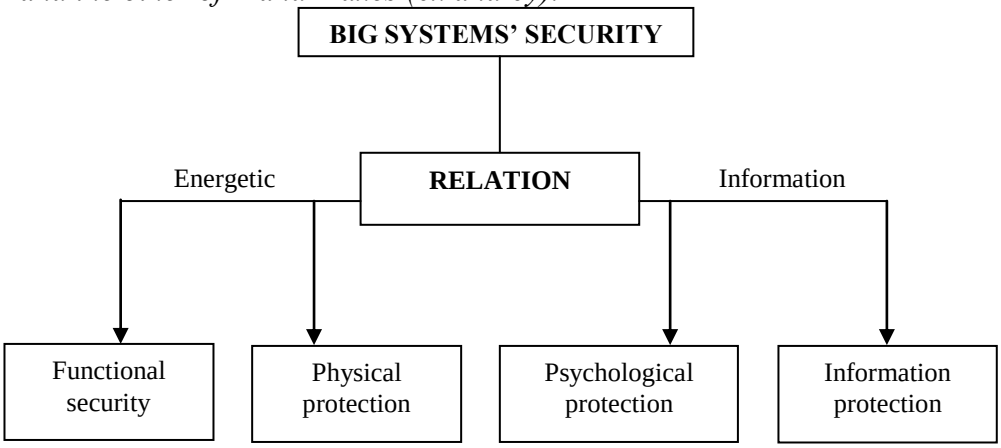

Fig. no. 5. Large systems' security components related to energetic-information ratio

Directly correlated with the energetic-information ratio, large systems' security has four components: 1) safe functioning (requiring confidentiality of actions, safe functioning of technical means and systems, and also the capacity to resist to the actions of the aggressive agents by adapting and remodeling its own systems); 2) physical protection (protection against criminals and emergency systems); 3) psychological protection and 4) information protection (fig. no. 5). Even though security components are divided in two categories (the energetic and the information ones), their interfusion is quasi-total (strong) and hard to dissociate/separate[24]. Approaching them separately is performed only for analytical goals (of studying), but in fact, they cannot be separated for real.

Security imposes to all large systems a hierarchical structure (organization), *„a distribution of possibilities of parametric remodeling, predicted causal connections (mistakes, exceptions, crimes, errors) and*

[23] Eugen Siteanu, *op. cit.*, p. 43.
[24] Eugen Siteanu, Bedros Naianu, Gheorghe Ilie, *op. cit.*, pp. 134-135.

tolerance or tuning, by assuming the role of moderator, amplification tool, catalyst or limiting tool"[25].

To conclude we may state that *„Therefore, security is at the same time an internal function of the system and process, in the sense that every system and process has an immunity mechanism and a feed-back operational characteristic which is simultaneously a manner of defense and adaptation in relation to the environment. The two dimensions of security – endogenous and exogenous – are directly connected to the dynamics of systems and processes and to that of the environment and change in time, according to the necessities and conditions imposed by the life of the system and the process and the external conditionings. Obviously, not all developments and transformations can qualify as „meta", but some of them do impose a new condition and thus a new configuration of security that may mean a plus of security, a minus of security or even insecurity. For instance, the mechanical adherence of Romanian agriculture to a communitarian transformational trend has actually led not to some food metasecurity as it would have been expected and as it was really expected by all of us after Romania joined the European Union, but to a food metainsecurity, having extremely serious effects on people's health and living."*[26]

Conclusions

Keeping in mind the normal association of quality-security, the cyber model of security optimization has been conceived, by considering its structure and flow of transforming the flaws into exceptions and crimes into errors. The cyber model requests tuning cycles and elements of high efficacy. The security system has the following inputs: its destination, the assumed level of risk and costs, and also the following output: the quality (the level of quality). The solutions/measures that have to be taken in order to counter the threats to the safety of the European system should be put into practice by a qualitative security, by a collective effort of all European states, by strengthening European and transatlantic solidarity as well as by good governance.

[25] Ibidem, p. 137.
[26] Eugen Siteanu, op. cit., pp. 46-47.

BIBLIOGRAPHY

*** *Mic dicţionar enciclopedic*, Ediţia a II-a, Editura ştiinţifică şi enciclopedică, Bucureşti, 1978;

ACADEMIA ROMÂNĂ, *DEX - Dicţionarul Explicativ al Limbii Române*, Editura Univers Enciclopedic, Bucureşti, 2009;

BĂDĂLAN E., BOGDAN V., *Organizaţii şi structuri de securitate*, Editura CTEA, Bucureşti, 2016;

ILIE G., *Risc şi securitate – articole, comunicări şi prelegeri* – vol I, Editura UTI Press, Bucureşti, 2015;

ILIE G., URDĂREANU T., *Securitatea deplină*, Editura UTI, Bucureşti, 2001;

SITEANU E., BEDROS N., ILIE G., *Fiabilitatea produselor tehnice*, Editura AISTEDA, Bucureşti, 2000;

SITEANU E., *Metasecurity – a concept of intempestive geometry*, Annals series on military sciences, volume 9, Issue 1/2017, Academy of Romanian Scientists Publishing House, Bucharest, 2017.