The Security of the Dynamic Systems

Sergiu Medar
„Lucian Blaga" University, Sibiu
sergiu48@yahoo.com
Adriean Pârlog
National Defence University „Carol I", Bucharest
adrian_parlog@hotmail.com

When the only tool you own is a hammer,
every problem begins to resemble a nail.
"Security is everyone business."
Abraham Maslow

Abstract. *In a world that is characterized by the globalization phenomenon, the current economic decision-making process is marked by a dynamic and objectively amassed complexity. Besides the ability to forecast the production of certain results, the manager must have at disposal scientifically-supported decisional variants in order to estimate the risk of the adopted strategy.*

The estimates rely on the available information, on the capacity to assess it, as well as on the manager's decisional behavior. As to the acknowledgement of the potential perturbations and the consequences of their occurrence, the manager has to analyze various alternatives of action and to choose the alternative that offers the best opportunities, concomitantly with a behavior that inflicts minimum risks.

Keywords: security culture; risk management; critical infrastructure; dynamics systems; competitive counterintelligence.

JEL Code: P51.
REL Code: 7J.

An ample process aimed at making sensitive the micro and macroeconomic decision makers towards the harsh need for the initiation of projects on the development of the concepts associated to the so-called *„security culture"* began in the aftermath of September 11.

In Romania, the main effort directions have been focused on the public promotion of certain topics such as:

- Public diplomacy and intelligence authorities;
- Energy diplomacy;
- Preemptive diplomacy;
- Trans bordering threats and citizen security;
- Bio-terrorist threat prevention and counteracting;
- Promotion of the concept pertaining to the *Protection of the critical infrastructure* at the level of community and local and regional authorities;
- Implementation of the program dubbed *„Terrorism beside us"* within the Romanian education system.

A program for the *Protection of the Critical Infrastructures (EPCIP)* was launched at European level on December 12, 2006, stipulating eleven sectors of interest and thirty-two critical services associated to these sectors:

Serial no.	Sector	Product or service
1	Energy	▪ *Gas and oil production, activities related to refining, chemical treatment and storage, including the pipelines;* ▪ *Electric energy production;* ▪ *Electric energy, gas and oil transportation;* ▪ *Electricity, gas and oil distribution;*
2	Information and communication technologies	▪ *Information systems and networks;* ▪ *Command, automated and device systems;* ▪ *Mobile and fix telecommunication services;* ▪ *Radio communication and navigation services;* ▪ *Satellite communication services;* ▪ *Broadcasting services;*
3	Water supply	▪ *Drinking water supply;* ▪ *Water quality control;* ▪ *Water quantity control and damming;*
4	Food	▪ *Food supply, food security and safety;*
5	Health	▪ *Medical and hospital care;* ▪ *Medication, serums, vaccines, pharmaceutical products;* ▪ *Bio-laboratories and bio-agents;*
6	Finance	▪ *Payment services/connected structures;* ▪ *Governmental financial systems;*
7	Defense, law enforcement and national security	▪ *Defense, law enforcement and national security;* ▪ *Border integrated management;*
8	Administration	▪ *Government;* ▪ *Armed forces;* ▪ *Services and administration;* ▪ *Emergency services;*
9	Transportation	▪ *Road transportation;* ▪ *Railroad transportation;* ▪ *Naval, fluvial, maritime and oceanic transportation;* ▪ *Air transportation;*
10	Chemical and nuclear industry	▪ *Production, processing and storage of the chemical and nuclear substances;* ▪ *Pipelines for perilous chemical products/substances;*
11	Space	▪ *Air traffic.*

If the issue concerning the protection of the critical continental infrastructure is so keenly made obvious at the level of the European Union, then who is interested at national level in the issue concerning the security of the large local and regional companies as part of the national infrastructure?

Romanian specialists from various ministries, state and private operators, as well as academicians and researchers and representatives of the civil society and of the media constantly participate in various European specialized structures, conferences, roundtables, workshops, scientific research projects in the field of security and have the opportunity to make remarkable and prized contribution to this field, to exchange expertise and information, conclusions, risk assessments, documentary papers, lessons learned and measures intended for the protection and recovery of the affected systems.

In a world that is so intensely characterized by the globalization phenomenon, the current economic decision-making process is marked by a dynamic and objectively amassed complexity. This complexity is the result of a strong combination of the material, human, energy, financial and information inflows.

The economic agents must assess the risk they assume by adopting some decisions out of a finite pool of possible decisions. The instability of the market, the limited possibility to find out the future actions of the competitors, the degree of political stability in the economic area, inflation, state currency policy, economic laws, etc., are only a few elements that influence the overall business risk.

Besides the ability to forecast the production of certain results, the manager must have at disposal scientifically-supported decisional variants in order to estimate the risk of the adopted strategy. The estimates rely on the available information, on the capacity to assess it, as well as on the manager's decisional behavior.

As to the acknowledgement of the potential perturbations and the consequences of their occurrence, the manager has to analyze various alternatives of action and to choose the alternative that offers the best opportunities, concomitantly with a behavior that inflicts minimum risks.

In most cases, the scientific study on a system or phenomenon may be conducted through real or artificial experimentation. In the economic field, the real experimentation is rarely because it requires great expenses and risks. The artificial experimentation, although sometimes it implies a significant intellectual and financial effort, allows the avoidance of some real situations that occasionally have catastrophic implications.

The analysis of the complex economic systems may be performed using the methods and procedures of the analytical dealing with the econometric patterns.

In such cases, fields like the *theory of systems, the theory of decision, the operational research, economic cybernetics*, etc. make use of the appropriate mathematical methods.

Given the complexity of the real economic systems, the stochastic reliance among different variables and considered parameters, not all systems might be represented properly through a pattern that can be managed by the use of the analytical

methods and that can encompass all issues of analysis/managerial decision for a real economic horizon. Most of the times, in such cases, the simulation method is seen as the viable and available alternative.

The approach of the economic systems as some self-adjusted complex systems underlines the existence of some feedback mechanisms having the shape of chains (cycles) of causal dependence among the fundamental variables. Extremely important variables, such as income/output are influenced by more feedback like mechanisms and their end-state level that is achieved at a specific moment is the result of the overlap and intermingling of the effects induced by these feedback mechanisms that are active within the economic system.

The occurrence and action of such adjustment and self-adjustment mechanisms that have been noticed long ago within the cybernetic approaches on the economic systems and on the biological, ecological and social systems is considered nowadays as being characteristic to the complex dynamic systems, irrespective of their nature. It is acknowledged that an economic system that is perceived as an evolving dynamic system naturally creates for itself the adjustment and self-adjustment mechanisms that are used subsequently to ensure stability and growth. No economic system can survive without these mechanisms that are able to offer it a certain position and control in the relation with other economic systems or other systems of the environment.

As to the current approach, we will focus on the issue of the security of the complex dynamic corporation-like systems that can be targeted by the pressure posed by various types of risks. In this context we start out with the idea that the approach on the foundation of a systemic concept regarding the business environment should take into account it multidimensional character but it ought not to be reduced to this value. We become aware of the development of a new type of economy based on intelligence, and this triggers a new dimension in the level and status of competition among companies that is usually adjusted to the complexity of changes in the economy and society.

It is difficult to define the security concept because of the fact that it represents a multidimensional class that can be tackled from multiple perspectives.

Theoretically, a *dynamic system* stands for the mathematic translation of an established „rule" describing the reliance on time of a position of a point in a multidimensional space such as the description of the performance of an economic agent, the patterns that describe the movement of a pendulum clock, the flow of a liquid in a pipeline, the number of fish in a lake each spring etc.

Types of systems

In most cases, through the security of a complex dynamic system from the perspective of the above-mentioned things we understand a state of balance that is necessary to ensure the permanence of the activity for which the system was designed, simultaneously with the process of making minimum the risk of the business and maximum the current and future

opportunities of the business. The security of the complex dynamic system (corporation) may be achieved through the framing, designing and implementing of an appropriate set of security measures that can be policies, processes, procedures, organizational structures and functions related to the insurance of the integrity of the personnel structure, of the patrimony, of the financial and information aspects.

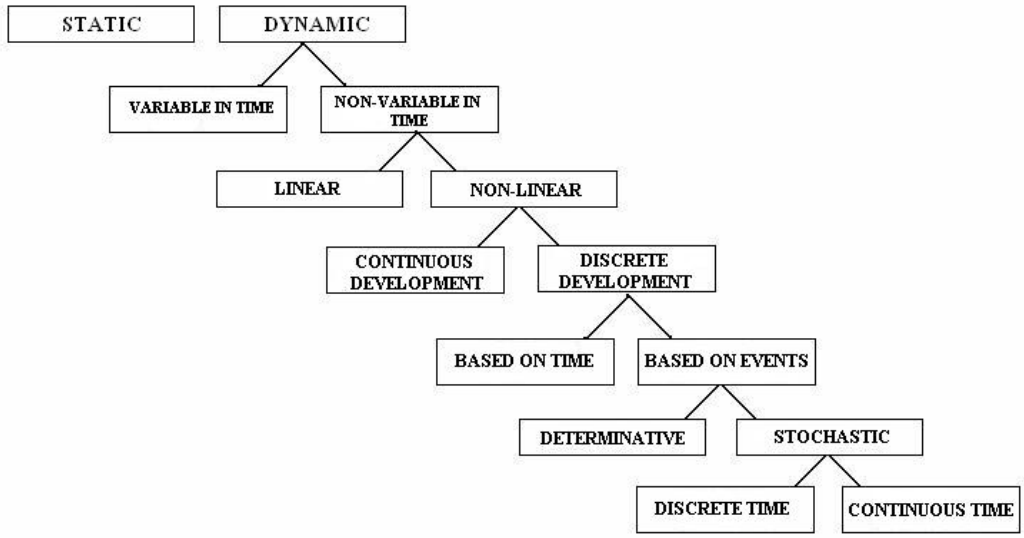

Figure 1. *Types of systems*

From the perspective of a manager, they may be oriented towards the „inside" of his own organization and represent efforts to identify and define his own weaknesses related to personnel, foreign persons, as well as to integrity of the material, financial and intelligence patrimony.

Additional to this approach, the manager must attach an equal importance to the „threats" that originate from within his organization. These threats are emphasized by the existence of a competition environment that becomes aggressive to a greater extent and it is not characterized by positive sum game all the time, but rather by null one.

The main concepts conveyed within the theoretical approaches in the domain of security of the complex dynamic systems are *vulnerability*, *attractiveness*, *threat* (potential threat) and *risk* that are to be described in the following paragraphs.

Vulnerability. The vulnerabilities of an economic system are in fact *weaknesses* that may be used by an adversary as *opportunities* that might be exploited in order to gain current or future advantage within the competition. The vulnerabilities may be triggered by practical weaknesses of the current activities, including those related to the management, human and material security or procedures of operational security.

Regularly, the vulnerabilities are analyzed and assessed by simultaneous examination of the threat and likelihood for an objective to become a target, as well as by examination of certain sequences of specific developments (an approach based on scenarios).

Attractiveness. The attractiveness of an economic system (target) is a complex estimation on the way this is perceived by a competitor or a specified adversary. The threat (potential threat) can be described as an indication, circumstance or event having a potential that can trigger losses or human, material, financial and information damages inflicted to a target. It can also be described as the intent or potential capability of a competitor to develop actions to the detriment of some goals related to his own interest.

The threat sources may be:

- Competitor companies;
- Activists with various leanings or pressure groups;
- Frustrated or dissatisfied employees or contractors;
- Members of some criminal groups (hacker, smugglers, participants in the organized crime activities);
- Terrorists or terrorist organizations.

The information on a threat (potential threat) is a reference that allows the analyst to understand the enemies who are interested in the targets, the history of the modus operandi, methods and assets, potential plans and what drives them to act, etc. This kind of information might be used to forecast the consequences inflicted by possible materialization of the threat or threats.

The adversaries can be divided into three large categories of threats:

- Internal;
- External;
- Internal with external connections.

Risk. The risk, as an abstract concept, is described through the negative consequences of the occurrence of an undesired event. It can be represented by a *numerical value* (the likelihood of the occurrence of an undesired event, of the hazard) and it can be counteracted through a scientific assessment aimed at preventing events or alleviating their consequences.

The undertaken risk is minim when the agreed alternative (which is well chosen and drawn up) is close to the most advantageous one, following the formula:

$$R(Si) = \max [U^*(S) - ui]$$

with:

$i = 1,2,...,n$, n is the number of situations;

U^* - optimum value of the used function of the system;

ui – current value of the used function.

The risk management is still a concern of the modern world. It appeared just at the beginning of the human groups and it was obvious under various preservation or confrontation shapes; it was developed gradually until it reached complex ways to mend itself, to preempt various types of threats or to adjust its vulnerabilities. A long and difficult road was crossed from *„it is better to have a little bit of luck than an appropriate treatment"* to *„reason instead of panic"* and *„aware action"*. Otherwise, a huge increase was performed from taking the hazard to identifying, assessing and controlling the risk concerning the occurrence of certain undesired events.

It is estimated that the security risk depends on the consequences of an attack against the economic-social system and on the happening likelihood of a threat. The latter depends on the attractiveness of the target to the adversary, on the type of threat used by the potential competitor, on the vulnerability degree of the system, as well as on the measures used to counteract the risk.

A risk is considered as being high if it is also characterized by an increased level of likely successful attack against a target entity that is of paramount importance for the system. This likelihood may rely on other factors such as: attractiveness to the adversary, level of threat, vulnerability, etc.

If the likelihood of performing a successful attack against a critical target is high, the risk is considered high and appropriate measures will be established to protect a critical target exposed to a high risk.

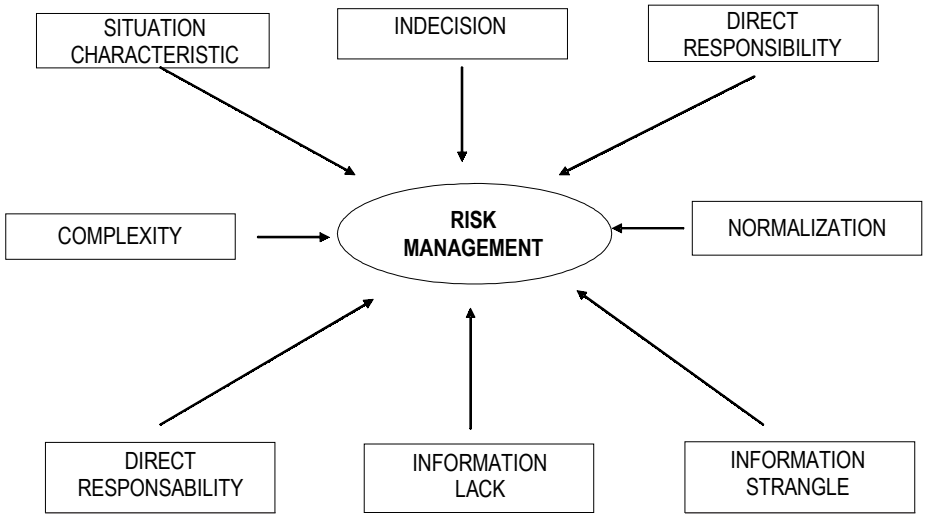

Figure 2. *Factors that influence the risk management*

The severity of the consequences in the aftermath of a security event against a target is usually measured in the number of victims, material, financial and information damages or losses that may be inflicted by a successful attack.

The deliberate human actions (following a plan) may generate serious effects that can be comparable with those generated by accidents, including by large earthquakes or deluges that may result in:

- Human victims;
- Damages or negative consequences over the environment;
- Direct or indirect financial losses of some economic agents;
- Disturbance concerning the well functioning of the national, regional economies and of some economic operations;
- Loss in the reputation of some companies;
- Need to evacuate the population that lives or works nearby the facilities with increased terrorist risk;
- Excessive publicity for certain subjects with high emotional impact in the media and within the population.

The critical infrastructure elements may pose dependences and interdependences that should be considered carefully. Wherever is needed, the stealing of dangerous materials must be included in the category of striking security events.

In general, the theoretic category called consequences is one of the key factors for

the determination of the critical importance level of the target and for the required security countermeasure level. During the stage related to the characterization of the target, the consequences are used to identify the special social value objectives. For instance, the terrorist structures do not seem interested in the targets that generate insignificant consequences (those that do not correspond to their criteria of valuable impact).

Targets' attractiveness

Not all targets have the same value for the competitor organizations. The attractiveness of an organization (target) is given by an assessment on the real or perceived value of a competitor (adversary).

The attractiveness factors of a target (competitor) can be measured taking into consideration the following aspects:

- Type of the triggered effect;
- Maximum number of victims;
- Maximum damages inflicted to the target;
- Maximum damages in the area;
- Major damages to the national infrastructure;
- Potential of the utilized materials to produce collateral damages;
- Distance until the target belonging to the national infrastructure;
- Difficulties in carrying out the attack, including the possibility for access and the level of security measures;
- Company's name or to what extent its reputation is damaged.

The attractiveness level of a target that is intended to be protected from the perspective of its security represents a significant target for the team that analyzes the status of the pondered dynamic system.

During the evaluation process, the attractiveness of a target can be assessed starting with the opponent's intentions or with the estimate on the interest as far as the target is concerned.

Security strategies can be developed taking into account possible threats and possible targets. The attractiveness along with the consequences is regularly used to assess targets in the context of the analysis on more specific scenarios.

A first step of the effort aimed at ensuring the security of a complex dynamic system (corporation) is the recognition and analysis of the threats and vulnerabilities and the result is a *state analysis* (SA) study. SA in itself is a dynamic and systematic estimate on the "success" probability of a "threat" to a dynamic system.

The process takes into consideration the possible "severity" of the impact on the corporation, on the human communities nearby critical systems (hydro dams, nuclear stations, water and power supplying systems, etc.).

Certain rational steps must be followed, no matter what methodology is used:

- General characterization of the dynamic system (industrial) with the purpose to be aware of the human values, the fix assets, the informational and material goods (values) that must be provided, their importance, connections, and influence within the infrastructure of the system;
- Recognition and characterization of threats to these goods and their assessment taking into consideration their attractiveness

as targets, as well as the impact on their destruction or break-in;

- Identification of possible vulnerabilities to security that might threat equipment and machines or their integrity;
- Determination of the risk posed by certain events, by identifying the likelihood for the occurrence of an incident and its consequences;
- The incident's level of risk and in the case the level of risk is high to offer recommendations for its decrease;
- Identification and assessment on the option intended for the decrease in risk (decrease of gross risk and cost-advantages analysis) and reassessment on the risk following the implementation of the appropriate countermeasures.

The basic idea of our approach relies on the fact that we agree that all risks on a system security cannot be efficiently monitored and prevented.

Generally, the goals pursued with the purpose to ensure security are related to the cascade use of four basic strategies to minimize the risk:

- Deterrence;
- Identification – detection;
- Annihilation – delay;
- Counter-response – counter-action.

The appropriate strategies in managing security can be various depending on the concrete circumstances of each goal and taking into consideration the type of the target and the threats.

To create *an effective security system* the following stages are necessary: risk assessment, definition on the security policy, implementation, management and audit.

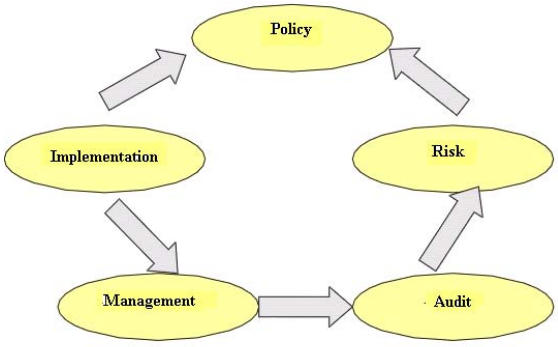

Figure 3. *Integrated system necessary to ensure the security of an organization*

An integrated system meant to ensure the security of a corporation (complex organizations) consisted of specialized subsystems directed towards:

- Physical security (considers the protected area, the building systems and safety rooms);
- Personnel security (considers the personnel vetting, security tests, appointment approval and any kind of access authorization);
- Papers security (hard and electronic format);
- Industrial security (considers mainly the technological and commercial data);
- Information security (INFOSEC);
- Communication security (COMSEC);
- Cryptographic security;
- Transmission security (TEMPEST).

The suggested approach does not offer the solution to the security measures that must be taken, but as an alternative it provides all means to identify, analyze, and lower vulnerabilities. The specific situations must be assessed independently through a local management system based on the best reason and applicable procedure system. Appropriate management decisions on the risk to a system security must be made according to the risks.

The flexible approach emphasizes the fact that there is no standardized approach of the security concept in the social life and resources are not always well used to immediately reduce high risk situations. On the other hand, all managers in this field are encouraged to cooperate with national intelligence, security, and guard agencies and with local emergency services on integrated and systemic basis, including by getting information, training and resources to stop some detrimental actions or by emergency situation management.

A sensitive issue in this field, that is also extremely difficult, is related to the costs to ensure security of an organization. Without having enough statistic data, inspired only by specialized literature, we are able to formulate some estimates on the efficiency – costs dependency in the security field.

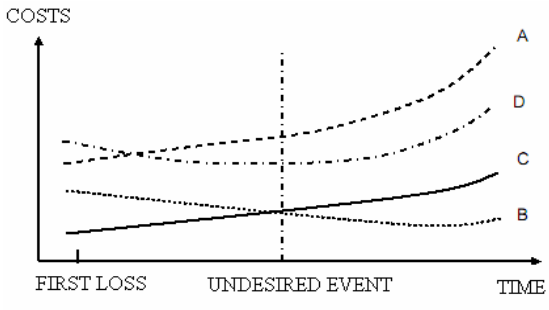

Figure 4. *Costs in the security field*

In Figure 4 we can notice the costs triggered by the undesired event that happened (A curve) that are lower previous to the event and they increase significantly after the event; costs for risk management implementation (B curve) are higher during the first implementation stage (investment costs) and almost constant after the implementation (function and maintenance costs) and costs caused by the undesired event when the risk management is implemented (C curve), which are not increasing too much after the event (increase is controlled by the management effectiveness).

Although the curves in Figure 4 are qualitative, we can notice that costs for the damage compensation are higher than those for risk management function and implementation (D curve) if a risk management does not exist.

The first benefit of the risk management is the opportunity rise added by the general management close to the moment of the undesired event for both the mitigation and elimination of human errors and prevention of system's malfunctions.

Corporate security management

Currently, given the fact that the global crisis has become a controversial subject, governmental structures and private ones are looking for solutions to get out from the dark spot with minimal losses, and some private companies can afford to even think about profits.

For private companies, the solution for leaving the crisis behind depends on the increase in the company's effectiveness, on maintaining, as much as possible, the present markets, on identifying new outlets, new financial sources, new ways to approach the outlets, on finding some methods to outrun the competitors in the targeted markets, on identifying some ways to entice potential clients, taking into account their demands, on educating customers according to the policy of the private companies, etc.

One of the most efficient ways used by the companies aware of this process is comprised by the concept called *Companies*

security management also known as *Business Intelligence*.

Currently, many private institutions, companies or specialists, more or less experienced, talk about *competitive intelligence*, *business intelligence* etc.

The truth is that two notorious dictionaries comprising terms in the intelligence field do not define business intelligence or competitive intelligence, even if they prove their real competence in defining other sensitive terms in this field.

National or foreign authors writing books in this field cannot reach an identical approach on the phenomenon and the more you read in this field the more confused you are on such terms.

Most people who have been concerned or are concerned with this field are more or less experienced in the field of national security and, unfortunately, just a few are experienced in the field of operational intelligence. Maybe, this is the reason why the definition of the basic terms is so confusing. Besides, during the talks held with some authors, they recognized years later after they had written the books that they has made confusions.

Based on the experience earned in the intelligence field at the level of national security and also on the talks, sometimes contradictory, held with various authors, we have tried to define the terms with the purpose to identify the ways and means that can help us to reach the end state – increase the company's effectiveness. The general concept can be identified as: *Companies security management – business intelligence*, which consists of two basic fields: *competitive intelligence* and *company's protection.*

Competitive intelligence

Competitive intelligence consists of all activities related to information planning, collection, processing, analysis and dissemination with the purpose to support the company's leadership to make a decision.

Simultaneously, the intelligence process also allows the identification of the ways to make the decisions in a company and to check, in the end or in the middle of the process, the effectiveness of the decisions.

Competitive intelligence comprises:

A. Competitive intelligence in one's company aims at getting information from inside one's company in order to increase its effectiveness. This means, first of all, to assess the company's current functioning level both as organizational structure and personnel. Analysis on the organizational structure means to find out responsibilities and the specific activity of each department or section of the company, their relations, the intelligence cycle, the hierarchy in the decision making process, each responsible decision level, the training level specific to each position and to what extent the *job description* for each position makes a functional system. Personnel appraisal refers to the real training level specific to each position, to the satisfaction degree of the job, to the way they get involved in the decision making process, to the team spirit, to the loyalty to the company, to the personnel horizontal and vertical relations and also to the way they interact with chiefs and subordinates, to their personal opinion referring to themselves and to their mates, to the necessary training for the activity they must perform, to the identification of potential leaders, etc.

B. Competitor intelligence – to get information on competitors, on competition. This means to get only valuable information intended to have an effect on or influence on the company's interests, not unsupportive information. In general, getting information on competitors is not very expensive but it involves some financial efforts. For this reason, similar to other situations concerning the information collection, it is necessary to get only information that is significant to a specific project or field. In this case, it is essential to get information on the competitor's intentions and opinion regarding that particular company. One of the most often pertinent procedures in the relations among the rival companies is misinformation. Companies with a good intelligence structure can identify misinformation and also get data on the intention that makes the subject of misinformation and, subsequently, they identify weak points or aspects that the rival company tries to avoid or to cover through misinformation.

C. Market intelligence – to get information on the company's possibility to interact with its outlet. This involves data on the current market situation, on its evolution on short and medium term, on market's demands on short and medium term regarding a particular product, on the competitors' presence in the market and the market overload potential, on the finding out of new outlets, on the expenditure needed to promote new products, on the choosing of the best moment to issue a new product for the market, on the need to educate the market with regard to a new product or to a product that is to be issued, on the identification of new clients, on getting information about potential clients (financial potential, intents to purchase new products, the moment when products are to be purchased, client decision process evolution, the possibility to make a partnership with the client, client education on the necessity and performance of a new product, etc).

D. Financial intelligence refers to the capital market financial evolutions in the areas of interest, to payment possibilities, to the optimal currency for possible bank deposits, to the possibility to make financial transactions, etc.

E. Assessment on the risk to new investments in the market means to get information on the political, economic, and financial stability in the areas where the investment is to be made, to assess the security situation in the area, to determine the corruption level in the area that might influence the competition, to determine the creditworthiness of the local companies that might become subcontractors, to determine elements of regional culture that might influence the negotiation process, data on members of the negotiation teams in order to be aware of their endurance negotiation capability, to assess the market possible evolution in that area, etc.

Company's protection (competitive counterintelligence)

Competitive counterintelligence refers to all measures taken to ensure the company's counterintelligence against intelligence collection actions of other interested companies or structures, to measures meant to protect the company against acts that might damage its resources and assets.

Company's protection means:

A. Physical protection of buildings and assets against damaging acts or against bad-intended persons trying to breach rooms without authorization. For this reason, it is necessary an estimation on possible threats to the company, an assessment on the company's vulnerabilities in front of those threats, an assessment of the risks emerging from these threats and after that a plan for the company's physical protection is drawn up;

B. Documents protection means to annihilate any possibility of getting out or copying some sensitive documents concerning the company and its interests. The current technology allows the full protection of these documents through RFI (radio frequency identification) procedure which means to attach a micro-broadcaster of low frequency like a stamp on each document which must be protected;

C. Personnel protection means both to know people before they are employed and to evaluate vulnerabilities of each person as possible source for the rival companies;

D. IT protection: from this point of view everybody knows that only the Intranet, that is physically separated from any other computer system, can guarantee total protection against the unauthorized leak of information from the IT network;

E. Communication system protection refers to the use of the legal means to protect communications against unauthorized interceptions.

Only one specialized department of the large companies, comprising a competitive intelligence division and a protection division (competitive counterintelligence) can apply the above mentioned means and ways to increase the company's economic effectiveness.

This department organization follows, in fact, the intelligence cycle: it takes over the intelligence needs from the company's leadership, it fills in the intelligence needs with data that the business intelligence structure considers necessary; it draws up the information plan necessary for the company, it plans the information collection, collects information, processes information, analyses information and changes it into intelligence; the last stage is intelligence dissemination.

The protection department (competitive counterintelligence) aims at assessing vulnerabilities, analyzing them with the purpose to identify those vulnerabilities that might turn into risks, at acting with the purpose to develop a risk warning system simultaneous with the analysis of risks that might turn into threats. Threats are eliminated by successive protection rings depending on the significance of damages they might cause to the company. Finally, some threats are likely to escalate until they reach the conflict stage. In this case, the protection department must have an intervention plan they should apply in the crisis moment previously to the conflict.

A company can either have its own department of business intelligence or it can cooperate with a company specialized in business intelligence.

Both the competitive intelligence process and the competitive counterintelligence one refer to the exclusive use of information collection through legal means. The main information collections legal means are: open sources and human sources.

The only legal way to collect information by HUMINT is elicitation (blind exploitation). As long as the elicitation does not aim at getting top secret information, then this method is legal. Illegitimacy is beyond this barrier. Elicitation is an extremely efficient method in competitive intelligence but requires a specialized training.

As stated before, as long as these means are the only ones used, in the above mentioned circumstances, business intelligence is a legal activity. The border between legal and illegal is very clear cut, but it is also very thin. For this reason, the personnel working in the specialized departments should be trained paying a great attention to the legal aspects.

In case this information collection process reaches a stage when information relevant for national security is obtained, then it is absolutely necessary for the company to convey them to the national security structures without going on with the investigations on its own.

The economic advantages resulting from the increased effectiveness of the companies that have specialized structures for business intelligence exceed the budget allotted for the expenditures necessary for the development of these compartments. Therefore, I believe that this can be a solution for the large companies to face the crisis and even to increase profit.

References

Laws

Legea nr. 182/2002 privind protecția informațiilor clasificate

Legea nr. 101/2003 privind organizarea și funcționarea ORNISS

Hotărârea de Guvern nr. 585/2002 - Standardele naționale de protecție a informațiilor clasificate

Legea nr. 161 din 19 aprilie 2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției

Legea nr. 506 din 17 noiembrie 2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice

Legea nr. 677 din 21 noiembrie 2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date

Legea nr. 455 din 18 iulie 2001 privind semnătura electronică

Legea nr. 544 din 12 octombrie 2001 privind liberul acces la informațiile de interes public

Hotărârea nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice și metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică

Ordinul Avocatului Poporului nr. 52 din 18 aprilie 2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal

Ordinul Avocatului Poporului nr. 53 din 18 aprilie 2002 privind aprobarea formularelor tipizate ale notificărilor prevăzute de Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date

Ordinul Avocatului Poporului nr. 54 din 18 aprilie 2002 privind stabilirea unor situații în care nu este necesară notificarea prelucrării unor date cu caracter personal care cad sub incidența Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date

Hotărârea nr. 781 din 25 iulie 2002 privind protecția informațiilor secrete de serviciu

Legea nr. 182 din 12 aprilie 2002 privind protecția informațiilor clasificate

ISO/IEC 27000 - *Fundamentals and vocabulary* - 2007

ISO/IEC 27001 - ISMS - *Requirements* (revised BS 7799 Part 2:2005) - 2005

ISO/IEC 27002 - *Code of practice for information security management* (în prezent ISO/IEC 17799:2005) - 2005

ISO/IEC 27003 - *ISMS implementation guidance* (în curs de elaborare) - 2008

ISO/IEC 27004 - *Information security management measurement* (în curs de elaborare) - 2007

ISO/IEC 27005 - *Information security risk management* (prin integrarea ISO/IEC 13335 MICTS Part 2) (în curs de elaborare) - 2008

ISO/IEC 27006 - EA 7/03 - *Accreditation Guidelines*- 2007

ISO/IEC 27007-27010 - *Allocation for future use*

Specialty related papers

*** Convenția Consiliului Europei privind criminalitatea informatică

*** Legea nr. 64 din 24 martie 2004

*** *The Management of Security Assistance, The Defence Institute of Security Assistance Management*, 15th edition, 1995

*** *Methodes de conception et securité*, Systems Securité, vol.4, nr. 1, Paris, 1995

http://www.sans.org/2008menaces/

Aghion, P., Howitt, P. (1998). *Endogenous Growth Theory*, MIT Press, Cambridge MA

Antsaklis, P.J., Lemmon, M., Stiver, J.A. (1996). *Learning to Be Autonomous – Intelligent Supervisory Control*, IEEE Press

Arrow, K.J., „The role of securities in the optimal allocation of risk-bearing", Rev. *Econom. Stud*., 31:91

Arkin, V.I., Evstigneev, I.V. (1987). *Stochastic Models of Control and Economic Dynamics,* Academic Press, London

Arnold, L. (1998). *Random Dynamical Systems*, Springer-Verlag, Berlin

Azariadis, C. (1993). *Intertemporal Macroeconomics*, Blackwell Publishers, Cambridge, MA

Barrow, R.J., Sala-i-Martin, X. (1995). *Economic Growth*, McGraw-Hill, New York

Bergin, J., Lipman, B.L., „Evolution with state-dependent mutations", *Econometrica*, 64/943, 1996

Blaug, M. (1992). *The Methodology of Economics*, Cambridge University Press, Cambridge, 2nd edition

Brock, W.A., Malliaris, A.G. (1989). *Diferential Equations, Stability and Chaos in Dynamic Economics*, North-Holland, Amsterdam

Chiarella, C. (1990). *The Elements of a Nonlinear Theory of Economic Dynamics*, Springer-Verlag, Berlin

Cohen și colab. (1998). *A Preliminary Classification Scheme for Information System Threats, Attacks, and Defenses*

Cooley (editor) (1995). *Frontiers of Business Cycle Research*, Princeton University Press, Princeton NJ

Crauel, H., Gundlach, M. (editors) (1999). *Stochastic Dynamics*, Springer-Verlag, Berlin

Day, R.H., *Complex Economic Dynamics*, MIT Press, Cambridge MA, (Volume I) 1994, (Volume II) 2000

Evstigneev, I.V., Taksar, M.I., „A general framework for arbitrage pricing and hedging theorems in models of financial markets", *Preprint SUNYSB-AMS-00-09*, S.U.N.Y. at Stony Brook, 2000

Flaschel, P., Franke, R., Semmler, W. (1997). *Dynamic Macroeconomics*, MIT Press, Cambridge MA

Hodgson, G.M. (1994). *Economics and Evolution: Bringing Life Back into Economics*, Polity Press, Cambridge MA

Hopenhayn, H.A., Prescott, E.C., „Stochastic monotonicity and stationary distributions for dynamic economies", *Econometrica*, 1992

Kandori, M., Mailath, G.J., Rob, R., „Learning, mutation, and long run equilibria in games", *Econometrica*, 1993

Ilie, Ghe. (2006). *Securitatea mediului de afaceri,* Editura UTI Press, București

Ilie, Ghe., Stoian, I., Ciobanu, V. (1996). *Securitatea informațiilor,* Editura Militară, București

Liteanu, T. (2004). *Securitate și instituții,* Editura ANI, București

Masse, G., Thibault, F. (2001). *Intelligence économique: un guide pour une economie de l'intelligence*, De Boeck Université

Medar, S. (2006). *Informațiile militare în contextul de securitate actual,* Editura CTEA, Buucrești

Medar, S. (2007). *Intelligence pentru comandanți,* Editura CTEA, București

Montrucchio, L., Privileggi, F., „Fractal steady states in stochastic optimal control models", *Ann. Oper. Res*., 1999

Pârlog, A., „O propunere de evaluare a vulnerabilității de securitate a unui sistem social (sistem fizic sau grup uman)", *Studia Securitatis,* an. I, nr.1/ 2007, Sibiu

Pârlog, A. (2007). *Necesitatea transformării continue a sistemelor de securitate, Dinamica intelligence-ului. Provocări, oportunități și priorități,* vol. I, Editura ANI, București

Pârlog, A. (2007). *Ierarhie sau rețea în sistemele de securitate?, Dinamica intelligence-ului. Provocări, oportunități și priorități*, vol. II, Editura ANI, București

Pârlog, A. (2007). *Abordări ierarhice structurate și în rețea ale conceptului de securitate,* inclusă în lucrarea S. Medar, *Capabilități ale serviciilor moderne de informații militare*, Editura CTEA, București

Patriciu, V.V., Ene-Pietrosanu, M., Vaduva, C., Bica, I., Voicu, N. (2004). *Securitatea Comerțului Electronic*, Editura ALL

Patriciu, V.V., Ene-Pietrosanu, M., Bica, I., Priescu, J. (2006). *Semnături Electronice și Securitate Informatică*, Editura ALL

Puu, T. (1997). *Nonlinear Economic Dynamics*, Springer-Verlag, Berlin

Schenk-Hoppfie, K.R., „Economic growth and business cycles: A critical comment on detrending time series", WP 54, *Inst. Empir. Res. in Econom.*, Univ. Zurich, 2000

Stalling, W. (1999). *Cryptography and Network Security*, Prentice Hall

Vasiu, I. (1998). *Criminalitatea informatică*, Editura Nemira, București

West, C. (2001). *Competitive intelligence,* Palgrave, NY

Witt, U., „Evolutionary concepts in economics", *East. Econom. J.*, 1992