Cyberspace and Critical Information Infrastructures

Dan COLESNIUC
Ministry of National Defense
drcamc@gmail.com

Every economy of an advanced nation relies on information systems and interconnected networks, thus in order to ensure the prosperity of a nation, making cyberspace a secure place becomes as crucial as securing society. Cyber security means ensuring the safety of this cyberspace from threats which can take different forms, such as stealing secret information from national companies and government institutions, attacking infrastructure vital for the functioning of the nation or attacking the privacy of the single citizen. The critical information infrastructure (CII) represents the indispensable "nervous system", that allow modern societies to work and live. Besides, without it, there would be no distribution of energy, no services like banking or finance, no air traffic control and so on. But at the same time, in the development process of CII, security was never considered a top priority and for this reason they are subject to a high risk in relation to the organized crime,
Keywords: *Information Systems, Cyberspace, Critical Information Infrastructure, Cyber Security, Risk Management, Strategy*

1 Introduction

In developed countries, information infrastructures are at the same time a fundamental bedrock that makes contemporary societies work as well as a source of vulnerability. The diffusion of telecommunications, the Internet and the penetration of computers and local computer networks in so many facets of life today have changed all that. For this reason, information systems are considered a critical asset, not only for traditional intelligence purposes but also for security issues. Thus, is becoming very important an appraisal of some critical aspects of some critical elements of cyber warfare deals with the risks for Critical Information Structures (CII). While representing an essential groundwork that allow modern societies to work and live, they have been developed without considering security as a top priority. Intelligence gathering has always been a critical and inescapable aspect in international politics and new technologies offer unprecedented tools to monitor governments, economies, defense and security planning that can become targets to external threats.

The U.S. National Institute of Standards and Technology (NIST) defines critical infrastructures as those "system and assets, whether physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters"[1]. Likewise, the European Commission describes critical infrastructures as "physical and information technology facilities, networks, services and assets that, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in EU States"[3].

While there are some differences between the United States and the EU and other advanced countries such as Japan, Australia, Canada, South Korea and others as to what precisely constitutes CII, these differences tend to be more terminological than substantial (see Table 1 for examples).

DOI: 10.12948/issn14531305/17.4.2013.11

Table 1. Critical Infrastructures in the US and the EU approach

United States	European Union
Chemical	See "Production"
Emergency Services	See "Healthcare"
Communications	Communications and Information Technology (e.g. telecommunications, broadcasting systems, software, hardware and networks including the Internet)
Financial Services	Finance (e.g. banking, securities and investment)
Energy	Energy installations and networks (e.g. electrical power, oil and gas production, storage facilities and refineries, transmission and distribution systems)
Information Technology	See "Communications and Information Technology"
Nuclear Reactors, Materials and Waste	Production, storage and transport of dangerous goods (e.g. chemical, biological, radiological and nuclear materials)
Transportation Systems	Transport (e.g. airports, ports, railway, mass transit networks, traffic control systems)
Water and Wastewater Systems	Water (e.g. dams, storage, treatment and networks)

IT and communication systems (IT&C) are essential for the smooth running of most modern activities, so their security should be a major concern for organizations.

In that approach, are considered a number of factors that increased the risk of electronic attack against computer systems [2]:

- difficulties inherent security;
- insufficient awareness and user education systems and attitudes or practices that do not comply with the procedures manual;
- availability of information on the penetration of computer systems without authorization;
- unclear legal regulations and jurisdictional difficulties;
- intensification of the globalization phenomenon.

The most remarkable feature of CII and computer networks in general is that "security" was never a top concern for early software developers and engineers. If it's take a look to the history of the Internet, everybody is aware that its protocol (the TCP/IP) was born "open", with no protection or self-encryption mechanism. Simplicity and speed were a priority, because it was supposed that only a close-knit, think-alike community of scientists would ever find it useful and want to use it. But, when it was the business community's turn to embrace the Internet, those very features were warmly welcomed because they meant more "efficiency" (in terms of time and speed) and lower costs.

2 Critical Information Structures and Electronic Warfare

Emerging security risks include cyber defense, energy security, counter-terrorism, nuclear policy and the fight against proliferation of weapons of mass destruction.

Critical information infrastructures (CII) are mostly developed and built at the "national" level, they are also linked to the infrastructures of other countries, thus the collapse of a portion of one country's CII would have serious impact on the neighbors situation as well.

The opening stage of any future war against even a relatively modern state would imply some form of cyber warfare, or more specifically cyber attacks on its CII, soon

DOI: 10.12948/issn14531305/17.4.2013.11

followed, depending on the circumstances, by physical attacks. Apparently, cyber warfare would thus not be so different from electronic warfare in the past. But in some aspects the former is larger and has incorporated the latter. First, electronic warfare is aimed only at blocking or disrupting the enemy's communication; cyber warfare by targeting its CII, in addition to hampering communications, may also impede the circulation and distribution of currencies, power, gas, water and the functioning of air traffic control and health services. In addition, cyber warfare would have both tactical and strategic effects, depending on the resources employed, it may be possible to disabled communications (and the many services dependent on them) nationwide [6].

The potential destructiveness of cyber warfare is so great that some observers have compared it to air power. Thus, all countries in the NATO and the EU have begun to extensively invest in cyber-defense, since these countries tend to be among the most advanced in the world.

The targets of the sophisticated techniques of intrusion, APT (Advanced Persistent Threat) are the sensitive information and intellectual property from the private and public institutions.

For quite a long time, the management and distribution of services and goods was achieved through "proprietary" channels that hardly ever overlapped and rarely needed similar policies or sets of instructions to function. Above all, maintenance of those systems required that personnel physically checked nodes, controllers and pipes to monitor the performance of the systems themselves.

At some point, it was discovered that it would be much more efficient and hence less expensive to remotely control the nodes and switches. The Internet was already available at virtually no cost, provided that Internet protocols were used (and other such protocols that make computer networks at large work). It was a "merge" that greatly benefited companies and their customers, but "security" was not a top priority.

CII was never easily grasped by businesses and consumers (and only partially so by governments). But IC&T (first and foremost TCP/IP) "consigned" its own structural vulnerabilities.

Also important for CII, can help illustrate the mechanisms, in the case where there is no pressure, either from government or consumers, to make redundancy the rule for CII, then there is no need or benefit to do so. Redundancy is the duplication or triplication of control systems and procedures, so that if one safety-check or data monitor fails or is compromised from the outside, there is another back-up, and perhaps yet another, and the infrastructure will continue to perform smoothly.

Many of the principles of critical infrastructure protection and applied aspects of these are general and are recommended to be taken into account throughout the life of the facilities, systems and processes. The effort that it will make government and relevant business sectors have to be accumulated and should lead to important changes, holistic in the critical infrastructure sectors.

An important role has solution providers, relevant service providers and professional and academic environments, which should provide the necessary specialists, inventions, innovations, development and change.

The government sector has the most responsibilities in this area but more information and knowledge are to the operators level, solution providers (representing business) and academic level.

Once the victim has been positively identified (and administrator's privileges acquired), cyber-warriors in the service of a sovereign government or black-hat hackers working for organized crime may steal all the information, change every security parameter, place back-doors (many of these, so they can go back into the perimeters whenever they want), place a time-bomb set to "explode" at a certain point in the future (thus disabling the computer) and so on [8].

DOI: 10.12948/issn14531305/17.4.2013.11

Cyber threats are characterized by asymmetry, limited possibilities of identifying those who generate such attacks, and the opportunity to use these means by non-state actors.

In general, cyber attacks are dangerous precisely because:

1) It does not require large expenditures, many of the methods used to produce them can be downloaded from the Internet or purchased online at a relatively low price;

2) Their generation does not necessarily imply knowledge and extensive experience, the attackers may have enough skills to be able cause great damage, not as happened in the case of sophisticated cyber attacks like Stuxnet and Flame;

3) Cyber attacks are disproportionate in terms of the effort to generate them and the consequences that may arise. Damage may be more extensive than those expected or those that the attacker had originally intended to produce. 4) Finally, perhaps the most debated aspect of cyber remains the anonymity of who generated them. Taking advantage of the complexity of the Internet and legislation gaps many states, the person behind cyber ensure their so-called "safe haven cyber".

To prevent extending the dangers mentioned above, many countries of the world have shifted policies to the new challenges of cyberspace, adjusting national strategies for cyber security needs and national specificity. Thus, France and Britain have concentrated their efforts on combating and preventing cyber crimes and cyber terrorism, Japan and Finland have highlighted the role of cyberspace in economic development; Lithuania focused on the need to protect personal data in cyberspace, Luxembourg, Estonia and Canada have promoted national strategies by education campaigns and awareness of the dangers of cyberspace and safeguards that any consumer should take [5].

Based on the strategic concept of NATO, defined by the Lisbon Summit in 2010, Romania has come up with proposals and solutions not only in the operational field, but also in areas such as cyber defense, counter-terrorism and energy security.

In terms of partnership, Romania contributes directly to the development of materials cyber defense and is part of a multinational project, on the development of capabilities in cyber defense, including a number of countries such as Canada, Denmark, Great Britain and others. It is about the sensors that notify the various potential attacks or infiltration into systems, but it also means some software that can analyze in real time and be able to generate solutions. And in other areas, such as the fight against terrorism, in Romania is running an Excellence Centre, its initiatives and projects being highly appreciated at the international level and it's very well connected with the section of the fight against terrorism from the euro-atlantic Alliance level.

In terms of cyber security at the supranational level can be rightly considered NATO. In 2007, the "shutting down" of Estonia was achieved by a Distributed Denial of Service attack (DDoS). DDoS are quite common and have been repeated in many instances and circumstances and the most dramatic have been widely reported as "cyber wars". But these events, even when are organized on a grand scale, amount to little more than mischief and nuisances. Some of the tools used by script-kiddies and real cyber-warriors may be the same or very similar: "trojans" are employed by both. But while the former then transform the taken-over computers into "robots" (bots) to saturate (with ad hoc "worms") web servers, the latter, once inside, try hard not to be conspicuous. Cyber-prankers want their exploits to be recognized by the public, while the professionals want their victims to stay in the dark and feel "safe" as long as possible. Indeed, their intention is for nobody to ever know that they were inside the system (even after they have left). They too may use worms and bots, but to reconnoiter networks and servers, until they find the specified target. Stuxnet has been a great example of this type of operation [5].

DOI: 10.12948/issn14531305/17.4.2013.11

Of interest, in particular, in the context of a multidisciplinary treatmen, the seven principles outlined by the British Foreign Office, are indispensable reference defined in view of the development of globally shared rules of behavior. It has been made, in particular, of the need for:

- states shall act in cyberspace in a proportionate manner and in accordance with international law;
- is guaranteed to anyone access to space and cyberspace technologies that allow the use;
- are respected diversity (linguistic, cultural and ideological) of final users;
- cyberspace remains open to innovation, the free movement of ideas, information and forms of expression;
- is respected the right to privacy of the individual and is adequately protected the intellectual property;
- to be placed in an joint methodologies for combating the crime cybernetics;
- it promotes competitive cyber space, suitable for securing to those who promotes real economic principles.

Following the attacks in Estonia, the Alliance has created Center of Excellence NATO Cooperative Cyber Defence (CCDCOE) from Tallinn and promoted new common defense policies against cyber attacks. Although the issue of cyber security appeared on the Alliance's agenda since the Prague Summit in 2002, incidents in Estonia and subsequently in Georgia led NATO to prioritize cyber security and take the first joint strategy of the 28 Member States in 2011, under the new Strategic concept adopted at the Lisbon Summit, reiterated in the Chicago Summit in May 2012. NATO's efforts are not limited to setting standards for information systems of the member states, which are of major importance in the Alliance, for protecting the capacity of infrastructure against the critical cyber attacks, NATO actively cooperate in this regard with its partners.

By the Emergency Ordinance no. 98 of 3 November 2010, Romania sets the organizational roles and responsibilities for the identification, designation and protection of critical infrastructure.

Thus, it was nominated a total of 10 critical infrastructure sectors: energy, information technology and communications, water supply, food, health, national security, administration, transportation, chemical industry, nuclear and space research.

Each sector is coordinated by one or more public authorities with owners / operators of critical infrastructure will go through iterative stages of identifying and designating critical infrastructure of national interest and those of European interest.

Also, each operator of critical infrastructure will develop a security plan which generally should contain the following:

- identification of the main components;
- perform a risk analysis based on major threat scenarios, vulnerability of each element and the potential impact;
- identification, selection and prioritization in terms of countermeasures and procedures, distinguishing between permanent security measures, which identify indispensable security investments and resources that are relevant for using in any situation.

Finally will be included information regarding to the general measures, such as:

- technical measures: including installation of detection, access control, protection and prevention
- organizational measures: including procedures for alerts and crises control measures and verification, communication, awareness and training, graduated security measures that can be activated by different levels of risks and threats, and measures in the field of information systems security.

On the base of the security plan it’s possible to design an IT&C system, consisting of collections of data and information processed, concerning to requirements,

DOI: 10.12948/issn14531305/17.4.2013.11

analysis and synthesis of the future architecture.

Functional relationship and interdependence of this databases (metadatabase), information and knowledge (see Figure 1) is supervised by an automatic balance component (system analysis & control).

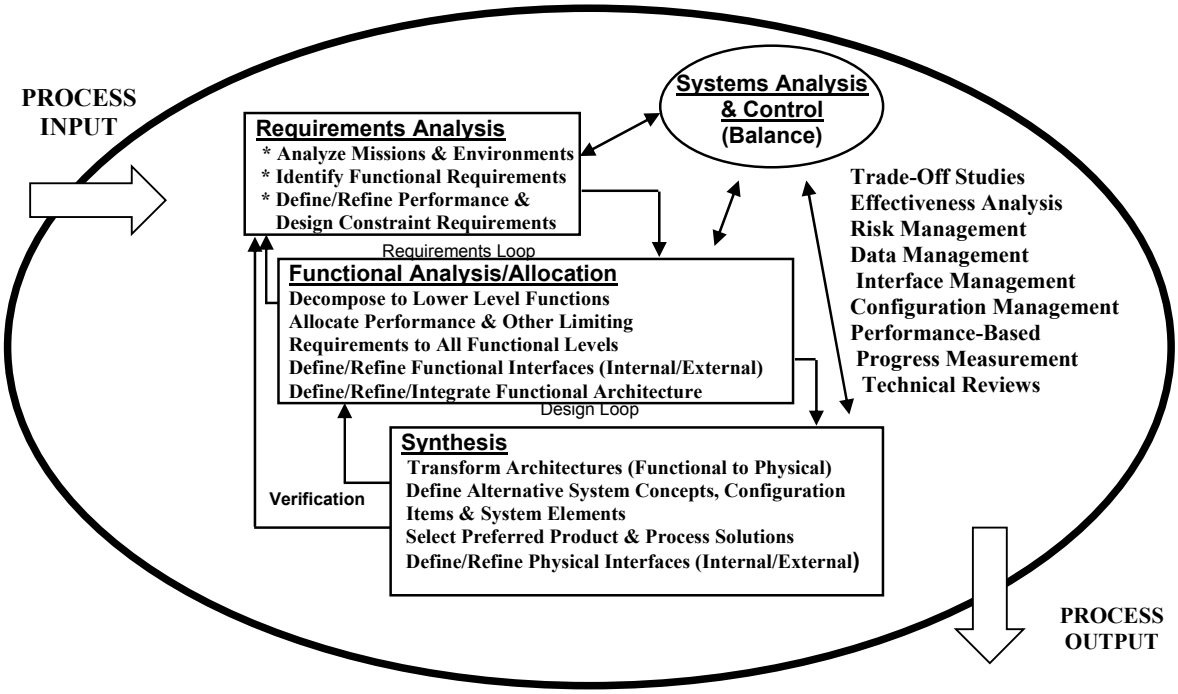

Fig. 1. The development of IT&C system on based a security plan

The process input is referring to the main component, such as:

- needs/objectives requirements;
- technology base;
- output requirements from prior development effort;
- program decision requirements;
- requirements applied through;
- specifications & standards.

As respects the process output, the main points that are evaluated are the following:

- Development Level Dependent;
- Decision Data Base;
- System/Configuration item Architecture;
- Specifications & Baselines.

The possibility that an organization's IT&C systems are sufficiently protected against certain attacks or loss is called "systemic risk." Some specialized publications is considered the risk of a subjective assessment, which refers to the future, thereupon there is only imagination. Instead, experts consider that "risk" is defined as the possibility that a threat to materialize.

The risk in the context of IT&C systems, is defined by the amount of
threats (events that cause damage), vulnerability and value of the information presented:

Risk = Threats + Vulnerabilities + value information.

Thus, threats, vulnerabilities and potential impact should be combined to obtain a measure of the risk regarding to the information.

One of the key elements of a national cyber security strategy is the risk assessment process. It consists of three steps [2]:

- risk identification – identification of important assets/organizations/sectors and main sources of risk;
- risk analysis - determining the likelihood that a potential vulnerability can be exploited and the impact that the threat

DOI: 10.12948/issn14531305/17.4.2013.11

could have on a critical economic sector;
- risk evaluation - taking decisions about the significance of risks for a critical economic sector and whether each specific risk should be accepted or treated.

In the following, a risk management process (see Figure 2) is used as a useful paradigm to frame some recommendations for setting an effective national cyber security strategy.

The target of these recommendations are in general all companies that manage or control critical infrastructures, security professionals working in economic sectors sensitive to cyber attacks and all government agencies and bodies involved in the definition and implementation of the cyber security strategy.

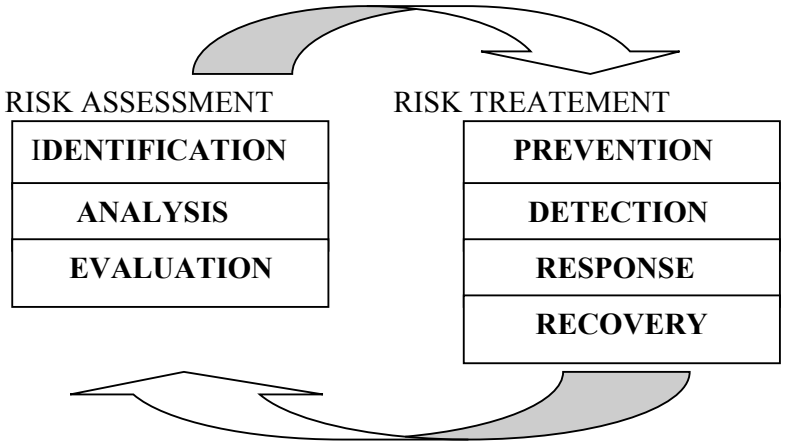

Fig. 2. Risk management process

These recommendations do not aspire to be a complete set of rules to be followed, but rather they represent a set of points that the national strategy on cyber security should take into account. Recommendations consider the legislative scenario, experiences from other countries, and results of the questionnaire.

The risk management process have to identify what could go wrong (identification of risk) evaluating which risks should be deal with (risk analysis and evaluation) and implementing strategies to deal with those risks, preventing or detecting all situations of risk, and implementing the adequate response.

As shown by Figure 3, the initial identification process starts with an identification of potential risk items in each of the four risk areas. Risks related to the system performance and supporting products are generally organized by the main objectives and initially determined by expert assessment of teams and individuals in the development enterprise.

In an attempt to limit the threat, become essential to propose solutions for ensuring the security of data and reduce the cost of managing computer systems, such as "cloud computing" and taking initiatives to provide support info-operational technical concerning to the critical national infrastructure.

In that context it have to have in attention some issues regarding to:
- acquire and integrate, at the national operative strategy, systems of the latest generation, necessary for the development of the performance of the institutions;
- enhancing a technological structure that supports the information activity in terms of traceability and knowledge of the interests of the threats;
- achieve standards and operating procedures compatible with the settings of the EU and NATO also through the planning and conduct targeted exercises;
- standardize the flow of the Technological Intelligence to the technical and operational structures

DOI: 10.12948/issn14531305/17.4.2013.11

"emergency" active at the national territory (Computer Emergency Response Team-CERT);
- develop any useful synergy between private and public sector, in order to evolve knowledge and awareness of the cyber threat;
- strengthen cooperation of the international organizations, for the intensification of information exchange and the initiation of a common project based on uniform methods of work.

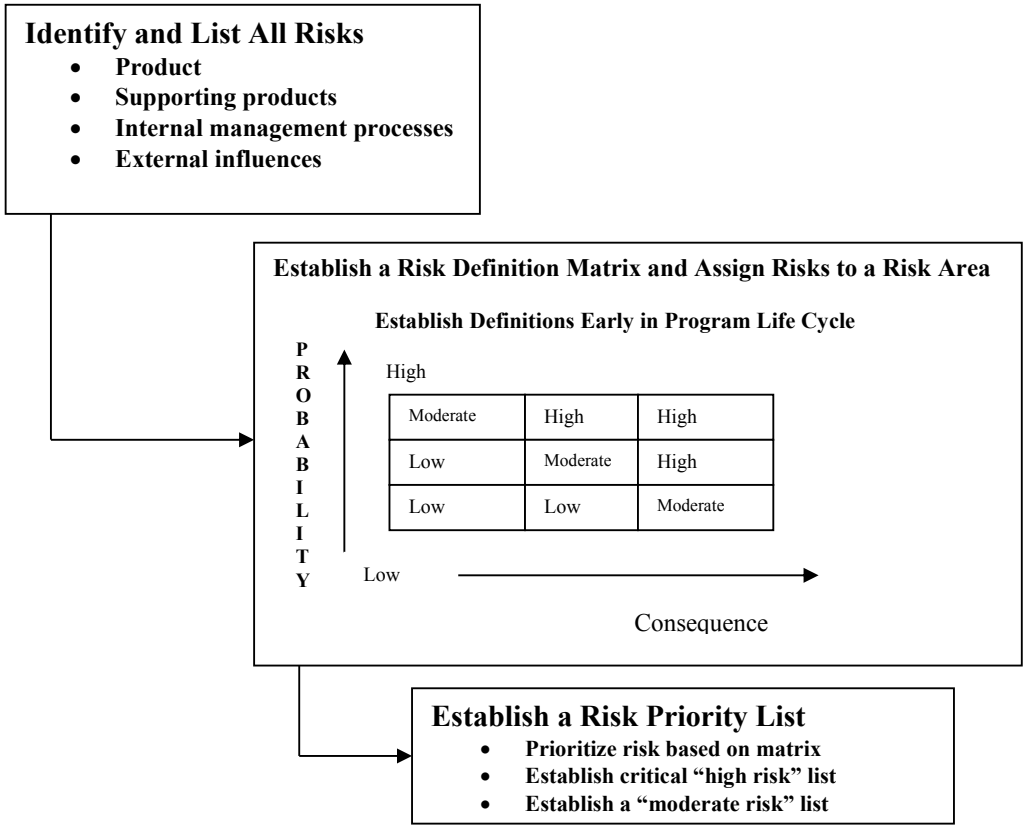

Fig. 3. Risk identification

The risk of an attack against of the critical infrastructure can be evaluated as:

$R = (T \times E \times Pr) / M$ (1)

where:
R – the risk of an attack;
T - potential threat due to specific environmental factors;
E - severity of the consequences of a possible attack ($E \geq 1$);
Pr - likelihood of occurrence of the risk factors;
M - totality of security measures.

Generally, the risk is analyzed by a minimum acceptable value, situation in which the risk of an attack can be expressed by:

$R = c \times R_{m,}$ (2)

where:
R - the risk of an attack;
R_m - minimum risk quantified;
c - coefficient of quantification the level of potential risk.

Likewise, immediate threats (It) of the virtual networks is estimated by:

$It = T / P, \quad P = Gm \times S \times Mp$ (3)

where:
P - protection measures of the CII;

DOI: 10.12948/issn14531305/17.4.2013.11

Gm – general protection measure specific for the analyzed infrastructure;
Gm = n1 x n2 x…;
n1 - immediate intervention capacity;
n1 - training level of the staff;
S - the security level that is guaranteed;
S = s1 x s2 x...;
s1 - intrusion detection;
s2 - operational range of reaction;
Mp - all measures of network protection;
Mp = m1 x m2 x…;
m1 - strength of the network in case of the cyber attacks;
m2 - the capacity of isolation of the vital area of the CII.

On the other hand, the factor P can be quantified by the formula:

$$P = Ma \times Hs \times I \times Ci \quad (4)$$

where:
Ma - implementing measures to strengthen the IT&C architecture;
Hs - software and hardware own capacities against the cyber attacks;
I - immediate capacities of intervention;
Ci - effectiveness of intervention mesures by the specialists.
In this context, the real risk of an attack can effectively evaluate by formula:

$$Rr = It \times E \times Pr \quad (5)$$

In practice, for Pr = 1 is considered to be a normal possibility regarding cyber attacks against the CII, and for Pr > 1 the alert level increase from medium to high (Pr >1,3).
In this contextual approach, SCADA (Supervisory Control And Data Acquisition) and remote control systems have thus become ubiquitous, as no company could afford to disregard one of the fundamental tenets of the market economy, namely that if all competitors cut costs (i.e. switch to SCADA), one should do likewise or be punished by consumers and forced out of the market. Until recently, the need to pay higher prices for "more secure" CII was never manifest to or easily grasped by businesses and consumers (and only partially so by governments). But IC&T (first and foremost TCP/IP) "consigned" its own structural vulnerabilities to SCADA. As demonstrated by SANS Institute researchers in 2013, many professionals working with SCADA are well aware of the intrinsic vulnerability of these systems. Nevertheless, ameliorating this state of affairs remains a hard sell even now [5].

3 Conclusions

Information security concerns most often that managing risk. No system will ever be infallible or foolproof, but by understanding the threats facing the organization every day, the existing vulnerabilities and its processes, asset sites with high risk and security resources can be managed more effectively.
CII vulnerabilities will not go away and societies' dependence on CII can only increase. Governments should train their citizens and businesses to cope with disruption and malfunctioning and should continue to invest considerable sums of money in the protection of CII. It can never be too soon for cyber security to become everybody's concern.
The aim, of a national cyber security strategy is to increase the global resilience and security of national IT&C assets that support critical functions of the state or the society as a whole [5]. Setting clear objectives and priorities is of paramount importance for successfully achieving this aim. In order to manage risk in a proper way, it is necessary to design an effective risk management process by identifying what could go wrong (identification of risk) evaluating which risks should be deal with (risk analysis and evaluation) and implementing strategies to deal with those risks, preventing or detecting all situations of risk, and implementing the adequate response.
Efforts made in improving the protection of national critical economic sectors cannot be made in isolation with respect to the rest of the world because cyber threats intrinsically cross borders.
Ensuring cyber security for a nation is a duty that cannot disregard good technology skills and competences. Any government

DOI: 10.12948/issn14531305/17.4.2013.11

organization that is involved in the national cyber security strategy thus needs to have such skills in-house and its governance needs to be aware of and able to assess cyber and information technology competences, it will either overestimate or underestimate a threat or simply not understanding what is going on. This is why many countries decided to converge all activities related to cyber security inside a single organization which is at the Presidency or Government level.

References

[1] European Union, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", 2013.
[2] R. Kissel, (ed.) Glossary of Key Information Security Terms, NIST IR 7298 National Institute of Standards and Technology (NIST), US Department of Commerce, http://csrc.nist.gov/publications;
[3] European Commission, DG Home Affairs, http://ec.europa.eu/dgs/home-affairs/elibrary/glossary/index_c_en.htm;
[4] The distinction between "critical infrastructures" and "critical information infrastructures";
[5] SANS Institute, SCADA and Process Control Security Survey, February 2013,www.sans.org/reading_room/analysts_program/sans_survey_scada_2013.pdf;
[6] European Union Agency for Network and Information Security (ENISA), "National Cyber Security Strategy. Practical Guidebook", pg. 8, December 2012;
[7] European Union Agency for Network and Information Security (ENISA), Glossary, http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary;
[8] M. Libicki, *Cyberdeterrence and Cyberwar*, Santa Monica, CA, Rand Corporation, 2009.

Dan COLESNIUC is Lecturer at National University of Defense, Bucharest, Romania. He was project manager of Romanian Project Management Excellence National Award 2008 competition. He was for the third time in the leading position for this competition. He is an experienced trainer and assessor in Project management Excellence Award, in 2007 attending the international training workshop held in Warsaw and being involved in international assessor teams.

DOI: 10.12948/issn14531305/17.4.2013.11