SECURITY CULTURE – THE FIRST LINE OF CYBER DEFENSE

Professor, Colonel (Ret.) Gheorghe BOARU, PhD*
Benedictos IORGA, PhD candidate**

***Abstract**: The development and universal accessibility of internet environment, the accelerated technological boom and easy access to high technology have generated favorable conditions for the emergence of a new environment for social life expression under all its aspects, which we all acknowledge as the cyberspace. By default, cybercrime, threats and attacks in the digital environment and cyber aggressions treated as unavoidable parts of virtual life have come forward aggressively from the beginning and have created the fifth space of social confrontation.*

Relating to the development of the elements that define cyber space as a new combat area, we can notice that security culture has evolved too slowly and does not have a significant contribution to the prevention of crime actions, cyber frauds and challenges from the online environment. A theoretical and technical justification of this slow evolution is largely based on the assumption that cyber space is a dynamic and fluid field for the manifestation of millions of new users. These new users get the first contact with digital technologies and their level of awareness and training is at an initial level of "default", fact that will be exploited permanently. However, the efforts to enrich the cyber security culture and to accelerate the rhythm of cultural progress should soon become a part of state policies for World Wide Web.

***Keywords**: cyberspace, cyber-attack, cyber defense, information security, security culture, target, network, computer system.*

Although it can be considered an Utopia, the actual reality proves that we are living in two different environments, each one with its laws and rules, but that coexist and develop simultaneously – the social environment or "real life" and the digital environment or "virtual reality".

* boarugheorghe@yahoo.com
** iorgaben@yahoo.com

We breath – we navigate, we speak – we socialize online, we feed ourselves – we simulate, we go to school – we are e-learning clients, we compose letters – we are sending an e-mail, we make investments – we make on-line transactions, all these are just a few elements that coexist in those two totally different spaces according to their characteristics, but that are linked by the integrating human part – the one that has generated, develops and exploits them.

The virtual reality, as a part of the social life, appeared starting with 1982, at the same time with the definition of TCP - IP[1] protocol and with the notion of INTERNET[2] and rapidly developed until the actual stadium, when we can affirm that a global population of 7.262 billion people has over 2.9 billion users for the INTERNET[3] global network. Of course, the accelerated developing rate of network environment and also the dependency of proper development on everything implied by human society in point of information and network environment as a way of processing data will lead in a very short period of time to the equalization of digits mentioned before or to the reversal of the report numbers. Not only a few voices sustained the dependency of all what means cyberspace and online environment, the whole "picture" does not represent anything else but a change of rules regarding the human life and new step of society evolution, being defined, mainly by the absence of frontiers, the access to impressive informational resources, permanent dynamism and, last but not least, anonymity.

These characteristics, although extremely beneficial, may be destructive too and can create the image about a society or a state-type organizational structure, regardless its physical size or its characteristics as an entity (territory, size, frontiers, population, resource, economic development, and so on…) is all the more vulnerable as the level of information held is higher. According to the recent history of the cyber attacks and cyber threats, a relevant example that may serve as an argument for the previous assertion, worthy to be considered a part of the chaos

[1]The TCP/IP (**Transmission Control Protocol/Internet Protocol**) was created by the US DoD (US Department of Defense) from the requirement of a network that can survive in any conditions.
[2]The term was formed by the artificial and partial fusion of two English words: interconnected and network.
[3]http://www.worldometers.info/ro/, accessed at 22th April 2015, at 1600.

theory, is the incident from 2004 involving the American civilian aircraft - Delta Air Lines Company with the headquarters in Texas. The incident was generated by a programming error at the computing level equipped with the operating systems Windows XP or Windows 2000 that allowed the exploitation of a vulnerability system of "buffer overflow"[4] type, by a German student[5] through the remote introduction in the informatics infrastructure of the company, of a worm type sequence code, known ever since as "Sasser worm". The incident, besides the panic created and the financial damage at the worldwide level (over 500 million USD) endangered the safety of millions passengers and the activity of the American civilian aircraft, British coastguard, satellite communications system of the press agency AFP (Agency France-Press), affected the insurance Finnish company IF and the bank branches SAMPO BANK, University from Missouri, also the Department of Radiology at Lund University Hospital from Germany.

The main point of exposing this incident is not to underline the vulnerabilities from the online environment, but to illustrate the global interdependencies existing in cyberspace, also known in the virtual world as the "butterfly flight", because by the manner in which information is held, disseminated and evolves in the cyberspace, it can be associated with the manner of the butterfly flight (for example in Germany) that can produce a tornado in Texas and the effects will be experienced in Japan. From this point of view, the cyberspace can be defined as the virtual global environment, generated by all existing cyber infrastructures that include processed, stored and/or submitted information, the actions of virtual users, policies and security procedures applied at the entire network level.

[4] A buffer overflow appears when a program or a process tries to stock more data into a buffer (temporary data storage area) than it was meant to hold.

[5]Sven Jaschan was born in Waffensen, Germania and studied informatics in high school in Rotenburg. He was arrested on 7th May 2004 by the German police after an international investigation, being accused of informatics attacks that had generated about 500 million USD worth damage.

The cyberspace[6] concept is a poly-semantic term, still going through a theoretical foundation process, but that can be explained through human-technology interaction.

The novelty of the concept and the inexistence of a complete and descriptive map of this space have generated polemics, various approaches, different and tensioned interpretations, that have defined this concept as being a developing philosophy, a virtual reality, a product of social interaction or another human dimension. From this perspective, technically speaking, "cyberspace can be aborted from 3 known trends"[7]: **Gibsonian cyberspace[8]-** the user, technology and transmission environment are considered as a single entity; **the virtual reality-** a multidimensional environment where people can move freely and can interact both with the computer and with other human beings; **Barlovian cyberspace[9]-** seen as an electronic and digital transmission environment, where the user is located in a communication network of computers.

Regardless the manner of defining it or the theoretical and technical approaches presented, at the cyberspace level and at each default network environment component, we can identify 5 basic characteristics, represented by:

-*the existence of a software and hardware platform* which is flexible and opened, at the basis of each cyber infrastructure – no closed network environment can survive in time;

-*the existence of four component levels:* **physical infrastructure** (developing basis of cyberspace, represented by interconnected computers, servers, sensors, transmission environments, and so on...), **logical level** (the totality of logical protocols that allow the initiation and the establishment of

[6] The "cyberspace" concept comes from English, due to William Gibson that used this term for the very first time in a SF novel, which appeared in 1984, to describe a computer world in the real society.

[7] Featherstone, Mike&Burrows, Roger, 1996, Cyberspace/Cyberbodies/Cyberpunk. Cultures of Technological Embodiment, Sage, London: 5-7.

[8] William GIBSON "Cyberspace: a consensual hallucination, daily lived by billions of legitimate users, in every nation, by children that are taught mathematical concepts… A graphic representation of data extracted from banks of each computer of humans societies. An inconceivable complexity…".

[9] John Barlow's concept, the founder of action group *Electronic Frontier Foundation*, *Economic Informatics Magazine*, no. 3(27)/2003.

communications, applications and informatics services in the network environment), **informatics level** (the whole data, metadata, the information which was processed, stored and submitted by the physical infrastructure) and **human level** (the totality of active and passive users that work in the cyber environment);

-*the reliance on action and human interaction*, emphasized by the argument that the human being is the one who, by his/her actions, keeps alive the network environment and it is not the computer which is defining nowadays the concept of cyberspace, but rather the interaction user-computer system does it.

-*the fact that it exists and evolves according to the human behavior models and society's demands,* virtually transposed from real life. This statement can be sustained by the following example: the characteristic of a public network segment will be generated by the social-behavior characteristics and the INTERNET users' specific demands from a specific region. To be more precise, if in a given area the rate of criminal action is high, the attacks and aggressions, performed in the online space on that network segment mentioned before, will be higher and will wear the mark or the operating mode specific to those users.

-*the existence of a high degree of insecurity,* generated by the anonymity of users, the lack of manifestation frontiers and development of component elements;

Each of these characteristics is representative for all that means the entire cyberspace or even local network environment. Whether we speak about the physical infrastructure, logical infrastructure or platforms and the software and hardware technology used as a basis for the development of this space, the security feature remains maybe the most rigorous and problematic issue of nowadays' information society and also the most significant one that can generate regression in the virtual space.

Starting from the following dichotomy **cyberspace – virtual reality**, the online security issue cannot be more reduced in comparison with the one from the social environment. All in all, the totality of risks, threats and daily vulnerabilities at the level of individual and community security have known an exponential increase, generally generated by the cyberspace characteristics mentioned before. Due to anonymity, access to technology, lack of developing barriers, artificial intelligence, vast informational

resource volume, quick data processing capabilities, ingenuity of users and last but not least the relatively reduced costs of transposing their will into the virtual environment, the notion of security in the cyberspace seems to be rather hilarious. During an interview about the security of the cyber environment, Keith B. Alexander, the commander of "US Cyber Command/NSA", stated that "the security in the dynamic cyber environment failed because the opponents change the rules by the simple exploitation of some new facilities and vulnerabilities"[10]. Richard Thieme, US government consultant on technology issues, during an international security conference - BLACKHAT from Las Vegas (2011), pointed out that "security in the cyber environment is a myth or, at best, a joke", and this is an axiom by the utter manner in which cyber environment is built, as a sum of virtual realities that can never be safe or, most of the time, without counterpart in reality.

Online insecurity is the result of risks, threats and vulnerabilities from network environments generated by individuals, interest groups, governmental and non-governmental organizations capable to develop cyber-attacks and cyber-aggressions that will overpass the resilience of cyber infrastructures. From this point of view, cyber security can be defined as being that normal state of network environment, obtained as an effect of applying some security technique measures and some proactive security policies, which permanently provide not only the confidentiality, availability, integrity and authenticity for network's data and information, but also continuous and secured access to network's resources and services. Like social and military security, cyber defense being a core pillar of cyber security, it is defined as the entire spectrum of actions having the goal to protect the cyber environment by detecting, stopping and countering any cyber aggressions. Online security is not a new issue, but new are the effects that generate insecurity in the current cyberspace.

If approximately 30 years ago a virus or a destructive code sequence could affect a computer and maybe a network segment at the most, nowadays the effects can be devastating not only by amplitude, but also by economic and social implications. Recent cyber espionage history showed

[10]The next wave, vol.19, no.4, 2012, p.1 - Building a national program for cyber security science / NSA - Central security agency.

how the already famous cyber-attacks such as "Stuxnet", „Flame", „Gauss", „Operation Tallinn", "red-October", "Epic-Turla" had the effect of mass-destruction weapons over the informatics infrastructures, so this new weapon type can be identified as being "the cyber-weapon". In the civilian environment, things are far from being simple; the interdependence between society and informational environment implies the fact that attacks over the civilian informatics infrastructure of a state will generate panic and chaos at the entire society level. A relevant example is represented by the operation "Dragonfly" or "Energetic Bar RAT", since 2009, a part of US energetic infrastructure was remotely controlled via malware applications implemented in the management and distribution systems of the national electrical network. Among the Dragonfly group's targets some energy distribution network operators, large companies generating electricity, oil pipeline operators and industrial energy equipment suppliers are worthy to be mentioned. Most companies who were targeted are located in USA, Spain, France, Italy, Germany, Turkey and Poland; furthermore, the effects and destructive potential of those cyber-attacks types over a civilian infrastructure makes us aware of the risks of information society that we live in.

Starting from these very few examples and also taking in consideration the illustrious network intelligence operations and daily network cyber crimes, we can ascertain that by just a simple access for the following "cyber-attack" term using a search engine online, the result will be hundreds of thousands of pages, all of these illustrating or certifying different actions and operations from the virtual environment. Taking in consideration these arguments the following statement is more than obvious: after terrorism, cyber security has gradually become the second concern not only for security structures, but also for national and international organisms. Every day we learn about another cyber-attack carried out on military installations, official websites, electrical networks, financial banks and institutions, credit cards targeted by sustained cyber-aggressions. Nowadays reality can easily confirm it. Comparing with "yesterday's authors" represented by a renegade group or a single hacker intending to get profit, "today's authors" are more likely to be organized-crime or terrorists groups, criminal syndicates or even governments. Over the last few years, worldwide cyber security valences have gained a major strategic

importance, where military conflicts have overcome the usage of classic arsenal, mostly developing in the cyber area, having a potentially devastating impact in a very short time. Practically, through network environment a permanent war can be waged without being stated as such in accordance with the laws of armed conflict. The bell-known cyber-threats like infected Computer Networks, harmful software, hacktivism as an online protest and persistent advanced threats in order to be removed or at least restricted, it is imperative to "be shielded" by latest technology systems and obviously consistent budgets and financial resources are necessary.

All these aspects can only give birth to the following natural question: "What is the security solution for cybernetics?" Asking the experts, especially those from technical area, the answer may be different mainly based on personal experience. An IT hardware engineer replied that the best solution to secure network environment or a cybernetic subspace is represented by the last firewall solution that implement the Advanced Firewall Protection technology known as Next Generation Firewalls (NGFW). Technically, it is difficult to contradict this answer taking in consideration that the chosen solution is top of the range concerning dedicated hardware security solutions that ensures QoS (quality of service) types features, intrusion prevention systems and filtering malware technologies, for which the research invested price only amounted to around 100 million USD.

In order to ensure data sharing, a communications specialist will recommend the permanent usage of connection systems that use not only secure hardware solutions like flux concentrators VPN technology with IP Security (IPsec) and Secure Sockets Layer (SSL) features, but also non-standard tunnel-encryption AES 512 bits or hardware.

A software products' developer will mostly recommend not only the update for all add-ons and system security measures for operating systems and applications used, but also permanent installation and update for an antivirus solution with extended features – "firewall protection" and "advanced malware detection" software types.

Last but not least, a local security administrator will probably impetuously demand firstly the purchase of solutions mentioned before and after that, the necessity of applying all recommended solutions. Furthermore, he will implement a security policy suitable for the network

environment that serves for the organization to which it belongs, in order to reduce operating systems vulnerabilities, to limit the access to useless ports, to control network-level security audit and last but not least, to ensure only those necessary resources for the proper system's performance.

All these hypothetic solutions and answers are real and can definitely increase the security level of a global cybernetics network. Even more, they will definitely ensure a high level of service and applications availability in conjunction with confidentiality of the processed data in the network environment, even if the costs are consistent. For example, the annual cost for the global economy to counteract the effects of cybercrime is estimated at "over 400 billion USD." The most optimistic appraisal was "over 375 billion USD"[11], but even so, this represents far more than the GDP of many countries or way over the cumulative income of many multinational companies. Moreover, the costs for this case are the cumulative effects induced by the compromise of millions of zeta bytes confidential information belonging to users who were attacked online, approximately 40 million people in the USA, 14 million in Turkey, 20 million in Korea, 16 million in Germany and more than 30 million in China in 2013 based on the report of the Center for Strategic and International Studies. Of course, speaking from the point of view of the same security administrator, when talking about securing a network environment in cyberspace, especially when the level of confidential information protected is high, the financial factor or resource should matter the least, in order to secure that data.

Although as we mentioned, the proposed technical solutions are founded and supported by solid arguments, at the basis of their deployment and use is "man" or better said a "virtual user". From this perspective, the user is the weakest link of the whole mechanism of security in cyberspace, which makes the success of cyber-attacks and aggressions build and operate mainly this link. The user, as previously stated, is a gear in the framework of the forth defined level, which owns a personal experience limited in terms of virtual behavior, following his/her personal training and especially the security culture held.

[11] http://www.mcafee.com/ca/resources/reports/rp-economic-impact-cybercrime2.pdf, accessed at22thMarch 2015, at 2000.

Security culture can be defined as the first line of cyber defense and is the sum of values, norms, attitudes and actions in the virtual environment, which determines the understanding and assimilation of cyber security concept and other secondary concepts: information security, physical security, document security, personnel security, communications security, political security, insecurity etc.

Physically, security culture is not something tangible, that can be purchased or implemented like a hardware, but is rather the result of several factors that combine the individual experience of each user with technical and theoretical knowledge owned, with the values of the organization he/she is part of and, last but not least, the security procedures implemented at the level of that organization. Security culture at individual level is defined by all these elements mentioned before and the security culture at the organizational level is the cumulated picture of the security culture levels of that organization's members.

The best hardware security solution implemented at a network hub level or even the entire cyber environment level can be penetrated by some combined attacks based, for example, on social engineering techniques or on exploiting the staff's ignorance of the internal security procedures that can be applied to an organization. According to the latest reports regarding cyber-attacks on public email services users, over 60% of attacks concluded with compromised mail and mailboxes belonging to users was due to poor training regarding the minimal security culture that should be held for the use of electronic mail. Starting from a common mistake, for example, generating a password to access a system containing simplistic and familiar combinations of characters (p@ssw0rd, person's name, birth year) and reaching security breach by forcing some internal security policies defined within an organization (the use of unauthorized storage media, accessing the internet using the credentials of another user), all these elements have in common a poor security culture concerning the users.

From the perspective of an attacker it will always be easier to obtain confidential information attacking a user where he is most vulnerable, using limitations generated by lack of training, negligence in the handling of information and technical resources, the concern for quickly achieving a task by making detrimental compromises to the maintenance of security, rather than attacking a mail server or a domain controller that manages a

closed network because it involves – in addition to the consumption of technical resources – time and risks that cannot be estimated. Penetrating a network in order to obtain confidential information is the result of combined actions involving the superposition of several methods and attack techniques[12], based on documentation of the network infrastructure firewall solutions, traffic data, methods of security applied at the network level.

All these may be doomed to failure in the situation in which, behind that cyber infrastructure, management is performed by security personnel who have the necessary knowledge and technical equipment able to provide intrusion detection and the protection to reject that specific attack. At the expense of all the efforts for securing a network, for example in an organization, the experience and the reality of recent years have shown that the biggest vulnerabilities are not to be found in that specific local security environment of that network or at the configuration and network infrastructure, but the global security environment may be the point at issue, where users that operate freely are not constrained by the specific rules regarding the security protection implemented at that organization.

For example, at the level of large corporations, but also at closed government organizations, it is usually believed that a user – generally a person holding the position of employee – is free to manifest himself/herself in the social environment as he/she wishes, without being constrained by applying self-protection and security rules regarding his/her own person, when he/she is not in the perimeter of the organization. This aspect can be proven to be wrong and it is often a vulnerability that is intensively exploited by cyber-attacks, because it is much easier to access and penetrate a computer system or a home network wireless of a user, in his/her familiar environment, than attempting to get the same results by attacking the computer equipment used within the organization. From attacking a personal computer or smart-phone of a user, up to obtaining the confidential data owned by him within the organization, most of times there is just "one successful step", primarily due to the ingenuity and experience of that

[12] For exploitation - persistent advanced threats, for economic and politic espionage - operation GhostNet, malware infesting techniques, identity theft - spam techniques, phishing and pharming, for sabotage - Distributed Denial of Service type of attacks or generated spams by Bootnets (Conficker Network and Mariposa Network), for destruction - Stuxnet.

attacker in conjunction with the security culture and users' tricks (using the same security credentials, possession of information on personal computers that can help document the work in the organization, and so on…).

Regarding the operating techniques of the user, the most recent attacks (e.g. "epic-turla" attack or "turla-carbon") used social engineering methods combined with technical solutions attack malware type (70% penetration is based on solutions infestation of this type), taking advantage of the naivety of users and poor knowledge concerning the safety rules, particularly applicable to the closed government networks closed, where, theoretically, the control and application of management is more secure. The social engineering techniques, in conjunction with the possibilities offered by social networks by exploiting and documenting almost real-time behavior of a user in the virtual environment are a real cyber weapon regarding which hardware and software security solutions cannot resist, but can at most slow down or limit the effects of attacks. When an attacker aims to exploit even a closed network environment, belonging to an organization, including by exploiting "zero-days" vulnerabilities, it is very helpful to understand the online behavior of users and administrative staff security from the public area. Information obtained through online research using social networks and social engineering can lead to establishing the manner of reaction, the way of thinking and behavioral attitudes and technical skills of users and managers. Basically, an attacker discloses what that user or security administrator knows, what he/she can do, how much he/she can do and how they will react, therefore facilitating their subsequent technical actions or selling databases to other groups or organizational structures concerned.

The only defense line that can limit or eliminate these risks and vulnerabilities unfortunately is not a technical solution, but it is the security culture of each entity that interferes with the cyber environment.

Achieving the security status at network level involves, first of all, creative intellectual effort like education, research and security culture for each user. A structure cannot be competitive and is unable to use the resources, technology and its potential, being only a consumer of security. For this, each organization (regarding the internet this is perhaps the most visible) must be a security generator in its area of action, as the cyber environment is dependent on each network environment it makes up.

Therefore, the issue that emerges is that of what should be done to improve the security culture in the staffing organizations, in order to improve the safety in the cyber environment. This problem is not a simple one that can be performed instantly, because it involves an accumulation of actions undertaken and perhaps permanently integrated into a legislative and applied state policy.

A first step could be represented by providing a legal framework - by approving and implementing certain cyber security laws to govern the legal framework and the responsibilities of stakeholders in cyber infrastructures. Currently, most online attacks at user level are his/her responsibility, the user being bound to look after his security computer system terminal; the internet provider is not bound to ensure quality of service, including the security infrastructure concerning the terminals.

In this way, an attack on a computer system spreads fast in the network; the service provider has no responsibility other than to ensure an effective communication line, network assets and liabilities and to maintain the traffic level. Regarding security training on access to the internet, this is not done; it is the sole responsibility of the user. In case of contracting an electronic service in the Internet environment (and sometimes government networks), security trainings for the use of that service implies tacit acceptance by a tick, a memorandum (agreement, terms of use, EULA) that describes acceptable use policy general terms of service and responsibility that exonerate the responsibility of the services generator concerning the occurrence of security incidents in the online environment.

A second step is represented by the emergence of organized education cybernetics at school level, a solid argument in this sense being the fact that the concept and the "cyber" has nearly 35 years of development and the dependence of social life on this area is overwhelming, replacing other areas such as "arts" and "sports" in terms of impact on social life. Cyber education can be the first pillar of the security culture that will allow the cyber security sub-domain to adapt in order to face new challenges in the network environment, all the more as the online security has become an industry generating profit. Closely related to education cybernetics is the research into "cyber" which may be the second pillar of the security culture in order to understand current threats, to study the implications and effects, as well as documentation and development of new hardware and software

security solutions and new security procedures at institutional and governmental levels.

A third step may be the development of an inter-institutional governmental partnership or between government institutions and those from civil society to generate joint projects to improve the culture of cyber security to the users and consumers, given the staff's quality to be a user of private and governmental networks, but also an internet user.

Common objectives projects may include promoting actions of security culture through media, organizing courses, symposiums, trainings and seminars, workshops and conferences in public education institutions to address security culture issues from cyber environment; to establish contacts and permanently collaborate with international scientific institutions, also with experts; to support by financing the people or legal bodies who wish to initiate and refine in the cyber security culture; to attract local authorities inactions of editing, publishing and dissemination of information materials, printed and audio-visual; also to develop online platforms based on e-learning technology that will address the issue of security training and will certify an acceptable minimum level of training for online users from private and government networks.

The last step is to change the mentality of the current cyber security culture, particularly at the level of governmental organizations, local authorities and institutions of the national defense and public order. This can be achieved by adopting and implementing proactive strategies based on awareness, prevention, protection and response in network environments owned and leaving behind the current concepts on the development of security culture by static means mainly represented in documentary read by each user (which presents risks, rights and obligations in the network) that ends with the user's accountability concerning his actions in the cyber environment.

Although the current practice can be very wide-covering, speaking from the legal rights at the institutional and government level, it does not protect you and does not limit the effects of any cyber-attack over the critical infrastructure, as it can be achieved where the security culture of the users is a not only a high-level one, but it is also adapted to the specific area where they work in organizations. Most times, knowing what to do, when to do it, how to do it and implementing specific protective actions in the

network as quickly as possible can lead to the salvation of the whole organization or the entire critical infrastructure of the state.

Whatever the capacity for analysis and prediction of cybernetics evolution, security culture must evolve simultaneously or as much as possible in an anticipatory manner, based on the social human experience and must be consistent with the requirements of critical infrastructure protection and information processed in network environments. Achieving cyber protection at the entire infrastructure level through coercive or restrictive individual manners at all network environments cannot be a solution to social progress based on knowledge, although various forms of state organization apply these methods. Concepts like "open security", "open society" or virtual organizations (Anonymous) are attracting, in an increasing way, many active supporters in the online environment, also involved in aggressions against cyber security organizations. From this point of view, the trend of improving the cyber security culture should become natural in society, rooted to the average user, due to technical-scientific progress and the emergence of new social values and must not be turned into a rigid way of stopping the evolution and expansion of cybernetics.

An old proverb in the Bible tells us: "The cautious heeds his steps"[13] and this wise piece of advice can be successfully applied in cybernetics whenever we are online or when we manage a critical infrastructure network for the national security field.

This work was possible by the financial support provided through the Sectorial Operational Program Human Resources Development 2007-2013, co-financed by the European Social Fund, the project ***HRD/159/1.5/S/138822****, entitled* ***"Transnational Networks Integrated Management Doctoral Research and Postdoctoral Smart in 'Military Science', 'Security and Information' and 'Public Order and National Security' - Training Program for Elite Researchers - 'SmartSPODAS'."***

[13] The Bible, Genesis / Proverbs 14:15, page 47.

BIBLIOGRAPHY

***, *The next wave*, *Building a national program for cyber security science* , Central security agency, vol.19, no.4, 2012;
***, *Twenty Critical Controls for Effective Cyber Defense: Consensus Audit Guidelines*, 2009;
***, *Cybersecurity Strategy of Romania,* 2013;
FEATHERSTONE M., BURROWS R., *Cyberspace, Cyberbodies, Cyberpunk. Cultures of Technological Embodiment*, Publisher Sage, London, 1996;
RODOSEK G.D., *Challenges of cyber defense in future internet*, München University, 2011.

http://www.mcafee.com;
http://www.worldometers.info/ro/;
http://www.securelist.com/en/analysis/204792238/Gauss_Abnormal_Distribution;
http://rt.com/news/iran-us-israel-cyberwar-virus-weapon-770/;
http://news.yahoo.com/report-secret-u-cyberwar-against-iranian-nukes-began-065204641.html.