EU and Cyber Security

Dragos Ionut ONESCU

Abstract: ***Securing network and information systems in the European Union is essential to ensure prosperity and to keep the online economy running. The quick and constant development of information and communication technologies, globalization, the drastic increase in data volumes and the growing number of different types of equipment connected to data networks have an impact on daily life, the economy and the functioning of the state. On the one hand, this level of ICT development will contribute to the improved availability and usability of services, enhance transparency and citizen participation in governance, and cut public as well as private sector costs. Instead, the increasing importance of technology is accompanied by an increase in the state's growing dependence on already entrenched e-solutions, and cements the expectation of technology operating aimlessly. Social processes are also becoming increasingly dependent on a growing number of information technology resources, and in the future attention must be drawn to the fact that society at large, and each individual in particular, will be able to maintain control over the corresponding processes. The number of actors and state in cyberspace that are involved in cyber espionage targeted at computers connected to the Internet as well as closed networks continues to grow, with their aim being to collect information on both national security as well as economic interests. The amount and activeness of states capable of cyber-attacks are increasing. Meaningful and effective cooperation between the public and private sector in the development of cyber security organization as well as in preventing and resolving cyber incidents is becoming increasingly unavoidable. National defense and internal security are dependent on the private sector's infrastructure and resources, while at the same time the state can assist vital service providers and guarantors of national critical information infrastructure as a coordinator and balancer of various interests, please download TEMPLATE HELP FILE from the website.***

Index Terms: European Union; security; cyber security

I. INTRODUCTION

The European Union works on a number of fronts to ensure cybersecurity in Europe, from providing the delivery of better internet for kids to implementing the international cooperation on cybersecurity and cybercrime. As societies, governments and businesses become increasingly reliant on the Internet for the normal functioning of every-day activities and the supply of essential services, protecting cyberspace from malicious activities has become a critical action point for policymakers globally.

In February 2016, the European Commission published a strategy on cyber security, as well as a proposal for a directive concerning network and information security (NIS), which is currently still in debate.

Cyber security strategy, "cyber-space open, safe and secure," global vision of EU on best ways to prevent and manage threats and cyber-attacks, in order to promote European values of freedom and democracy and to ensure the growth of the digital economy in conditions of safety.

Evolution at European level has contained within the establishment of a European Centre to fight computer crime (IP/13/11), the legislative proposals linking to assaults alongside information structures (IP/10/12) and the inauguration of a global alliance against child sexual abuse perpetrated through the Internet (IP/12/1308). The strategy took into consideration the development and financing of a network of national centers of excellence to combat computer crime, to facilitate training and capacity building.

Modern computerized society based on Internet already represents a reality in which ignore borders and shall override any constraints of a spatial or temporal. Governments, firms, public and private sector, national and international financial bodies, education, culture and scientific research, all have effective forms of leadership, information and communication. An essential part of computer networks, particularly in internet and online communications is the information security.

For example, users will be taken to ensure that the e-mail is authentic. Occasionally customers, mainly when acting on behalf of assurance establishments looking for privacy of messages transmitted. In economic transactions, along with authenticity and confidentiality, has an important place and the need for checking the integrity of messages, data and programs, which means that they have not been altered during transmission over the network. In business transactions online it is very important that once received over the network, a command not only genuine, unedited content, but there is a possibility that the consignor should no longer recognize, refuse. In this context, cryptography becomes more and more used in the creation of mechanisms and security services.

It has created a new ' space '-cyberspace -there are new types of vulnerabilities new attack vectors, and the attackers are no longer limited by their geographic location. Cyberspace increases nearby the world everyplace there are computers and the internet, or any other communication device.

Moreover, modern human conflicts have expanded the physical space and in cyberspace through cyber-attacks. Such attacks affect data, processes and network environment. When such attacks are politically motivated, they are part of the so-called cyber warfare (cyberwarfare).

Cyberspace is characterized by the absence of borders, dynamism and anonymity, generating both the development opportunities of the information society and knowledge-based risks to its operation (at the individual level, State and even cross-border manifestation).

Revised Version Manuscript Received on June 22, 2017
Dragos Ionut Onescu, Strasbourg University/Babes-Bolyai University, E-mail: dragos.onescu@odasglobalconsulting.ro

With how a society is more computerized, the more vulnerable, while ensuring the security of cyberspace should be a major concern of all actors involved, particularly at the institutional level, where development and focuses responsibility application of coherent policies in this field.

Romania seeks both to develop a dynamic information environment based on interoperability and specific services of the information society and ensuring that fundamental rights and freedoms of citizens and national security interests, in an appropriate legal framework.

From this perspective, it felt the need to develop the culture of cyber security to users of computer systems and communications, often insufficiently informed of the potential risks, but also with the solutions to counter them.

Widespread knowledge of the risks and threats to which they are subject to the work going on in cyberspace and how to prevent and counter them require effective communication and cooperation between specific actors in this area.

Since the study a set of major security events happened at European and worldwide level, one can complete that defensive approach that is widely used today to defend computer systems is inefficient and, therefore, cyber-attacks had a significant success rate. Most computer systems managers perform a baseline configuration and their security, after which only monitors various parameters, observing the operation of them. When a problem is detected by the monitoring systems, they react to it and solves the problem. Nevertheless, in the circumstance of safety events, this substance to act is not adequate to defend dangerous systems because it can lead to irretrievable damage (theft of files, negotiating systems, their destruction, impaired the image of the organization affected, etc.). With this approach and reactive defensive attackers will always be one step ahead of those dealing with the protection of those systems. Another approach is to protect the security of information systems. This idea talk about an organization which dynamically test their systems and find weaknesses before enemies. This approach allows the Organization to proactively remediate security issues and be one step ahead of attackers. Offensive security techniques are practiced in evaluations of the Red type Teaming, penetration testing, and ethical hacking.

The academic approach to cyberspace security can have more choices. First and foremost is about the incorporation of knowledge of security in different programs and courses; it's about adding some basic courses (security in the operating system kernel, security in the database). Secondly, is it possible to create special courses either in computer science/computer engineering (as, for example, cryptography, digital signatures and PKI, security of electronic payments) or to another program, with the aim of raising awareness (Etched Hacking, behavior and ethics on Internet). An additional option, more complex, is the creation of special programs, to be dedicated to the preparation of experts and researchers in cyber security. They can make both engineering technical (engineering), as well as in other fields (mathematics, economics, law, judiciary, sociology).

The world is becoming increasingly complex and interdependent, and the phenomenon of globalization is increasingly as being irreversible. The emergence of a global economy, highly interconnected, international alliances, reconfigured the system accelerates the adoption of technologies and development of new high-profile economic centers. This interconnected world offers many new opportunities but significant risks to developers and international security.

In the present context of security proxies, subjected to extremely varied challenges, strategic documents related to national security was elaborated in 2008 in the EU States such as the United Kingdom and France finds difficulty progressive overlay and in making a delineation between national defense and international defense, between internal security and external security and, in a wider, between the defense and the security

Among these threats and vulnerabilities is developing new strategies for Defense and security you need to solve new problems: not only the defense or control of some bounded spaces but also the explosion of uncontrolled flows of people, goods or ideas.

Riposte can not only be global, associating all of the authorities and of civil society at national, European and international.

Being a sector in full evolution, cyberspace is like a desert-a continuous change hard to monitor and which may produce unexpected effects on the politics and security of certain spaces, regional.

Nowadays, we can say that the level of advance of an establishment is straight proportional to its degree of computerization, even though this is a vulnerability for her. Concurrently with the increasing computerization of a company must grow and the level of concern of officials, for the elaboration of legal rules which do not allow exploitation of these vulnerabilities.

Like any other actions, and he follows cyber-attack a number of predefined methodology: obtaining vital information in relation to the proposed target, finding out and accurate understanding of the weaknesses of the target, exploiting vulnerabilities, actual attack itself for triggering the desired effect and carrying out actions aimed at covering traces of allowing identification of person how made.

II. GREAT BRITAIN

The first National Security Strategy of the United Kingdom after the cold war the security in an interdependent world (Security in an interdependent World)-2008 outlines the nature of the new security challenges, threats and risks have evolved and what are the arrangements envisaged by the United Kingdom to overcome them now and in the future. The strategy clearly demonstrates that new security threats call for new approaches; it is now an activity require the radical update of issues subject to management and a more coordinated response than in the past.

The main part of the meet's security policy of the United Kingdom is to deliver usefully and advice policy to the Prime Minister, support for administration departments in emerging operational strategies and policies.

The document fixes the guiding principles for action to be materialized through cooperation and adaptation action against and riposte. The requirement of the actuality it is a set of skills against threats internally and externally on the pan; leading determinations concerning a better understanding of the threats for the purpose of early warning actions, where possible, and ensuring that they can be managed and minimized the negative effects that could result from the threats to accomplish. Security policy of the United Kingdom highlights the need for the Government to engage in a dialogue with experts, staff and public opinion in order to ensure a common understanding of the security challenges faced by the United Kingdom and of the measures taken to counteract them.

III. ESTONIA

Since April 26, 2007, the Estonian capital Tallin, in large groups of people of Russian ethnicity, took to the streets, showing the Government's decision to move the statue of a Russian soldier, hero of the Second World War. The monument would be moved from the center of the capital in a military cemetery. The soldier statue was made in 1947, in honor of the Soviet victory against Nazi Germany.

Cyber-attacks against Estonia were launched simultaneously with the beginning of the street demonstrations. On April 27, the websites of governmental establishments and news portal sites have been swamped by the cyber-attacks and therefore blocked. In the following days, the attacks have increased progressively, both in intensity and number of techniques used at the same time, increasing the number of targets.

The targets of these attacks were represented by the services offered by the Government sector, followed by the services offered by the private sector and the banking sector; for a short time, even emergency number 112 has been blocked. They also stopped government sites and political, among the most important being those of Presidency, Government (Prime Minister, all the ministries, less than that of culture), Parliament, police, city halls and other local services.

The only data about the origins of these attacks have been those that have originated in the territories of the 178 countries, most of them, including those who have targeted government sites, originating in Russia. The very First Estonian Minister, Andrus Ansip, in a British television interview with BBC News, accused Russia that Estonia Cyber-attacked. (http://news.bbc.co.uk/)

IV. ROMANIA

An increased number of cyber-attacks worldwide and the impact of their big shows weak security measures implemented in the cyber systems, but also a savvy and increased incentives from attackers. The degree of attractiveness of cyber war looming, what, paradoxically, in times of peace, is in full growth and represents the interests of a political, strategic and economic: low cost of such a war/attack, anonymity, minimum losses to human lives, the independence of time and place. Accordingly, national security has to be redefined, taking into account the impact that it had new ICT technologies and new risks to information in nature. Therefore, defending cybersecurity (cyber defense) is a major concern for many countries and organizations in an attempt to minimize the effects of cyber war.

One of the buildings of the national defense Strategy of Romania adopted in 2010 is even cyber security. Furthermore, the strategy emphasizes the need for improved methods for identifying risks to the safety and security of proactive steps.

According to the National Security Strategy, the development of Cybernetics of cooperation between public and private environment, in order to ensure cyber security, is a priority direction for action at the level of international organizations or alliances to which Romania is a party, bearing in mind that cyberspace brings Cyberinfrastructures alike owned and administered by the State and private entities.

Obligation for guaranteeing cybersecurity is the responsibility of all players involved, taking into account the complementary interests in this area to ensure the legality of operations, combat the phenomenon of cybercrime and protecting critical infrastructure interconnected with cyberspace and is based on mutual confidence.

The business environment in Romania but remains vulnerable and insufficiently prepared to cope with the multiple risks of current cyber security. The impact of globalization and the Internet, as well as the evolution of technology information to centralized systems serving trans-national corporate structures, expose the private sector directly to potential cyber-attacks. Furthermore, the databases of clients (in particular, banking, telecom and health), but also the evidence of employees of large employers, contain personal data protected by law whose safety is not always assured.

The local economic environment is connected to financial flows, and European and international resource, but not all drivers is professionals and well trained to prevent and to respond in case of need.

A good portion of private companies with foreign capital or the local national societies, or autonomous administrations or other State-owned entities present in the market do not have a Business Continuity Plan or disaster recovery, nor have adequate technical and human resources to implement effective and feasible in such solutions. With the exception of banks and other companies from sectors strictly regulated, there is no legal obligation for auditing of computer systems and their degree of protection, and no requirement to test their resistance to penetration testing illegitimate. The general level of awareness at the national level is reduced and the basic means available for SMEs, for example, are non-existent. Under the conditions of economic crisis, regional security climate and the difficulties Romania to recover certain historical gaps (infrastructure, health, education, European funds absorption, etc.), the private sector will continue to pass through the various turbulent.

In this context, it becomes very important role of responsible authorities.

In the field of cyber security to communicate and synchronize their concrete plans to improve the level of protection of vital and strategic areas, but also to create methods and tools by which the economic environment, business, social, etc.

Romania needs a modern cyber security law and efficiency, put into service of national strategic interest and synchronized with common agenda of European cooperation, NATO and international. Is the government mission to complete the bill and ensure its implementation by deploying dedicated institutional structures and support measures allowing raising concern and concrete solutions implemented in public and private sector for a viable cybersecurity.

A draft European directive is still under debate, but does not anticipate major changes, which is focused on five main concepts: the obligation of each European State to adopt a national cyber security strategy; creating a network of institutional cooperation; establishment of uniform requirements/standardized; and application/implementation of consistency by the Member States of those rules.

V. CYBER WAR WEAPONS

Generic, a firearm is defined as an object used in battle in order to cause injury, to disarm or to defend yourself. Even if the term "weapon" is relatively easy to understand, it covers a wide spectrum of action. With the passage of time, the weapons have evolved from simple blunt objects made of stone or wood, the much more dangerous objects with greater capacity for destruction and to the so-called "cyber weapons." In this case, when we speak of "cyber weapons" make reference to a code or a program meant to cause losses and physical problems among users of the internet, corporations or even security systems of international actors.

Cyber weapons encompass a broad spectrum in general can be reached from a generic instrument with low potential at specific weapons that have a much greater potential. To demonstrate this, we will use a polarity comparison. Low prospective of cyber weapons bring to mind paintball guns: they can be misguided for real weapons, are light and from a commercial perspective, used to "play" but not to produce serious wounds. But a closer inspection of these "weapons" they lose part of their nature threatening. Cyber weapons with high potential can be compared with the sophisticated systems, such as modern missiles or anti-radiation systems, which need specific information about the target, and involve major investments for research and development, the development of new tactics, talking about such trends.

All the arms used in the online attack are in common Cyber worms, such as Red October, the Trojan ZeuS Duqu and worms to Stuxnet or Flame.

Trojan Horse Duqu The horse of Troy was in stands Duqu 2010 received this name because of its action, it is a generator of files with the extension being DQ tool that allows remote access. Initially infected computers have been discovered in the administrations and enterprises from eight countries: France, Netherlands, Switzerland, Ukraine, India, Iran, the Sudan and Viet Nam, and it is believed that the four countries have become victims: United Kingdom, Indonesia, Hungary and Austria (unconfirmed sources).

Stuxnet Virus

The highest role of this worm was to change the administration of certain actions to conclude the physical damage of the affected plants. Firstly it was used to control Iran's nuclear activity for the production of material damage, being branded as a weapon of war. Also it was found affecting program Siemens industrial control machines used mainly within the oil rigs, power plants and in the water sector. Most infected computers have been discovered in Iran but a small number, and have been found in Indonesia, Pakistan and India, the virus is considered a real threat to all computer systems. Due to its complexity, it is believed that at his production, the authors had the support of a State, the first suspect that Israel intended to halt production of enriched uranium and thereby delayed the construction of the atomic bomb by Tehran.

If your native language is not English, please get a native English-speaking colleague to proofread your paper.

VI. CONCLUSION

The triumph of the establishments depends on, principally, of the usefulness of European-level collaboration to defend cyberspace and national synchronization guidelines, arrangements and measures taken at the international level.

In this context, it becomes very important role of the responsible authorities in the field of cybersecurity to communicate and synchronize concrete plans for improving the level of protection of areas vital and strategic, but also to create methods and tools by which economic, business, social etc. able to develop sustainable and competitive.

Given the dynamism of the global developments in cyberspace, as well as the objectives of the European Union in the development of the information society and the widespread deployment of electronic services, it is necessary to work out a more complex , that ensure the development and implementation of concrete projects for cyber security.

REFERENCES

1. Cyber Security Strategy was published as the two British security strategies under the direction of the Cabinet Office, the document is available at http://www.cabinetoffice.gov.uk/reports/cyber_security.aspex.
2. Estonia hit by „Moscow cyber war", „The Economist", the document is available at: http://news.bbc.co.uk/2/hi/europe/6665145.stm
3. Douglas W. Hubbard, Richard Seiersen, Patrick Cronin, How to Measure Anything in Cybersecurity Risk, Audible Studios, 2016
4. Robert K. Knake, Pete Larkin, Richard A. Clarke, Cyber War: The Next Threat to National Security and What to Do About It, Tantor Audio, 2014
5. George Cristian Maior,2009 strategic thinking and Uncertainty in international relations in the twenty-first century, RAO, Bucharest
6. The National Security Strategy of the United Kingdom-2008, (5.6)
7. http://nato.mae.ro/node/435
8. P. W. Singer, Allan Friedman, Cybersecurity and Cyberwar: What Everyone Needs to Know®, New York Times, 2003
9. Rid Thomas, Peter McBurney, Cyber-Weapons, The RUSI Journal, 157:1
10. R. J. Vidmar. (1992, August). On the use of atmospheric plasmas as electromagnetic reflectors. *IEEE Trans. Plasma Sci.* [Online]. *21(3).* pp. 876—880. Available: http://www.halcyon.com/pub/journals/21ps03-vidmar

AUTHORS PROFILE

Dragos Ionut Onescu, Dragos Ionut Onescu is General Manager at ODAS GLOBAL CONSULTING and President at ODAS Association. He helped the company to grow from humble beginnings into a solid, durable enterprise. Mr. Onescu is consultant of diferent international and european institutions, an expert to assist in evaluating EU projects and member in several international and professional associations.

Mr. Onescu has over ten years of management and leadership experience and he has the ability to recruit the best talent for his businesses and associations. He works with executives, helping them to develop organizational culture, inspired by some of the best success stories of all time.

Mr. Onescu graduated with a Bachelor of Science degree in International Affairs and three Masters Programs in Economic Governance & Public Sector of Michigan University and Babes-Bolyai University and European Affairs & Project Management at Babes-Bolyai University. He is a PhD in a binational doctoral programme (Cotutelle PhD Program), at University of Strasbourg, France and Babes-Bolyai University from Cluj-Napoca, Romania.