The impact of security and intelligence policy in the era of cyber crimes

Bahri Gashi, Fadil Zendeli

MSc. Bahri GASHI, Dr.sc. Fadil ZENDELI

Abstract

Creation of National Cyber Defense Strategy, is the only security and the best protection against cyber-crimes. This is the starting point, from where adequate policies and necessary legal measures begin, aiming the creation of a solid ground and responsible users by implementing comprehensive measures and legal restrictions.

The methodology used to achieve the recognition of users with applicable legislation and regulations on the use of the Internet, as well as legal obligations; implementation of procedures to use communication systems; signing and approval by users of their responsibilities; knowledge and information on the risks and threats stemming from the use of communication networks; certification of trained and specialized staff; classification and processing of information in a particular system; identifying unauthorized users who use classified information networks in public systems and private sector; creating barriers in distance entry networks and information systems, etc.

Various Security and Intelligence institutions covering and operating in these areas are responsible for the creation and promotion of National Cyber Defense Strategy, analyzing the risk to implement protective measures for preventing attacks on Cybercrime (Cyber Crimes).

www.dx.doi.org/10.21113/iir.v6i1.211

ILIRIA International Review – Vol 6, No 1 (2016)

Key Words: Security, Crime, Cyber, System, Communication, Intelligence, Information

1. Introduction

Usually cyber attacks against the infrastructure of a country have targeted several key areas of life and society of a country such as energy, drinking water, fuel, gas, economic capital, etc,. Such actions may be carried out by criminals, by states or by individual criminals, who operate remotely from another state. Such attacks are categorized as cyber crimes, cyber terror or cyber war (NATO, 2009).

2. What is "Cyber-Crime"?

For the purposes of this study, we use the terminology "cyber-crimes" which means illegal activities of criminals where the basic purpose is financial benefit.

Such activities exploit weaknesses in the use of the Internet and other electronic systems, to gain unauthorized access or information, whether used by citizens, businesses or government. (Cabinet Office Detica, 2011 pg.1).

The term "cyber-crime" means a range of malicious activities that exploit vulnerabilities in Internet usage systems and other electronic systems to gain unauthorized access or information whether used by citizens, businesses or government.

Attacks on information technology are classified as the third largest risk for US security, ranking immediately after the threats of nuclear war and weapons of mass destruction. These definitions are provided by the Center for Strategic and International Studies in Washington, report of 2009 (NATO, 2009).

Protection of information due to the connection it has with the areas mentioned above, plays an important role in the country's national security and every threat should be considered a national threat. Protection and information security (cyber security) is linked to national legal obligations, in the context of being a member or co-operator with the United Nations Organization, Council of Europe, European Union, OSCE, NATO, etc. Harmonization and alignment of national legislation with that of the above structures, remains an area where state institutions must do more.

Presenting commitment to information security issues at high levels of government, industry and civil society, it would allow Kosovo to continue its efforts to change and adopt new technologies, and improve national security policies and global economy.

Information space includes ongoing risk of attack, such as illegal telecommunications interference, electronic terrorism, pornography and other offensive content, theft by telemarketing, money laundering etc.

A part of this space is occupied by the internet, a part of the space of information, but researchers today tend to accept as equal the Internet and the information space. Because of the speed and the advantages that the Internet offers as part of the information space, it occupies a major place as a new communication technology.

There are other networks other than those mentioned above, such as networks LANs (Local Area Networks) and WANs (About Today, pg. 1). These networks are referred to as the intranet, because they are networks within a closed system. Such confined networks are mostly used in institutions that include military and financial field. These systems are used for the purpose of protection against attacks and threats to information, which often are secret in these institutions. Any distribution of information and its misuse in this closed system called intranet, which enters the area of information and communication, is a violation and is classified as a crime.

3. Attack risk perspective (Cyber Crimes) and historical evolution

In the 1960s, the first studies related to cyber-crime have been seen in newspaper articles and in this period this crime involved computer abuse, computer sabotage, computer espionage and illegal use of computer system. The first scientific study on this type of crime has started around the year 1970. In the mid-50s, a large number of businesses and state agencies created the processes of computer data (PCD), automated departments, which deal with administrative data entry. The main risk in that period was introduced electro-mechanical breakdown and poor computer programming (OECD, 2011, pg. 15).

In the `70s computer equipment costs were reduced dramatically, as well as programs for computers were at cheap prices, exactly in this period of time, the market for independent programs and their suppliers appeared.

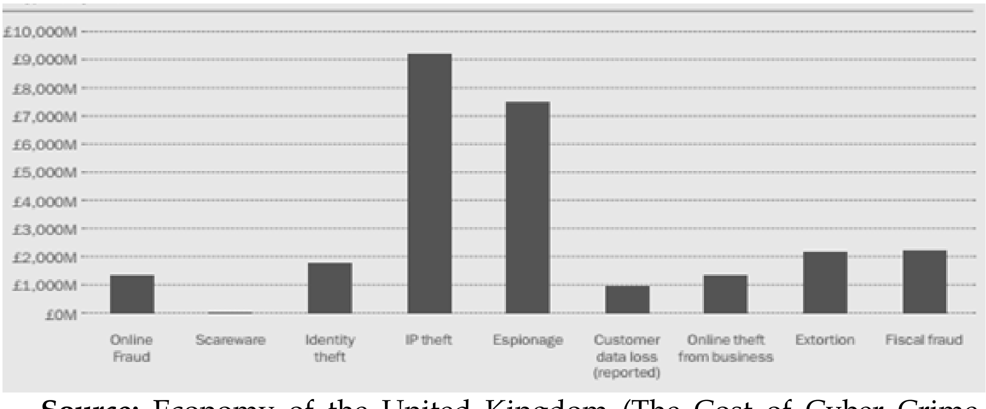
Over the `70s and ‘80s continued the trend of development and the use of computers. In the late '80s the use of computers was widespread both at home and in private companies, using the modems for external communications.

In the early ‘90s the development of web sites around the world, brought the increase of users, who were not intellectual or academic individuals. While in the period between 1993 and 1995, the Internet was completely open to commercial traffic and in 1996 was functioning in over 15 million computers. (OECD, 2011, pg. 15- 17).

If we speak in terms of risks and threats, this new information technology produced a new road or direction for criminal activity, which was covered by the possibility of anonymity, and many inexperienced users were exploited and deceived. The most important trend related to information security in business, is currently moving towards suspicious, not clear infrastructure.

A part of insurers secure more and more their customers, computer resources and capacity data storage, through various services such as Google Docs and Gmail. The market for providing these services is estimated at about 17 billion dollars in 2009, and is forecast to reach 44.2 billion dollars in 2013. (OECD, 2011, page 22).

Figure 1: The cost and different types of cyber crime



Source: Economy of the United Kingdom (The Cost of Cyber Crime, 2011 pg.2)

4. Cyber Crimes, Information Technology and Terrorism

Globalization process is known as accelerated economic, technological, political and cultural integration, thus involving transnational dimensions. (DAK web, Laurence E, 2003, faqe1). Globalization includes ethnic conflicts that exacerbate regional stability, terrorism, organized crime, drug trafficking, weapons of mass destruction. There are other risks that have not had an impact before, as the reduction of natural resources and hydrology, environmental pollution and the spread of infectious diseases, all of which impact on global security environment.

Besides the above mentioned risks, globalization brings people and countries together, through information and communication technology. Balkan region, Kosovo, Albania, Macedonia, mainly have developed several policies such as electronic government, free market economy, respect for fundamental human rights, regional cooperation in the field of security and economic development. According to Wassily Leontief through technology we may have benefits but also irreparable damages, such as: reduction of the number of jobs, increasing social concerns, and progress in economic development (Kegley, 2010, pg. 529).

Globalization today is associated with technologies such as mobile phones, encrypted e-mail, website and satellite systems, through which it becomes possible to connect the leaders of various groups, including terrorist groups, in order to have communication and disseminate information among them, but also have the right to use the funds and recruit groups of people to utilize them for terrorist attacks and threats.

Information terrorism is displayed as the dark side of the information revolution. Terrorism is a potential danger, but some terrorist organizations have done more acts of vandalism than bombings and explosives. Cyber terrorism risk is an expanding phenomenon, and part of it is the beginning of the war in communications. Terrorism today uses new teaching and different forms of organization, which affect the information revolution, resulting in consequences and damage to information technology system. (Arquilla, et al., 2000, pg. 179).

In the fight against terrorism and cyber-crime it is important to create a "dynamic policy" and the use of a strategic counter-communication plan that includes measures in law enforcement, military achievements, political, diplomatic, social and economic measures. These measures and the anti-communication plan must be implemented at all levels of government in collaboration with international partners to harmonize international achievements within a main strategy. (Magazine for Defense and European Security, 2010, pg. 19).

5. International policies in Cybercrime prevention

The "cyber-crime" and the attitude of countries towards the composition and prevention of this crime is an international challenge. Today's international organizations have built and created structures of information, one of them is the European Union and the office for "research and coordination of critical information infrastructure". This office has the task to test EU countries at how these countries protect their critical infrastructure against possible attacks of information.

This office also identifies research groups and programs based on information technology security at critical infrastructure.

The Convention on Cybercrime was adopted in 2001 by the Council of Europe and of a Consultative Assembly of 43 seats, located in Strasbourg. The Convention came into effect in June 2004. (Convention on Cybercrime, Budapest, 23 November 2001)

This convention is the first and only international agreement that deals with the problems of the law on the Internet and other information networks. The Convention requires the participation of countries in updating and harmonizing their laws on the crime of piracy, violations of copyright, computer fraud, child pornography and any other illegal activity. Out of the 42 countries that have signed the convention, ten countries have completed the ratification process.

The Bush administration submitted the Convention on Cybercrime to the Senate, to review and subsequently approve, in November 2003. On 26 July 2005, the US Senate Foreign Relations Committee approved the signed Convention. According to the US administration, the US will comply with the Convention based on existing legislation and in this case there is not required implementation of new legislation (Beka, 2013, pg. 20).

6. Conclusions

To achieve this standard of transformation, it is necessary the implementtation of several plans in the field of communication technology. These plans include the provision of a sustainable system of communication within the country and across borders in a global dimension. This requires communication technologies that benefit the country and of course the trained human recourses to use the information infrastructure.

In developing and transitional countries such as Kosovo it is an effort to walk the path of developed countries. These conclusions are the result of cyber security research and theories related to study conditions in developing countries and the effectiveness of programs that these countries have established. These analyzes lead us to a conclusion that a better approach starts with identifying the differences between developing and developed countries and how these changes affect the strategies of the country.

National cyber defense strategy in our country should contain successful approaches and models, some of which have been implemented in developed countries. In this strategy should be established and decided the creation of groups of national computer emergency response from the government, according to the EU model. This national group is defined as a government organization and has as its mission the protection of information technology and communication in cyberspace, especially government technology and critical local internet infrastructure. Developing countries are recognizing the value and importance of groups in national computer emergency response, as a structure that responds properly to any kind of cyber threat. In our country, we continuously need to establish a governing group, which will lead cyber defense policy.

The importance of establishing a strategy is mentioned above to describe how developing countries, as well as our country, must achieve the goal by including government actions and activities of the group of government or an institution established to protect cyberspace. The best strategy for our country would be building capacity cyber security in the period when required and is necessary. The conclusions show that the strategy of "cyber security" of a country must have the group or state agency to meet and perform the duties and responsibilities.

Despite international standards and models of organizations such as NATO and the EU are determined, the rules and their application are not the same in all countries.

By creating this strategy these changes may include our country, even though we are less protected in that area and are suffering less cyber-attacks compared with developed countries; we also have different and limited resources of which we can build a response to the attacks. Finally we can say that the impact of security and intelligence policies are postulated to identify current and future needs for the protection of cyberspace, constructed according to the needs of national security to prevent cyber-crimes.

List of References

About Today, "Introduction to LANs, WANs, and Other Kinds of Area Networks", Available from: http://compnetworking.about.com/od/basicnetworkingconcepts/a/network_types.htm [last accessed 05.04.2016]

Arquilla John, Ronfeldt David and Zanini Michele, (2000), Information-Age Terrorism, Current History. Available from: http://www.nps.edu/Academics/Centers/CTIW/files/info_age_terrorism.pdf [last accessed 28.03.2016]

Beka Rudina, (2013), Thesis, "Role of new information technologies in national security assistance". Available from: www.uamd.edu.al/new/wp-content/uploads/2013/01 [last accessed 25.02.2016]

Cabinet Office Detica "The Cost of Cyber Crime". 02.11.DET.CCR.001

Charles Kegley Jr., (2010), Global political trends and transformation, UFO University Press, 12th edition.

Council of Europe, (2001), "Convention on Cybercrime", Budapest. Available from: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf [last accessed 11.05.2016]

E. Rothenberg Laurence (2002-2003), "Issues in Global Education", No. 176. Available from: http://www.globaled.org/issues/176.pdf [last accessed 11.02.2016]

Magazine for Defense and European Security, (2010), "Concordian", Publication of the Center for International Studies G. Marshall and security in Garmisch. Terrorist Using of information technology, Germany.

NATO, (2009), Parliamentary Assembly, Report.

OECD - "Reducing Systemic Cybersecurity Risk" (2011).