Cyber security in Kosovo

Naim Baftiu
University "Ukshin Hoti" Prizren

Abstract

Internet cyber space represents one of the most important drivers of innovation, growth and competitiveness of national economies worldwide. This cyber freedom and human values should be protected in the same way as in the offline world. Digital infrastructure should be protected from potential incidents, misuse and malicious activities. Government institutions should have the leading role, set policies and guidelines to ensure not only the opening and the involvement of every citizen, but also the security of cyberspace.
In Kosovo, the use of information and communication technology (ICT) has expanded rapidly since 2000, while ICT is already playing an important role in all aspects of our lives. Internet penetration in Kosovo is 76.6%, which is very similar to the average of the European Union (EU), while the behavior of the citizens of Kosovo on the Internet appears to be similar to global trends. Most of Kosovo's institutions have shifted their daily chores online, including organizations that provide critical infrastructure sectors such as energy, water, health, transportation, and communication. These systems improve the quality and speed of services provided, by helping organizations that work in the most productive manner, thus contributing to the improvement of living standards. However, at the same time, they are exposed to different risks in the Internet space. These risks remain in violation inevitable in ICT, and can cause lack of service or misuse of services, resulting in damage (loss) potential of human lives, economic losses greatly, destruction of public order as well as threats to state security. Main purpose of this paper is to analyze the policies for the cyber security taken from the Government of Kosovo.

Keywords: Internet, security, services, Kosovo.

Introduction

Internet freedom and human values should be protected in the same way as off-line. Digital infrastructure should be protected from potential incidents and malicious acts. Public institutions have a major role, initially set guidelines and policies clear and transparent, to ensure not only the opening and the involvement of every citizen, but also security in cyberspace.
Referring to the "Analysis of the strategic review of the security sector in Kosovo", cybercrime as unconventional crime was identified as one of the risks, challenges or global threats that may affect the security of Kosovo. The Republic of Kosovo is committed to promote stability and security, not only domestically, but also be a significant contributor to the security of the region and beyond. Thus, international cooperation in the field of cyber security remains a priority for Kosovo. There is no harmonized definition of "cyber" and "cyber security". Meaning of cyber security and other important terms varies from country to country. In this chapter, the definitions of specific terms appear aligned with the underlying meaning of these terms in the

EU countries. The purpose of this list is to raise awareness of the general population to computer terminology.
"Cybernetics" (cyber) is defined as "anything that has to do with, or including, computers or computer networks (like the Internet)."
According to the International Organization for Standardization (ISO), "cyber" is a "complex environment arising from the interaction of people, programs and services on the Internet, through equipment networking technology related to it, which does not exist in physical form" .

Cyberspace

Cyberspace is the virtual space of all IT systems associated data at a global scale. Home cyberspace is Internet as universal network and publicly accessible and transport links, which can be supplemented and further extended to any number of other networks of data. IT systems in isolated virtual spaces are not part of cyberspace.[1]

Cybersecurity

In Cyber Security of the European Union (cyberspace open, safe and protected), "cyber security generally refers to protective measures and actions that can be taken to protect domain cyber, even in the civil and the military, from those threats related to or which may impair communication networks and interdependent infrastructure. cybersecurity strives to maintain the availability and integrity of networks and infrastructure, as well as the confidentiality of information held on them.

Cyber crime

According to the aforementioned Strategy of the European Union Cyber Security, "Cyber crime generally refers to a wide variety of criminal activities, where computers and information systems as a tool to engage either the primary or the primary target. Cyber crime includes traditional offenses (eg fraud, forgery and breach of identity), works on the content (eg Internet distribution of child pornography or incitement of racial hatred) as well as works that are unique computers and information systems (eg attacks against information systems, denial of service and malware (malware). " It consists of criminal acts committed in networks, via electronic communication networks and information. The problem is limitless, which can be classified into three broader definitions:

- Internet-specific crimes, such as attacks against information systems or phishing (ie fake banking site to obtain passwords that allow access to victims' bank accounts);
- Fraud and cyber counterfeiting, identity theft, phishing, spam, cloning of credit cards and other cards, as well as malicious coding;
- illegal content online, including materials with child sexual abuse, hatred, incitement to terrorist acts and idealism of violence, terrorism, racism and xenophobia.

Cyber attacks, cyber espionage and cyber sabotage

Cyber attack is an attack on IT in cyberspace, directed against one or more of technological systems in order to breach the security IT. Targets security, confidentiality, integrity and availability of IT can be compromised, individually or

[1] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52013JC0001.

in group. Cyber attacks against the confidentiality of an IT system, which performed or managed by foreign intelligence services, called cyber espionage. Cyber attacks against the integrity and availability of IT systems, called cyber sabotage.
Cyber protection is mainly used in a military context, but may have to do with criminal activities and spying. NATO uses this definition to explain cyber defense 'ability to protect the delivery and management services in Communication Systems and Information (CIS) in response to possible action, close but also incurred malicious arising in cyberspace ". Cyber protection consists of the following tasks: Protection, Detection, Response and Recovery.[2]
This way ensures continuous progress of cybersecurity, procedures and products, and in accordance with the changing circumstances in the immediate environment and wider.

Challenges, risks and threats to the security of cyberspace in Kosovo

Given that cyberspace is a space for possible criminal misconduct, has a number of risks and threats that threaten the safety of people in cyberspace of the Republic of Kosovo. Many of the risks and impacts of cyber incidents are common to the Government of the Republic of Kosovo and the private sector. The aim of the strategy is to mitigate cyber security risks, as well as those risks that do not tolerate extremely high impact. Primary risks and threatening elements dealing with ICT systems in the Republic of Kosovo are motivated by:

- Revenge, curiosity, conducted by staff within the organization or former employees (laid off) and the so-called "script-kiddies" (young people who use scripts ready for attacks);
- Monetary Benefits: The committed by organized crime;
- Spying activation: Cyber attacks dealing with seamless intervention of a third party in Communication Systems and Information, reading, changing, removing or adding information. Such interference can also be used to abuse the attacked systems of communication and information, and to attack other systems;
- National security: We conducted by state-sponsored actors;
- Terrorism: Cyber Terrorism has to do with efforts to target high level, made with terrorist purposes, which is an ongoing threat and has the potential to cause great damage. While terrorism is often associated with loss of life, we can not overlook important consequences as intimidation or impulse that may be caused by cyber terrorism.

Extremist and radical groups increasingly using cyberspace for organization and propaganda to promote their activities, recruit new members and organize terrorist acts, which constitute threats to the national security of the Republic of Kosovo.[3]
Critical Information Infrastructure is constantly targeted by cyber attacks. These attacks particularly targeted specific targets selected from terrorists and hackers

[2] *European Commission - http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime/index_en.html*

[3] *Trusted Introducer - https://www.trusted introducer.org/directory/country_ LICSA.html*

seeking sensitive information or that can destroy this critical infrastructure.[4]

Risks

- Lack of National Cyber Security Council with its functions;
- Do alignment CERT and CERT-s state other FIRST7 he introducer Trusts;
- Lack of knowledge and understanding of opportunities for cyber attacks that constitute a real threat.

Vulnerability

There is no proper safety and security in cyber space. However, the possibility of cyber attacks is much greater than the physical attack. Authorities and ordinary citizens in Kosovo have already been victims of cyber attacks, and of course that also will face such attacks in the future.

One of the biggest challenges lies in raising awareness of users since most of them use cyberspace. According to world statistics, the majority of cyber incidents are caused due to human error. As a result, the internal threat is very real.

Despite the limited direct impact, risks relating to cyber attacks can not be underestimated. National Cyber Security Strategy has the following strategic objectives:

- Protection of critical information infrastructure;
- Institutional development and capacity building;
- Construction of a public-private partnership;
- The response to incidents;
- International Cooperation.

Protection of Critical Information Infrastructure

It aims to create a safe cyberspace in the Republic of Kosovo, with specific actions and measures for the protection of critical information infrastructure, disruption or destruction of which would have severe consequences on vital societal functions.

Protection of critical information infrastructure will be part of the Law on Identification and Protection of Critical Infrastructure which will be developed in 2016. The public and private sector should create a base of strategic and organizational advanced based on exchange intensify information. Where necessary, and in case of specific threats, the protection measures will be required. Moreover, it will assess the necessity to harmonize the rules for maintenance of critical infrastructure in technological crisis.

Identification of critical information infrastructure

It is necessary to identify and assess critical information infrastructure in the Republic of Kosovo for the best protection possible. Critical Information Infrastructure will be identified and assessed based on a number of criteria defined, taking into account document ENISA's methodologies for the identification of assets and services Critical Information Infrastructure.

[4] *FIRST-it - https://www.first.org/members/teams*

The following steps will be followed to identify critical information infrastructure:

- Determination of the assets to be treated (eg, voice communications, data communications, data storage, data processing) that can be classified as critical;
- Identification of infrastructure that is technically necessary for the functioning of these services;
- Establishment of objective criteria for the level of protection required for each element of the infrastructure, the categorization of infrastructures and the use of criteria such as the number of users affected, the level of sensitivity of information concentrate, stored, transmitted or processed in those infrastructures etc.;
- Examination of criteria development scenarios that take into account the distortion of the selected functioning infrastructure, within regular activities.

Institutional development and capacity building

As access to safeguards is more biased, it is important to understand and accept that the maintenance of acceptable levels of security in cyberspace can only be achieved through cooperation between the different parties involved, within a reaction coordinate the different threats that have already been mentioned in the chapter.
Coordination of the relevant competent authority or government is absolutely necessary. This coordination is productive when done by an entity that is in a position to organize and coordinate the various actors and actions in Kosovo, the correct response to threats presented today, as well as new threats in cyberspace.
State Cyber Security Council should be set up to strengthen cooperation within the public authorities and cooperation between public authorities with the private sector, and to provide recommendations on strategic issues at the highest political levels.
The Council consists of representatives from the following institutions: Ministry of Internal Affairs, Kosovo Police, Kosovo Agency for Forensics, the Ministry of Security Force of Kosovo, the Agency of Kosovo Intelligence Agency Information Society, the Security Council of Kosovo, Ministry of Justice, Kosovo Prosecutorial Council, the Kosovo Judicial Council, Ministry of Finance, Customs Service, Ministry of Education, Science and Technology, Ministry of Foreign Affairs, Regulatory Authority for Electronic and Postal Communications, Central Bank of Kosovo. In special cases, it will include ministries, agencies and other institutions.
Business representatives will be invited as members as needed. Academic representatives will also engage in technical level. National Cyber Security Council aims to coordinate preventive tools and interdisciplinary approaches to cybersecurity in the public and private sector.

Special protective measures

We will work to promote a culture of cyber security throughout society, including cooperation with the educational system, industry, and the promotion of events as "European Cyber Security Month". Particular attention should be paid to government officials, the new generations as well as Internet users and continuous delivery of new programs for information security in all levels of education, in order to use advanced

information systems.[5]
These necessary measures be taken to facilitate:

- Management expertise and knowledge in the field of Internet, adjusting the training necessary flexibility in relation to threats faster and constantly changing;
- Participation in national and international simulation, training (workshops, courses, etc.); Providing an exercise program for cybersecurity testing and detail ment opportunities response events. Domestic and international training exercises play an important role in the development and assessment of cyber security capacity;
- Ways of awareness and information campaigns to be offered to all citizens of Kosovo;
- Provision of adequate courses for all parties involved, since it is important that the parties have sufficient knowledge in the field of cyber security. Therefore cyber aspects incorporated into existing educational curricula in Kosovo.

Human capacity for cybersecurity

In order to harmonize the activities and training of all institutions involved in this strategy will be drafted joint training curricula. The main goal is to organize training to improve coordination and cooperation between the institutions involved, but training will be organized for a specific institution or group.
The important part is to design scenarios and holding joint exercises, through which institutions involved will test their capabilities in response to the various challenges. Keeping these exercises will improve capacity in response to different threats, both nationally and institutional.

Technical infrastructure

Technical infrastructure plays an important role in strengthening cyber security in Kosovo and all institutions involved are committed to advancing information technology systems.
Among other things, TRA will establish a platform for the collection and registration of cyber incidents and Kosovo Police will advance equipment for investigating cyber crime.[6]

Research and development of cyber crime investigation

The Republic of Kosovo will continue to intensify research on IT security and critical infrastructure protection. Research and development capacities will be established within Kosovo, and will be used for participation in national and international projects, in accordance with available resources.
Research and development is a key element in improving the response of Kosovo to cyber security threats.

[5] *Strategjia Shtetërore për Sigurinë Kibernetike dhe Plani i Veprimit 2016 – 2019.*
[6] https://www.trusted-introducer.org/processes/registration.html https://www.first.org/membership/process.

In particular, they should establish procedures for sharing information with:

- Internet service providers;
- Banking sector;
- Energy Sector;
- Water Sector;
- Transportation (air and land);
- Academic field.

They should organize joint activities on cybersecurity education, which will focus on providing advice on cyber security curricula, certification of information security experts and further development of teaching modules.

Conclusions

Cybersecurity and providing full functionality of Computer emergency response teams (CERT / CSIRT) within Kosovo is an integral and vital part of security, but also the fulfillment of the commitments of the Government. The main functions-ve CERT / CSIRT States are preventing serious incidents related to security of networks and information, but also immediate reaction and convenient to those incidents when they occur.

For a high security in Kosovo are needed:

- the necessary infrastructure, and
- staff with advanced training relevant.

Cyber security policy should include more practical steps that an organization should take when an incident of cyber security. Tasks in the treatment of documented incidents are primarily directed towards providing information assets, while minimizing any damage as soon as possible. Beyond providing immediate protection for certain tasks facing the incident will reinforce the learning of the organization, and can assist in the prosecution and investigation of criminals in the area of cyber security. It is good practice to become exercises for dealing with incidents, as well as constantly updated procedures, so that when these are needed in the real world, be standardized, verified and reliable.

Kosovo will follow an active approach to international engagement in cybersecurity through:

- the signing of bilateral or multilateral agreements with key allies and other countries to strengthen cooperation in cybersecurity;
- participation in regional forums, with a focus on capacity-building initiatives within the region;
- membership in international organizations to assist in promoting international best practices and to develop and promote a coordinated global approach to combating cyber security threats, including "spam".
- AKI should make identifying threats that jeopardize the security of Kosovo. Threat to the security of Kosovo is considered the threat to territorial integrity, institutional integrity, constitutional order, stability and economic development, as well as global security threats against Kosovo.

References

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52013JC0001.
http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime/index_en.htm .
https://www.trusted introducer.org/directory/country_LICSA.html.
https://www.first.org/members/teams.
https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/Methodologies-for-identification-of-ciis.
https://www.trusted-introducer.org/processes/registration.html.
https://www.first.org/membership/process.