CYBER SURVEILLANCE IN BOSNIA AND HERZEGOVINA FROM THE PERSPECTIVE OF CYBER SECURITY PROFESSIONALS IN B&H

Professional paper

Anes Mirojević, Aleksandar Jokić, Mladen Peranović, Olja Božanović

AUBIH – American University in Bosnia and Herzegovina

Abstract

This paper project is about the issues concerning cyber surveillance in Bosnia and Herzegovina (B&H). It is an attempt to put into perspective the current status of cyber space and its surveillance, the issues at hand from a perspective of pioneer cyber security experts attending the master's program at the American University in B&H. It is an effort to answer the following questions:

1. *Is there any cyber surveillance in B&H?*
2. *What are the main struggling issues and challenges in B&H?*
3. *The perspective of cyber security and surveillance in B&H?*

Keywords: *Cyber surveillance, cyber space, critical infrastructure, Cert, security*

Introduction

In this project paper, we will try to answer the main questions proposed by a group of student working together in finding the right answers. The questions are:

1. Is there any cyber surveillance in B&H?
2. What are the main struggling issues and challenges in B&H?
3. The perspective of cyber security and surveillance in B&H?

First of all, keep in mind the fact that all involved in this project feel the need to develop a cyber-security strategy on a state level in B&H, and with that regard, the issue of cyber surveillance.

Starting at the point of the definition of cyber surveillance, we will try to answer the questions, propose concrete solutions and steps to be taken with a goal of reaching a solution for proper definitions of rules and regulations for the development of cyber surveillance in B&H according to the needs of the cyber space of which B&H is a part of.

Cyber surveillance has different motives and goals, especially when we take into consideration the world's super powers, but in this paper we will concentrate on the need to provide surveillance on a state level with the intention of protecting the common user and the critical infrastructure in B&H.

1. Definition of cyber surveillance and its uses

Cyber surveillance is a mechanism for the surveillance of persons, objects or processes that is on new technologies and that is operated from and on data networks, such as the Internet. Its purpose is to facilitate surveillance, in keeping with the quantity, rapidity or complexity of the data to be processed. As with surveillance as a whole, it refers to gathering and analysis of information in the persuit of various finalities-in particular, preventing cetain risks, orienting human behaviour and in the vent of a problem, locating the persons responsible. [1]

Cyber surveillance as is the case with any other surveillance, can be motivated with a number of various reasons. Nation states use surveillance methods to prevent the potential risks that might endanger a countries Critical Infrastructure (CI), to prevent and reveal crime and the persons involved in it. States are also using surveillance to gather information to prevent terrorist attacks, and sometimes to invade you privacy without your consent (this of course is hard to prove). It could be used for espionage, preparation for an attack of a criminal activity and etc. All of the mentioned can be and is used in cyber surveillance. Just to emphasize, cyber surveillance does not recognize physical boundaries of geo-locations and countries. When you connect to the internet, you never know which server you are using, for example when you access Facebook or for that matter, any web lo-

cation, or online service. This is one of the major reasons why cyber surveillance is a mulita disciplinary subject with very exciting rule-less environment.

Even though several countries like the USA, Germany, China, and Russia are trying to take control, it is impossible to do so. The rules and regulations we have in the physical world, simply do not apply to the cyber space. But still, countries are able to provide services in order of protecting their CI and their way of living, but it is a constant struggle to fight off all the challenges of the cyber world. This paper will concentrate on the creation of a positive environment of cyber security and cyber surveillance with all legitimate and noble intentions of protection of B&H citizens and the countries CI with the supporting entities.

2. Is there any cyber surveillance in B&H?

In the attempt to answer the first question, we have to look at the situation we have on the ground. Working from the smaller fragments up to the global view, we can start with the industries. First of all most of the industries and businesses in B&H have governing regulatory bodies which enforce rules with the intent of protecting the CI of a certain industry.

First of all we have the Internet Service Providers (ISPs) and the telecommunication companies, which provide the services of connecting to the cyber realm to their users. In B&H the governing body for these industries is the Regulatory Agency for Communications (RAC). The Bosnian RAC follows the general rules of the EU, since B&H is attempting to meet the EU standards. This is the case, because B&H has the goal of becoming a full member of the EU family. Other reasons are motivated by the geographical location of the country and its need to cooperate with the neighboring countries.

The ISPs and the telecommunication companies, are using their in-house cyber surveillance tools which are mandatory and as such enforced by the RAC for the companies and businesses in these fields of the industry , and if they do not meet the regulations, their license to operate will be terminated. Using different kinds of software tools to monitor the services and users they provide, the companies involved must report to the RAC. Besides the RAC, ISPs and telecommunication companies must cooperate with the state governing bodies, the police and other security agencies.

The information which they collect is provided to the state bodies and security agencies, mostly based on the court order.

The police and security agencies, which in B&H form a web of forces form Cantons, Entities and the state agencies. Both the Ministries of interior of Republic of Srpska and the Federation of B&H, try to cooperate on a local level with the intent of fighting crime. The police and security agencies, have established international connections and cooperate with other security bodies on an international level. For example, both of the ministries of interior are known for their cooperation with the American Federal Bureau of Investigation (FBI).

Unfortunately, the mentioned do not have a state monitoring body which conducts surveillance in order of prevention. Most of their efforts are triggered when a cyber-incident occurs.

The financial sector and Banks, are a very popular target for cyber-attacks. With the development of online services for Banks, online payments and the user of payment cards, have shown to be a very lucrative goal for cyber-attackers. It is because of this that the Federal Banking Agency and the Banking Agency of RS, have enforced rules and regulations for financial institutions, for cyber surveillance with the intent of preventing and discovering cyber-attacks and incidents which could lead to loss of data and money. These rules are enforced through the provisions of the Decision of Minimal Standards on Management of Information Systems in Banks [2], [3].

The standards cover major issues in respect to the protection of ICT systems in Banks, providing guidance on preventive measures and internal and external cyber surveillance on users and clients.

The most popular tool for conducting surveillance is the Security Information and Event Manager, called the SIEM. The controls are conducted by an independent body called the Information Security Officer (ISO). The ISO's job is to coordinate activities using surveillance methods for fighting and preventing cyber incidents. The ISO should work with the authorities and the Banks management board in order of maintaining control and enforcing preventive and reactive measures towards potential and executed cyber-attacks.

The trend in B&H is for any major organization to have an ISO, which is the case for organizations which control the CI. For example this is the case with electric power companies in the country.

Besides the mentioned, the ISO in an organization also must play by the rules of the national law on the Protection of Personal Data in B&H. Along with the Personal Data Protection Agency of B&H, the ISO surveilles the handling of databases and storages containing personal data for their protection in accordance with the law. This is a point where ISOs play the role of Personal Data Protection Officers in organizations. [4]

Still the only puzzles missing in order of full national oriented cyber security with cyber surveillance as part of it are the National Cyber Security Strategy (NCSS) and the national Computer Emergency Readiness Team (CERT).

So it is safe to say that there is to some extent in existence of cyber surveillance in B&H, but there is no governing body on the national level. B&H is the only country in Europe that does not have a national CERT.

3. What are the main struggling issues and challenges in B&H?

Cyber security experts in B&H are in most cases left to fight the challenges alone. It is only in the case of a cyber-incidents occurrence that other parties might get involved. The major issue is setting up cyber surveillance to prevent, assist and properly educate all in the fight against cyber treats on a national level in B&H. As mentioned before, B&H is the only country that does not have a national CERT. So we are left without guidance and assistance in the challenges we face every day. Along with the mentioned another problem evolves since it is very hard to ask for assistance on an international level, because only national CERTs are playing the role of a national point of contact.

On the other hand groups of enthusiasts have created communities where they share valuable experiences, information and knowledge which has given some results. Now we have a Cyber Security Center for South East Europe (SEECSC). Goals of this center is explained in the following: The SEECSC offers quality cybersecurity education, research, and services to overcome the region's challenges of securing and protecting the cyberspace. Our primary goal is to bring valuable projects to enhance region's capability in cyber security and further cyber security-related research and education activities in the region. [5] It is important to note that SEECSC is an international initiative coming from B&H, but including the countries of the region. (Croatia, Serbia, FYR Macedonia, Montenegro and Albania)

The financial sector with Banks in B&H has showed the initiative to cooperate on a national level where valuable information will be shared. It is not a secret that one of the goals is to create a CERT for financial institutions. As this paper is being written, the initiative has been passed to the Union of Banks in B&H (UBBiH). Banks from every part of the country want to be a part of this initiative, since the need has been discovered for a governing body on a national level. Since most banks in B&H are international banks, the realization of this initiative will also produce cooperation on the international level as well. Some international exchanges have are already been made with efforts to prevent cyber incidents which some countries in the region have experienced.

The third initiative is from the Ministry of Security in B&H, which has passed the initiative for the establishment of a national CERT to the respective government bodies. Unfortunately, the politicians in B&H do not see the global picture and this initiative is very slow in realization. But still we hope that it will see the light of day.

So the answer to the question at hand is that there are several struggling points to realize ideas on a national, state level, but progress has been seen in the last couple of years. As long as there are people fighting to reach the mentioned goals, there is hope.

4. The perspective of cyber security and surveillance in B&H?

Cyber security and cyber surveillance along with it is a new and young multi-disciplinary science in B&H. From the perspective of cyber security pioneers in B&H, we feel that there are several challenges and battles to be fought and overcome. The constant problem being mentioned in this paper is regarding national level activities and the lack of support.

One of the goals of this paper was to show that cyber security has a bright perspective in B&H like in every other country of the world. The constant growth of use of internet and its services, creates the need and motive to stay in the fight for this science.

Just the fact that this paper is being written as a part of a Master's program in cyber security, shows that steps are being taken in the right direction every day. The steps might be small, but they are significant.

B&H has a national strategy of becoming an EU member, which can be seen as a light at the end of a tunnel in the aspect of government involvement in the process of creating all the need tools, laws and regulations for a cyber-security 'aware' country. We hope that major improvements will be made towards reaching the mentioned goals, and that it will not be a case of reaction to a major cyber-security incident. This was the case with many other countries, and we hope that a national CERT and supporting cyber security tools will not be triggered by a serious incident.

Many cyber security specialists have left the country, leaving the fight behind in B&H, while proving to be very good at cyber security. This trend has had a fall in the recent years, since people in B&H are becoming more aware of the need for professionals in the fields of cyber security and information security.

We have a growing mass of security specialists taking up the fight to achieve goals which other countries have overcome in a much easier manner. The time has come to make the final push towards national level activities, and if the government won't make it, the industries and other levels of organizations will.

Maybe the steps taken in B&H towards cyber security are being taken from the inside out, but they are being made.

To conclude all of the mentioned, the perspective of cyber security and cyber surveillance in B&H is a bright one. All of those who know how the government apparatus is slow in B&H, might think otherwise, but it is our goal to prove them wrong.

5. Conclusion

Cyber surveillance to some extent exists in B&H. It is mostly driven by the private sector, but nevertheless it exists.

The challenges are being assessed and positive results can be seen by the day. Like it is with every science, it will be a constant struggle to meet the need of cyber security as a science.

Although there are no national level bodies to support cyber security at this time, it is just a question of time, when they will be formed. It is our job to support the efforts and make new ones in the process.

References

[1]http://www.dictionnaire.enap.ca/dictionnaire/docs/definitions/definitions_anglais/cyber_surveillance.pdf

[2] http://www.fba.ba/images/banke_podzakonski_2/BANKE_MINIMALNI_STANDARDI_13_bos.pdf

[3] http://www.abrs.ba/propisi/odluke/OdlMinStandUpravljInfSistemimaUBankama.pdf

[4] http://www.azlp.gov.ba/images/PropisiBOS/Zakon_o_%20zastiti_licnih_podataka_u_BiH_BOS.pdf

[5] http://seecsc.org/about.php#overview

CYBER NADZOR U BOSNI I HERCEGOVINI SA STANOVIŠTA STRUČNJAKA IZ OBLASTI CYBER SIGURNOSTI U BIH

Sažetak

U ovom istraživačkom radu će se govoriti o problemima vezanim za nadzor cyber sigurnosti u Bosni i Hercegovini (BiH). U radu će se pokušati staviti u perspektivu trenutni status cyber prostora i nadzora istog, postojeće probleme iz perspektive pionira stručnjaka iz oblasti cyber sigurnosti koji pohađaju master studij na Američkom Univerzitetu u BiH. Rad će pokušati dati odgovore na sljedeća pitanja:

1. *Da li postoji cyber nadzor u BiH?*
2. *Koji su glavni problemi u BiH?*
3. *Kakva je perspektiva cyber sigurnosti i nadzora u BiH?*

Ključne riječi*: Cyber nadzor, Cyber proctor, Kritična infrastruktura, Cert, sigurnost*

Received: November 27, 2015
Accepted: November 28, 2015
Correspondence to:
Anes Marojević
AUBIH – American University in Bosnia and Herzegovina
E-mail: marojevic.a@gmail.com