PRISHTINË Kolegji AAB

FACULTY OF LAW

DEPARTEMENT: CIVIL LAW

MASTER STUDY

THEME:

CYBERCRIME AS A NEW FORM OF CONTEMPORARY CRIME

Mentor:

Prof. Ass. Dr. Xhemajl Ademaj

Candidate:

Abdurrahim Gashi

Pristinë, 2015

KEY WORDS

Based on the methodology for the compilation of key words on this master thesis, there will be some few words given, or some key concepts and authors, as well as more specific ones.

Keywords:	Specific words:
Security	*Hacker*
Crime	*Phishing*
Cybercrime	*Software*
System	*Hardware*
Communication	*Cyber space*
Information etc.	*Net crime etc.*

Concept: Cyber Space "-" Cybercrime ", contemporary criminality is based on cases handled within the subject, and simultaneously replacing classical methodology in that technology, and it remains" The essence of cybercrime in the globalized world. " The strategic studies usually requires creating appropriate strategies, namely those national - national development and continuous updating of the war strategies against cybercrimes.

INTRODUCTION

Research on the topic "Cybercrime as a new form of contemporary crime" was chosen because in Kosovo there is no genuine study by experts who are familiar with two aspects: legal aspects and technical - technological aspects of IT field.

By bringing these two aspects and long experience in this field, we have proven to offer a serious topic of treatment for this phenomenon with great expertise.

Cybercrime is a new form of display to us, whereas as a result is much less studied and compared this type of crime with other countries.

OBJECT OF THE RESEARCH

The aim of the thesis is to have extensive knowledge on cybercrime, which to us is relatively new. Our lawyers, judges and prosecutors do not have enough knowledge about the form, development, mode of carrying out these criminal acts.

Another essence of this study is to achieve an understanding of cybercrime, forms, way of performing, the protection mode and the investigation method and combating cybercrime in Kosovo, which has as its objective to be a good basis for starting and expanding the study in this field.

When was cybercrime displayed? How has cybercrime emerged? What is cybercrime? Who can commit cybercrimes? With what can cybercrimes be done? To whom can such crimes be carried out? What can the attackers suffer? What do we need to know to protect ourselves against these crimes? Is it legal basis sufficient in Kosovo to fighting cybercrime?

All these questions that have arisen as hypotheses of analysis, while studies have been proven as stable during the processing of the topic: "Cybercrime as a new form of contemporary crime."

IMPORTANCE OF THE TOPIC

This topic has managed to acquire a new dimension to science and judicial practice in Kosovo, because of the recent increased commission of these offenses, but we have tried to explain, writing about the performance, the way of defense, legislation applicable to this field and providing the necessary information about what cybercrime is, and if you are a victim of this crime, where to announce and what steps should be taken.

Methodology: The research methods will be realized by the application of different methods of study, to achieve a satisfactory result in the elaboration of this topic.

Analysis: It is an appropriate method for the study of cybercrime in Kosovo.

Historical method: Has a particular importance, which will address the issue of cybercrimes in its historical view.

Comparative method: As a method of special importance of scientific methodology will help us in the elaboration and study of this issue.

Through its comparative cybercrime reports will be prepared by other countries of the world, the way of handling this phenomenon in other countries and other comparative aspects.

Inductive and deductive methods: Will help a lot in creating opinions and thoughts on the subject.

Expected results: Upon the completion of this study, we believe that somehow have provided information for this area, making this area known for the academic world, which is still unexplored to us, to be more attractive and help legal experts as lawyers, prosecutors, judges, and employees, who are in charge of implementing the law as basic knowledge and much needed for cybercrimes.

FINAL REVIEWS

Recommendations and conclusions

The world which is becoming more and more virtual, for this reason, cybercrime, in other words, illegal interference in computer systems or personal address by hackers, is constantly increasing. The target of the attacks of this phenomenon, which is spreading rapidly in our country, it is becoming increasingly worrying. Among the key questions raised in this regard are: What are the risks? How can we guard against? What does the law provide to highlight cybercrime etc.

Relying on the treatment of this topic, I think cybercrime, as a new form of contemporary criminality, is a new topic to us and treated improperly, whereas cybercrime to us is a new phenomenon as it is worldwide. We should pay more attention to this phenomenon, because the method of detection is very difficult, and the consequences are enormous.

Obviously, we can conclude that the information technology industry in the future is the main axis of any cybercrime as such. Safety of technology, namely its systems are key in states and societies, also as a tool of globalization will remain and advance further in view of modern-day society, much more important is getting its role in the challenges of permanent threat to the security system.

The benefits gained from the new communication technologies have driven some developed countries to try to transform their society into an information society. To achieve this standard of transformation, it is necessary to implement some plans in the field of communication technology. These plans are to ensure a sustainable system of communication within the country and across borders in a global dimension. This requires communication technology, that bring the country benefits and certainly specialized human capital to use the information infrastructure. The issue lies in the fact on how many monetary power of our country will be available for the evolution of this technology? The Albanian state has invested in technology infrastructure, but lacks in terms of design and implementation of a defense strategy of cyberspace, so that investments made in this technology to return in monetary benefits for the country.

One of the issues addressed in this topic is the importance of establishing a national strategy for cybersecurity. Scientific research and analysis indicate that the impact of the creation of the national strategy for cybersecurity in the developing countries is vital, from which we as the new state should be taught.

This theme has supported the approximate comparison with developed countries and informs how developed countries like the US and EU countries can achieve concrete results towards cyber security problems. The countries that are in democratic transition, such as the Balkans countries and our country are trying to walk in the footsteps of development of developed countries, but still far from specific targets. These reviews are the result of the survey of cyber security problem and theories related to the studied conditions in developing countries and the effectiveness of programs that these countries have set as strategic priorities.

This analysis serves as a conclusion or a good orientation, from where you can identify the differences between developing countries and developed countries. These changes should affect the country's strategies for cybersecurity. National cyber defense strategy in our country should put emphasis on successful approaches and models, some of which have been implemented in developed countries.

Currently, Kosovo has the same ICT infrastructure as the developing countries, while developed countries like the US have critical infrastructure of developed information.

Kosovo also has the same level of difficulties and challenges as developed countries when it comes to information security.

Strategies and programs must be tailored to the country's needs and readiness to implement them without avoiding coverage of future needs of the country. This critical infrastructure, which today is not complete, will be designed and developed in the future, if Kosovo tries to keep up with the rapid pace of development in the field of information and communication technology.

Political and financial support in this sector would not be complete without the government's commitment, which would bring a reaction as a result of the creation of the strategy and supporting actions against cyber threats.

The conclusions show that the cyber security strategy of a country, must have the group or government agency to fulfill and perform the duties and responsibilities against cyber-attacks.

Methods to be trained are in relation to other aspects of a country, as it may be the relationship with the government and trained technicians and experts in this field. There are several areas where experience is necessary, as it can be through training and assistance provided for policy-makers, to build a national strategy, building national group skills to deal with the security of cyberspace, training for some users and network administrators in the country etc.

Kosovo should establish groups of responses to national emergencies computer (CERTs), similar to such national structures as in developed countries.

With the creation of the National Strategy on Cybercrime, Kosovo provides staffing and technological aspects, which include our country in protected areas and are trying to have the capacity to get defensive against cyber-attacks compared with developed countries, which have different sources from which we can build a system for responding to cyber-attacks.

This master study has tried to draw firm conclusions from the research paper, which tend to be as oriented recommendations for one of the main factors of cyber security challenges, technology, namely the challenges of cybercrime, as a new form of contemporary crime. At the same time, the role of new communication technologies is important in the economic development of a country's development, which also includes such areas of the economy that do not produce products of this technology, but have an indirect impact.

In conclusion, we can say that many of the global security resources are too expensive to deal with. However, this topic shows that the course of action in Kosovo, of course, for developing countries, there is the claim that the needs of this group are the same as in developed countries, but our country should identify current and future needs for space protection cyber, built according to our national security needs.