CYBER SECURITY ISSUES IN ALBANIAN HIGHER EDUCATION INSTITUTIONS CURRICULA

Author(s): **Enriko Ceko** [a]

[a] Dr. Canadian Institute of Technology. Director Scientific Research Unit. Street Xhanfize Keko 12

Abstract

Cybercrime and the phenomena accompanying, currently with international nature, targeting the main sectors of world economy, are main challenges facing individuals, families, societies and states, four main operators in the open market. An appropriate response to cybercrime, having a high and complete cyber security system, employing legal instruments, IT protocols and ISO standards related with this issue, is a priority.

Undertaking this research, a review of curricula and syllabuses of economic, law and IT faculties of public and private higher university institutions in Albania have been done, as well as discussing the issue with lecturers of Cyber Security, Cyber Law and Quality Management discplines on these HUI's too. Aims of this manuscript is evidencing the lack of scientific information about cyber security, cyber law and ISO standards for IT, Economy and Law faculty students in Albania.

The importance of this manuscript is related on improving the current situation of now day's students, which don't have skills, knowledge and competencies to enter in the labour market, when cyber security issues are the main risks of public and private sector operators.

This manuscript rises for the first time, awareness on offering a better curricula and syllabuses on the issue of cyber security in higher education institutions in Albania.

Keywords: *cyber crime, ISO standards, legal instruments, higher education institutions, curricula, syllabus, international agenda, etc.*

1. Introduction

Recently there has been a very large increase in the number of cybercrimes around the world, regardless of the level of development of countries. This has attracted the attention of many specialists in various fields, who have noticed that one of the ways to reduce the number of cybercrimes and cyber attacks is to improve the quality of curricula, programs and syllabi in study programs in educational institutions. high.

During conversations with industry representatives, faculty and students it turns out that information security education is a very important issue.

According to the leaders of higher education institutions, the development of programs, curricula and syllabi of IT protocols, cyber security, cyber security legislation and quality management is very important for the coming years.

There is a growing demand in the country for human resources equipped with full skills, knowledge and competencies in school for cyber security, IT protocols, cyber security legislation and quality management, given that having qualified human resources, knowledge and competence in the field of cyber security is already a matter of national security.

In the first place, educational institutions in general and those of higher education in particular must be careful about cyber security within these institutions, due to due to the protection of students' own data and on the other hand, educational institutions should ensure that their students gain sufficient skills, knowledge and competencies to enter the job market as professionals in relation to IT protocols, cyber security, cybersecurity legislation and quality management systems, to withstand the work pressure they will face when they start work and be able to solve problems that arise in their daily work related to these issues.

They need to have solid skills, knowledge and competencies related to cyber security and cybercrime to detect, cure and prevent cybercrime. For this, higher education institutions should provide interdisciplinary programs, curricula and syllabi related to IT protocols, cybercrime, cyber security legislation and ISO standards related to cyber security, compared to the current situation where these aspects are addressed separately.

2. Literature review related to cyber crime

2.1 Cybercrime, Infrastructure and Services

The Internet, this social, economic, political, environmental, cultural, sports, legal, etc., space, is one of the fastest growing areas of infrastructure development both in terms of techniques and technologies used. Nowadays information and communication technologies (ICT) have an increasing tendency towards digitalization. The growing demand for Internet services and multiple computer connections has led to the inclusion of technologies that did not exist years ago.

Also, nowadays, the main sectors of the economy such as electricity, transport, agriculture, health, education, etc. as well as public order and military protection services, are almost interconnected and interdependent with the use of ICT (Luiijf/Klaver . 2000) and they require standards to operate, ISO standards included.

Nowadays, for developing countries, not only the establishment of basic information infrastructure is required, but the availability of ICT also, as a main basis for the use and development of service networks, while application and respect of ISO standards is acute demand (Aggarwal. 2009).

Electronic communication has replaced letters, fax, etc. and the use of the Internet in economic terms, seen from the point of view of private operators is very important, because most of the private sector communication is realized through the Internet (Zittrain. 2006). Telephone services through internet networks are becoming more usable than communication via fixed and mobile telephony (Masuda. 1980)

Services provided through ICT by governments are increasing day by day. ICT applications, such as e-government, e-commerce, e-education, e-health and e-environment, etc., are opportunities for development, because through these services facilities are provided even for the most remote areas of country (Ndou. 2004). This helps reduce poverty and improve the quality of life of citizens, based on standards too (European Commission. 2009).

With an appropriate approach, many developing countries have managed to make successful investments in ICT, offering applications that improve the productivity of the economy and continuously improve the quality of products and services offered in a territory provided by market operators in a certain society and this in paralell with ISO standards application and respect. Given the right approach, context, and implementation processes, investing in ICT applications and tools and ISO standards can result in improved productivity and quality (Ceko. 2014, 2017, 2019). The costs of internet services and investments in this sector are already lower than comparable services offered offline. Some online services are already free such as, (1) free e-mail, compared to traditional mail, (2) online encyclopedia, (3) Wikipedia, etc., compared to books, on-line public services, compared to the public administration and the queue in the offices of various institutions, etc. This causes the number of users to increase steadily, including people from all walks of life, from those with the highest incomes to those with the lowest incomes. In the same time, cost of certification with ISO standards around the globe has ben reduced continuosly.

This is also the main reason why online identity theft, the act of seizing credentials and / or personal data, and the use for criminal purposes is today one of the main threats to the existence, to the quality and to further improvement of e-government and e-Business services (Molla. 2004)

2.2 Advantages and risks associated with these developments

The introduction of ICTs in many aspects of daily life and the combination of these services with each other and with other technologies, has led to the further development of the information society, offering even more opportunities for citizens and public and private entities too (Barney 2007). This in paralel wth ISO standards application.

Nowadays, the elimination of barriers to information is also seen as a support for freedom in general and political, economic and social freedom in particular, because information is passed on to stakeholders without filters and outside the control of state authorities.

Today's technology and atandards has brought significant improvement in the quality of life of citizens mainly in aspects of daily life such as the banking sector, online shopping, mobile services, development of television equipment, etc., but it is precisely these developments that are associated with numerous new and serious threats (Kellermann. 2020).

Practically, the supply of raw materials, water, electricity, or various controls such as traffic control, road, air, sea, etc., air conditioning systems, are intertwined with ICT (Comey. 2006). This means that in addition to threats to the individual or natural or legal entity, threats to society and its way of life are also increasing. This further increases the risk of attacks on information infrastructure and Internet services. This brings not only enormous financial damage, estimated at tens of billions of dollars each year, but also enormous psychological damage to our global society (Kellermann. 2020). Globally, it is estimated that each year the benefits of cybercrime are more than $150 billion, competing with drug activity, causing extensive damage to citizens and public & private organizations, damage and loss that for the last years are estimated to be at about $400-450 billion a year. It is already believed among specialists in this field that the costs of cybercrime are greater than the costs of physical crimes.

In the first steps of ICT development, the target of cyber attacks was critical infrastructure, now, nowadays, the target of cyber attacks is any kind of ICT infrastructure. This adds to the importance of taking action against these attacks and against cybercrime (European Commission. 2009).

2.3 Relationship aspects of cyber security and cybercrime

A distinction can hardly be made between cyber security and cybercrime, although in terms of terminology this has been realized. The 2010 UN General Assembly resolution states that cybercrime is a major challenge for cyber security. It is this security that is influencing to a great extent the continuous development and improvement of information technology and internet services.

International acts related to cybercrime and cyber security require in first instance protection of critical and non critical infrastructure, as an essential element for the country's security and sustainable development. Having a safer Internet, aimed at protecting public and private users, has become a priority policy in many different governments (Gercke. 2009, Gercke. 2013).

2.4 Infrastructure protection strategy.

Since cybercrime mainly targets the infrastructure on which almost all the activity of economic agents is built and supported, the fight against this crime is a very important component of cyber security at the national and international level. Cybercrime generally aims to gain access to information. Information can be ordinary and critical. The unauthorized use of ordinary and critical information can have very dangerous consequences globally (Sieber. 2005).

Efforts against cybercrime globally are focused on drafting and enacting appropriate legislation against the misuse of ICT for criminal purposes or other activities aimed at affecting the integrity of common infrastructure and critical national and international infrastructure and building (Dutta / De Meyer / Jain/Richter. 2006), applying and respecting standards, ISO standards included.

At the national level, coordination of actions related to the prevention, preparation, response and recovery from incidents is required by government authorities, while at the regional and global level, this means cooperation and coordination between partners, because it is impossible for a single country or a single government, however capable it may be, to develop technical protection systems or institutions, technologies and standards for educating users to prevent cybercrime, since the perpetrators may engage in criminal activity against a country or government from very long distances. For this reason, transnational cyber security strategies are needed to reduce the risk of cybercrime in a given country.

This is also the main reason why legal, technical and institutional challenges related to cyber security and cybercrime issues are global challenges, which can only be overcome through a coherent strategy, which takes into account the different role of stakeholders in the framework of international cooperation (Gercke. 2009. 2013).

Seen in this light, at the World Summit on the Information Society (ISSIS), in Provisions 108-110, (Tunisia Agenda for the Information Society), an International Action Plan has been defined. Also at the WSIS Summit in Geneva, the focus was on building confidence in the security of ICT use, launching the Global Cyber Security Agenda (GCA), which serves as a global framework for international dialogue, to enhance partnership and cooperation. between governments, industries, regional and international academic and research organizations - to coordinate international action and response, to increase cyber security and information society security globally.

The Global Cyber Security Agenda has five areas of activity:

1. Legal measures
2. Technical and procedural measures, standards
3. Organizational structures
4. Capacity building
5. International cooperation

However, today more than ever it is successful that the fight against cybercrime is not just a matter of a few individuals or a few agencies, but is a very serious issue that requires a comprehensive approach, not just focusing on technical measures, because these measures only and alone, cannot prevent cybercrime, but it is imperative that law enforcement agencies be allowed to investigate and prosecute cybercrime.

This brings us to another challenge, which is the legislative challenge through which we can tackle criminal activities carried out over ICT networks. This requires technical and procedural measures and standards, designed and accepted internationally, technical and procedural measures and standards that promote the adoption of appropriate approaches to improve security and risk management in cyberspace, including accreditation schemes, protocols and standards.

We mention here ISO standards:

- **ISO 20000-1: 2011** - Information technology -- Service management
- **ISO/IEC 27000:2016** - Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary
- **ISO/IEC TR 27019:2013** - Information technology -- Security techniques -- Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry
- **ISO/IEC 27006:2015** - Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems
- **ISO/IEC 27013:2015** - Information technology -- Security techniques -- Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
- **ISO/IEC 27007:2011** - Information technology -- Security techniques -- Guidelines for information security management systems auditing
- **ISO/IEC 27009:2016** - Information technology -- Security techniques -- Sector-specific application of ISO/IEC 27001 -- Requirements

- **ISO 27799:2016** - Health informatics -- Information security management in health using ISO/IEC 27002
- **ISO/IEC TR 27015:2012** - Information technology -- Security techniques -- Information security management guidelines for financial services
- **ISO/IEC 27017:2015** - Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- **ISO/IEC 27001:2013** - Information technology -- Security techniques -- Information security management systems – Requirements
- **ISO 22301 – 2016** – Business continuity Management System, Requirements

These are the main standards developed by International Standards Organization related to information technology, IT security, etc, which leads to protection against cybercrime and for a better, safe and qualitative cyberspace (Ceko. 2014, Ceko. 2017, Ceko 2019).

At the national, regional and international level, it is necessary to establish and put into full operation the organizational structures, whose work focuses on the prevention, detection, response and management of crises caused by cyberattacks, including the protection of critical systems and not critical information infrastructure.

This requires adequate capacity building that focuses their work on elaborating strategies to build sufficient capacity to raise awareness, transfer know-how, and place the goal of increasing cyber security on national policy agendas.

At the international level, work should focus on international cooperation, dialogue and coordination in dealing with cyber threats.

An important part of the cyber security strategy is also the institutional reform, which consists in the development of a suitable legislation in general and a suitable specific legislation for cybercrime, drafting the necessary material criminal provisions for the criminalization of acts of this nature such as are (1) computer fraud, (2) illegal access, (3) intrusion into the personal data and sensitive data of public and private entities, (4) copyright infringement, (5) pornography with and for children, etc (Wigert. 2012).

Although, in fact, in the Criminal Law / Code of most of the countries around the globe, there are provisions for similar acts committed outside the network and ICT, it does not mean that these provisions can be applied or transactionalized for criminal acts committed through the Internet and ICT (Gercke. 2007). This requires an analysis of the legal framework and standards in action with the aim of identifying potential gaps and filling these gaps with current, contemporary and appropriate legislation for the development of the country, combined with meeting the needs of law enforcement agencies with tools, equipment and appropriate technologies for identifying and investigating cybercrime (Yang, Miao. 2007).

In this regard, it should be borne in mind that perpetrators of crimes of this nature can act from almost any country in the world, taking measures to cover up and disguise their true identity, and in this case it is obvious that the means and the instruments needed to investigate cybercrime are quite different from those used to investigate crimes of a non-cyber nature.

At the national, regional and international level, it is necessary to establish and put into full operation the organizational structures, whose work focuses on the prevention, detection, response and management of crises caused by cyber attacks, including the protection of critical systems and not critical information infrastructure.

This requires adequate capacity building that focuses their work on elaborating strategies to build sufficient capacity to raise awareness, transfer know-how, application and respect of standards and place the goal of increasing cyber security on national policy agendas.

At the international level, work should focus on international cooperation, dialogue and coordination in dealing with cyber threats.

An important part of the cyber security strategy is also the institutional reform, which consists in the development of a suitable legislation in general and a suitable specific legislation for cybercrime, drafting the necessary material criminal provisions for the criminalization of acts of this nature such as are (1) computer fraud, (2) illegal access, (3) intrusion into the personal data and sensitive data of public and private entities, (4) copyright infringement, (5) pornography with and for children , etc.

2.5 Implications for developing countries

For developing countries, finding strategies and solutions to respond to the threat of cybercrime is a major challenge. Building a comprehensive strategy against cybercrime requires legal instruments, advanced technologies, standards and safeguards. Building a strategy is not a matter of time, but the creation and construction of technologies and safeguards requires a lot of time and funding, but it should be borne in mind that the long-term benefits of avoiding the costs and harms caused by cybercrime are very large and far exceed more initial costs for taking safeguards and making investments in advanced technologies and approving and respecting standards ISO standards included (Aggarwal.2009).

The need to protect individuals, families, businesses and governments is a basic requirement that all operators want, but not all of these operators are directly involved in this issue. Mainly directly involved in this issue are governments and through them law enforcement agencies and public agencies providing IT and ICT products and services as well as private IT and ICT operators, which in fact doesn't have any knowledge about ISO standards in this field mostly. This brings difficulties in promoting the activity of businesses in the sector of electronics, internet and online services (Ekundayo & Ekundayo. 2009).

Carrying out grafting on investments in cybercrime protection technologies has resulted in more cost and less effectiveness, compared to making solid and one-of-a-kind investments that result in lower costs, combined with the application of international standards in this field, ISO standards included.

3. Related works to higher education institutions connected with cyber security issues

Recently due to the increase in the number of cybercrime worldwide, regardless of the level of development of countries. This has attracted the attention of many specialists in various fields who have noticed that one of the ways to reduce the number of cybercrimes and cyber-attacks is to improve the quality of curricula, programs and syllabi in study programs in educational institutions. up.

Some of the works related to this issue are listed below:

A paper on the risk that higher education institutions themselves have due to cybercrime emphasizes the importance that these institutions themselves should pay to cyber security due to the violation of student data as one of the biggest sources of risk to higher education institutions. This was also observed in a survey of 154 higher education institutions, 40 of which reported that security aspects became much more important issues during the pandemic period.

The massive shift of the pandemic towards distance work and distance learning increased the risks of institutional security and privacy in many areas.

On the other hand, institutions should also be aware of how they are collecting and using student data, respecting transparent standards of data governance, as students expect their institutions to use their data ethically and accountable, but often do not understand how institutions use their personal data. With a focus on effective leadership and the implementation of technologies and practices to strengthen overall information security, higher education can emerge from the pandemic capable of managing cyber security risks that will undoubtedly continue to surface (Kelly. 2021).

In a book claiming that the technological revolution is not everything for universities, it is argued that the alleged technological revolution in education has not yielded the expected effectiveness and that the modernization of education is more complex than the modernization of any other product and / or service and does not can be done overnight (Reich 2020)

Another study, which is directly related to the curriculum, syllabi and programs in this field, states that cyberattacks exploit a number of technological and social vulnerabilities to achieve a malicious target. The emergence of new and sophisticated Cyber Threats requires highly skilled operators with solid knowledge about concepts and technologies related to cyber security and cyber security, but this requires agile learning methods, in addition to a highly demanding training process limited by complexity internal technology and wide range of application areas. Although the existing Cyber Security and Cyber Security curricula cover a wide range of training topics and strategies, the content of these programs lacks a specific aspect, such as the depth of education / training and its connection to professional development (Santos & Pereira. 2017).

Another paper states that to address the issue of cyber security there is an urgent need for cyber security professionals with adequate motivation and skills to prevent, detect, respond to or even mitigate the effect of such threats. For this purpose, in recent years, several educational programs have been created both at the bachelor and master level, in parallel with a number of initiatives undertaken in the field of cyber security to assist in the framework of cyber security education by the subjects of administration. public. Due to the interdisciplinary (and sometimes multidisciplinary) nature of cyber security, educational institutions face many issues when designing a cyber security curriculum (Mouheb & Abbas. 2019).

Another paper notes that the cyber security curriculum has improved dramatically over the last decade, from a few years ago to several training courses, now in a comprehensive computer science program at the bachelor and / or master level, making cyber security be already involved in undergraduate programs in computer science, information systems, etc., and, further, in some specific programs for cyber security, but this is not enough. The broad field of cyber security requires more specialized education, because employers require graduates to contribute in their daily work to certain areas and not only in the field of information technology or cyber security (Amin. 2016).

Another paper states that the ability to prevent successful cyberattacks against a nation's critical infrastructure depends on the availability of a skilled and educated workforce, made possible by education systems that can build such capabilities. While it is possible to hire foreign nationals or transfer many operations, this is not a sustainable solution and raises other concerns.

The current literature provides strategic guidance for the development of a national cyber security workforce; however, there has been relatively little research to identify the factors responsible for hindering the development of cybersecurity education in developing economies. Based on the qualitative analysis of data from 28 semi-structured interviews with heads of education from thirteen Ecuadorian institutions of higher education, it has emerged that the challenges faced by local cybersecurity education include: cyber security skills, structural skills, social integration, economic resources and governance capacity (Catota, Morgan, Sicker. 2019)

4. The core of manuscript

Cyber security risks are increasing in number and becoming more and more complex. This requires the public and private sectors to respond quickly, accurately and consistently to meet their strategic, operational vision, mission and objectives.

The pandemic period further encouraged the use of computers, laptops, smartphones, tablets, etc., such as those that are the individual and collective property of various entities such as individuals, families, businesses and government

In this context, public and private entities should take measures to ensure that their work is in line with the use of best cyber security practices.

However, it seems that in higher education things are not moving at the same pace to provide this response to cybercrime. This is not just about modernizing education in the technological field but about improving the curricula and syllabi of subjects related to cyber security, cybercrime legislation and field standards, including some of the ISO standards.

Although in some of the higher education institutions in Albania there are existing curricula and syllabi related to cybercrime, it seems that students studying in the fields of IT, law, economics, engineering, do not have interdisciplinary knowledge about this issue.

Although the existing Cyber Security curricula and syllabi cover many different topics, they lack interdisciplinarity.

Law students study the aspect of cybercrime only in relation to the Criminal Code, the investigation of cybercrime, the types of punishments, the extent of punishments given in such cases, without obtaining any knowledge about IT protocols and related ISO standards with cybercrime.

Students pursuing studies in the field of IT receive only information about IT protocols and receive no information about the legal aspects of cybercrime and nothing about ISO standards related to cybercrime.

Students of the faculties of economics and engineering, in the course Management (Total) Quality learn about ISO standards in general at best in one or two lectures, but learn almost nothing about specific standards against cybercrime and on the other hand do not receive no information regarding the legal aspects of cybercrime and IT protocols.

But, after all, in the labour market, mainly in the professions IT, lawyer, economist, engineer, etc., requires interdisciplinary skills, knowledge and competencies related to cybercrime and not just skills, knowledge and competencies, related only to the narrow field of study that these students have completed.

This requires the provision of curricula and syllabi that integrate aspects of IT protocols, cybercrime legislation and ISO standards related to cybercrime.

5. Analyzing situation related to curricula and syllabuses of cyber security, cyber law and quality management in higher university institutions in Albania.

There has been a real revolution in higher education in Albania, mainly in the field of information technology, a field in which before 1990 - 2000 there was no development that went hand in hand with developments in the international arena.

In the higher education in the country in the period 1990 - 2000 a lot of good work has been done in terms of improving the curricula and programs of special subjects mainly in the field of economics and justice, due to the intention to adapt studies in these fields. with the conditions of the market economy, when previously in these areas the view of the centralized economy and justice within the dictatorship of the proletariat prevailed.

Even in the engineering study curricula and programs a significant improvement was made to adapt the skills, knowledge and competencies of the students to those required by the labor market, given that the principles of these sciences are the same all over the world, regardless of systems.

Specifically, in 2006 with the opening for the first time of private higher education institutions in their programs and curricula, in the faculties of economics, the subject of Quality Management in bachelor and Total Quality Management was introduced for the first time in master (University College "Qiriazi") and further in some other HEIs also the course Management of operations and industrial quality in bachelor (Ismail Qemali University, Vlora), Total quality management in master (University "Aleksandër Xhuvani", Elbasan), Quality Management in Bachelor and Total Quality Management in Master (Professional Business Academy), Quality Management in Bachelor and Total Quality Management in Master (University College "Wisdom"), etc.

Then, over the years and with the emergence of cybercrime issues, in some HEIs, mainly private in the faculties and study programs in the field of information technologies, special subjects for cybercrime were introduced, courses were offered cybercrime training for students and professionals (Canadian Institute of Technology).

In parallel, in some private HEIs in the faculties of law were introduced in special subjects such as Criminal Law, etc., the concepts of cybercrime and then the module "Practical methods of detecting criminal offenses" in the course Practical methods of detecting criminal offenses, (Faculty of Law, University of Tirana, Integrated Program in Law, (Curriculum 2020 - 2021) and a program entitled "Integrated expert in the field of cybercrime (University College" Luarasi (curriculum 2020 - 2021) ".

Even in HEIs that have faculties of information technology in both bachelor and master programs are introduced courses of cyber security profile (Canadian Institute of Technology, University College "Luarasi")

However, in all cases, it appears that:

- Curricula, programs and syllabi of IT faculties do not contain information on aspects of legislation in the field of cybercrime and information related to ISO standards related to cyber security.
- Curricula, programs and syllabi of law schools do not contain information on aspects of IT protocols and information related to ISO standards related to cyber security.
- Curricula, programs and syllabi of the faculties of economics and engineering do not contain information on IT protocols and legislation in the field of cybercrime.

6. Authors contribution

This paper addresses for the first time aspects of curriculum improvement and syllabi of study programs and courses which are directly related to cybercrime, in higher education institutions in Albania, aiming to make these curricula and syllabi acquire a more interdisciplinary nature, including in the study programs of the faculties of IT, law, economics and engineering, in combination with information on IT protocols, cybercrime legislation and ISO standards related to cybercrime.

As the labour market requires a workforce equipped with skills, knowledge and competencies appropriate to the latest developments in public and private organizations, which have as one of their main objectives, security, in general, and security against cybercrime, in particular.

7. Recommendations:

1. Cybercrime and the phenomena that accompany this activity are challenges facing operators in the market, challenges that require appropriate response, for high and complete cyber security.
2. Cybercrime has an international nature, but it is very important that in each country, the responsible bodies create a complete picture of cybercrime phenomena, including descriptions of the crimes committed, aiming at explanations for the most common criminal offenses in the field of cybercrime such as hacking, identity theft, denial of service, cyber attacks, etc.
3. Clarification of issues of investigation and prosecution of these crimes, and analysis of different legal approaches regarding substantive criminal law, procedural law, digital evidence, international cooperation and responsibilities of Internet service providers, including issues of best practices, affect the fair resolution of these criminal offenses.
4. For developing countries, it is necessary and indispensable to pursue the international cyber security agenda, which requires (1) the development of national strategies for the development of cybercrime legislation, applicable and interoperable globally, (2) the establishment of infrastructure and (3) the appropriate legal framework and international standards, ISO standards included, as integral components of a cyber security strategy.
5. Higher education institutions in Albania in the field of IT, law, engineering and economy, have to work hard to prepare programs, curricula and syllabi in the field of IT protocols, cyber security, quality management, in IT, law, economic and engineering faculties and programs to offer interdisciplinary disciplines and modules where

skills, knowledge and competencies related to cybersecurity, cybercrime, cyber law, quality management and especially ISO standards related to cybersecurity should have been integrated.

REFERENCES

1. Aggarwal (2009). Role of e-Learning in A Developing Country Like India, Proceedings of the 3rd National Conference, INDIA, Com

2. Barney, Prometheus (2007). Wired: The Hope for Democracy in the Choudhari / Banwet / Gupta, Identifying Risk Factors in for E-governance Projects, (2001). Age of Network Technology, 2001; Wgarwal & Ramana, Foundations of E-government, page 270.

3. Brian Kelly (26th May 2021). Cybersecurity in higher education: going from 'no' to 'know'.

4. Ceko Enriko (2017). Total Quality Management. Wisdom Press.

5. Ceko Enriko (2014). Quality management tools. Planetar Press.

6. Ceko Enriko (2019). The importance for Albania fighting cybercrime.

7. Comey (2006). Internetworking with TCP/IP – Principles, Protocols and Architecture

8. Djedjiga Mouheb. Sohail Abbas April 2019). Cybersecurity Curriculum Design: A Survey. In book: Transactions on Edutainment XV (pp.93-107)

9. Dutta / De Meyer / Jain/Richter (2006) The Information Society in an Enlarged Europe

10. Ekundayo / Ekundayo (2009) Capacity constraints in developing countries: a need for more e-learning space? The case of Nigeria, Proceedings ascilite Auckland, page 243;

11. European Commission (2009). Final Report on Study on Critical Dependencies of Energy, Finance and Transport Infrastructures on ICT Infrastructure

12. Faisal Amin (Feb 2016). Cybersecurity Education Challenges and Opportunities for Academic Institutions.

13. Frankie E. Catota, M. Granger Morgan and Douglas C. Sicker (2019). Cybersecurity education in a developing nation: the Ecuadorian environment. Journal of Cybersecurity, 1–19

14. Gercke (2006). The Slow Wake of a Global Approach Against Cybercrime, Computer Law Review International, page 141

15. Gercke (2013). Cybersecurity Strategy, Computer Law Review International, 136

16. Hayden (September 2012). Cybercrime's impact on Information security, Cybercrime and Security, IA-3.

17. Henrique Santos. Teresa Pereira (March 2017). Challenges and reflections in designing Cyber security curriculum. IEEE World Engineering Education Conference (EDUNINE)

18. Justin Reich (15th September 2020). Failure to Disrupt: Why Technology Alone Can't Transform Education Hardcover

19. Kellermann (2020). Technology risk checklist, Cybercrime and Security, IIB-2

20. Masuda (1980). The Information Society as Post-Industrial Society

21. Molla (2004) , The Impact of eReadingness on eCommerce Success in Developing Countries

22. Ndou (2004). E-Government for Developing Countries, Opportunities and Challenges, DJISDC, page 18

23. Luiijf/Klaver (2000). In Bits and Pieces, Vulnerability of the Netherlands ICT-infrastructure and consequences for the information society

24. Sieber (2005). The Threat of Cybercrime, Organized crime in Europe: the threat of Cybercrime

25. Wigert (2012). Varying policy responses to Critical Information Infrastructure Protection (CIIP) in selected countries, Cybercrime and Security, IIB-1

26. Yang, Miao (2007). ACM International Conference Proceeding Series; Vol. 113; Proceedings of the 7th International Conference on Electronic Commerce, page 52-56

27. Zittrain (2006). History of Online Gatekeeping, Harvard Journal of Law & Technology, Vol. 19, No. 2.