Policy Paper on Cyber Security 2015 - 2017

Republic of Albania

Tirana, 2015

Table of Contents

List of abbreviations……………………………………………………………...3

Definitions...……………………………………………………………………...5

Introduction..................……………………….. ………………………………..7

Current situation in Albania...9

Legal and institutional framework..……………………………………………..11

Vision, principles and strategic objectives……………………………………..19

Policies that should be followed...…………...…………………………………….21

SWOT Analysis (Strengths, Weaknesses, Opportunities, Threats)........................27

Accountability, monitoring and analysis...29

List of Abbreviations

ASPA	Albanian School of Public Administration
ASP	Albanian State Police
ALCIRT	National Agency for Cyber Security
CERT	Computer Emergency Response Team
CIIP	Critical Information Infrastructure Protection
CISD	Classified Information Security Directorate
CIRT	Computer Incident Response Team
CSIRT	Computer Security Incident Response Team
DCM	Decision of the Council of Ministers
ENISA	European Union Agency for Network and Information Security
EPCA	Electronic and Postal Communications Authority
EU	European Union
FIRST	Forum for Incident Response and Security Teams
GOVNET	Government Network
ICT	Information and Communications Technology
IED	Institute for Education Development
IMPACT	International Multilateral Partnership Against Cyber Threats
IRPDPC	Information Right and Personal Data Protection Commissioner
ISP	Internet Service Provider

ITU	International Telecommunications Union
NAEC	National Authority for Electronic Certification
NAIS	National Agency on Information Society
NATO	North Atlantic Treaty Organization
MoD	Ministry of Defence
MoIA	Ministry of Internal Affairs
MoJ	Ministry of Justice
MSIPA	Minister of State for Innovation and Public Administration
SIS/SHISH	State Intelligence Service
TAIEX	Technical Assistance Information Exchange
TF-CIRT	Task Force Computer Incident Response Team

Definitions

Computer system – is defined as every kind of device or group of interconnected or related devices, one or more of which, pursuant to a program, performS automatic processing of data.

Computer data – is defined as any representation of facts, information or concepts in a form suitable for processing in a computer system, including a suitable program to cause a computer system to perform a function.

Note: The above-mentioned definitions are taken from the Law No. 8888, dated 25.4.2002 "On ratification of "The Convention on Cyber Crime""

Computer network – is defined as a telecommunications network, which allows computers to exchange data.

Personal data[1] – is defined as every piece of information regarding a natural person, identified or identifiable, directly or indirectly, especially referring to an identification number or one or more specific factors for his physical, physiological, mental, economic, cultural or social identity.

Electronic Communications Service[2] – is defined as the service, normally against a payment, which is provided, in full or partially, from the transfer of signals via electronic communications networks, which includes telecommunications and transmision services in the networks that are used for radiotelevision transmisions and in the cable television networks, but excluding the services, which provide content through electronic communications networks and services, or that exercise editorial control over the content that is provided for transmision, making use of electronic communications networks and services. It does not include the services of information society, which do not consist fully or partially of transmision of signals to electronic communications networks.

Cyber space – is defined as the global virtual space of all the information and communications systems that are interconnected at the level of data.

Cyber threat/attack – is defined as every attempt that is directed/intended to get access, manipulate, interfere with or damage the integrity, confidentiality, security and/or availability of data of an application or data from a computer system, without being entitled to do this.

[1] LAW No. 9887, dated 10.03.2008, as amended "On Protection of Personal Data"

[2] LAW No. 9918, dated 19.05.2008 on "Electronic Communications in the Republic of Albania"

Cyber crime – is defined as the unauthorized interference with and/or through the use of ICT; the punishment for this offence is provided in the Criminal Code of the Republic of Albania[3]

Critical Information Infrastructure – is defined as the information and communications systems and networks, the violation or damage of which would have a serious impact on the health, safety, and/or economic wellbeing of citizens, and/or effective functioning of the economy of the Republic of Albania.

Cyber War – is defined as every act of war and/or around cyber space, which is connected mainly to the information technology.

Cyber-espionage – is defined as the cyber attack, whose object is to violate the confidentiality of an ICT system (e.g. digital espionage).

Cyber sabotage – is defined as the cyber attack, whose object is to violate the integrity and availability of ICT**.**

***Note:** The words 'computer' and 'cyber' will be considered the same in this document to the effect of standartization.*

[3] LAW No. 9859, dated 21.1.2008 "On some additions and amendments to the Law No.7895, dated 27.1.1995 "The Criminal Code of the Republic of Albania", as amended

LAW No. 10023, dated 27.11.2008 "On some additions and amendments to the Law No.7895, dated 27.1.1995 "The Criminal Code of the Republic of Albania", as amended

LAW No. 10054, dated 29.12.2008 "On some additions and amendments to the Law No.7905, dated 21.3.1995 "Criminal Procedure Code of the Republic of Albania", as amended

LAW No. 144/2013 “On some additions and amendments to the Law No.7895, dated 27.1.1995 "The Criminal Code of the Republic of Albania", as amended

Introduction

The fast developments of the Information and Communications Technology and the extent of its use almost in all the areas of the activity of society, have highlighted the need for safe and reliable services. The increase in the use of ICT and Internet is changing the society by creating new ways of connection, communication, cooperation and economic development through the access to cyber space. This has made our society more and more dependant on the use of these technologies.

In addition to the positive elements, the access to cyber space increases the potential risk for the damage or misuse of data and computer systems. As a consequence of the increase of cyber risks, the security of the integrity of data and confidentiality and a safe access to the cyber space have become one of the biggest challenges, which our society has to face nowadays, turning it into an issue of national security.

Albania ranks one of the countries where the development of telecommunications, access to Internet and informatization of the society is advancing very quickly. The increase in the use of communication represents an added value for the economic and social development of the country, but at the same time it makes it vulnerable to cyber attacks against state and private actors. The cyber attacks have the potential to seriously damage the exchange of information between the public institutions, the telecommunication and financial and banking system, by interrupting also vital services.[4]

This document is developed in support of the new Investment Program of the Albanian Government on ICT:

- Improvement of services that are provided to the public;
- A safe information society; and

The National Security Strategy 2014-2020 (a paragrah is cited from this strategy '...on setting and complying with the highest standards for the retention and protection of information in all the forms that it exists, by focusing special efforts for the protection from cyber attacks').

[4] National Security Strategy (NSS), 2014 – 2020

This document is also in line with the Digital Agenda for Europe 2020 (a sentence is cited ... The increase of the trust in ICT through strengthening the security policy for the networks and information) as well as in line with the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace).

The purpose of this Policy Paper is to review and coordinate the obligations that stem from the commitments that are undertaken for a safe cyberspace, in order to ensure fulfillment of responsibilities of all the actors in a coordinated way. In this way, the further development of the information society could be ensured as a safe, reliable and open environment as well as the promotion of the values and opportunities provided by the use of cyber space.

Following an analysis of the current situation and developments, this document defines the vision and the objectives for the development over the period 2015-2017 and provides the main directions of the policies that will be followed in order to achieve these objectives. The document is based on the best European models and practices with regard to the objectives and solutions that are foreseen, always taking into consideration the specific features of the Albanian society and economy.

There is an Action Plan attached to this Policy Paper, which is going to be reviewed at least once a year. The main documents where the Policy Paper on Cyber Security 2015 – 2017 is based on are as follows:

- Digital Agenda of Albania (2014 - 2020)
- National Security Strategy (NSS)
- Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace[5]

All stakeholders from the public and private sectors are consulted in order to draft this document and assistance is provided also by the European Union experts throuth TAIEX.

[5] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace - Join(2013) 1 final - 7/2/2013

Current situation in Albania

The Cross-cutting Strategy on Information Society 2008-2013 (CSIS) approved by the DCM No. 59 dated. 21.1.2009, in addition to being a strategic document that defined the main directions and objectives for the development in the area of information society over the period
2008 – 2013, was the only document which briefly mentioned cyber security as one of the areas, which should be considered as a priority due to the vision of the Albanian Givernment to increase and develop E-Government through the provision of e-services.
Computer security was mentioned in the initiatives in the area of information society in the CSIS:

- Children's Online Safety and encourage the coordination of the process on Codes of Conduct
- Setting up the National Agency on Cyber Security (ALCIRT)
- Developing the Public Key Infrastructure and providing safe services

In accordance to the Law "On Protection of Children's Rights", "The Action Plan on Children 2012 -2015" approved by Decision of the Council of Ministers No. 182 dated 13.03.2012, the Albanian legislation in force and the best European practice in this area; "The Safer Social Networking Principles for the EU countries", published by the European Commission in February 2009 and the document on "The European Framework for Safer Mobile Use by Younger Teenagers and Children", signed by different mobile operators in Europe in February 2007, Albanian operators signed on 7 February 2013 "The Code of Conduct for the safer and responsible use of electronic communications networks and services in Albania".

Also, in the course of implementation of the Cross-cutting Strategy on Information Society 2008-2013 (CSIS), the National Agency on Information Society has provided the following services:

- Safe authentication and identification for 25 institutions, 2500 users;
- Safe Internet for 65 institutions;
- Automatic and central instalation of applications in 2000 PCs of the Ministeries that are in domain;

- Central management of anti-virus protection for 7 institutions, 1000 computers;
- e-signature through Public Key Infrastructure (PKI) for 2 institutions;

The use of Information and Communications Technology has considerably increased over the recent years. According to the data published by EPCA, the number of active users of mobile phone services reached approximately 3.7 million users by the end of 2013. The penetration rate of mobile telephony based on active SIM cards reached 130%.

The broadband Internet access has considerably increased by 14% during 2013 for fixed broadband connections as well as for mobile broadband, for modem card and USB connections 88 - 101% respectively during 2013. In total, the number of broadband subscribers (fixed and mobile) was increased by 36% during 2013.

The total number of fixed broadband connections reached up to 182.556 at the end of 2013 and the number of broadband service users based on mobile phones reached up to 1.231.269 at the end of 2013.

The number of Internet users in Albania is increased several times over the recent years. According to the data published by the International Telecommunication Union, the penetration of Internet in Albania over the last ten years has increased from 0.97% in 2003 to over 60% in 2013. [5]

Year	**2003**	**2004**	**2005**	**2006**	**2007**	**2008**	**2009**	**2010**	**2011**	**2012**	**2013**
Albania	0.97	2.42	6.04	9.61	15.04	23.86	41.20	45.00	49.00	54.66	60.10

In the meantime, the number of violations of the security of networks and information is increasing rapidly. This brings about financial losses and generates new risks and threats for the development of the Information Society. In this context, it is necessary to undertake measures for a safe development of the Information Society.

[5] Source: http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

Referring to the official statistics from the Albanian State Police on cyber crime, which is provided as an offence by the Criminal Code of the Republic of Albania, it results that **180** criminal offences were reported over the period January – December 2014; **76** of them are detected, with **86** offenders, **74** of them are on bail, **10** are arrested and **2** are at large. **108** criminal offences were reported over the period January – December 2013, **63** of them are detected, with **69** offenders, out of whom **58** are on bail, **9** arrested and **2** are at large.

Compared to the same period of the previous year, there were reported **72** criminal offences more, with **17** more offenders, **1** more arrested person.

Divided by criminal offences, the figures are as follows:

- Article 119/a, "Dissemination of racist or xenophobic materials via the computer system", **1** case is reported, the offender is not identified.
- Article 143/b, "Computer fraud", **49** cases reported, with **14** offenders on bail and **1** arrested
- Article 186/a, "Computer Forgery'', **28** cases reported, with **20** offenders, out of whom **4** are arrested and **16** on bail,
- Article 192/b, "Unauthorized Computer Access", **14** cases reported, with **7** offenders on bail.
- Article 293/a, "Unlawful Surveillance of Computer Data", **1** case reported with **2** ofenders on bail,
- Article 293/b, "Computer data interference", **33** cases reported with **16** offenders, out of whom **2** are arrested and **14** on bail,
- Article 293/c, "Computer systems interference", **4** cases are reported with **3** offenders on bail.
- Article 121 "Unlawful interference with privacy", **4** cases are reported, no offenders are identified
- Article 117, third paragraph, "Pornography", **38** cases reported with **14** offenders on bail.
- Article 121/a "Persecution", **4** criminal cases are reported, **3** of them are detected, with **2** offenders, who were tried on bail and **1** is arrested.
- Article 137/a "Theft of electronic communication network", **1** criminal offence is reported

and it is detected, with **1** offender, who is on bail.

- Article 149/a "Violation of Industrial Property Rights", **1** criminal offence is reported and it is detected; **1** offender has been tried while being on bail.
- **1** case is reported with **1** offender, who is on bail, for Slander, an offence which is provided for by Article 120 of the Criminal Code.

Divided by areas, the criminal offences are as follows:

No.	**Computer crimes**	**Reported**	**Detected**	**Total number of perpetrators**	**Arrested**	**On bail**	**Wanted**
1	In the area of technology and information	53	29	30	2	28	-
2	Via the computer network	127	47	56	8	50	-
3	**Total**	**172**	**76**	**86**	**10**	**78**	**-**

Divided by the Regional Police Directorates, the reported criminal offences are as follows:

No.	**Regional Police Directorate**	**Reported criminal offences**	**Detected criminal offences**	**Total number of offenders**	**Detained and arrested**	**On bail**
1	Durrës	7	1	1		1
2	Korca	4	2	2		2
3	Dibër	1	-	-	-	-
4	Berat	1	-	-	-	-
5	Fier	5	4	4	-	4
6	Elbasan	5	4	4		4
7	Shkodra	9	3	3	-	3

8	Kukës	2	2	3	3	-
9	Lezha	3	3	3	-	3
10	Tirana	61	27	31	6	25
11	Vlora	6	4	5	-	5
12	HQ	77	27	30	1	29
	Total of computer offences	**180**	**76**	**86**	**10**	**76**

In order to provide a suitable protection to the users and to increase their trust in the information technology and also to encourage the advanced and safe use of the ICT it is of particular importance to initiate amendments to the law.

Taking specific actions and measures is considered as very necessary, in order to make society aware of the potential risks in the area of security of networks and systems and to eliminate these risks, including protection of children from the unlawful contents in the cyber space.

The attacks against the critical information infrastructures at country level could have serious consequences on their operation, by causing also big financial losses, that is why the need arises firstly, to identify them and then to take strong security measures at the highest security level of these infrastructures, which are of vital importance for the operation of the society. [6]

[6] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace - Join(2013) 1 final - 7/2/2013

Legal and institutional framework

The fast development of ICT is conditioned also on adjusting the relevant legislation. In general Albania complies with the obligations that stem from the ASA in this area. There are some laws that regulate the criminal prosecution of computer crimes in the Republic of Albania, such as: the Law No. 8888 dated 25.04.2002 “On Ratification of the Convention on Cyber Crime”, which is reflected in the Criminal Code and the Law No. 9262 dated 29.07.2004 “On ratification of Additional Protocol of the Convention on Cyber Crime, for the criminalization of acts of racist and xenophobic nature that are committed via computer systems”, which is reflected also in the Criminal Code, respectively in the Law No. 9859, dated 21.1.2008 “On some additions and amendments to the Law No.7895, dated 27.1.1995”, "Criminal Code of the Republic of Albania" and the Law No. 10023, dated 27.11.2008 on Some Additions and Amendments to the Law No. 7895, dated 27.1.1995 "The Criminal Code of the Republic of Albania; and the Law No. 10054, dated 29.12.2008 On some additions and amendments to the Law No. 7905, dated 21.3.1995.[7]

The legal framework of government structures that deal with security and cyber crime in Albania

National Agency for Cyber Security (ALCIRT) is the central authority that identifies, foresees and take measures against cyber threats/attacks in accordance with the legislation in force.

The Classified Information Security Directorate (CISD) is the authority that checks and ensures the security of classified communications and information systems and approves their accreditation by issuing the Security Certificate for them.

The National Authority for Electronic Certification (NAEC) is the authority in charge of supervision of the implementation of the Law "On Electronic Signature" and sublegal enactments that are issued in accordance with this law. The NAEC accredits the providers of eletronic certification service.

[7] For other amendments to the Criminal Code refer to the Law No. 144/2013 “On some additions and amendments to the Law No. 7895, dated 27.1.1995 “The Criminal code of the republic of Albania”, as amended

[8] Other document for reference: DCM No.766, dated 14.9.2011 “On setting up the national Agency for Cyber Security (ALCIRT)”, as amended

The National Agency on Information Society (NAIS) is in charge of administration of the Public Key Infrastructure (PKI) and ensures compliance with Article 19 of the Law No.9880, dated 25.2.2008 "On Electronic Signature”. The Agency ensures safe authentication and identification, safe Internet and DNS for the public administration in the services that it provides at the Government Data Center.

The Albanian State Police is the institution in charge of prevention, detection and investigation of the criminal offences, among which are included also the criminal offences in the area of ICT, which are dealt with by the Computer Crime Section.

The General Prosecution Office exercises criminal prosecution against criminal offences in the area of cybernetics through the Cyber Crime Section. This structure checks the activity of the special units that deal with cyber crimes, which are set up at District Prosecution Offices.

The State Intelligence Service (SIS/SHISH) via the Cyber Crime Section is in charge to search, detect and analyse cyber crimes that threaten the national security.

The Ministry of Defence plays a role in the cyber security via the Computerization and Innovation Directorate, but also other institutions that are mentioned in the following paragraphs, which are subordinated to the Minister of Defence (DE and IPSA).

The General Staff of the Armed Forces of the Republic of Albania, the Communications Directorate is in charge of the development of Communications and Information Systems (CIS) in the Armed Forces of the Republic of Albania, based on the national, NATO and international standards.

The Directorate for Encryption (DE) is the National Authority for the Security of Communications and the National Dissemination Authority.[9]

The Intelligence Protection and Security Agency (IPSA) via the Cyber Protection Section and INFOSEC is in charge of foreseeing, identification and analysis of cyber threats that threaten the ICT systems of the Armed Forces of the Republic of Albania.

The Bank of Albania (BA) has the authority of the institution that has the exclusive right to approve the start of banking activity through issuing of licence and to supervise every subject, which has got the licence to conduct banking activity in the Republic of Albania.

[9] LAW No.8457, dated 11.2.1999 “On "State Secret" classified intelligence.

DCM No. 922 dated 19.12.2007 “On security of “State Secret” classified intelligence, which is generated, retained, analysed or transmitted in the communication systems (INFOSEC)”

DCM No.690, dated 5.10.2011 “On approval of the Regulation “On criphtographic protection of “State Secret” classified intelligence

In the area of security of his ICT systems, the subject sets objectives, strategies and security requirements and also approves procedures for the administration, operation, protection of the systems and data as well as for their disposal.

The Electronic and Postal Communications Authority (EPCA) supervises, checks and monitors the activity of the providers of the electronic communications networks and electronic communication services. The ECPA supervises the implementation of the necessary measures that are taken by the providers for the security and integrity of public electronic communication services and networks regarding the protection of personal data.

Information Right and Personal Data Protection Commissioner (IRPDPC) is the independent authority in charge of supervising and monitoring the protection of eletronic personal data in accordance with the law, in the course of their retention, processing and transmission, by complying with and guaranteeing the fundamental human rights and freedoms.

Other institutions that will support the achievement of the objectives of the documentt

The Albanian School of Public Administration (ASPA) is the institution that is tasked with the professional education and training of the employees of public administration. Trainings are focused on developing sustainable management capacities, increasing their level of accountability, establishing a cadre of professional, impartial and efficient officials to perform their functions. This institution will provide assistance to organize trainings for IT professionals of the public administration.

The Education Development Institute (EDI) is the institution that is charged with developing the ICT Curricula for pre-university education (k-12), which includes some very important sets of topics of the cyber security area, the content of which consists of safe use of Internet by pupils and teachers.

Pursuant to the DCM No. 303, dated 31.3.2011 “On setting up Information and Communication Technology Units in the relevant ministries and subordinate institutions”, there is an IT Directorate in each institution, which is in charge of security in ICT systems and in this context, it is also in charge of cyber security.

Vision, principles and strategic objectives

THIS DOCUMENT DEFINES THE FOLLOWING VISION:

For a safer, more reliable and more sustainable cyber space for the citizens, business and the Government, in support of the economic and social development of Albania.

The cyber space should be considered as a multidimentional area, with several layers and territories, beyond the national borders. The cyber security should be based on the following basic principles:

- **Protection of fundamental human rights, freedom of speech, personal data and privacy:** Cyber security could be efficient only in case it is based on the fundamental human rights and freedoms, pursuant to the Charter of Fundamental Rights of the European Union and universal values of the EU. Reciprocally, the rights of individuals could not be ensured without having safe networks and systems in place. Every exchange of information, when it includes personal data, should be made in accordance with the EU legislation on Data Protection and the Law No. 9887, dated 10.03.2008, as amended "On Protection of Personal Data" and should also take into consideration the rights of individuals in this area.

- **Providing access to all citizens:** Limited access and/or lack of access to Internet and the digital illiteracy constitute a disadvantage for citizens, taking into account that the digital world characterizes the activity within the society. Every human being should be able to access Internet and have an unlimited information flow. The integrity and security of Internet should be guaranteed in order to provide safe access to all.

- **Shared responsibility**: Cyber security can not be regarded as a problem that impacts or belongs to one institution, public institutions, private sector or to citizens. It is a problem that impacts all the areas of life and society. As such, it asks for necessary security measures by all the users of ICT and the cyber space.

- **Strengthening the cooperation and coordination**: Based on the shared responsibilities, it is necessary to increase the cooperation and coordination between all the actors. In order to achieve the goal it is necessary to strengthen of interinstitutional cooperation, the cooperation with the public and private sector and the cooperation with the academic world.

- **International cooperation**: The cyber space, as a space without borders, asks for an international cooperation and coordination, in order to ensure cyber security. Also, as Albania has joined NATO and the progress it has made towards EU membership, it is more and more an active partner of the initiatives and programes on cyber security and it should fulfil its commitments to the ally countries.

- **Administration of risk**: The increase in the use of ICT and the trend for an ever more interconnected world has increased the risks that we are facing. Albania will undertake the necessary measures for the administration of risk based on the best standards and practices, in order to ensure the cyber security.

- **Abiding by the values**: This document will serve as orientation to take all the measures, to develop the policies, standards, guides and procedures in order to ensure protection from the cyber risks, by complying at any time with the fundamental rights and freedoms and other democratic principles.

The strategic objectives that will be followed in order to achieve the vision and observe the above-mentioned principles are as follows:

i. Complete the legal framework in the cybersecurity area
ii. Raise the awareness of cyber security
iii. Increase the level of knowledge, skills and capacities for expertise in the cybersecurity area
iv. Identification and Protection of Critical Information Infrastructure (CIIP)
v. Developing and implementing minimum cybersecurity requirements
vi. Increase the investments in order to enhance security in the state networks/systems

vii. Strengthening the partnership with other counterpart structures inside and outside the country;

Policies that should be followed

Completion of the legal framework in the cybersecurity area

Pursuant to the developments and initiatives, the necessary measures will be taken to analyse, adjust and complete the legislation in the cyber area. The best practices from the world, recommendations and international initiatives in this area, especially those from NATO and EU, will be assessed on a continuous basis, by adjusting the measures in the cybersecurity area, in accordance with the commitments that are undertaken to international partners. If it will be deemed necessary, they will be adjusted and approved, thus ensuring the increase of cybersecurity and the fight against cyber crime. It results from the analysis that was conducted to develop this Document that there are some ambiguities in the existing legal and institutional framework, which need to be addressed in the course of completion of legislation, as follows:

a) Modernization of the legislation in force and reviewing it periodically in order to address cyber security connected to the developments of cyber space in Albania and harmonization with the international legislation, in order that the legislation that remains is suitable and effective. Initiatives will be undertaken in this context to encourage the use of qualified electronic signatures in electronic transactions as well as legal initiatives for the use of safe electronic identification, electronic seals in electronic government services, banking services, etc. in order to ensure the identity in the virtual world, being it for natural or legal persons. The wider use of Web Pages and Web Servers certificates will be encouraged also, in order to ensure the safe identity of web pages of public institutions and other private companies, which provide electronic services to citizens or other businesses in cooperation with public institutions.

b) Ordering/making it obligatory the periodic auditing and assessment of suitability and efficiency of the security of information systems, pursuant to the legal and regulatory framework in force.

These measures will be taken in order to complete the current legislation in force[11], which foresees auditing of state databases, leaving the systems in general outside the spectrum of action.

c) Education and raising the awareness of actors in the public and private sectors regarding the legal and regulatory framework in force.

d) Developing a unified reporting system for individuals and businesses to report cyber crimes, in order for the necessary measures to be taken and the institutions in charge of strengthening the law could define the level of impact of cyber crime on individuals and economy oin Albania.

f) It will be assessed on a continuous basis whether it is necessary to set up the relevant structures at other public administration institutions. Strengthening and the support to increase the capacities in the area of cybersecurity will be a continuous process, in order that the state could serve as a model in the area of cybersecurity.

g) Strengthening the institutions and increase in the security in the public administration by applying procedures and basic requirements that are accepted by all the actors.

h) It is very necessary to clearly define structures and procedures that will ensure coordination at political-strategic and operational level, by involving all the actors in the public or private sector.

Raising the awareness for cybersecurity

It is widely known that the majority of cyber attacks are successful as a consequence of wrong configuration or failure of ICT users to implement the minimum protection measures.

a) The Government will undertake initiatives and develop programs for the education and training of ICT users. These programs will include all the levels of public administration, such as: IT experts, administrators of systems and ICT, etc.

[11] LAW No. 10325, dated 23.9.2010 “On state databases” and the DCM No. 945, dated 2.11.2012 on Approval of the Regulation for "The Administration of state databases system"

b) Dissemination and publishing of information on the risks of the cyber space and issuing instructions and providing advice for mimimum security will be an ongoing process, which will aim at raising awareness and increasing the level of security of ordinary users. In addition to publishing information on these risks in the Web Pages of specialized institutions, a close cooperation will be established with the media in order for the public to be informed in the quickest possible way and to have access to information as widely as possible.

c) An assessment will be made on the introduction of educational programs in the pre-university system and conducting awareness campaings in order to increase and develop the culture for a safe use of cyber space.

d) Cooperation with the private sector, as one of the sectors that is mostly impacted from cyber attacks, will be strengthened by undertaking initiatives and joint projects. Raising awareness and implementation of standards from the private sector will be encouraged and supported. This cooperation will be increased especially with the electronic communications companies, Internet Service Providers, banking sector, energy sector, etc.

Increase the level of knowledge, skills and capacities for expertise in the area of cyber security

Activities are going to be organized in the short and middle-term period in order to increase the necessary human resources capacities in the area of cyber security. Regulations will be developed, which will include the concept of cyber security in the elementary schools, high schools and institutions of higher education. Auditing measures on cyber security in the internal auditing processes of the organizations will be discussed as well.

a) Attention will be paid to boost the technical capacities of human resources in the framework of strengthening the institutions. This will be achieved through trainings tailored to the needs, which will aim at developing the skills of participants to prevent cyber attacks, minimize the damages and provide an effective response to information security incidents.

b) Participation in international conferences, meetings, workshops and exercises related to cyber security.

c) Participation in the Multinational Cyber Defense Education and Training Project in the framework of NATO Smart Defence Initiative.

d) Arrange symposiums and conferences where the economic, social and legal aspects of cyber security will be discussed as well.

Identification and Protection of Critical Information Infrastructure (CIIP) in Albania

The development of technology and the continuous integration of the systems has resulted that some of the systems have become vital for the operation of the digital society, regarding them as critical infrastructure.

a) Developing the necessary procedures and processes for the identification, inventory and ensuring their security has become a priority. Developing and implementation of minimum procedures and standards will be mandatory.

b) Due to the fact that these are not only public systems, but could belong also to the private sector, the cooperation and exchange of information with the private sector will be encouraged in order to ensure the basic security for these systems. With reference to this objective, another very important aspect in addition to the protection of these critical systems, is the “resilience”, which will ensure continuity of business activities in cases of force majeure or different cyber attacks. The protection and resilience capacity of critical infrastructure and encouraging operators that own them to implement a full security architecture (including risk management and emergencies) will ensure effectivity, reliability and continuity of services that are provided by them.

c) Defining the legal/regulatory basis, based on which the providers of critical infrastructures should report about serious cyber incidents. An analysis should be conducted for every case (which is reported or not) as cyber crime, the reasons why did it happened and actions that should be generated and reflected into laws, regulations or procedures, in order to avoid the recurrance of the incident.

d) Encouraging and providing support for the certification of critical infrastrures according to the security standards.

Developing and implementation of the minimum requirements on cyber security

The increase of the security in the state administration, the increase in the use of ICT systems in the public administration and also ensuring their security is one of the priorities of this Document.

a) Standards, guidelines and procedures based on the best international practices will be aligned and approved in order to be implemented in the public administration.

b) It is a priority to develop and approve risk analysis procedures concerning security for the systems that are used and electronic services that are provided by institutions. The risk analysis will be an ongoing process and it will be conducted periodically. The implementation of these procedures will be one of the key elements to increase the level of cyber security.

c) Further development of procedures to coordinate investments in order to analyse security and harmonize projects at the design stage will be assessed.

d) Developing training and awareness programs in the area of cyber security for all the levels of administration is regarded as a process, which ensures the use and provision of digital services to the administration in a safe and reliable way.

Increasing investments in order to increase security in the public networks/systems

The increase in investments to increase security in public networks/systems will be a priority, in order to minimise their vulnerability and increase sustainability.

a) Public institutions will be encouraged to invest in computer hardware and softwares as proactive and reactive measures to ensure the systems that they administer.

b) Setting up BCCs (Business Continuity Centers) and DRCs (Disaster Recovery Centers) for public networks/systems will be encouraged.

c) Setting up a monitoring system will be encouraged, which will inform institutions on time about the cyber risks that threaten them, by monitoring 24\7 the most important network nodes, traffic and events that take place in the system, in order to enable drawing of conclusions from saved logs, without interfering with or monitoring the content.

Strengthening the partnership with other counterpart structures inside and outside the country

The coordination and cooperation of all the actors is the basic element to ensure success. Due to the dynamic and speed of the development of ICT, the cooperation with the private sector will be strengthened. The security could be increased and the ICT in the public administration could be further developed in consistence with the developments and trends of technology.

a) The increase of cooperation and coordination between the public institutions will be strengthened in order to ensure the interaction and coordination of security and minimizing the damages from cyber attacks.

b) The Albanian Government will support and take the necessary encouraging measures to strengthen the cooperation with the private sector regarding exchange of information on the vulnerabilities of ICT products and technologies, the new types of attacks, institutionalization of relations, developing plans of measures and coordinated actions and the mutual exchange of information regarding cyber attacks.

c) The increase of cooperation with the academic world will be encouraged and supported. The Exchange of information, analyses, experiences, developing joint projects and assessing security technologies and systems are considered not only as an opportunity to increase the cyber security in public institutions, but also as an investment for the development and boosting the capacities for the coming generations.

d) Albania supports and will be part of the international initiatives, which aim at increasing and strengthening the security. The cooperation will be strengthened especially with NATO and EU, by becoming an active member of the joint initiatives for cyber security. The membership of Albania in the well-known international cybersecurity organizations and associations and the increase of cooperation is a priority.

SWOT Analysis (Strengths, Weaknesses, Opportunities, Threats)

A SWOT analysis was conducted related to strengths, weaknesses, opportunities and threats that could impact on the failure to successfully implement the policy, in order to develop this document.

Strengths	**Weaknesses**
a. An approach that aims at strengthening the cooperation between the Government and the operators of the Critical Information Infrastructures b. Institutions that are committed for the implementation of the Policy Paper and institutions that are more and more aware of the risks that threaten the cyber space; c. A structured Action Plan, with definite mechanisms that will facilitate monitoring of the implementation of this document.	a. Lack of experience in the area of cyber security: i. Lack of strategy at national level in this area so far; ii. Lack of regulatory framework. b. The need for large investments in order to reach levels that are comparable to the region and EU; security has not been highlighted so far from the initial stages of setting up ICT infrastructures; c. The existing legal and institutional framework needs to be completed d. Lack of specialized and certified experts for the cyber security; e. Low level of knowledge among the population for navigating Internet safely.
Opportunities	**Threats**
a. There are already established structures in charge of different stages of the cyber security management process; b. Access to the best international practices and opportunities to be based on strategic regional documents as well as	a. Lack of coordination and will to fulfill the obligations; b. Fragmentation of resources and overlapping of investments.

documents from European partners and NATO; d. The investments from the Government in the area of ICT are increasing more and more in the area of technology as well as human resources.	

Accountability, monitoring and evaluating analysis

Developing the cyber security under the circumstances of an information technology that is changing daily asks for particular attention from the public institutions. They should define the necessary requirements and ways to speed up the proces of active involvement of the private and public sectors, in order to discuss the policies of this Document and to implement them efficiently.

Government Institutions play a leading role in terms of:

1. Completion of the legal framework in the area of cyber security;
2. Critical Information Infrastructures Identification and Protection (CIIP);
3. Developing and implementing the basic cyber security requirements;
4. Increase in investments in order to increase the security in the public networks/systems
5. Strengthening the partnership with other counterpart structures inside and outside the country;
6. Raise awareness of cyber security
7. Raise the level of knowledge, skills and capacities for expertise in the area of cyber security

The Government Institutions should develop the preconditions and should encourage the private sector, NGOs and especially the operators of the Critical Information Infrastructures to:

- Take part in the process of improving the legal framework in the area of cyber security;
- To be active in the process of identification of the Critical Information Infrastructures;
- To pay particular attention to the increase of human capacities;
- Take an active part in defining the minimum requirements for cyber security;
- Take part in meetings with representatives from public and private institutions in order to find solutions for important issues;
- Present projects and participate in public discussions on legislation;
- Take part in public – private partnerships;
- Increase participation in monitoring the results of this Policy Paper.

This Policy Paper will be monitored by the Interinstitutional Working Group for developing “The Policy Paper for Cyber Security”, which was set up according to the Order No. 120 dated

20.03.2014 issued by the Prime Minister, the Minister in charge of Public Administration and Innovation, The National Agency for Cyber Security (ALCIRT) and the Departament of Developing Programming, Financing and Foreign Aid at the Council of Ministers.

The preconditions for the efficient and successful implementation of "The Policy Paper for the Cyber Security 2015 – 2017" include:

- General consesus and the free will to implement the proposed objectives and activities;
- Promotion of "The Policy Paper for the Cyber Security 2015 – 2017" as well as its objectives for the public and private sectors and citizens;
- An efficient monitoring and assessment system in order to check whether the objectives that are defined in the Policy Paper are achieved;
- Encouraging cooperation between public authorities and becoming aware of the best practices in the region on a continuous basis.

The implementation of this Policy Paper will be based on the use of a number of indicators related to inputs, processes, products and the effects of the Action Plan. The indicators will be assessed periodically by the public institutions according to the division of work and their jurisdiction in the area of cyber security. The indicators will be collected by ALCIRT, according to the indicators defined in advance in this document for the fulfillment of every policy, in cooperation with different public institutions. Based on these indicators, the Minister in charge of Public Administration and Innovation will develop annual reports on the progress of Policy Papers; the annual reports will be made available to the public.

The process of setting up a monitoring system and the effective assessment will be supported by activities to strengthen human and structural capacities as well as investment in safer ICT infrastructures. Informing the public and monitoring the implementation of the Policy Paper and its results by civil society and the operators of the private sector will also constitute one of the basic elements of the monitoring and accountability system.