Information & Security: An International Journal

Bahiti & Josifi, vol.32, 2015 http://dx.doi.org/10.11610/isij.3210

TOWARDS A MORE RESILIENT CYBERSPACE: THE CASE OF ALBANIA

Rovena BAHITI and Jona JOSIFI

Abstract: The fast growth of the Information and Communications Technologies and the extent of their use almost in all areas of societal activity have highlighted the need for safe and reliable services. Albania is among the countries where the development of telecommunications, access to Internet and informatisation of the society are advancing very quickly. This adds value to the economic and social development of the country, but at the same time it makes it vulnerable to cyber attacks from state and private actors. In addition to the positive aspects, the access to cyber space increases the potential risk of damage or misuse of data and computer systems. As a consequence of the increase of cyber risks, the protection of data integrity and data confidentiality and the safe access to the cyber space have become some of the greatest challenges, which our society faces nowadays, turning them into matters of national security. Following an analysis of the current situation and developments, this paper highlights recent developments in the field and provides analysis the state of play in Albania. Challenges and solutions that are foreseen are also addressed in the paper, taking into consideration the specific features of the Albanian society and economy.

Keywords: safe internet, e-services, critical information infrastructure, cyber threats, CERT, policy, incident.

Introduction

The underlying motivation for conducting this study relates to the fact that Internet is a common resource and its security must also be a shared responsibility. Not a single individual, business or government entity is solely responsible for the security in Internet. Everyone has a role in securing their part of cyberspace, comprising the equipment and networks used in the process. Individual actions have a collective impact, which means that if the Internet is used safely, it is going to be safer for everyone.

Albania is among the countries where the development of telecommunications, Internet and computerisation of the society are progressing very quickly. At the same time, the cases of network and information security breaches are also growing rapidly. The cyber attacks can potentially severely damage the exchange of information with and among public institutions, in the telecommunication and financial sectors, more specifically the banking system, causing financial loss and disruption of vital services. These attacks create new risks and threats to the development of the information society. In this context, it was deemed necessary to take some steps for ensuring the development of the information society. Following international best practices, the setting up of National Agency for Computer Security (ALCIRT) was one of steps taken in response to the requirements of the day with regard to security standards. The following sections describe briefly some of ALCIRT's commitments and its ongoing initiatives to create a safe cyber environment for citizens, businesses and the government.

Background

Albania has a resident population of over 3 million people.[1] In 2014, in Albania there were nearly 3.5 million (3,473,361) mobile phone users and nearly 1.1 million (1,058,354) Internet users from mobile phones, which means that almost one third of the mobile users have access to Internet through their mobile phones. On the other hand, the percentage of Internet users is calculated to be over 60 percent of the total population.

The Cross-cutting Strategy on Information Society 2008-2013 (CSIS) was approved by decision of the Council of Ministers (CoM) no. 59 on 21 January 2009. In addition to being the strategic document that defined the main directions and objectives for the development in the area of information society over the period 2008–2013, it was the only document which briefly mentioned cybersecurity as one of the areas, which should be considered as a priority due to the vision of the Albanian Government to establish and develop an e-government framework and provide e-services.

Cybersecurity was among the initiatives in the area of information society in the CSIS including:

- Promoting children's online safety and encouraging the signing of a Code of Conduct
- Setting up the National Agency for Cyber Security (ALCIRT)
- Developing the Public Key Infrastructure and providing trusted services.

The best European practices in protecting children's rights online are embedded in "The Safer Social Networking Principles for the EU countries" of February 2009 and the "The European Framework for Safer Mobile Use by Younger Teenagers and Children," signed by a number mobile operators in Europe in February 2007. Albania transposed respective requirements by adopting the Law “On Protection of Children’s Rights,” as well as “The Action Plan on Children 2012 – 2015,” approved by decision of the CoM no. 182 of 13 March 2012. Furthermore, 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.”

In the course of the CSIS implementation, the National Agency of Information Society has provided the following services:

- Safe authentication and identification for 25 institutions and 2500 users
- Safe Internet for 65 institutions
- Automatic and central installation of applications for 2000 PCs of ministries that are in the .gov.al domain
- Central management of anti-virus protection for seven institutions and 1000 computers
- e-signature through Public Key Infrastructure (PKI) for two institutions.

The use of ICT has considerably increased over the recent years. According to data published by the Electronic and Postal Communications Authority (EPCA), at the end of 2013 the number of active users of mobile phone services reached approximately 3.7 million users.

The penetration rate of mobile telephony based on active SIM cards reached 130 percent. Broadband Internet access for fixed broadband connections has increased by 14 percent during 2013, while for mobile broadband, modem card and USB connections the increase ranged from 88 to 101 percent. In total, during 2013 the number of broadband subscribers (fixed and mobile) increased by 36 percent. The total number of fixed broadband connections reached 182 556 at the end of 2013, while the number of broadband service users based on mobile phones increased to over 1.23 million.

The number of Internet users in Albania has increased spectacularly over the recent years. According to data published by the International Telecommunication Union (ITU), the penetration of Internet in Albania over the last ten years has increased from 0.97 percent in 2003 to over 60 percent in 2013.[2]

Table 1: Internet penetration in Albania.

Year	**2003**	**2004**	**2005**	**2006**	**2007**	**2008**	**2009**	**2010**	**2011**	**2012**	**2013**
Albania	0.97	2.42	6.04	9.61	15.0	23.9	41.2	45.0	49.0	54.7	60.1

In parallel, however, the number of violations of the security of networks and information is also 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.

Referring to the official statistics from the Albanian State Police on cyber crime—treated as an offence by the Criminal Code of the Republic of Albania—180 such criminal offences were reported in the period January - December 2014, as compared to 108 between January and December 2013. This represents an increase by 72 offences, with offenders being 17 more, and the number of arrested persons also increased by one.

Legal and organisational framework

In order to provide appropriate protection to the users and to increase their trust in ICT, as well as to encourage the advanced and safe use of technologies, it is of particular importance to have relevant legislation in place.[3] In general, Albania complies with the obligations that stem from the Stabilisation and Association Agreement (SAA) with the European Union 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 of 25 April 2002 “On Ratification of the Convention on Cyber Crime,” which is reflected in the Criminal Code; and Law No. 9262 of 29 July 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,” also reflected in the Criminal Code, respectively in Law No. 9859 of 21 January 2008 “On some additions and amendments to Law No.7895 of 27 January 1995, “The Criminal Code of the Republic of Albania” and Law No. 10023 of 27 November 2008 “On Some Additions and Amendments to Law No. 7895 of 27 January 1995, “The Criminal Code of the Republic of Albania;” and Law No. 10054 of 29 December 2008 “On Some Additions and Amendments to Law No. 7905 of 21 March 1995.”[7]

Regarding the structuring of the organisations to deliver cybersecurity in Albania, several steps have been undertaken. In 2007, the National Agency for Information Society (NAIS) was established as a specialised agency on e-government and information society. E-governance developments during 2008-2014 were focused on the central level and mainly on the public Government to Business (G2B) and Government to Government (G2G) services, with e-taxation, e-procurement, e-customs, e-Driving licence among the main achievements.

In 2009, a cybercrime sector was established within the Albanian State Police, while in 2014 such a unit was formed within the Albanian General Prosecution.

The Albanian National Agency for Cyber Security (alias ALCIRT) was established in September 2011 as a public legal entity, under the Prime Minister's authority, with headquarters in Tirana, Albania. ALCIRT was created with the support of USAID's Albanian Cyber Security Program – a two-year initiative that helped build the Government of Albania's (GoA) capacity to prevent and respond to cyber security incidents. The project utilised the expertise of Carnegie Mellon University's Software Engineering Institute (SEI), which conducted a series of workshops and training to help key GoA and non-governmental institutions understand cyber security models, build skills to resist operational threats, and develop processes for managing cyber security incidents.

ALCIRT is the central authority that identifies, foresees and takes measures against cyber threats/attacks in accordance with the legislation in force. The organisational structure of ALCIRT is approved by orders of the Prime Minister. The Agency is funded by the state budget and from any other legitimate funding source. The Director of ALCIRT is appointed, dismissed and/or discharged by orders of the Prime Minister. The staff is composed of six employees (Director and five experts). ALCIRT's main tasks and responsibilities are to:

- Coordinate responses to threats and take countermeasures on cyber attacks;
- Act as the central point of contact for information exchange in the field of incidents/emergencies with analogous institutions (sectional CIRTs and international entities);
- Provide assistance on issues that may arise during computer incidents;
- Counsel, propose and collaborate with relevant governmental structures for designing and implementing specific procedures in order to increase the level of protection of data and networks/state computer systems against unauthorised activities and/or efforts to develop unauthorised activities;
- Conduct control/monitoring of the implementation of standards and procedures to protect data and networks/state computer systems and, in certain cases, require specialised assistance;
- Participate in the preparation of the national strategy for data security and networks/ state computer systems;
- Participate in the preparation of the legal basis on issues related to the field of ICT security and computer crime in particular;
- Cooperate in the field of computer security with other state institutions and international organizations, civil society and the private sector; and

- Organise awareness campaigns and trainings, publish information and educational materials on ICT security, provide safety tips for Internet users nationwide (i.e. to government, business and citizens).

Other relevant authorities

The National Agency for Information Society (NAIS) is in charge of administering the Public Key Infrastructure (PKI) and ensuring compliance with Article 19 of Law No. 9880 of 25 February 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 Centre.

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 issued in accordance with this law. The NAEC accredits the providers of electronic certification services.

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 taken by the providers for the security and integrity of public electronic communication services and networks regarding the protection of personal data.

The Information Right and Personal Data Protection Commissioner (IRPDPC) is the independent authority in charge of supervising and monitoring the protection of electronic 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.

Pursuant to decision of the CoM No. 303 of 31 March 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 cybersecurity.

Building a resilient cyber space

In early 2014, ALCIRT took the initiative and led an interagency working group for drafting the National Policy Paper on Cybersecurity. The document is nearing completion and is expected to be approved soon. In this document, GoA has assessed the current situation and the trends related to cybersecurity in the country. The Government of Albania is currently implementing, under the leadership of the Minister of Innovation and Public Administration, several programmes to increase the digitisation of government services for citizens. The ability to protect these new systems and

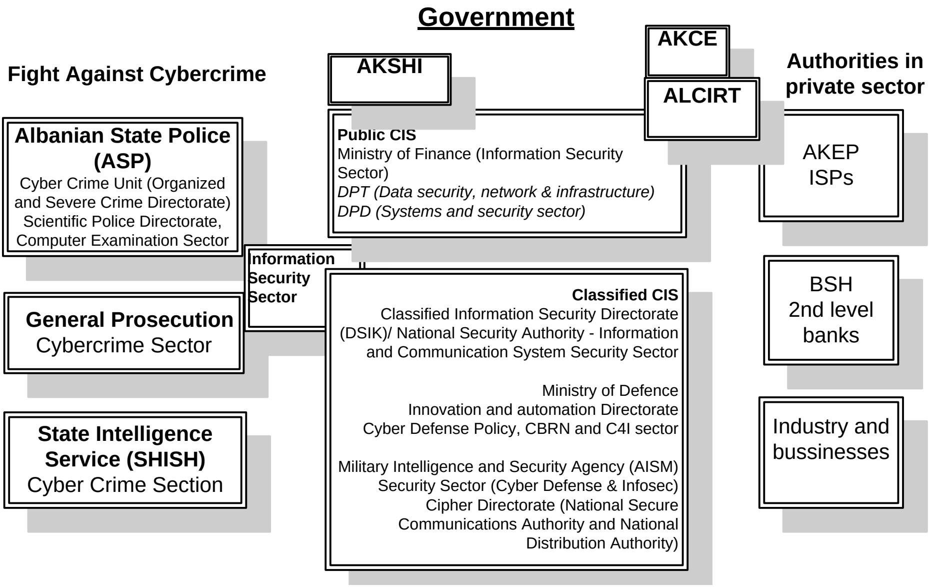
Government
Fight Against Cybercrime
AKSHI
AKCE
ALCIRT
Authorities in private sector
Albanian State Police (ASP)
Cyber Crime Unit (Organized and Severe Crime Directorate)
Scientific Police Directorate, Computer Examination Sector
Public CIS
Ministry of Finance (Information Security Sector)
DPT (Data security, network & infrastructure)
DPD (Systems and security sector)
AKEP
ISPs
Information Security Sector
General Prosecution
Cybercrime Sector
Classified CIS
Classified Information Security Directorate (DSIK)/ National Security Authority - Information and Communication System Security Sector
Ministry of Defence
Innovation and automation Directorate
Cyber Defense Policy, CBRN and C4I sector
Military Intelligence and Security Agency (AISM)
Security Sector (Cyber Defense & Infosec)
Cipher Directorate (National Secure Communications Authority and National Distribution Authority)
BSH
2nd level banks
State Intelligence Service (SHISH)
Cyber Crime Section
Industry and bussinesses

Figure 1: Institutional roadmap in the field of cybersecurity in Albania.

services is becoming increasingly important for Albania. The document is developed in support of the new Investment Programme of the Albanian Government on ICT, which envisages, among others, the improvement of services that are provided to the public and a safe information society.

The National Security Strategy 2014 – 2020, in line with the Digital Agenda and the Cybersecurity Strategy of the European Union for Europe 2020, also deals with the issue of cybersecurity, and in particular with "...setting and complying with the highest standards for the retention and protection of information in all the forms that it exists, by making greater efforts for the protection from cyber attacks."

The purpose of the policy paper is to review and coordinate the obligations that stem from the commitments undertaken for a safe cyberspace, in order to ensure fulfilment of responsibilities of all the actors in a coordinated manner. In this way, the further development of the information society could be ensured in a safe, reliable and open environment, benefitting from the opportunities provided by the use of the cyber space. Following an analysis of the current situation and developments, the policy paper 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, taking into consideration the specific features of the Albanian society and economy. All stakeholders from the public and private sectors are consulted in order to draft this document. Assistance is provided also by the European Union experts through TAIEX. The *strategic objectives* that will be followed in order to achieve the vision comprise the following:

i. Completing the legal framework in the area of cybersecurity;
ii. Raising the awareness of cybersecurity;
iii. Increasing the level of knowledge, skills and capacities for expertise in the cybersecurity area;
iv. Identifying and Protecting Critical Information Infrastructure (CIIP);
v. Developing and implementing minimum cybersecurity requirements;
vi. Increasing 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.

The cyber space is considered as a multidimensional area, with several layers, going beyond the physical national borders. In terms of this policy paper, cybersecurity should be based on the following basic principles:

1. *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.

2. *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 characterises the activity within the society.

3. *Shared responsibility*: Cyber security cannot be regarded as a problem that impacts or belongs to one institution, public institutions, the private sector or to citizens. It is a problem that impacts all areas of life and society.

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

5. *International cooperation*: The cyber space, as a space without borders, demands international cooperation and coordination in order to ensure cybersecurity. Also, as Albania has joined NATO and has made progress towards EU membership,

it is increasingly an active partner of the initiatives and programmes on cybersecurity and should fulfil its commitments to the allied countries.

6. *Risk management*: The increase in the use of ICT and the trend for an ever more interconnected world has increased the risks we are facing. Based on the best standards and practices, Albania is undertaking the necessary measures for the administration of risk in order to ensure the cyber security.

7. *Abiding by the values*: The policy paper 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.

Crossroads

Based on these developments and in line with NATO objectives in cyber defence, ALCIRT has constantly emphasised the importance and necessity of establishing CERTs in different institutions.

The increased use of ICT brings up the need for capacity building and increased interinstitutional cooperation for the prosecution and prevention of risks arising from cyber crime. Also, a close cooperation at regional and global level and the improvement of legislation for the security of networks and information in accordance to NATO and EU practice is needed (see also ENISA guidelines).

In order to fulfil the legal framework, ALCIRT has begun work on drafting a new law on security of networks and information systems. This involves dealing with many key issues, with focus on two of them:

- Establishment of a counselling body for strategic planning, responsible for supervising policy implementation, including all relevant entities in the cyber domain;
- Re-organising the process of incident response through the national CERT.

Creating and managing a computer incident response team, especially a national one, is not an easy task. In the case of Albania, two options are being considered:

- Using in-house capability: CERT capacity building as part of the permanent CIRT staff; or
- Outsourcing incident response efforts: Establishing a team composed by both public and private experts who will intervene whenever certain incident occurs. In the case of outsourcing, experts from the field may apply, regardless of where they work full time, and the selection will be carried out by a

special commission. Winners will be equipped with security clearance issued by the relevant authority.

To take the right decision, a number of key factors need to be taken into account:

- Number of incidents: Our statistics show that the number of incidents is increasing but is nevertheless still quite low. Hence, so far there is no need to keep regular personnel around to wait for incidents to occur.
- Cost: The overall cost of dealing with security-related incidents, due to their low number, is likely to be lower because the outsourced incident response personnel will need to deal only with incidents that do occur.
- Expertise portfolio: Outsourced experts usually will offer different professional capabilities that are often not available within one particular organisation.

Time and authorities' vision will show what needs to be done in what circumstances.

Conclusion

Pursuant to ongoing developments and initiatives, certain measures need to be taken in Albania, starting from analysing, adjusting and completing the legislation in the cyber arena. The best practices from the world, recommendations and international initiatives in this area, especially those from NATO and EU, are to be assessed on a continuous basis. Taking also into account 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, we see as crucial the development of programmes for education and training of ICT users.

The development of technology and the continuous integration of variety of systems made some of the systems vital for the operation of the digital society, i.e. they have turned into *critical infrastructure*. The attacks against national critical information infrastructures could have serious consequences for their operation, causing also significant financial losses. Hence, the priority task should be to identify and ensure the highest security level for these infrastructures, which are of vital importance for the functioning of the society.[4] Developing the necessary procedures and processes for the identification, inventory and ensuring their security has become a priority. The implementation of baseline security standards needs to become mandatory.

Increasing the investments to improve security in public networks/systems that are offering e-services to the public, is key in order to minimise their vulnerability and increase sustainability. Public institutions have to invest in computer hardware and software—both in proactive and reactive measures—to ensure that the systems that they administer will be less vulnerable and their functionality can be quickly restored in the wake of an attack. That includes setting up BCCs (Business Continuity Centres) and DRCs (Disaster Recovery Centres) for public networks/systems.

The coordination and cooperation among all the actors is the core element to ensure success. Due to the dynamics 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 and remain relevant to technological developments and trends.

Notes:

[1] In 2015, Albania's estimated population is 3 191 957, according to www.countrymeters.info.

[2] ITU Statistics, available at www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

[3] A list of relevant Albanian relevant laws includes:

- Law No. 9887, dated 10.03.2008, as amended "On Protection of Personal Data;"
- Law No. 9918, dated 19.05.2008 on "Electronic Communications in the Republic of Albania;"
- 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;
- Decision of the Council of Ministers No.766, dated 14.9.2011 "On setting up the national Agency for Cyber Security.

[4] European Commission and High Representative of the EU for Foreign affairs and Security Policy, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace," February 2003, available at: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf.

Rovena BAHITI is the Director of the National Agency for Cyber Security (ALCIRT) in Albania. *E-mail*: rovena.bahiti@cirt.gov.al.

Jona JOSIFI is an expert at the National Agency for Cyber Security (ALCIRT). *E-mail*: jona.josifi@cirt.gov.al.