REPORT ON CYBERSECURITY MATURITY LEVEL IN ALBANIA

CONTENTS

DOCUMENT ADMINISTRATION

Lead researchers: Dr Maria Bada, Mr. Faisal Hameed

Reviewed by: Professor William Dutton, Professor Michael Goldsmith, Dr Jamie Saunders, Professor Basie Von Solms and Professor Federico Varese

Approved by: Professor Michael Goldsmith

Version	*Date*	*Notes*
1	*9/10/2018*	*First Draft*
2	*31/10/2018*	*Submitted to WB*
3	*2/11/2018*	*Second draft addressing comments from WB*
4	*15/01/2019*	*Second draft addressing comments from Albania*

LIST OF ABBREVIATIONS

AF	Air Force
AKEP	Authority of Electronic and Postal Communications
AKCESK	The National Authority for Electronic Certification and Cyber Security
AKCE	National Authority for Electronic Certification
AKSHI	National Agency for Information Society
ALCIRT	National Cyber Security Agency (The national Computer Incident Response Team for Albania), now part of AKCESK
AMF	Financial Supervisory Authority (financial market regulator)
ANSP	Albania Air Navigation Service Provider or Albcontrol
BSH	Bank of Albania
CBMs	Confidence Building Measures
CEO	Chief Executive Officer
CI	Critical Infrastructure
CMM	Cybersecurity Capacity Maturity Model
CNI	Critical National Infrastructure
CPC	Criminal Procedure Code
CRCA	The Children's Human Rights Centre of Albania
CSIRT	Computer Security Incident Response Team
CSDP	Common Security and Defence Policy
DDoS	Distributed Denial of Service
DR&BCP	Disaster Recovery & Business Continuity Planning
DRC	Disaster Recovery Centre
DSIK	Department of Classified Information Security
ENISA	European Union Agency for Network and Information Security
ESDC	European Security and Defence College
EU	European Union
EUROJUST	The European Union's Judicial Cooperation Unit
GDPR	General Data Protection Regulation
GCSCC	Global Cyber Security Capacity Centre
HIDS	Host Intrusion Detection Systems

ICSE	International Cyber Shield Exercise
ICT	Information and Communication Technologies
IIIs	Important Information Infrastructures
IGF	Internet Governance Forum
ISSIS	Cross-cutting Strategy for the Information Society
ISO	International Organization for Standardisation
ISP	Internet Service Provider
ITU	International Telecommunication Union
LOTL	European List of Trusted Lists
MITIK	Ministry for Innovation in Information and Communication Technology
MoD	Ministry of Defence
MOU	Memorandum of Understanding
NAEC	The National Authority for Electronic Certification
NAIS	The National Agency for Information Society
NGOs	Non-governmental organizations
NATO	North Atlantic Treaty Organisation
NCIRC	NATO Cyber Incident Response Centre
NCS	National Cybersecurity Strategy
NIDS	Network Introduction Detection Systems
NIS Directive	The EU Network and Information Systems Security (NIS) Directive
OSCE	Organisation for Security and Cooperation in Europe
OST	Transmission System Operator (of Albania)
PhD	Philosophiae Doctor (doctor of philosophy)
PKI	Public Key Infrastructure
SMEs	Small and Medium Enterprises
SSL	Secure Sockets Layer
TAIEX	Technical Assistance and Information Exchange instrument of the European Commission
TLS	Transport Layer Security
UNODC	United Nations Office on Drugs and Crime
VPNs	Virtual Private Networks

EXECUTIVE SUMMARY

In collaboration with the World Bank (WB), the Global Cyber Security Capacity Centre (GCSCC, or 'the Centre') undertook a review of the maturity of cybersecurity capacity in Albania at the invitation of the National Authority for Electronic Certification and Cyber Security (AKCESK). The objective of this review was to enable Albania to gain an understanding of its cybersecurity capacity in order to strategically prioritise investment in cybersecurity capacities.

Over the period (3-4 September 2018), the following stakeholders participated in roundtable consultations: academia, criminal justice, law enforcement, information technology officers and representatives from public sector entities, critical infrastructure owners and important information infrastructure owners, policy makers, information technology officers from the government and the private sector (including financial institutions and Albanian Banks Association), telecommunications companies the banking sector as well as international partners.

The consultations took place using the Centre's Cybersecurity Capacity Maturity Model (CMM), which defines five *dimensions* of cybersecurity capacity:

- *Cybersecurity Policy and Strategy*
- *Cyber Culture and Society*
- *Cybersecurity Education, Training and Skills*
- *Legal and Regulatory Frameworks*
- *Standards, Organisations, and Technologies*

Each dimension comprises factors which describe what it means to possess cybersecurity capacity. Factors consist of aspects and for each aspect there are indicators, which describe steps and actions that, once observed, define the state of maturity of that aspect. There are five stages of maturity, ranging from the start-up stage to the dynamic stage. The start-up stage implies an ad-hoc approach to capacity, whereas the dynamic stage represents a strategic approach and the ability to adapt dynamically or to change in response to environmental considerations. For more details on the definitions, please consult the CMM document.[1]

Figure 1 below provides an overall representation of the cybersecurity capacity in Albania and illustrates the maturity estimates in each dimension. Each dimension represents one fifth of the graphic, with the five stages of maturity for each factor extending outwards from the centre of the graphic; 'start-up' is closest to the centre of the graphic and 'dynamic' is placed at the perimeter.

[1] Cybersecurity Capacity Maturity Model for Nations (CMM), Revised Edition, https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cmm-revised-edition (assessed 25 February 2018)

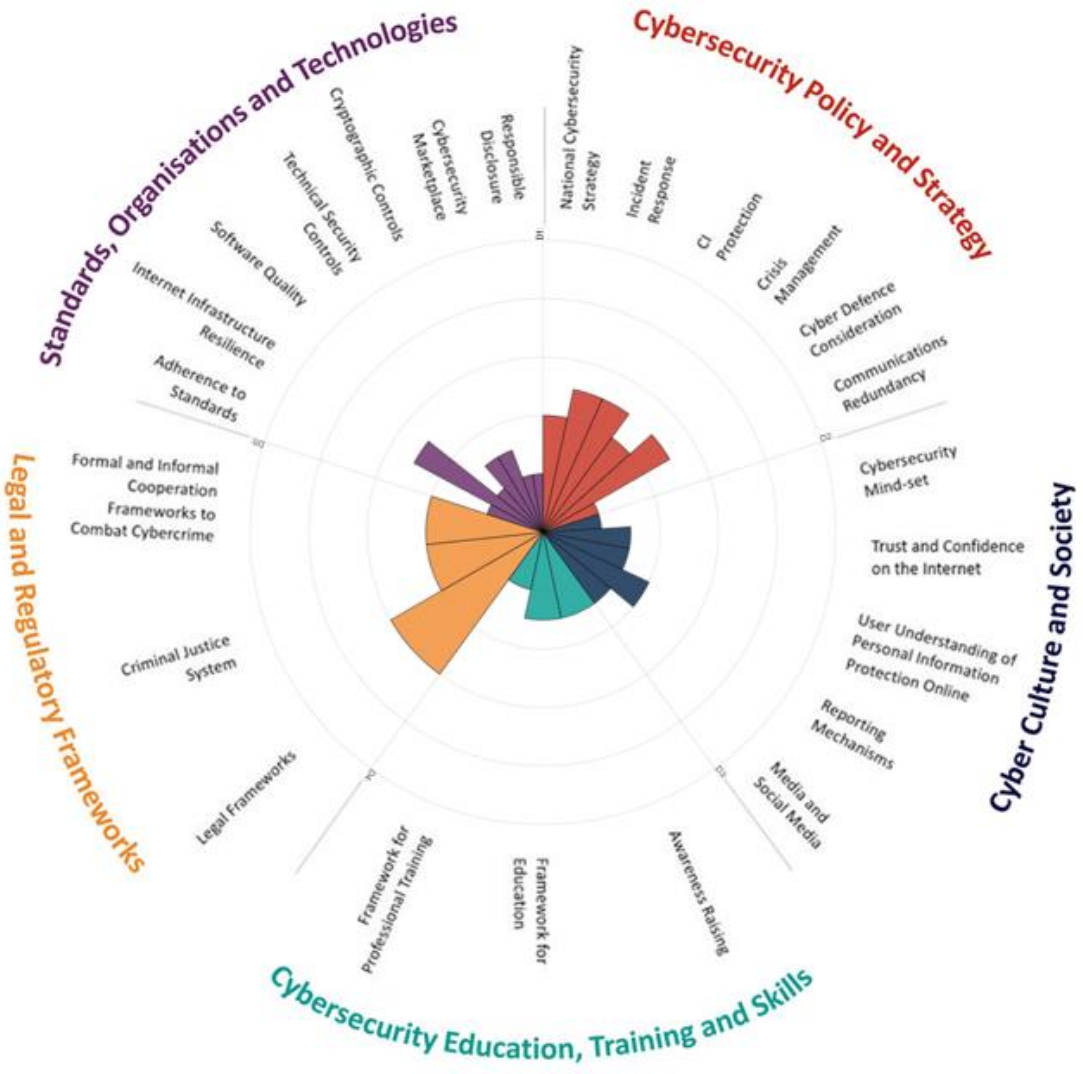

Figure 1: Overall representation of the cybersecurity capacity in Albania

Cybersecurity Policy and Strategy

Albania's commitment towards cybersecurity and cyber-resilience has notably progressed after it recently adopted various national digital transformation and national security strategies. The National Cross-cutting Strategy "Digital Agenda of Albania 2015-2020" is led by the Ministry of Infrastructure and Energy. The strategy superseded the National Cross-cutting Strategy on Information Society (2008-2013), a key document in stipulating Cybersecurity at a high level. The current Digital Agenda of Albania (2015-2020) has interwoven the cybersecurity theme across the strategy. Guaranteeing high security levels for the information networks is a core element of the second objective of the strategy.

From a national security perspective, the National Security Strategy (2014)[2] promotes the adoption and implementation of a National Cybersecurity Strategy as part of its objectives. The strategy emphasized ''safeguarding and protecting information in all forms of its existence'', focusing on special efforts to protect against cyber-attacks. From an overarching cybersecurity strategy perspective, processes for strategy development have been initiated by the National Cyber Security Agency (The national Computer Incident Response Team for Albania –previously known as ALCIRT, now part of AKCESK). The National Cybersecurity Strategy (2018-2023) has been articulated and is under development.

There are three main authorities that are responsible for different parts of incident response in Albania. The Ministry of Defense (MoD) is responsible for handling the MoD and Air Force related cyber incidents. The Albanian State Police and the prosecutor's office Cybercrime Investigation Unit are handling cybercrime incidents. However, AKCESK serves as the official national coordinating body for the reporting and management of cybersecurity incidents for the Important information infrastructures and critical information infrastructures operators.

The Law No.2/2017 on Cybersecurity dictates critical information infrastructure operators and important information infrastructure operators and their responsibility on reporting incidents. The law defines Critical Information Infrastructures (CIIs) as well as Important Information Infrastructures (IIIs).

Although the scope of reporting requirements has been specified by the Law on Cybersecurity, at the time of the review we were not able to determine the maturity of the threat and vulnerability disclosure among CII owners as well as between CI and the government. The Law No.2/2017 on Cybersecurity defines the state of cyber-crisis, the duration of the crisis and high-level actions to be taken during a crisis. Only the Council of Ministers can declare the crisis and only the Prime Minister can extend the duration of the crisis. It is understood that general crisis management is necessary for national security, but cybersecurity is not yet considered as a component. AKCESK mandated CIIs to manage the continuity of operations as part of the regulation on the content and method of documenting security measures[3]. Crisis management exercise design and planning authority may have been allocated in principle (either directly or via consultants), but cybersecurity crisis management planning has not been thoroughly outlined.

The MoD has progressed the notion of cyber-protection by initiating its own Cyber Defence Strategy (2014-2017)[4] which was designed to ensure orientation, coherence and focus, for a

[2] National Security Strategy (2014) National Security Strategy (2014) http://www.mod.gov.al/images/PDF/strategjia_sigurise_kombetare_republikes_se_shqiperise.pdf

[3] http://akce.gov.al/publicAnglisht_html/wp-content/uploads/2016/04/regullore%20mbi%20p%C3%ABrmbajtjen%20dhe%20m%C3%ABnyr%C3%ABn%20e%20dokumentimit%20t%C3%AB%20%20masave%20t%C3%AB%20siguris%C3%AB.pdf

[4] The Ministry of Defence (MoD) has progressed the notion of cyber-protection by initiating its own Cyber Defence Strategy (2014-2017) http://www.mod.gov.al/images/PDF/Strategjia_per_Mbrojtjen_Kibernetike.pdf

comprehensive approach in developing military capabilities in cyber space. The second iteration of the strategy has been initiated (2018-2020) for the MoD and the Air Force[5].

Digital redundancy measures are considered (in an ad-hoc manner) by private companies and other organizations, but there is nothing coordinated and systematic at the national level. Private institutions have disaster recovery capabilities.

Cyber Culture and Society

The cyber ecosystem in Albania is in its early stages. Within the private sector, leading firms have begun to place priority on a cybersecurity mind-set such as by identifying high-risk practices. As participants stated, chief executive officers (CEOs) and members of the board or management do place a priority on cybersecurity and are developing a cybersecurity mindset but usually this is only in the context of large organisations. At the local level, or for small and medium enterprises (SMEs), there is a lack of a cybersecurity mindset. Participants mentioned that one of the reasons for the general lack of a cybersecurity mindset is that in rural areas there is limited access to the Internet as well as limited levels of digital illiteracy which put their residents at a disadvantage. Moreover, the existing cybersecurity awareness efforts are too limited in scale to provide a sufficient level of knowledge across society as a whole.

Most Internet users tend to be overly trusting of websites and regarding what they see or receive online. At the same time, given the relative lack of e-service provision in the past, there is a lack of trust of the Internet for services.

The Government continues to increase e-service provision, but also recognises the need for more experience and the application of security measures to establish more trust in these services. However, many users are unfamiliar with or lack trust in the e-government services provided, which is important since the Internet could be regarded as an 'experience technology', requiring experience to fully understand its risks and opportunities.

E-commerce services have started emerging in the country. However, a small proportion of the population is using e-commerce services and the private sector recognises the need for security measures to foster trust and increase their uptake.

Awareness around the protection of personal information and the security of personal data is generally low. Users and stakeholders within the public and private sectors have general but limited knowledge about how personal information is handled online.

Participants mentioned that there are reporting mechanisms in place for users to report computer-related or online incidents and crimes. Residents can report incidents to the Albanian State Police through a specialised online platform or in person.

In Albania there is only ad-hoc media coverage of cybersecurity, with limited information provided and reporting on specific issues that individuals face online, such as online child protection or cyberbullying. Also, there is very limited discussion on social media about cybersecurity.

[5] The second iteration of the strategy (2018-2020) for protection of the MoD and the Air Force. http://www.mod.gov.al/images/PDF/2017/Strategjia_Mbrojtjen_Kibernetike_2018_2020.pdf

Cybersecurity Education, Training and Skills

A national programme for cybersecurity awareness raising, led by a designated organisation (from any sector) which addresses a wide range of demographics is yet to be established. In the last few years Albania periodically carried out awareness activities for a safer internet, as well as activities on the international day of Safer Internet. Albania celebrates October as a cybersecurity awareness month. Moreover, there is a child security week in March.

The officially recognized CIRT (AKCESK) is the legal mandated Agency created by Decision of Council of Ministers to organize awareness campaigns, trainings, publish informative materials either for the private or public sector. AKCESK, in conjunction with the Ministry of Education, Sport and Youth and the banking sector conducted a pilot programme for schools on raising awareness about cyberbullying. Additionally, the Cybercrime Unit works with NGOs to visit schools and provide training for children. The private sector is starting to consider cybersecurity awareness; however, it is still at an early stage.

The need for enhancing cybersecurity education in schools and universities has been identified by the Government, industry, and stakeholders in academia. Currently, public and private universities and colleges offer educational courses in cybersecurity-related fields, such as information security, network security and cryptography, but cybersecurity-specific courses are not yet offered. The Ministry of Education, Sport and Youth mandates that only doctorate (PhD) holders can teach courses. As participants mentioned, this mandate creates a significant challenge, since there are not enough lecturers who are specialised in cybersecurity.

The need for training professionals in cybersecurity has been recognized by the Government but has not been documented on the national level. Albania does not have certified government and public-sector agencies under internationally recognized standards in cybersecurity. Within the public institutions training on cybersecurity issues both for IT staff and general staff is very limited and often depends on the respective management in the institution, i.e. if a specific member of staff can attend a general cybersecurity training or certification course.

Internationally accredited IT Security and Governance training and certification courses are being offered in Albania[6]. As mentioned by the review participants, the perception of the private sector boards and CEOs towards cybersecurity needs significant improvement. Another concern shared by the participants is the challenge in retaining security professionals within Albania, as often they leave the country to seek better opportunities in the EU or North America.

Legal and Regulatory Frameworks

Albania does not have an all-encompassing regulation that deals explicitly with cybersecurity. Instead, several official guidelines have been adopted that refer to cybersecurity issues. The most relevant legislative frameworks and guidelines related to Albania's Internet landscape are:

[6] https://www.invensislearning.com/al/it-security-and-governance-training-albania/

- *Law No. 7895 from 27.01.1995, Criminal Code of Albania*[7]
- *Law No. 7905 from 21.03.1995, Criminal Procedure Code of Albania*[8]
- *Law No. 9918 from 19.05.2008, On electronic communications*[9]
- *Law No. 9887 from 10.03.2008, On protection of personal data*[10]
- *Law No. 8888, date 25.4.2002 for Ratification of ''Convention for Crime in the Cybernetic Area''*[11]
- *Law No.9880, dated 25.02.2008, On electronic signature*[12]
- *Law No.10128, dated 11.05.2009, On electronic commerce*
- *Law No. 9643 of 20.11.2006 amended, for the public procurement that enables the electronic procurement*[13]
- *Law No. 9723 of 3.5. 2007 on the registration of businesses On the National Center of Registration*
- *Law no. 10273 from 29.4.2010, On electronic document*
- *Law no.2/2017 "On cyber security*"
- Law no.107/2015 "On electronic identification and trust services"

Albania has signed and ratified the Budapest Convention for Cyber Crime and has reflected in the Penal Code and Penal Procedure Code the requirements of the Convection.

The Constitution of Albania proclaims that fundamental human rights and freedoms are indivisible, inalienable, and inviolable and stand at the base of the entire juridical order. Moreover, Law No. 9887, Article 11 from 10.03.2008, "On protection of personal data'', speaks on processing of personal data and freedom of expression. Moreover, comprehensive legislation on protection of children online has been adopted and enforced under Articles:

- *Article 117/2 of the Criminal Code on Pornography*[14].
- *Law N. 23/201231*[15]

Albania has also adopted an action plan for the protection of children's rights (DCM No. 182/2012)[16].

As mentioned above, the Law No. 8888 of 25 April 2002 "On Ratification of the Convention on Cyber Crime" is reflected in the Criminal Code; and so is the 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". Similarly,

[7] http://rai-see.org/wp-content/uploads/2015/08/Criminal-Code-11-06-2015-EN.pdf
[8] http://www.wipo.int/wipolex/en/details.jsp?id=54
[9] http://aida.gov.al/images/ckeditor/law-nr-9918-date-19.05.2008-.pdf
[10] http://www.institutemedia.org/Documents/PDF/Law%20on%20protection%20of%20personal%20data.pdf
[11] http://www.cybercrimelaw.net/Albania.html
[12] http://aida.gov.al/images/ckeditor/Law%20no%209880%20date%2025.02.2008.pdf
[13] https://albaniaenergy.org/onewebmedia/ACERC%20Law%200004.pdf
[14] https://www.legislationline.org/documents/section/criminal-codes/country/47
[15] https://www.coe.int/en/web/cybercrime
[16] http://akshi.gov.al/wp-content/uploads/2018/03/Digital_Agenda_Strategy_2015_-_2020.pdf

procedural cybercrime legal provisions are fully implemented in the Law on Criminal Procedural law.

Within the criminal justice system in Albania, capacities are at a formative stage of development. A central forensics laboratory exists within the Cybercrime Unit of State Police. However, there was a general consensus among stakeholders that more resources are necessary to be provided to the Cybercrime Unit as well as continuous training for the employees. A limited number of specialised cybercrime prosecutors have the capacity to build a case based on electronic evidence. According to the legislation, there is a requirement for submission of evidence to the court by the prosecutor but also by the victim. Therefore, the legal authority is needed before any further action.

A separate court structure or specialized judges for cybercrime cases and cases involving electronic evidence do not exist. As participants noted, judges are not currently being trained in cybercrime. Concerns were raised regarding the difficulties that judiciary are having due to lack of resources.

Albania has established regional and international cooperation mechanisms. The country is one of the parties to the 1959 Council of Europe Convention on Mutual Legal Assistance in Criminal Matters; it also ratified First and Second Additional Protocols to the European Convention on Mutual Assistance in Criminal Matters, as well as the Convention on Extradition. With regard to international cooperation the Criminal Procedure Code (CPC) includes preservation and expedited disclosure of computer data, access to computer data, comprising search, seizure and disclosure of data stored in the computer system located in Albania, when the search and seizure would be admissible and interception of communications. Participants mentioned that there is a strong collaboration mechanism with Interpol and Europol and there have been joint operations with Europol in the past.

Standards, Organisations, and Technologies

Based on the review, there is no obligation to implement national (or sector-specific) ICT security standards. However, the finance sector -banks- follow standards adhered to in other European countries, such as the General Data Protection Regulation (GDPR) or (International Organization for Standardisation) ISO standards, although the banks are not certified.

Similarly, there are no mandatory standards for the procurement of hardware and software. The finance and other private sector adhere to different standard requirements, but local level companies do not necessarily follow such requirements.

Focusing on standards in software development, there are guidelines in place in both public and private sectors, but the extent to which these guidelines are related to cybersecurity is not clear. It was noted that within private sector most developers do adaptation and system integration, rather than software development. But if so they follow ISO standards and conduct penetration testing or other security assessments.

There is no inventory of secure software for the use in public and private sectors in Albania. The adoption of technical security controls in the country varies across sectors and organisations, but they are mostly ad-hoc and not consistently deployed.

Cryptographic controls for protecting data at rest and in transit are recognised and deployed in an ad-hoc manner by multiple stakeholders and within various sectors.

The domestic market provides limited cybersecurity technologies. No domestic market for cybercrime insurance products has yet been developed in the country. Currently, there is also no policy in place for responsible information disclosure. Except for the classified information which is handled by Albanian NSA.

Additional Reflections

Even though the duration of this review was shorter (2 days), the stakeholder engagement in the review, the representation and composition of stakeholder groups was, overall, balanced and broad.

This was the 27th country review that the GCSCC have supported directly.

INTRODUCTION

At the invitation of the National Authority for Electronic Certification and Cyber Security (AKCESK) and in collaboration with World Bank (WB) the Global Cyber Security Capacity Centre (GCSCC) has conducted a review of cybersecurity capacity of Albania. The objective of this review was to enable Albania to determine areas of capacity in which the government might strategically invest in, in order to improve their national cybersecurity posture.

Over the period 3-4 September 2018, stakeholders from the following sectors participated in a three-day consultation process:

- *Universities*
- *Internet Society representatives*
- *Internet registries (NAEC)*
- *Internet Governance representatives*
- *Cybersecurity Policy Review Team*
- *Attorney General's office*
- *National cybercrime units*
- *Inspector General of the police*
- *Local police representation*
- *Ministry of Justice*
- *Ministry of Defence*
- *Relevant intelligence agencies (foreign and domestic)*
- *National and/or sectoral incident response teams*
- *Ministerial information security officers*
- *Health sector*
- *Energy sector*
- *Transportation sector*
- *Water sector*
- *National security representatives*
- *Telecommunications sector*
- *Internet service providers*
- *Finance sector*
- *Major industry leaders / Major information technology companies*
- *International NGOs*
- *UN offices*
- *World Bank*
- *Embassy partners*

DIMENSIONS OF CYBERSECURITY CAPACITY

Consultations were premised on the GCSCC Cybersecurity Capacity Maturity Model (CMM)[17] which is composed of five distinct *dimensions* of cybersecurity capacity.
Each dimension consists of a set of factors, which describe and define what it means to possess cybersecurity capacity therein. The table below shows the five dimensions with the five dimensions together with the factors of which they are comprised:

DIMENSIONS	FACTORS
Dimension 1 Cybersecurity Policy and Strategy	D1.1 National Cybersecurity Strategy D1.2 Incident Response D1.3 Critical Infrastructure (CI) Protection D1.4 Crisis Management D1.5 Cyber Defence D1.6 Communications Redundancy
Dimension 2 Cyber Culture and Society	D2.1 Cybersecurity Mind-set D2.2 Trust and Confidence on the Internet D2.3 User Understanding of Personal Information Protection Online D2.4 Reporting Mechanisms D2.5 Media and Social Media
Dimension 3 Cybersecurity Education, Training and Skills	D3.1 Awareness Raising D3.2 Framework for Education D3.3 Framework for Professional Training
Dimension 4 Legal and Regulatory Frameworks	D4.1 Legal Frameworks D4.2 Criminal Justice System D4.3 Formal and Informal Cooperation Frameworks to Combat Cybercrime
Dimension 5 Standards, Organisations, and Technologies	D5.1 Adherence to Standards D5.2 Internet Infrastructure Resilience D5.3 Software Quality D5.4 Technical Security Controls D5.5 Cryptographic Controls D5.6 Cybersecurity Marketplace D5.7 Responsible Disclosure

[17] See Cybersecurity Capacity Maturity Model for Nations (CMM), Revised Edition, available at https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cmm-revised-edition.

STAGES OF CYBERSECURITY CAPACITY MATURITY

Each dimension comprises factors which describe what it means to possess cybersecurity capacity. Factors consist of aspects and for each aspect there are indicators, which describe steps and actions that once observed define which state of maturity this specific element of aspect is. There are five stages of maturity, ranging from the *start-up* stage to the *dynamic* stage. The start-up stage implies an ad-hoc approach to capacity, whereas the dynamic stage represents a strategic approach and the ability to dynamically adapt or change against environmental considerations. The five stages are defined as follows:

- **Start-up:** at this stage either no cybersecurity maturity exists, or it is very embryonic in nature. There might be initial discussions about cybersecurity capacity building, but no concrete actions have been taken. There is an absence of observable evidence of cybersecurity capacity at this stage.
- **Formative:** some aspects have begun to grow and be formulated, but may be ad-hoc, disorganised, poorly defined – or simply new However, evidence of this aspect can be clearly demonstrated.
- **Established:** the indicators of the aspect are in place, and functioning. However, there is not well thought-out consideration of the relative allocation of resources. Little trade-off decision-making has been made concerning the relative investment in this aspect. But the aspect is functional and defined.
- **Strategic:** at this stage, choices have been made about which indicators of the aspect are important, and which are less important for the particular organisation or state. The strategic stage reflects the fact that these choices have been made, conditional upon the state's or organisation's particular circumstances.
- **Dynamic:** At this stage, there are clear mechanisms in place to alter strategy depending on the prevailing circumstances such as the technological sophistication of the threat environment, global conflict or a significant change in one area of concern (e.g. cybercrime or privacy). Dynamic organisations have developed methods for changing strategies in-stride. Rapid decision-making, reallocation of resources, and constant attention to the changing environment are features of this stage.

The assignment of maturity stages is based upon the evidence collected, including the general or average view of accounts presented by stakeholders, desktop research conducted and the professional judgement of GCSCC research staff. Using the GCSCC methodology as set out above, this report presents results of the cybersecurity capacity review of Albania and concludes with recommendations as to the next steps that might be considered to improve cybersecurity capacity in the country.

The assignment of maturity stages is based upon the evidence collected, including the general or average view of accounts presented by stakeholders, desktop research conducted and the professional judgement of GCSCC research staff. Using the GCSCC methodology as set out above, this report presents results of the cybersecurity capacity review of Albania and

concludes with recommendations as to the next steps that might be considered to improve cybersecurity capacity in the country.

METHODOLOGY - MEASURING MATURITY

During the country review specific dimensions are discussed with the relevant group of stakeholders. Each stakeholder cluster is expected to respond to one or two dimensions of the CMM, depending on their expertise. For example, Academia, Civil Society and Internet Governance groups would all be invited to discuss both Dimension 2 and Dimension 3 of the CMM.

In order to determine the level of maturity, each aspect has a set of indicators corresponding to all five stages of maturity. In order for the stakeholders to provide evidence on how many indicators have been implemented by a nation and to determine the maturity level of every aspect of the model, a consensus method is used to drive the discussions within sessions. During focus groups, researchers use semi-structured questions to guide discussions around indicators. During these discussions stakeholders should be able to provide or indicate evidence regarding the implementation of indicators, so that subjective responses are minimised. If evidence cannot be provided for all of the indicators at one stage, then that nation has not yet reached that stage of maturity.

The CMM uses a focus group methodology since it offers a richer set of data compared to other qualitative approaches.[18] Like interviews, focus groups are an interactive methodology with the advantage that during the process of collecting data and information diverse viewpoints and conceptions can emerge. It is a fundamental part of the method that rather than posing questions to every interviewee, the researcher(s) should facilitate a discussion between the participants, encouraging them to adopt, defend or criticise different perspectives.[19] It is this interaction and tension that offers advantage over other methodologies, making it possible for a level of consensus to be reached among participants and for a better understanding of cybersecurity practices and capacities to be obtained.[20]

---

[18] Relevant publications:
Williams, M. (2003).Making sense of social research. London: Sage Publications Ltd. doi: 10.4135/9781849209434
Knodel, J. (1993). The design and analysis of focus group studies: a practical approach. In Morgan, D. L. SAGE Focus Editions: Successful focus groups: Advancing the state of the art (pp. 35-50). Thousand Oaks, CA: SAGE Publications Ltd. doi: 10.4135/9781483349008
Krueger, R.A. and Casey, M.A. (2009). Focus groups: A practical guide for applied research. London: Sage Publications LTD.

[19] Relevant publications: J. Kitzinger. 'The methodology of focus groups: the importance of interaction between research participants.' Sociology of Health & Illness, 16(1):103–121, 1994.
J. Kitzinger. 'Qualitative research: introducing focus groups'. British Medical Journal, 311(7000):299–302, 1995.
E.F. Fern. 'The use of focus groups for idea generation: the effects of group size, acquaintanceship, and moderator on response quantity and quality.' Journal of Marketing Research, Vol. 19, No. 1, pages 1–13, 1982.

[20] J. Kitzinger. 'Qualitative research: introducing focus groups'. British Medical Journal, 311(7000):299– 302, 1995.

With the prior consent of participants, all sessions are recorded and transcribed. Content analysis – a systematic research methodology used to analyse qualitative data – is applied to the data generated by focus groups.[21] The purpose of content analysis is to design "replicable and valid inferences from texts to the context of their use".[22]

There are three approaches to content analysis. The first is the inductive approach which is based on "open coding", meaning that the categories or themes are freely created by the researcher. In open coding, headings and notes are written in the transcripts while reading them and different categories are created to include similar notes that capture the same aspect of the phenomenon under study.[23] The process is repeated and the notes and headings are read again. The next step is to classify the categories into groups. The aim is to merge possible categories that share the same meaning.[24] Dey explains that this process categorises data as "belonging together".[25]

The second approach is deductive content analysis which requires the prior existence of a theory to underpin the classification process. This approach is more structured than the inductive method and the initial coding is shaped by the key features and variables of the theoretical framework.[4]

In the process of coding, excerpts are ascribed to categories and the findings are dictated by the theory or by prior research. However, there could be novel categories that may contradict or enrich a specific theory. Therefore, if deductive approaches are followed strictly these novel categories that offer a refined perspective may be neglected. This is the reason why the GCSCC research team opts for a third, blended approach in the analysis of our data, which is a mixture of deductive and inductive approaches.

After conducting a country review, the data collected during consultations with stakeholders and the notes taken during the sessions are used to define the stages of maturity for each factor of the CMM. The GCSCC adopts a blended approach to analyse focus group data and use the indicators of the CMM as our criteria for a deductive analysis. Excerpts that do not fit into themes are further analysed to identify additional issues that participants might have raised or to tailor our recommendations.

In several cases while drafting a report, desk research is necessary in order to validate and verify the results. For example, stakeholders might not be always aware of recent

---

[21] K. Krippendorff. Content analysis: An introduction to its methodology. Sage Publications, Inc, 2004.
H.F. Hsieh and S.E. Shannon. 'Three approaches to qualitative content analysis.' Qualitative Health Research,
15(9):1277–1288, 2005.
K.A. Neuendorf. The content analysis guidebook. Sage Publications, Inc, 2002.

[22] E.F. Fern. 'The use of focus groups for idea generation: the effects of group size, acquaintanceship, and moderator on response quantity and quality.' Journal of Marketing Research, Vol. 19, No. 1, Volume and Number? pages 1–13, 1982.

[23] S. Elo and H. Kyng¨as. 'The qualitative content analysis process.' Journal of Advanced Nursing, 62(1):107–115, 2008.
H.F. Hsieh and S.E. Shannon. 'Three approaches to qualitative content analysis.' Qualitative Health Research, 15(9):1277–1288, 2005.

[24] P.D. Barbara Downe-Wamboldt RN. 'Content analysis: method, applications, and issues.' Health Care for Women International, 13(3):313–321, 1992.

[25] I. Dey. Qualitative data analysis: A user-friendly guide for social scientists. London: Routledge, 1993.

developments in their country, such as whether the country has signed a convention on personal data protection. The sources that can provide further information can be the official government or ministry websites, annual reports of international organisations, university websites, etc.

For each dimension, recommendations are provided for the next steps to be taken for the country to enhance its capacity. If a country's capacity for a certain aspect is at a formative stage of maturity, then by looking at the CMM the indicators which will help the country move to the next stage can be easily identified. Recommendations might also arise from discussions with and between stakeholders.

Using the GCSCC CMM methodology, this report presents results of the cybersecurity capacity review of Albania and concludes with recommendations as to the next steps that might be considered to improve cybersecurity capacity in the country.

CYBERSECURITY CONTEXT IN ALBANIA

Albania has a resident population of approximately 3.5 million people[26]. The number of Internet users in the country has increased spectacularly over the recent years. According to Electronic and Postal Communications Authority (AKEP -Autoriteti i Komunikimeve Elektronike dhe Postare) the number of broadband subscribers that access Internet from fixed networks in Q4 2016 amounted to approximately 266 thousand, which represents an increase of 1.8% compared with the previous quarter and by about 10% compared with that same quarter in 2015. Also, the number of subscribers to fixed networks that have access to integrated services (Telephone / Internet / TV) at the end of the third quarter to fourth amounted to about 187 thousand, an increase of 5.5% compared to Q3 2016 and 25% in Q4 2015[27].

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[28].

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[29]. The percentage of Internet users was 63.3 % in 2015 and 66.4% in 2016 of the total population[30]. Similarly fixed-broadband subscriptions have risen from 7.6% in 2015 to 8.2% in 2016.

The ICT market development led Albania to be ranked 89th on the ITU's Global ICT Development Index 2017 ranking[31]. Moreover, the World Economic Forum[32] report, which placed Albania 75th out of 137 countries on the Global Competitiveness Index 2017-2018 edition, considers the country to possess an "efficiency driven economy", based on pillars measuring the three economic stages (as reflected in the ranking sub-indexes).). From the current measure of these pillars, it becomes evident that Albania has an opportunity to

[26]http://reports.weforum.org/global-competitiveness-index-2017-2018/countryeconomy-profiles/#economy=BRA

[27]https://www.akep.al/en/lajme/562-publikohen-treguesit-statistikore-te-tregut-te-komunikimeve-elektronike-per-tre-mujorin-e-katert-te-vitit-2017

[28] www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

[29] R.Bofati and J.Josifi: "Towards a more resilient cyberspace: the case of Albania", Information & Security: An International Journal, vol. 32, 2015, available at: https://procon.bg/system/files/3310_albania.pdf

[30]https://www.itu.int/en/ITUD/Statistics/Documents/publications/misr2017/MISR2017_Volume1.pdf

[31] https://www.itu.int/net4/ITU-D/idi/2017/index.html

[32]http://reports.weforum.org/global-competitiveness-index-2017-2018/countryeconomy-profiles/#economy=BRA

improve its ranking further by addressing issues related to skill-sets (talent), access to capital, and innovation[33]. .

[33]https://www.itu.int/en/ITUD/Innovation/Documents/Publications/Albania%20Country%20Review%20Innovation%20June%202016.pdf

REVIEW REPORT

OVERVIEW

In this section, we provide an overall representation of the cybersecurity capacity in Albania. Figure 2 below presents the maturity estimates in each dimension. Each dimension represents one fifth of the graphic, with the five stages of maturity for each factor extending outwards from the centre of the graphic; 'start-up' is closest to the centre of the graphic and 'dynamic' at the perimeter.

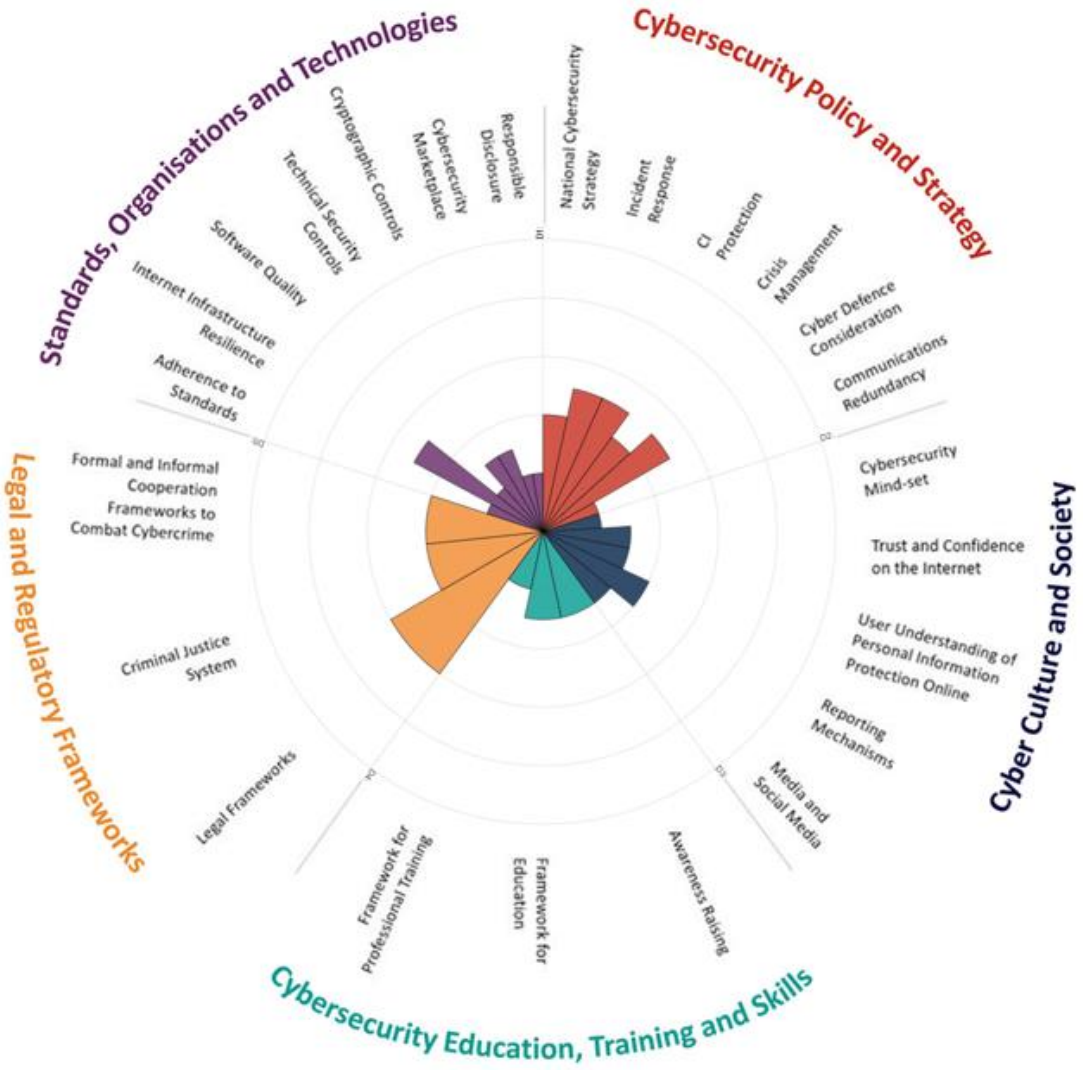

Figure 2: Overall representation of the cybersecurity capacity in Albania

DIMENSION 1
CYBERSECURITY STRATEGY AND POLICY

The factors in Dimension 1 gauge Albania's capacity to develop and deliver cybersecurity policy and strategy and to enhance cybersecurity resilience through improvements in incident response, crisis management, redundancy, and critical infrastructure protection capacity. The Cybersecurity policy and strategy dimension also includes considerations for early warning, deterrence, defence and recovery. This dimension considers effective policy in advancing national cyber-defence and resilience capacity, while facilitating the effective access to cyberspace increasingly vital for government, international business and society in general.

D 1.1 NATIONAL CYBERSECURITY STRATEGY

Cybersecurity strategy is essential to mainstreaming a cybersecurity agenda across government, because it helps prioritise cybersecurity as an important policy area, determines responsibilities and mandates of key government and non-governmental cybersecurity actors, and directs allocation of resources to the emerging and existing cybersecurity issues and priorities

Stage: Formative

Albania's commitment towards cybersecurity and cyber-resilience has notably progressed after it recently adopted various national digital transformation security strategies. The National Cross-cutting Strategy "Digital Agenda of Albania 2015-2020,"[34] is led by the Ministry of Infrastructure and Energy. The strategy superseded the National Cross-cutting Strategy on Information Society (2008-2013)[35], a key document in stipulating Cybersecurity at a high level. Prior to that was the first ICT strategy, adopted in 2003. The current Digital Agenda of Albania (2015-2020) has interwoven the cybersecurity theme across the strategy. Guaranteeing high security levels for the information networks is a core element of the second objective of the strategy. Secure information society is a main section of the strategy which covers secure communications and electronic certifications; computer security; and safer internet practices.

[34] National Cross-Cutting Strategy "Digital Agenda of Albania 2015-2020," http://akshi.gov.al/wp-content/uploads/2018/03/Digital_Agenda_Strategy_2015_-_2020.pdf
[35] National Cross- cutting Strategy on Information Society (2008-2013.) http://shtetiweb.org/wp-content/uploads/2014/05/Information-Society-strategy_printed_version_en.pdf

One of the main principles for the development of the Digital Age is trust and security of information networks. It also emphasizes the role of the government in implementing a system of norms, sanctions and resources in order to guarantee the data and ICT systems security. The strategy further disseminates cybersecurity within various strategic priorities and their objectives. Examples such as the increase of security of the physical and logical infrastructure of the governmental network, GovNET was part of the 4th of Objective of the 1st Strategic Priority. Another example is the increase of security through the establishment of the Business Continuity Center and the Backup for governmental services, as well as the establishment of the Disaster Recovery Centre –DRC for governmental systems as the 2nd Objective of the 2nd Strategic Priority. However, the *Increase of safety of information networks,* which is the 6th Objective of the 1st Strategic Priority, covers the most cybersecurity initiatives. The strategy document incorporates a comprehensive high-level action plan which links strategic priorities to the objectives and relevant initiatives and projects. The program includes implementation deadlines, responsible institutions and the allocated budget. As such, a coordinated cybersecurity program is being developed through a multi-stakeholder consultative process within the Digital Agenda. However, budgets reside in disparate public departments without a discrete cybersecurity budget line. The strategy includes linkage between cybersecurity, national risk priorities and business development, but these are generally ad-hoc and lack detail.

It has also reiterated the position of the National Agency for Cyber Security (ALCIRT) as the national institution for response to cyber-incidents and cybersecurity capacity building. Established in 2011, ALCIRT was strategically positioned under the Prime Minister's authority[36] until 2016.

ALCIRT is now imbedded as part of the National Authority for Electronic Certification and Cyber Security (AKCESK)[37] [38]. Currently AKCESK is in charge of participating in preparing the national cybersecurity strategy, drafting relevant legislation, cooperating with all relevant institutions, international organizations, civil society organisations (CSOs) and the private sector and organizing awareness campaigns, trainings and education materials on ICT.

ALCIRT (now AKCESK) has produced the National Policy Paper on Cybersecurity (2015-2017)[39]. The document aims to assess the current situation and trends in relation to cybersecurity in the country. It also summarizes the relevant legal and institutional framework as well as key government structures that deal with cybersecurity. The document references previous national digital and security strategies. The policy paper also articulates the cybersecurity vision, principles and strategic objectives. An accompanying action plan is referenced in the policy paper. However, an overarching national cybersecurity strategy still does not exist, although Working Group for the drafting of the strategy has been created.

[36] R.Bofati and J.Josifi: "Towards a more resilient cyberspace: the case of Albania", Information & Security: An International Journal, vol. 32, 2015, available at: https://procon.bg/system/files/3310_albania.pdf

[37] National Authority for Electronic Certification and Cyber Security (AKCESK) http://akce.gov.al/publicAnglisht_html/index.html

[38] https://www.diplomacy.edu/sites/default/files/Cybersecurity%20in%20Western%20Balkans.pdf

[39] National Policy Paper on Cybersecurity (2015-2017)39. http://akce.gov.al/publicAnglisht_html/rreth-nesh/raportidokumentittepolitikave.pdf

From a national security perspective, the National Security Strategy (2014)[40] promotes the adoption and implementation of a National Cybersecurity Strategy as part of its objectives. The strategy emphasizes ''safeguarding and protecting information in all forms of its existence, focusing on special efforts to protect against cyber-attacks''.

The MoD progressed the notion of cyber-protection by initiating its own Cyber Defense Strategy (2018-2020)[41] for protection of the MoD and the Air Force. More on Cyber Defense in covered in Section D1.5.

From an overarching cybersecurity strategy perspective, processes for strategy development have been initiated by AKCESK. The National Cybersecurity Strategy (2019-2025) has been articulated and is under development. The next draft is due in mid-2019. It will include a national cybersecurity program that spans the next five years. Consultation processes have been agreed for key stakeholder groups, including international partners and it will incorporate feedback from the ITU workshop, US-CERT review, this CMM review, as well as consultations with various stakeholders lead by the Working Group.

D 1.2 INCIDENT RESPONSE

This factor addresses the capacity of the government to identify and determine characteristics of national level incidents in a systematic way. It also reviews the government's capacity to organise, coordinate, and operationalise incident response.

Stage: Formative to Established

There are three main authorities that are responsible for different parts of incident response in Albania. The Ministry of Defense (MoD)[42] is responsible for handling the MoD and Air Force related cyber incidents. The Albanian State Police and the prosecutor's office Cybercrime Investigation Unit are handling cybercrime incidents[43]. However, AKCESK serves as the official national coordinating body for the reporting and management of cybersecurity incidents for the for CII and III[44].

The new Law No.2/2017 on Cybersecurity[45] Dictates that each critical and important infrastructure should build up their own CSIRT (sectorial CSIRT) which should be connected

[40] National Security Strategy (2014) http://www.mod.gov.al/images/PDF/strategjia_sigurise_kombetare_republikes_se_shqiperise.pdf
[41] MoD Cyber Defense Strategy (2018-2020) http://www.mod.gov.al/images/PDF/2017/Strategjia_Mbrojtjen_Kibernetike_2018_2020.pdf
[42] The Ministry of Defense (MoD) http://www.mod.gov.al/
[43] Dushi, D. and Bërdufi, N., 2017. Law Enforcement and Investigation of Cybercrime in Albania. European Scientific Journal, ESJ, 13(12).
[44] Law Enforcement and Investigation of Cybercrime in Albania https://eujournal.org/index.php/esj/article/download/9228/8769
[45] The new Law No.2/2017 on Cybersecurity http://akce.gov.al/publicAnglisht_html/wp-content/uploads/2016/04/Ligji%20_Per_Sigurine_Kibernetike_Nr_2_Date_26.1.2017.pdf

with the National CSIRT. The law mandates institutions to have their reporting duties established as they perform periodic reporting to the authority.

AKCESK's Emergency Monitoring and Response Sector is the central authority that identifies, foresees and takes measures against cyber threats/attacks and acts as the central point of contact for information exchange in the field of incidents and emergencies. AKCESK mentioned that incidents in general are organized and coordinated. AKCESK maintains a centralized national registry of cybersecurity incidents. AKCESK prioritizes incidents and categorizes incident's criticality in accordance to Law No.2/2017 on Cybersecurity.

ALCIRT (and now AKCESK) was initially supported by the USAID's[46] Albanian Cyber Security Program, involving training workshops provided to the government and non-government sector by Carnegie Mellon University's Software Engineering Institute (SEI). The training workshops focused on building skills to resist operational threats and develop processes for managing cybersecurity incidents. AKCESK is in the processes of becoming a member of the global Forum of Incident Response and Security Teams (FIRST). Moreover, there is a Memorandum of Understanding MoU between regional (Kosovo[47] and the former Yugoslav Republic of Macedonia[48], Romania, UBT-CERT) and is in process of signing MOU with (Serbia, Montenegro, Cyprus and Slovenia) CSIRTS, according to AKCESK.

The Council of Europe (CoE) and other specialist entities have provided AKCESK with relevant incident response training. AKCESK provides incident response awareness training as well.

The official portal for AKCESK[49] seemed to be not functional at the time of this review. AKCESK also have a cyber incident reporting facility in both Albanian[50] and English[51]. Although the English reporting section was not working at the time of the review. Cyber Albania portal[52] also seems to be accepting incident reports. AKCESK's Escalation Procedure 'In Case Of A Computer Incident'[53] (2016) provides detailed incident response processes. The document highlights the escalation procedures, the internal and external parties to be notified, incidents workflow, and the required documentations. The role of AKCESK is also stipulated to be in analyzing national incidents, providing advice to the affected organization and notifying the General Emergency Headquarters. Although, the role of the General Emergency Headquarters is not clear. Coordination with other national CSIRTs was not mentioned by review participants. It was not clear what constitutes a national incident and on what basis institutions would seek help based on the criticality of the incident. Currently, the point of contact with AKCESK is the official email info@cesk.gov.al, according to the escalation procedure document.

[46] https://www.diplomacy.edu/sites/default/files/Cybersecurity%20in%20Western%20Balkans.pdf
[47] Kosovo CSIRT MoU http://akce.gov.al/publicAnglisht_html/wp-content/uploads/2016/04/mou_kosove.pdf
[48] FYROM CSIRT MoU http://akce.gov.al/publicAnglisht_html/wp-content/uploads/2016/04/mow_mkd.pdf
[49] http://www.cirt.gov.al/
[50] http://akce.gov.al/publicAnglisht_html/raportoincident.html
[51] http://akce.gov.al/publicAnglisht_html/publicAnglisht_html/index.html
[52] http://cyberalbania.al/
[53] ALCIRT Escalation Procedure In Case Of A Computer Incident http://akce.gov.al/publicAnglisht_html/wp-content/uploads/2016/04/Procedura_pershkallezimit_Incidentit.pdf

Despite the substantial responsibilities of AKCESK, it lacks adequate resources, as it only has six employees. This is particularly challenging as they also lack the infrastructure and technical capacities to respond to cyber-incidents and perform the adequate coordination between various sectors.

The Financial Supervisory Authority AMF which overseas insurance, stock exchange, financial institutions excluding banks report incidents to the State Police, not AKCESK. The financial authority board meets on a regular basis to discuss incidents and cybersecurity matters. However, participants claimed that the country did not face any significant cybersecurity crime incidents until now.

As a member of NATO, Albania signed an MoU with the NATO Cyber Incident Response Centre (NCIRC) on enhancing cyber defense in 2013 and is currently negotiating the signing of the new version of this MoU. This version is based on the cyber defense document "NATO Enhanced Cyber Defence Policy", endorsed by all NATO countries at the Wales Summit in 2014.[54]

D 1.3 CRITICAL INFRASTRUCTURE (CI) PROTECTION

This factor studies the government's capacity to identify CI assets and the risks associated with them, engage in response planning and critical assets protection, facilitate quality interaction with CI asset owners, and enable comprehensive general risk management practice including response planning.

Stage: Formative to Established

Until recently, the concept of cybersecurity in national critical infrastructure was in its infancy in Albania. However, significant progress is now being achieved. The Law No.2/2017 on Cybersecurity dictates critical infrastructure providers and their responsibility on reporting. The law defines Critical Information Infrastructures (CIIs) as well as Important Information Infrastructures (IIIs). The Council of Ministers is responsible for approving the list of CIIs based on the proposal of the minister responsible within the specific CIIs or IIIs area. It covers various governmental and private sectors. The operators of CIIs and IIIs are obliged to implement security measures and to document their implementation. This list is updated at least once in two years. The list[55], which was created in 2018, is currently maintained by AKCESK. AKCESK defined baseline security policies and procedures as well as a methodology[56] for identification and classification of CIIs and IIIs to be followed by the operators.

[54] https://www.diplomacy.edu/sites/default/files/Cybersecurity%20in%20Western%20Balkans.pdf
[55] AKCESK CIIs List: http://akce.gov.al/publicAnglisht_html/standarde/index.html
[56] AKCESK CIIs selection methodology http://akce.gov.al/publicAnglisht_html/wp-content/uploads/2016/04/infrastruktura.pdf

AKCESK performed various meetings with workshops with the CIIs and IIIs. It established connection bridges between different CIIs, and key controls were identified to be evaluated and audited by AKCESK. European Union Agency for Network and Information Security (ENISA) guidelines were followed, the methodology was published and disseminated to relevant stakeholders.

AKCESK's National Policy Paper on Cybersecurity (2015-2017)[57] places the identification and protection of CIIs as one of its key objectives. Defined by Law 2/2017 for both Critical and Important Infrastructure. The policy paper further details the requirements to fulfil this objective:

- Developing the necessary procedures and processes for the identification, of CII.
- Ensuring CII's security as a priority.
- Developing and implementing minimum procedures and standards as mandatory.
- Encouraging cooperation and exchange of information with the various sectors.
- Ensuring continuity of business activities and "resilience" in cases of force majeure or different cyber-attacks.
- Defining the legal and regulatory basis for CIIs.
- Encouraging and providing support for the certification of critical infrastructures according to the security standards.

Although the scope of reporting requirements has been specified by the law on Cybersecurity, at the time of the review the GCSCC researchers were not able to determine the maturity of the threat and vulnerability disclosure among CIIs owners as well as between CI and the government.

CIIs have the basic capacity to detect, identify, respond to and recover from cyber threats, but such capabilities are uncoordinated and vary in quality in Albania. Protection of CI assets includes basic level cybersecurity awareness and data security policies, but no protection processes have been agreed.

[57] ALCIRT's National Policy Paper on Cybersecurity (2015-2017)
http://akce.gov.al/publicAnglisht_html/rreth-nesh/raportidokumentittepolitikave.pdf

D 1.4 CRISIS MANAGEMENT

This factor addresses crisis management planning addresses conducting specialised needs assessments, training exercises, and simulations that produce scalable results for policy development and strategic decision-making. Through qualitative and quantitative techniques, cybersecurity evaluation processes aim to produce structured and measurable results that would solicit recommendations for policymakers and other stakeholders and inform national strategy implementation as well as inform budgetary allocations.

Stage: Formative

The Law No.2/2017 on Cybersecurity defines the state of cyber-crisis, the duration of the crisis and high-level actions to be taken during a crisis. Only the Council of Ministers can declare the crisis and only the Prime Minister can extend the duration of the crisis.

Participants noted that certain CI stakeholders, as well as organisations from the finance sector maintain business-continuity plans depending on the criticality of the system. Cyber-crisis is not quantified as such, however the banking sector has realized the need for coordinated efforts. Banks are also participating in Disaster Recovery & Business Continuity Planning (DR&BCP) internally. The Financial Supervisory Authority AMF has initiated DR&BCP, and crisis management audits on its members starting from October 2018 onwards.

The Albania Air Navigation Service Provider (ANSP) or Albcontrol is part of Euro control since 2002. As such, the authority has contingency plans and every system/software is duplicated. The supplier Lockheed Martin is responsible for providing maintenance of the services and software. Crisis drills are performed annually, which involves various stakeholders including IT, Contactors, operations, as they switch from the primary site to the secondary site. The Energy transmission company OST performs crisis management exercises annually.

It is understood that general crisis management is necessary for national security, but cybersecurity is not yet considered as a component. AKCESK mandated CIIs and III's to manage the continuity of operations as part of the regulation on the content and method of documenting security measures[58].

Crisis management exercise design and planning authority may have been allocated in principle (either directly or via consultants), but cybersecurity crisis management planning has not been thoroughly outlined.

[58] http://akce.gov.al/publicAnglisht_html/wp-content/uploads/2016/04/regullore%20mbi%20p%C3%ABrmbajtjen%20dhe%20m%C3%ABnyr%C3%ABn%20e%20dokumentimit%20t%C3%AB%20%20masave%20t%C3%AB%20siguris%C3%AB.pdf

D 1.5 CYBER DEFENCE

This factor explores whether the government has the capacity to design and implement a cyber Defence strategy and lead its implementation, including through a designated cyber Defence organisation. It also reviews the level of coordination between various public and private sector actors in response to malicious attacks on strategic information systems and critical national infrastructure.

Stage: Formative to Established

Cybersecurity and cyber-defence is high on the agenda of Albania's defence-related institutions. From a national security perspective, the National Security Strategy (2014)[59] promotes the adoption and implementation of a National Cybersecurity Strategy as parts of its objectives.

The strategy emphasized safeguarding and protecting information in all forms of its existence, focusing on special efforts to protect against cyber-attacks. As such, cyber-defense is high on the agenda of Albania's defense-related institutions the Ministry of Defence (MoD) and the Air Force (AF), as the National Cyberdefence Strategy classifies cyber-attacks as a type one (highest importance) risk.

The MoD has progressed the notion of cyber-protection by initiating its own Cyber Defence Strategy (2014-2017)[60], which was designed to ensure orientation, coherence and focus for a comprehensive approach in developing military capabilities in cyber space. The second iteration of the strategy has initiated (2018-2020) for the MoD and the Air Force[61]. The strategy visions to develop defence capabilities and capacity building for cybersecurity. Such capabilities are made reliable, sustainable and efficient, focused on all strategic levels (operational and tactical operations) of MoD and Air Force (AF) while being in cooperation and coordination with national institutions. The cyber defence strategy has four key objectives:

1. *Implement full organizational and technical measures of cybersecurity in the systems and ICT.*
2. *Increase the responsibility of MoD / AF structures for cybersecurity.*
3. *Develop the level and skills of cybersecurity specialists and to SKI users.*
4. *Increase cooperation with responsible structures at national level and in the framework of NATO.*

[59] National Security Strategy (2014) promotes the adoption and implementation of a National Cybersecurity Strategy as parts of its objectives.
http://www.mod.gov.al/images/PDF/strategjia_sigurise_kombetare_republikes_se_shqiperise.pdf
[60] The Ministry of Defence (MoD) has progressed the notion of cyber-protection by initiating its own Cyber Defence Strategy (2014-2017)
http://www.mod.gov.al/images/PDF/Strategjia_per_Mbrojtjen_Kibernetike.pdf
[61] The second iteration of the strategy (2018-2020) for protection the MoD and the Air Force.
http://www.mod.gov.al/images/PDF/2017/Strategjia_Mbrojtjen_Kibernetike_2018_2020.pdf

A more detailed action plan on the implementation, the objectives and basic principles for security policies of systems liaison and information, will be published separately in the implementation of the Defence Strategy Cybernetics 2018 - 2020.

As a member of NATO, Albania signed the MoU with the NATO Cyber Incident Response Centre (NCIRC) on enhancing cyber defence in 2013 and is currently negotiating the signing of the new version of this MoU[62]. This version is based on the cyber defence document "NATO Enhanced Cyber Defence Policy", endorsed by all NATO countries at the Wales summit in 2014[63].

Albania is formally implementing the initial set of Organisation for Security and Cooperation in Europe (OSCE) "Confidence Building Measures" (CBMs) for cyberspace as of 2014 and has agreed in principle to further continue the process at hand with the approval of the second set of CBMs[64]. Albania has actively participated in the annual Cyber Coalition exercise, NATO's largest cyber exercise, since 2016[65].

It was not clear at the time of the review whether a central cyber command and control structure exists, or Cyber operations units are incorporated into the different branches of the armed forces.

D 1.6 COMMUNICATIONS REDUNDANCY

This factor reviews a government's capacity to identify and map digital redundancy and redundant communications among stakeholders. Digital redundancy foresees a cybersecurity system in which duplication and failure of any component is safeguarded by proper backup. Most of these backups will take the form of isolated (from mainline systems) but readily available digital networks, but some may be non-digital (e.g. backing up a digital communications network with a radio communications network).

Stage: Start-up

During the review it was not possible to obtain a clear comprehensive picture regarding communications redundancy in Albania. The Law No.2/2017 on Cybersecurity mandates CII and III operators to ensure appropriate resilience and continuity of operations.

Digital redundancy measures are considered (in an ad-hoc manner) by private companies and other organizations, but there is no measure coordinated and of systematic nature at the national level. Private institutions acknowledged having disaster recovery capabilities. Participants mentioned that a recovery system is in place, but the Government is in the

[62] https://www.diplomacy.edu/sites/default/files/Cybersecurity%20in%20Western%20Balkans.pdf
[63] https://www.nato.int/cps/en/natohq/official_texts_112964.htm
[64] https://www.diplomacy.edu/sites/default/files/Cybersecurity%20in%20Western%20Balkans.pdf
[65] https://www.nato.int/cps/en/natohq/news_138674.htm

process of creating a second one. The energy transmission company (OST) has complete redundancy duplication on multiple layers and networks.

Finally, there have been no exercises or drills conducted to test emergency response under circumstances with disrupted communications.

RECOMMENDATIONS

Following the information presented during the review of the maturity of *Cybersecurity Policy and Strategy*, the Global Cyber Security Capacity Centre has developed the following set of recommendations for consideration by the Government of Albania. These recommendations provide advice and steps aimed to increase existing cybersecurity capacity as per the considerations of the Centre's Cybersecurity Capacity Maturity Model. The recommendations are provided specifically for each factor.

R1.1 Develop, publish and implement a national cybersecurity strategy that is coherent with the Digital Agenda, National Security Strategy, and the Cyber Defense Strategy.

R1.2 Follow the new ITU Guide for Developing a National Cybersecurity Strategy.66

R1.3 Allocate budget to ensure the development and implementation of cybersecurity strategic plans. Consider aligning national legislative framework with provisions of NIS Directive and GDPR.

R1.4 Design a methodology to analyse the results of the national cyber risk assessment and incorporate lessons from this exercise in the development of the strategy.

R1.5 Initiate review processes of the forthcoming national cybersecurity strategy, including consistent stakeholder involvement.

R1.6 Design and disseminate coordinated cybersecurity programmes. Strengthen and promote inter-departmental cooperation in cybersecurity to ensure full implementation of the cybersecurity programmes.

[66] *The World Bank, Commonwealth Secretariat (ComSec), the Commonwealth Telecommunications Organisation (CTO), NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE). 2018. Guide to Developing a National Cybersecurity Strategy – Strategic engagement in cybersecurity. Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO). https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf*

R1.7 Design and conduct regularly scenario and real-time cyber exercises and drills that provide a contemporary picture of national cyber resilience.

R1.8 Allocate budget to ensure the implementation of cybersecurity strategic plans. Strategic plans might consider the implementation of the NIS and GDPR Directives.

INCIDENT RESPONSE

R1.9 Expedite the processes of joining FIRST to enable proactive and effective incident response67.

R1.10 Ensure that AKCESK has the necessary financial and human resources to fulfil its existing mandate for a national cyber incident response with clear processes and defined roles and responsibilities. Or consider outsourcing certain parts of incident handling to other organizations. Roles and responsibilities should include:

- *ensuring a high level of availability and business continuity;*
- *monitoring incidents at a national level;*
- *providing early warnings, alerts, announcements and disseminate threat intelligence to relevant stakeholders;*
- *responding to incidents;*
- *providing risk and incident analysis;*
- *establishing relationships with the private sector and other countries.*

R1.11 Consider establishing a unified and clear approach to incident notifications. Ensure good communication mechanisms between incident response entities.

R1.12 Establish metrics to monitor and evaluate the effectiveness of AKCESK.

R1.13 Establish regular training for the employees of the AKCESK and design metrics to assess the results of this training.

R1.14 Enhance the national cyber incident response escalation procedure detailing the role of the General Emergency Headquarters, coordination with other sectorial CSIRTs.

[67] https://www.first.org/

R1.15 Ensure the appropriate involvement of the financial authority in incident response.

R1.16 Perform the ENISA CSIRT Maturity Self-assessment Survey based on the SIM3 model to gain further insights on AKCESK maturity and capabilities68.

CRITICAL INFRASTRUCTURE (CI) PROTECTION

R1.17 Perform regular, detailed audits of CII assets with regards to cybersecurity and disseminate CII asset audit lists to relevant stakeholders. Monitor compliance of of regulatory responsibilities by CII owners.

R1.18 Establish a mechanism for regular vulnerability disclosure and information sharing between CII asset owners and the government. Establish regular dialogue between tactical and strategic/executive levels regarding cyber risk practices and encourage communication among CII operators.

R1.19 Ensure, data protection legislation (Law No. 9887 from 10.03.200) is adhered to possibly informed also by the GDPR guidelines in the sharing of threat-intelligence information.

R1.20 Mandate the design and implementation of appropriate regular cyber risk assessments for all CII stakeholders, in line with recommendations from the NIS Authority and identify the required information to be shared. Design cyber risk assessments for all CII stakeholders based on the national risk assessment approach.

CRISIS MANAGEMENT

R1.21 Design a cybersecurity needs assessment of measures and techniques for crisis management. The involvement of key stakeholders and other experts, such as think tanks, academics and civil society leaders should be sought.

[68]https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturity-self-assessment-survey

R1.22 Develop a national business continuity / disaster recovery / contingency plan for cyber incidents.

R1.23 Organise national cybersecurity exercises, identify metrics to evaluate the success of the exercises and ensure that lessons will inform the decision-making process for future exercises. Plan the exercises by engaging relevant participants, outlining their role in the exercise, and articulating the benefits of, and incentives for, participation.

CYBER DEFENCE

R1.24 Review command responsibilities and/or consider whether a centralised command unit should be established within the defence apparatus responsible for conflict using cyber means.

R1.25 Ensure dedicated Cyber Defence resources that are allocated based on national strategic objectives.

R1.26 Establish training programmes for MoD employees and develop awareness campaigns.

R1.27 Assess and determine cyber defence capability requirements, involving public and private sector stakeholders. Conduct continuous reviews of the evolving threat landscape in cybersecurity to ensure that cyber defence policies continue to meet national security objectives.

R1.28 Develop a communication and coordination mechanism for cyber defence in response to malicious cyber-attacks on military information systems and critical infrastructure. Clarify the role of defence, in CII and III's protection and how this operates.

COMMUNICATIONS REDUNDANCY

R1.29 Allocate appropriate resources on activities such as hardware integration, technology stress testing, personnel training and crisis simulation drills. Ensure that redundancy efforts are appropriately communicated to relevant stakeholders.

R1.30 Establish a process, involving all relevant stakeholders, to identify gaps and overlaps in emergency response asset communications and authority links.

R1.31 Link all emergency response assets into a national emergency communication network with isolated but accessible backup systems.

R1.32 Establish communication channels across emergency response functions, geographic areas of responsibility, public and private responders, and command authorities. Create outreach and education activities of redundant communications protocols tailored to the roles and responsibilities of each organisation in the emergency response plan.

R1.33 Allocate emergency communication exercise planning to a relevant authority. Conduct and test a needs assessment of measures with consideration of a simple exercise scenario. Since emergency exercises exist, as a first step include cyber elements within one of these scenarios.

R1.34 Identify metrics to evaluate the success of the exercise. Evaluate the exercises and feed the findings back into the decision-making process.

DIMENSION 2
CYBERSECURITY CULTURE AND SOCIETY

Forward-thinking cybersecurity strategies and policies need to engage a wide array of actors, including users. The days in which cybersecurity was left to experts formally charged with implementing cybersecurity have passed with the rise of the Internet. All those involved with the Internet and related technologies, such as social media, need to understand the role they play in safeguarding sensitive and personal data as they use digital media and resources. This dimension underscores the centrality of users in achieving greater cybersecurity maturity, but seeks to avoid conventional tendencies to blame users for problems with cybersecurity. Instead, cybersecurity experts need to build systems and programmes for users – systems that can be used easily, be trusted, and be incorporated in everyday practices online.

This dimension reviews important elements of a responsible cybersecurity culture and society such as the greater understanding of cyber-related risks by all actors, developing a learned level of trust in Internet services, e-government and e-commerce services, and users' employing even rudimentary techniques for protecting personal information online. This dimension also entails the existence mechanisms for accountability, such as channels for users to report threats to cybersecurity. In addition, this dimension reviews the role of media and social media in helping to shape cybersecurity values, attitudes and behaviour.

D 2.1 CYBERSECURITY MIND-SET

This factor evaluates the degree to which cybersecurity is prioritised and embedded in the values, attitudes, and practices of government, the private sector, and users across society-at-large. A cybersecurity mind-set consists of values, attitudes and practices, including habits, of individual users, experts, and other actors in the cybersecurity ecosystem that increase the resilience of users to threats to their security online.

Stage: Start-up

The cyber ecosystem in Albania is in its early stages. Participants mentioned that in some government agencies and leading companies a cybersecurity mind-set has started to develop but overall, users are generally unaware of the risks associated with use of the Internet.

Within the private sector leading firms have begun to place greater priority on a cybersecurity mind-set, such as by identifying high-risk practices. As participants stated, CEOs and members of the board or management do prioritise cybersecurity and are developing a cybersecurity mindset but usually this is the case only within the larger organisations. At the local level, or for SMEs, there is more of a lack of a cybersecurity mindset.

Users are perceived to have no or minimal recognition of the need to prioritise a cybersecurity mind-set and take no proactive steps to improve their cybersecurity. Participants mentioned that one of the reasons for the general lack of a cybersecurity mindset is that in rural areas there is limited access to the Internet as well as low levels of digital illiteracy, which constitute a disadvantage for most rural residents. Moreover, the existing cybersecurity awareness efforts are limited in scale and insufficient to provide knowledge for society as a whole (see D3.1).

D 2.2 TRUST AND CONFIDENCE ON THE INTERNET

This factor reviews the level of user trust and confidence in the use of online services in general, and e-government and e-commerce services in particular.

Stage: Start-up to Formative

Most Internet users are overly trusting in websites and in what they see or receive online. The lack of provision of e-services in the past has contributed to a lack of trust in the Internet. Most Albanian residents are living in villages which lack ICT infrastructure and connectivity, leaving them with little experience of online information or services usage. In line with this, stakeholders mentioned that IT literacy is low while older generation CEOs and board members are also exhibiting insufficient knowledge about IT to have a cybersecurity mindset.

The Government continues to increase e-service provision, but also recognises the need to increase the uptake of these services, as well as the application of security measures to establish trust in their usage. At present, there is a broad perception that users in Albania are unfamiliar with or lack trust in the e-government services provided.

There has been a significant investment in IT, such as through the Government's modernisation programme in IT services and the development of the national portal, known as e-Albania. In 2015, the Albanian government launched the e-Albania portal[69], the country's first portal for e-services. This portal launched the first 150 e-services resulting in nearly all government institutions, agencies and authorities incorporating their e-services in this one portal. The e-Albania portal is the primary portal for all government-related services such as e-tax declarations, certificates, health cards, national ID card, etc. As stated in the Digital Agenda Strategy 2015-2020[70], the expansion of GovNET (G2G) infrastructure has led to the establishment of such innovations as an infrastructure for interaction, e-tax, e-procurement,

[69] www.e-albania.al

[70] http://akshi.gov.al/wp-content/uploads/2018/03/Digital_Agenda_Strategy_2015_-_2020.pdf

e-customs, e-patents, e-fines services, Civil State National Register, and issuance of biometric documents.

Also, there have been efforts by the Albanian government to gain experience from the Estonian government to reduce physical documents and other paperwork. In addition, since 2012, the e-government portal has undergone regular penetration testing and has been protected, having received a valid Symantec portal certificate.

Albania's Cross-cutting Strategy on Information Society[71] was focused on the development of e-governance at the central level including some objectives for e-governance at the local level. At the local level there are municipalities or districts that have developed e-governance practices, such as providing information related to services, and opportunities for e-participation. In the meantime, there are a large number of municipalities and city halls that are still far from being able to utilize the ICTs or e-government resources.

Citizens are required to use the e-government services via the e-Albania portal. However, participants mentioned, that there is a considerable number of citizens who are using middle-men, proxy users, or paid services to help them with their e-government needs, partly due to their lack of ICT literacy. In addition, there is a general problem of negative perceptions surrounding the Internet, since a number of famous people have fallen victim of fraud and cybersecurity incidents.

While e-commerce services are being provided, the private sector recognises the need for improving the application of security measures to establish trust in ecommerce services. From a security perspective, all transactions have to be digitally signed with e-signatures and trusted services. However, participants mentioned that a limited proportion of users trust in the secure use of e-commerce services.

Stakeholders stated that the latest trend has been to transition services to cloud provision. However, there is a general uncertainty and lack of trust in the cloud services, since the concept is based on something not physically tangible with physical locality. Another concern raised during the review was the fact that in Albania, there is insufficient level of trust among different stakeholders, making the cooperation even more difficult in the online world.[72]

[71]http://shtetiweb.org/wp-content/uploads/2014/05/Information-Society-strategy_printed_version_en.pdf

[72]Dushi, Desara. (2017). Cybersecurity in Albania: a Multistakeholder Approach. https://www.researchgate.net/publication/315495692_Cybersecurity_in_Albania_a_Multistakeholder_Approach

D 2.3 USER UNDERSTANDING OF PERSONAL INFORMATION PROTECTION ONLINE

This factor looks at whether Internet users and stakeholders within the public and private sectors recognise and understand the importance of protection of personal information online, and whether they are sensitised to their privacy rights.

Stage: Start-up to Formative

Awareness around the protection of personal information and concerns over security of personal data is generally low. Users and stakeholders within the public and private sectors often lack a general knowledge about how personal information is handled online. As mentioned above, participants noted that personal information is often shared through social media, especially by young users. Also, the lack of trust in privacy and data protection is one of the major barriers to the greater use of e-government services (see D2.1).

The Law No. 9887 of 10.3.2008 "On the Protection of Personal Data[73] aims at defining the rules for the protection and legal processing of personal data in Albania. The Law states that the legal processing of personal data shall respect and guarantee the fundamental rights and freedoms of persons and, in particular, their right to privacy. However, as stakeholders mentioned, the GDPR is being transposed step by step into local Albanian laws, resulting in progressing a sense of awareness around cybersecurity generally and the ISO27001 certification, in particular.

Overall, there is no public debate over this issue, but some discussions take place, usually among those who are generally well informed.

D 2.4 REPORTING MECHANISMS

This factor explores the existence of reporting mechanisms functioning as channels for users to report internet related crime such as online fraud, cyber-bullying, child abuse online, identity theft, privacy and security breaches, and other incidents.

Stage: Formative

Participants mentioned that there are reporting mechanisms in place for users to report computer-related or online incidents and crimes. Citizens can report incidents to the Albanian State Police in person or through a specialised online platform.

[73]https://www.afapdp.org/wp-content/uploads/2018/05/Albanie-Loi-n%C2%B0-9887-sur-la-protection-des-donnees-personnelles-2008.pdf

The Police will record the incident, categorise it, obtain evidence and share the information with the prosecution office. For example, if an incident is targeting or affecting CI and II's then it is reported to the AKCESK. Moreover, cooperation mechanisms have been established with Interpol and relevant agencies. Another reporting mechanism is the Albanian National Child Helpline (ALO 116 ANCH)[74], which is a free service available to children and youth 24/7 and the mobile phone application isigurt.al. However, it was not possible to identify specific efforts in promoting the existing reporting channels in a coordinated manner but rather on an ad-hoc basis.

Overall, participants mentioned that the State Police cybercrime investigative unit has limited resources and lacks specialized hardware to cover incident handling at a national level. Therefore, attention needs to be placed on ensuring sufficient resources and continued trainings for employees of the Unit.

D 2.5 MEDIA AND SOCIAL MEDIA

This factor explores whether cybersecurity is a common subject across mainstream media, and an issue for broad discussion on social media. Moreover, this aspect speaks about the role of media in conveying information about cybersecurity to the public, thus shaping their cybersecurity values, attitudes and online behaviour.

Stage: Start-up to Formative

In Albania there is ad-hoc media coverage of cybersecurity, with limited information provided and limited reporting on specific issues that individuals face online, such as online child protection or cyberbullying. Also, there is little discussion on social media about cybersecurity. As participants mentioned, the media and bloggers on social media are most interested in cyber incidents that celebrities might have fallen victims of and not in specific issues such as cyberbullying. Any coverage would usually last for three days and then fade away.

It was suggested by stakeholders that the State Police need to cooperate with media to promote greater levels of cybersecurity awareness. Close cooperation between the police, the media, the chamber of commerce is needed to raise the awareness of online fraud and other computer related risks.

[74] http://www.alo116.al/

RECOMMENDATIONS

Based on the consultations, the following recommendations are provided for consideration regarding the maturity of *cyber culture and society*. These aim to provide possible next steps to be followed to enhance existing cybersecurity capacity as per the considerations of the GCSCC's Cybersecurity Capacity Maturity Model.

CYBERSECURITY MIND-SET

R2.1 Enhance efforts at all levels of government, especially officials, and the private sector to employ cybersecurity good (proactive) practices. Design systems that enable users across society to embed secure practices more easily into their everyday use of the Internet and online services.

R2.2 Develop coordinated training programmes for employees in the public sector.

R2.3 Routinize cross-sectorial cooperation and information sharing among private and public sector organisations on cybersecurity risks and good practice.

R2.4 Identify vulnerable groups and high-risk behaviour across the public to inform targeted, coordinated awareness campaigns.

R2.5 Promote collaboration with the NGOs and private sector in providing youth educational programmes safe and responsible behaviour online.

R2.6 Consider setting up a multi-stakeholder group (including business, government, law enforcement agencies, and academia) to run joint projects and initiatives as well as facilitate on-going discussions on cybercrime and cybersecurity issues.

TRUST AND CONFIDENCE ON THE INTERNET

R2.7 Promote use of e-government services and trust in these services through a coordinated programme, including the compliance to web standards that protect the anonymity of users.

R2.8 Ensure that security measures are in place for existing e-government services for businesses and public organisations.

R2.9 Work towards harmonizing the e-governance development, both on the central and local level.

R2.10 Implement feedback mechanisms for use to ensure that e-services are continuously improved, and trust is strengthened among users.

R2.11 Employ processes for gathering user feedback within government agencies in order to ensure efficient management of online content.

R2.12 Consider educating the public by developing an effective Cybersecurity Communication Strategy/Plan (for e.g.: strategic approach to cyber crises, promoting the benefits of using e-government services and suggesting deadlines to register).

R2.13 Establish ISP programmes to promote trust in their services based on measures of effectiveness of these programmes.

R2.14 Encourage the development of e-commerce services with emphasising the need for a security (for e.g.: use of SSL encryption, post trust certificates/logos of third-party authentication services on the homepage).

USER UNDERSTANDING OF PERSONAL INFORMATION PROTECTION ONLINE

R2.15 Promote the understanding of protection of personal information online among users and promote the development of their skills to manage their privacy online.

R2.16 Encourage a public debate regarding the protection of personal information and about the balance between security and privacy to inform policy-making.

R2.17 Promote the compliance to web standards that protect the anonymity of users.

R2.18 Develop user-consent policies designed to notify practices on the collection, use or disclosure of sensitive personal information.

REPORTING MECHANISMS

R2.19 Develop programmes to promote the use of the existing reporting mechanisms by public and private sectors for reporting online fraud, cyber-bullying, child abuse online, identity theft, privacy and security breaches, and other incidents.

R2.20 Encourage different stakeholders (public-private sector, Police, CERT) to coordinate the reporting mechanisms and their roles and responsibilities, and to collaborate and share good practices to improve the mechanisms.

R2.21 Raise awareness about new and existing reporting channels among the wider public and across stakeholder groups and cooperate with the private sector in this regard.

R2.22 Employ effectiveness metrics for all existing mechanisms and ensure that they contribute to their improvement.

R2.23 Ensure that the Cybercrime Investigative Unit within the Police has sufficient resources and technical equipment to cover all regions.

MEDIA AND SOCIAL MEDIA

R2.24 Encourage media and social media providers to further extend the coverage beyond threat reporting and focus on informing the public about proactive and actionable cybersecurity measures, as well economic and social impacts.

R2.25 Develop programmes and campaigns to raise awareness among media providers and leading social media actors, especially during the Cybersecurity Awareness Month (October) (see also R3.1).

R2.26 Encourage a frequent discussion about cybersecurity on social media.

R2.27 Ensure that the debate in social and mainstream media and the attitudes expressed inform policymaking.

DIMENSION 3
CYBERSECURITY EDUCATION, TRAINING AND SKILLS

This dimension reviews the availability of cybersecurity awareness-raising programmes for both the public and executives. Moreover, it evaluates the availability, quality, and uptake of educational and training offerings for various groups of government stakeholders, private sector, and the population as a whole.

D 3.1 AWARENESS RAISING

This factor focuses on the prevalence and design of programmes to raise awareness of cybersecurity risks and threats as well as how to address them, both for the general public and for executive management.

Stage: Start-up to Formative

A national programme for cybersecurity awareness raising, led by a designated organisation (from any sector) which addresses a wide range of demographics is yet to be established. In the last few years Albania carried out periodic awareness activities for a safer internet, as well as activities on the international day of Safer Internet. Albania celebrates October as a cybersecurity awareness month. Moreover, there is a child security week in March.

It was stated by participants that raising awareness for parental control, protection of children from the illegal and harmful internet and online media content requires more attention and the engagement of different institutions and actors, such as the private sector, NGOs, media, schools and parent community. Albania is part of the Global Alliance against the Sexual Exploitation of Children in the Internet, established on December 5, 2012. The alliance countries have agreed to work in achieving four objectives:

a) Increase the efforts for the identification of victims and ensuring that they will receive the necessary assistance, support and protection;

b) Increase the efforts in investigating the sexual exploitation cases against children on the internet and identify and prosecute persons violating the law;

c) Increase the awareness of children, parents, educators and the community in general in relation to the dangers;

d) Reduce the availability of child pornography on the internet and re-victimization of children.

At the national level, the Children's Human Rights Centre of Albania (CRCA)[75], the National Authority for Electronic Certification and Cyber Security (AKCESK), the Albanian National Child Helpline (ALO 116), in cooperation with government institutions, NGOs and internet service providers (ISPs) are organising a national conference on the framework of Safer Internet Day in 2018. Signing of the National Action Plan 2018-2020 and the Code of Conduct (by the private sector) will be the most important outcomes of this event. Within these efforts the aim is to engage schools, teachers and parents to lead their own action, to be the needed change and to promote the message and slogan: "Create, connect and share respect: A better internet starts with you". Additionally, actions include:

- *Social media campaign.*
- *Open awareness hours with parents, since they have a crucial role in child online safety.*
- *Promotion of the reporting mechanisms and tools for child online protection such as a mobile phone application, isigurt.al, alo116.al, and so on (see D2.4).*

AKCESK is the legal mandated Authority created by Decision of Council of Ministers (DoCM 141 Dated 22.2.2017) to organize awareness campaigns, trainings, publish informative materials either for the private or public sector. AKCESK in conjunction with the Ministry of Education, Sport and Youth and the banking sector conducted a pilot programme for schools on raising awareness about cyberbullying. However, this effort was limited in scope.

Additionally, the Cybercrime Unit works with NGOs to visit schools and provide trainings for children. For example, the State Police conducted Child safety online programs which were directed at students and concerned the areas of child abuse and child online safety. The one or two-months sessions were for students, teachers as well as parents. Participants stressed on the importance of such initiatives, since Albania faced a couple of cases when children fell victim to suicide games, for which the support from Europol was requested.

The private sector is starting to consider cybersecurity awareness, however this process is still at early stages. As review participants noted, even the most prominent corporations do not regard security awareness as a significant concern. Executives are made aware of general cybersecurity issues, but not how these issues and threats might affect their organisation. Stakeholders from civil society mentioned that there are also regular meetings with the European Commission and the Internet Governance Forum (IGF) on cybersecurity awareness.

Overall, review participants agreed that awareness, training and IT skills are necessary for the country and that the gap they perceive Albania is facing has to do with the lack of personal development in cybersecurity. There is a gap in education and also between parents' and

[75] https://www.betterinternetforkids.eu/web/albania

children's literacy. Although internet penetration is 70%, especially among the youth, the majority of the population do not seem to worry about their computer literacy.

Social media such as Facebook are being used for commercial purposes and users share their information freely online. There is still a lack of awareness of security among the youth and, as participants mentioned, young people are more concerned about the rating of the product and the sellers, as opposed to the security of the environment. PayPal is often used for online purchases, as parents do not trust providing their credit cards directly. Social engineering attacks are proliferating, as people tend to give away sensitive information freely and willingly to anyone claiming to be from IT or management. Awareness programmes have been initiated to counter the *status quo*. Participants suggested that by providing adequate training and education the existing gap shall be bridged.

Participants have expressed a view of the need to have a top-down approach in raising the awareness levels on the national level: starting from the highest level of Government, then trickling down to the ministers' level, and so on.

D 3.2 FRAMEWORK FOR EDUCATION

This factor addresses the importance of high quality cybersecurity education offerings and the existence of qualified educators. Moreover, this factor examines the need for enhancing cybersecurity education at the national and institutional level and the collaboration between government, and industry to ensure that the educational investments meet the needs of the cybersecurity environment across all sectors.

Stage: Start-up to Formative

The need for enhancing cybersecurity education in schools and universities has been identified by the Government, industry, and stakeholders in academia.

ICT in education constituted one of the main directions set out in the Cross-cutting Strategy for the Information Society (ISSIS) 2008-2013[76]. Currently, there are 1,496 computer laboratories in the pre-university education. The internet network has been installed in schools by allowing students and teachers to utilize different information sources, as well as specifically to assist in their work of curricular projects. Each school has a dedicated broadband connection, but this remains confined only in the computer laboratories. Moreover, the ratio of computer use per student varies from school to school: it stands at approximately 1:27, while in some cases it is even lower.

Currently, public and private universities and colleges offer educational courses in cybersecurity-related fields, such as information security, network security and cryptography, but cybersecurity-specific courses are not yet offered.

[76] http://akshi.gov.al/wp-content/uploads/2018/03/Digital_Agenda_Strategy_2015_-_2020.pdf

Luarasi University College[77] offers a Bachelor in Information Technology and Innovation and a Bachelor in Economics and Information. Moreover, a Master of Science in Information Technology and Innovation is also offered. This year for the first time Luarasi University has initiated a professional one-year Master's of Science degree program in cybersecurity. Within this programme modules in information and cybersecurity assurance, cybersecurity governance, and cybersecurity law will be taught.

EPOKA University[78] offers a Bachelor in Computer Engineering and a Masters programme in Computer Engineering. CIT University[79] offers a Bachelor in Software Engineering, a Bachelor in "Computer Engineering and Information Technology", a Bachelor in Industrial Engineering, a Master of Science in Software Engineering, a Master of Science in Computer Engineering and Information Technology, and Master of Science in Telecommunication Engineering. Lastly, the University of Tirana[80] offers a Masters in Information Security and a Professional Master in Information Technology and Business Process Management.

The National University is currently developing a programme that will include workshops with the banking sector, chief information officers, mobile telecoms, insurance companies to understand the needs of the private sector.

The Ministry of Education, Sport and Youth mandates that only doctorate (PhD) holders can teach courses. As participants mentioned, this mandate creates a significant challenge since there are not enough lecturers who are specialised in cybersecurity. In addition, the market requires technical and professional cybersecurity skills that are not necessarily obtained through rigorous theoretical programs. Similarly to other countries, in Albania the lack of cybersecurity professionals is one of the most crucial issues. Therefore, there is a need for professionals to teach. It was suggested by stakeholders that the solution could be in engaging lecturers as well as cybersecurity experts in educational programmes. Experts have the technical know-how and could bridge the existing gap.

D 3.3 FRAMEWORK FOR PROFESSIONAL TRAINING

This factor addresses the availability and provision of cybersecurity training programmes building a cadre of cybersecurity professionals. Moreover, this factor reviews the uptake of cybersecurity training and horizontal and vertical cybersecurity knowledge transfer within organisations and how it translates into continuous skills development.

[77] www.luarasi-univ.edu.al
[78] www.epoka.edu.al
[79] http://www.cit.edu.al
[80] http://www.feut.edu.al/stafi.html

Stage: Start-up

The need for training professionals in cybersecurity has been recognized by the Government but has not been documented on the national level, as review participants noted. In Albania public and public sector agencies are not certified under internationally recognized standards.

Within the public institutions training on cybersecurity issues both for IT staff and general staff is very limited and often depends on the respective management in the institution, i.e. if a specific member of staff can attend a general cybersecurity training or certification course. As stakeholders stated, it is not easy for the Government to allocate resources for training employees.

Internationally accredited IT Security and Governance training and certification courses are being offered in Albania[81]. Experts can select from a range of courses such as IT Security and Governance Certification Courses, Foundation Level IT Security and Governance Certification Courses (Ethical Hacking Foundation Training and Certification and COBIT 5 Foundation Certification Training Course), Intermediate Level IT Security and Governance Certification Courses (i.e. CGEIT Course) or Advanced Level IT Security and Governance Certification Courses (i.e. CRISC Course, COBIT 5 Assessor Certification Training Course, COBIT 5 Implementation Certification Training Course).

Recently, a Training programme on Common Security and Defence Policy (CSDP TP SAP 2017) has been offered in Albania[82] with participation of representatives from Western Balkan countries and EU member states. The training programme is held under the aegis of the European Security and Defence College (ESDC), with support of the ministries of defence of Austria, Hungary, and Albania, and the Technical Assistance and Information Exchange instrument of the European Commission (TAIEX).

As mentioned by the review participants, the perception of the private sector boards and CEOs towards cybersecurity needs significant improvement. Often, some worry of the financial burdens cybersecurity brings about. Also, it is common that the technical IT staff are usually generalists who do everything computer-related, including cybersecurity. IT staff lack the ability to demonstrate the value of cybersecurity to the management and the boards as they do not speak the “business language”. Stakeholders also stated that often organisations face intense requirements for cost savings, which result in having second-hand used computer equipment.

Another concern shared by the participants is the challenge in retaining security professionals within Albania, as they often leave the country to seek better opportunities in the EU or North America. However, the Albanian market has produced demand for specific types of expertise; first it started to seek specialists in IT infrastructure, then in programming, networking, web design, cloud. And now there is a need for specialists in cybersecurity. Stakeholders suggested that the primary need is in preparing staff for cybersecurity from the university level.

[81] https://www.invensislearning.com/al/it-security-and-governance-training-albania/

[82] https://europeanwesternbalkans.com/2017/10/06/training-programme-common-security-defence-policy-closes-albania/

RECOMMENDATIONS

Following the information presented on the review of the maturity of *cybersecurity education, training and skills*, the following set of recommendations are provided to Albania. These recommendations aim to provide advice and steps to be followed for the enhancement of existing cybersecurity capacity, following the considerations of the GCSCC Cybersecurity Capacity Maturity Model.

AWARENESS RAISING

R3.1 Strengthen the mandate of AKCESK to perform the role of developing and implementing a planned national cybersecurity awareness-raising programme. Coordinate and cooperate with key stakeholders from all sectors.

R3.2 Consider creating a national single online portal linking to appropriate cybersecurity information and disseminate the cybersecurity awareness programme via this platform.

R3.3 Coordinate awareness-raising efforts, for instance through a dedicated cybersecurity awareness month and develop materials for specified target groups and sectors, based on international good practice.

R3.4 Integrate cybersecurity awareness-raising efforts into ICT literacy courses and build upon existing initiatives as established vehicles for cybersecurity awareness-raising campaigns.

R3.5 Develop a dedicated awareness-raising programme for executive managers within the public and private sectors, as this group is usually the final arbiters on investments into security. The programme could focus on emphasizing the responsibility and accountability of Executive leaders and Board members towards Cybersecurity.

R3.6 Promote awareness raising efforts of cybersecurity crisis management at the executive level.

R3.7 Promote awareness of risks and threats at all levels of the government.

R3.8 Enact evaluation measurements to study effectiveness of the awareness programmes at a level where they inform future campaigns taking into account gaps or failures.

FRAMEWORK FOR EDUCATION

R3.9 Create cybersecurity education programmes for instructors of cybersecurity to ensure that skilled staff is available to teach newly-formed or existing cybersecurity courses.

R3.10 Create accredited cybersecurity-specific degree courses at undergraduate and post-graduate level, in addition to the other existing cybersecurity-related courses in the various universities in Albania.

R3.11 Promote efforts by universities and other bodies to hold seminars/lectures on cybersecurity issues aimed at non-specialists.

R3. 12 Integrate specialised cybersecurity courses in all computer science degrees at universities and offer specialised cybersecurity courses in universities and other higher education bodies.

R3.13 Collect and evaluate feedback from existing students for further development and enhancement of cybersecurity course offerings.

R3.14 Create initiatives to advance cybersecurity education in the primary and secondary school curricula.

R3.15 Develop partnerships for the development of interfaces for research, innovation and interaction between universities and the private sector.

R3.16 Revisit the requirement by the Ministry of Education, Sport and Youth that mandates that only PhD holders can teach courses.

R3.17 Introduce cybersecurity experts as instructors in university-level educational programmes and coordinate efforts to prepare and entice more teachers/lecturers to be involved with Cybersecurity teaching.

R3.18 Ensure the sustainability of research programs.

R3.19 Develop effective metrics to ensure that educational and skill enhancement investments meet the needs of the cybersecurity environment and gather statistics on the supply and demand of cybersecurity graduates.

FRAMEWORK FOR PROFESSIONAL TRAINING

R3.20 Identify training needs and develop training courses, seminars and online resources for targeted demographics, including non-IT professionals. Cooperate with the private sector to develop those offerings.

R3.21 Provide training for experts on various aspects of cybersecurity, such as technical training in data systems, tools, models, and operation of these tools.

R3.22 Establish continuous training for IT employees and general employees regarding cybersecurity issues within all sectors.

R3.23 Develop metrics to evaluate the take up and success of cybersecurity training courses.

R3.24 Create special initiatives to retain skilled cybersecurity professionals in Albania

R3.25 Create a knowledge exchange programme targeted at enhanced cooperation between training providers and academia.

R3.26 Ensure that affordable security professional certification is offered across sectors within the country. Different forms of professional Cybersecurity certification, e.g. ISACA certifications, will provide suitable skills at a faster rate.

R3.27 Develop a central platform for sharing training information for experts and create a national-level register of cybersecurity experts.

DIMENSION 4
LEGAL AND REGULATORY FRAMEWORKS

This dimension examines the government's capacity to design and enact national legislation directly and indirectly relating to cybersecurity, with a particular emphasis placed on the topics of ICT security, privacy and data protection issues, and other cybercrime-related issues. The capacity to enforce such laws is examined through law enforcement, prosecution, and court capacities. Moreover, this dimension observes issues such as formal and informal cooperation frameworks to combat cybercrime.

D 4.1 LEGAL FRAMEWORKS

This factor addresses legislation and regulation frameworks related to cybersecurity, including: ICT security legislative frameworks; privacy; freedom of speech and other human rights online; data protection; child protection; consumer protection; intellectual property; and substantive and procedural cybercrime legislation.

Stage: Established

Albania does not have an all-encompassing regulation that deals explicitly with cybersecurity. Instead, several official guidelines have been adopted that refer to cybersecurity issues.

During 2008 and subsequently, a series of legislative initiatives have been taken and these institutions have been created: the Ministry for Innovation in Information and Communication Technology (MITIK - now defunct), e-Albania (government portal), National Agency for Information Society (AKSHI), the Authority of Electronic and Postal Communications (AKEP), National Electronic Certification Authority (AKCE) evolved by law 2-2017 as AKCESK, Protik (ICT resource center) and the Computer crime Division at the General Directorate of State Police, which are fully committed to completing the legal framework and regulation of direct and indirect relationships between state institutions with each other, and between them and private institutions and citizens[83].

[83] http://www.mcser.org/journal/index.php/mjss/article/viewFile/1236/1265

The most relevant legislative frameworks and guidelines related to Albania's Internet landscape are:

- *Law No. 7895 from 27.01.1995, Criminal Code of Albania*[84]
- *Law No. 7905 from 21.03.1995, Criminal Procedure Code of Albania*[85]
- *Law No. 9918 from 19.05.2008, On electronic communications*[86]
- *Law No. 9887 from 10.03.2008, On protection of personal data*[87]
- *Law No. 8888, date 25.4.2002 for Ratification of ''Convention for Crime in the Cybernetic Area''*[88]
- *Law No.9880, dated 25.02.2008, On electronic signature*[89]
- *Law No.10128, dated 11.05.2009, On electronic commerce*
- *Law No. 9643 of 20.11.2006 amended, for the public procurement that enables the electronic procurement*[90]
- *Law No. 9723 of 3.5. 2007 on the registration of businesses On the National Center of Registration*
- *Law no. 10273 from 29.4.2010, On electronic document*[91]
- Law no 2/2017 On Cyber Security[92]
- Law no 107/2015 On Electronic Identification and Trust Services[93]

Albania has signed and ratified the Budapest Convention for Cyber Crime and has reflected in the Penal Code and Penal Procedure Code the requirements of the Convection. As seen above, several legal instruments refer to cybersecurity related issues such as the Law on Personal Data Protection, the Law on Electronic Commerce, the Law on Electronic Communications, and the Law on Electronic Signature.

National agencies have specific laws that are required to be implemented. Every organisation has produced their rules regarding internet traffic.

The Constitution of Albania proclaims that fundamental human rights and freedoms are indivisible, inalienable, and inviolable and stand at the base of the entire juridical order. In addition, Article 17 of the Constitution specifies that any limitation to the rights and freedoms must be established by law, in the in the public interest or for the protection of the rights of others and should be proportionate. Limitations should not infringe the essence of the rights and freedoms and may not exceed the limitations provided for in the European Convention on Human Rights. The Constitution guarantees among others:

- *Article 22 – Freedom of expression*
- *Article 23 - Right to information*

[84] http://rai-see.org/wp-content/uploads/2015/08/Criminal-Code-11-06-2015-EN.pdf
[85] http://www.wipo.int/wipolex/en/details.jsp?id=54
[86] http://aida.gov.al/images/ckeditor/law-nr-9918-date-19.05.2008-.pdf
[87] http://www.institutemedia.org/Documents/PDF/Law%20on%20protection%20of%20personal%20data.pdf
[88] http://www.cybercrimelaw.net/Albania.html
[89] http://aida.gov.al/images/ckeditor/Law%20no%209880%20date%2025.02.2008.pdf
[90] https://albaniaenergy.org/onewebmedia/ACERC%20Law%200004.pdf
[91] http://cesk.gov.al/publicAnglisht_html/wp-content/uploads/2016/04/ligji10273.pdf
[92] http://cesk.gov.al/publicAnglisht_html/wp-content/uploads/2016/04/Ligji%20_Per_Sigurine_Kibernetike_Nr_2_Date_26.1.2017.pdf
[93] http://cesk.gov.al/publicAnglisht_html/wp-content/uploads/2016/04/ligji107.pdf

- *Article 36 - Freedom and secrecy of correspondence or any other means of communication*
- *Article 37 - Inviolability of the residence.*

As a rule, national legislation provides for the requirement of judicial oversight, namely requiring judge's authorisation for certain procedural measures if fundamental rights are in danger (for example in cases of interception of communications or for obtaining traffic data). Moreover, Law No. 9887 from 10.03.2008, "On protection of personal data, Article 11'', speaks on processing of personal data and freedom of expression.

Albania's Law No. 9887 "On protection of personal data'' aims at defining the rules for the protection and legal processing of the personal data. The Law refers to "Electronic instruments" meaning the computer, computer programmes and any other electronic or automatic means used for the processing data. As participants mentioned the data protection authority is effectively considering to enforce the GDPR and discussions have been initiated on this matter.

Comprehensive legislation on protection of children online has been adopted and enforced under Articles

- *Article 117/2 of the Criminal Code on Pornography*[94].
- *Law N. 23/201231*[95]

Albania has adopted an action plan for the protection of children's rights (DCM No. 182/2012)[96]. This document also foresees a few activities for the online protection of children. Pursuant to this plan, in February 2013 the largest electronic communications companies in Albania and the IT association company, AITA signed the Code of Conduct, as a self-regulatory practice. Upon the signing of this code the companies engaged in delivering technical filtration techniques and parental advice for the protection of children and young people from the illegal and harmful electronic communications. Also, objectives 4.2 and 5.2 of the National Child Strategy of Albania[97] refer to the protection from inappropriate and harmful content and establishment of helplines. Albania has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child[98]. Moreover, Albania has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography[99].

Currently, Albania does not have any officially recognized agency that offers institutional support on child online protection. Albania is part of the Global Alliance against the Sexual Exploitation of Children in the Internet, established on December 5, 2012. Moreover, the

[94] https://www.legislationline.org/documents/section/criminal-codes/country/47
[95] https://www.coe.int/en/web/cybercrime
[96] http://akshi.gov.al/wp-content/uploads/2018/03/Digital_Agenda_Strategy_2015_-_2020.pdf
[97] http://www.crca.al/sites/default/files/publications/National%20Strategic%20Plan.pdf
[98] https://www.ohchr.org/Documents/ProfessionalInterest/crc.pdf
[99] https://www.ohchr.org/Documents/ProfessionalInterest/crc-sale.pdf

Children's Human Rights Centre of Albania (CRCA)[100] organises projects targeting schools awareness, teachers, and parents on online safety as well (see D3.1).

Currently, the legislation protecting consumers from business malpractice online has not been developed. Albania has enacted Law no. 9902, dated 17.04.2008 "On consumer protection"[101], Law No.9880, dated 25.02.2008, "On electronic signature", Law no.107/2015 "On electronic identification and trust services" and Law No.10128, dated 11.05.2009, "On electronic commerce". The Electronic Certification Directory which is part of AKCESK is in charge of supervision of the implementation of the Law on electronic signature, Law on electronic identification and trust services and sublegal enactments issued in accordance with those laws. AKCESK accredits the providers of electronic certification and trust services.

The Albanian legislative acts governing copyright and intellectual property are the Law on Industrial Property, No. 9947 dated 7 July 2008[102], and the Law on Copyright and Related Rights, No. 9380, dated 28 April 2005[103] (amended). The Law on Copyright and Related Rights governs the rights and obligations of participants in the creative, productive and commercial activities and any other evaluation, utilization, exercise, literature, art or science activity.

As mentioned above, the Law No. 8888 of 25 April 2002 "On Ratification of the Convention on Cyber Crime," 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". The Criminal Code of the Republic of Albania[104] covers the following substantive provisions related to cybercrime:

- *Article 74/a Computer-related distribution of pro-genocide or crimes against humanity materials*
- *Article 84/a Threat under motives of racism and xenophobia through computer-based system*
- *Article 117 /2 Pornography*
- *Article 119/a Distribution of racist or xenophobic materials through computer-based system*
- *Article 119/b Insult under motives of racism and xenophobia through computer-based system*
- *Article 137/a Theft of electronic communication network*
- *Article 143/b Computer-related fraud*
- *Article 186/a Computer-related forgery*
- *Article 192/b Unauthorized computer access*
- *Article 293/a Unlawful interception of computer-related data*
- *Article 293/b Interference with computer-related data*
- *Article 293/c Interference with computer-related systems*
- *Article 293/ç Misuse of equipment*

[100] https://www.betterinternetforkids.eu/web/albania
[101] http://www.erru.al/doc/Consumer_Protection_Law_No.9902,_17.04.2008_English_version.pdf
[102] http://www.wipo.int/edocs/lexdocs/laws/en/al/al069en.pdf
[103] http://www.wipo.int/edocs/lexdocs/laws/en/al/al054en.pdf
[104] http://rai-see.org/wp-content/uploads/2015/08/Criminal-Code-11-06-2015-EN.pdf

Similarly, procedural cybercrime legal provisions are fully implemented in the Law on Criminal Procedural law, Article 299/a of the Criminal Procedure Code (CPC) - expedited preservation and maintenance of computer data; Article 101 of the Law no. 9918 from 19.05.2008 "On electronic communication" - preservation and administration of data for the purpose of criminal prosecution; Article 299/b of CPC - expedited preservation and partial disclosure of computer data; Article 191/a of CPC - obligation to produce computer data; Article 208/a of the CPC - seizure of computer data; Articles 221-223 of the CPC - interception of communications (including provisions on the limits, authorisation and procedure).

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", and article 17 of Law no.107/2015 "On Electronic Identification and Trust Services". 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 under supervision of AKCESK as a national accreditation body. For citizens the PKI is administered by ALEAT (Part of IDEMIA) on behalf of Ministry of Interior.

Review participants mentioned that there has been an increase in hacking incidents on private emails and social media accounts of high-profile individuals as well as fraud incidents. Regarding cross border investigations and electronic evidence from companies and ISPs outside of the country, stakeholders stated that the current legislation is not sufficient. Stakeholders stressed the need for amendment of the legislation as well as advancing forensic investigations capabilities.

This factor studies the capacity of law enforcement to investigate cybercrime, and the prosecution's capacity to present cybercrime and electronic evidence cases. Finally, this factor addresses the court capacity to preside over cybercrime cases and those involving electronic evidence.

D 4.2 CRIMINAL JUSTICE SYSTEM

Stage: Formative

Within the criminal justice system in Albania capacities are at a formative stage of development.

In June 2014, the cybercrime sector and special structures near 8 district prosecution offices were established. The Cybercrime Unit of the Albanian State Police was established and in General Prosecutor's Office, in 2014, the Directorate of Control of Investigation of Economic Crimes and Corruption (Task Force) was set up to control the investigation of corruption, economic crime, and investigation along with the work of the Sector of Cyber Crime

Investigation (Prosecution Office's Medium-Term Strategy for 2015-2017 and the Action Plan).

In recent years, more and more importance is being paid to the investigation of such offenses, strengthening more and more measures in this field, including international cooperation. Within this cooperation, a manual for internal use for cybercrime investigators has been created with the support of UNODC (Dushi et al., P. 585)[105].

A central forensics laboratory exists within the Cybercrime Unit of State Police. The laboratory has professional tools and equipment including investigating mobile phones and CCTV. According to review participants, the majority of cases handled by the forensics laboratory are not cybercrime related. The laboratory mainly examines the physical evidence of computer-related offenses. The laboratory currently has eight employees with expertise and certifications on mobile forensics.

Participants were concerned that the forensics laboratory deals with 1000+ cases on a yearly basis, while investigations can be lengthy and time-consuming. Also, they are invited as witnesses to present the evidence at court. Therefore, there is a lack of capacity to respond to the current needs in addressing cybercrime. There was a general consensus among stakeholders that more resources are necessary to be provided to the Cybercrime Unit as well as continuous training for the employees. Participants referenced an example of efforts on training Law Enforcement and staff from the Armed Forces by the British Embassy. That is a fellowship programme on Cybersecurity in coordination with UK universities provided for the Western Balkan countries.

A limited number of specialised cybercrime prosecutors have the capacity to prosecute a case based on electronic evidence. The Department of Cybercrime Investigation in the General Prosecutor Office's has increased close to 10 prosecutors and in the Serious Crimes Prosecutor's Office[106]. Prosecutors have received training in the past on cybercrime and digital evidence through the OSCE regional training programme. However, Participants said that currently within the prosecutor's office there are 3-4 prosecutors who specialize on computer crime related cases.

According to the legislation, there is a requirement for submission of evidence to the court by the prosecutor but also by the victim. Therefore, legal authority is needed before any further action. For this reason, police personnel found at the scene should immediately contact the prosecutor's office to inquire if they have proper jurisdiction (UNODC, 2013). Besides the legal issues in the case of the data stored on the computer, police personnel should also be aware that the data on the computer or computer tests are generally very complex to carry out. Therefore, only specially qualified personnel should be allowed to examine and analyze computer evidence (Dushi et al., 2017).

A separate court structure or specialized judges for cybercrime cases and cases involving electronic evidence do not exist. As participants noted, judges are not being trained in

[105] D.Dushi and N. Berdufi. (2017) Law enforcement and investigation of cybercrime in Albania. Published at the conference proceedings ESI Journal. ISF 2017 Conference, 7-9 February 2017 at University of Oxford, United Kingdom.

[106] http://eurokonventa.al/wp-content/uploads/2015/03/Recommendations-WG-II-Session-4.pdf

cybercrime currently. Concerns were raised regarding the difficulties that judiciary are having due to lack of resources.

D 4.3 FORMAL AND INFORMAL COOPERATION FRAMEWORKS TO COMBAT CYBERCRIME

This factor addresses the existence and functioning of formal and informal mechanisms that enable cooperation between domestic actors and across borders to deter and combat cybercrime.

Stage: Formative

Albania is one of the parties to the 1959 Council of Europe Convention on Mutual Legal Assistance in Criminal Matters, and it also ratified First and Second Additional Protocols to the European Convention on Mutual Assistance in Criminal Matters, as well as the Convention on Extradition.

Albania cooperates with other states on the basis of the provisions of the CPC (Title X Jurisdictional Relations with Foreign Authorities) and Law No.10193 from 03.12.2009, "On jurisdictional relations with foreign authorities in criminal matters". The legal competence to begin and lead criminal investigations belongs to the Prosecution Service, with the support of the police. Prosecution Service also has the power to send and receive international cooperation requests. The Prosecution Service and the Ministry of Justice share evidence with a country and communicate with Europol and Interpol on computer-related cases.

At a regional level, regular meetings are taking place among National CSIRT teams regarding needs assessment. Participants shared a concern regarding the lack of cooperation between ISPs and the Police. According to the legislation, ISPs can formally only be contacted through the prosecutor's office and this can cause delays. There is, however, regulation that specifies the time for responding to the demand of the police.

With regard to international cooperation the CPC includes preservation and expedited disclosure of computer data, access to computer data, comprising search, seizure and disclosure of data stored in the computer system located in Albania. When the search and seizure will be admissible interception of communications would be feasible.

Albania is Party to the 1959 Council of Europe Convention on Mutual Legal Assistance in Criminal Matters, it also ratified First and Second Additional Protocols to the European Convention on Mutual Assistance in Criminal Matters, as well as the Convention on Extradition.

Participants mentioned that there is a strong collaboration mechanism with Interpol and Europol and there have been joint operations with Europol in the past. An example mentioned by stakeholders was an exercise conducted in 2015 with 135 states participating in which 15 people were arrested in Albania. Also, there are cooperation mechanisms between the State

Police and Europol regarding child pornography, child abuse, and child trafficking. Albania is also a member of the European Union's Judicial Cooperation Unit (EUROJUST).[107]Albania is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Albania participated in the ITU Regional Forum on Cybersecurity for Europe and CIS in October 2012 at Sofia, Bulgaria as well as in the International Cyber Shield Exercise 2014 in Turkey (ICSE 2014).

RECOMMENDATIONS

Following the information presented on the review of the maturity of cybersecurity *Legal and Regulatory Frameworks*, the following set of recommendations are provided to Albania. These recommendations aim to provide advice and steps to be followed for the enhancement of existing cybersecurity capacity, following the considerations of the GCSCC Cybersecurity Capacity Maturity Model.

LEGAL FRAMEWORKS

R4.1 Consider setting up a periodic process of reviewing and enhancing laws in Alania relating to cyberspace to address the dynamics of cybersecurity threats (e.g.: cyberbullying, sexting and accessing/downloading child pornography images).

R4.2 Enact commencement orders for existing legislation and assign institutions to monitor the enforcement of cybersecurity, cybercrime and data protection laws.

R4.3 Ensure that in the case of cross-border investigation, procedural law stipulates what actions need to be conducted in order to successfully investigate cybercrime.

R4.4 Consider developing a separate strategy covering cybercrime specifically that would also clarify the roles and responsibilities of the actors (CIRTs, law enforcement, Ministries) involved in handling computer security incident response and cybercrime investigations.

R4.5 Dedicate resources to ensure full enforcement of existing and new cybersecurity laws and monitor implementation.

[107] http://eurojust.europa.eu/Pages/home.aspx

R4.6 Ensure that in the case of cross-border investigation, procedural law stipulates what actions need to be conducted in order to successfully investigate cybercrime.

R4.7 Adapt and implement legal provisions on e-commerce, regarding cybercrime incidents such as online fraud, spam, and phishing sites.

R4.8 Consider developing a platform for sharing electronic evidence between regional cybercrime forces.

R4.9 Enhance cooperation between ISPs and law-enforcement agencies for sharing of information and for removal of copyright-infringing content from websites.

R4.10 Revise and enforce legislative provisions that obliges ISPs to provide technical assistance for law enforcement when they conduct lawful electronic surveillance.

CRIMINAL JUSTICE SYSTEM

R4.11 Invest in advanced investigative capabilities in order to allow the investigation of complex cybercrime cases, supported by regular testing and training of investigators.

R4.12 Allocate resources dedicated to the State Police cybercrime unit or establish operational cybercrime units at the local level, based on strategic decision-making in order to support investigations.

R4.13 Strengthen national investigation capacity for computer-related crimes, including human, procedural and technological resources, full investigative measures and digital chain of custody.

R4.14 Develop and institutionalise specialised training programmes for police, prosecutors and judges on cybercrime and electronic evidence.

R4.15 Provide training to prosecutors and judges for familiarity with international legislation, and exchange of best international experience of computer crimes investigation.

R4.16 Consider establishing standards for the training of law enforcement officers on cybercrime.

R4.17 Dedicate sufficient human and technological resources in order to ensure effective legal proceedings regarding cybercrime cases.

R4.18 Consider appointing cyber experts in support of prosecutors and judicial police officers.

R4.19 Consider requesting reliable and accurate cybercrime statistics from the State Police Cybercrime Unit and AKCESK in order to better inform decision-makers about the current cybercrime threat landscape in Albania when developing policies and legislations to address this matter.

R4.20 Establish a formal mechanism to enable the exchange of information and good practices between prosecutors and judges, in order to ensure efficient and effective prosecution of cybercrime cases.

R4.21 Work on building on the cooperation between the AKCESK and other sectors on collecting and analysing cyber-incidents through an information-sharing platform.

R4.22 Collect and analyse statistics and trends regularly on cybercrime investigations, on cybercrime prosecutions and on cybercrime convictions.

FORMAL AND INFORMAL COOPERATION FRAMEWORKS

R4.23 Strengthen international cooperation to combat cybercrime based on existing legal assistance frameworks and enter further bilateral or international agreements.

R4.24 Consider setting up a Threat Intelligence Platform for real-time information sharing between the State Police Cybercrime Unit and AKCESK.

R4.25 Allocate resources to support the exchange of information between public and private sectors domestically and to enhance the legislative framework and communication mechanisms.

R4.26 Enhance cooperation between the public sector and banks and other financial institutions regarding the sharing of incidents, in order to increase the level of cybersecurity awareness in Albania.

R4.27 Facilitate informal cooperation mechanisms within the police and criminal justice system, and between police and third parties, both domestically and across borders, in particular ISPs.

R4.28 Consider establishing a 24/7 point of contact within the Cybercrime Unit of the State Police in order to provide instant assistance for mutual legal assistance requests.

R4.29 Strengthen informal cooperation mechanisms within the police and criminal-justice system, and between police and third parties, both domestically and across borders. Consider know-hows from other areas, such as anti-corruption cooperation.

R4.30 Consider revising the data retention period according to international best practices, for instance GDPR.

DIMENSION 5 STANDARDS, ORGANISATIONS AND TECHNOLOGIES

This dimension addresses effective and widespread use of cybersecurity technology to protect individuals, organisations and national infrastructure. The dimension specifically examines the implementation of cybersecurity standards and good practices, the deployment of processes and controls, and the development of technologies and products in order to reduce cybersecurity risks.

D 5.1 ADHERENCE TO STANDARDS

This factor reviews government's capacity to design, adapt and implement cybersecurity standards and good practice, especially those related to procurement procedures and software development.

Stage: Start-up

The Law No.2/2017 on Cybersecurity Chapter III Articles 8 and 9[108] empowered AKCESK to develop and implement minimum requirements on cybersecurity for CIIs and IIIs. AKCESK standardisation section stipulates the content and method of documenting of security measures. The operators of CIIs and IIIs are obliged to implement security measures and to document their implementation. As a result, AKCESK has developed a regulation[109] on the content and method of documenting security measures. This is to achieve a high level of cybersecurity by defining security measures, rights, obligations for CIIs and IIIs and defining

[108] The new Law No.2/2017 on Cybersecurity http://akce.gov.al/publicAnglisht_html/wp-content/uploads/2016/04/Ligji%20_Per_Sigurine_Kibernetike_Nr_2_Date_26.1.2017.pdf
[109] http://akce.gov.al/publicAnglisht_html/wp-content/uploads/2016/04/regullore%20mbi%20p%C3%ABrmbajtjen%20dhe%20m%C3%ABnyr%C3%ABn%20e%20dokumentimit%20t%C3%AB%20%20masave%20t%C3%AB%20siguris%C3%AB.pdf

the content and manner of documenting security measures according to the regulation. The regulation comprised of 20 security objectives, being divided into technical and organizational measures. The security measures and the manner of documentation constitute the list of minimum requirements for CIIO and IIIO. For each of the security objectives, more detailed security measures are listed, together with the way of documenting them. Although the regulation mentions that these measures are based on international standards used by electronic communications sector providers in the EU, no explicit cross reference to relevant cybersecurity standards were found in the regulation. However, ISO/IEC 27001 was highlighted as an example of security controls baseline to be followed.

Review participants from the Government mentioned that security best practices are followed. Mainly asset management and third-party modules are followed within ISO 27001 but not all modules. It is also highlighted that there are no certification schemes for security standards. There have been no formal audits of security measures and standards so far. The Aviation Authority is ISO 27001 certified and their environment is reviewed regularly. The transport sector also adheres to the ISO 27001 standards.

The Energy sector also follows ISO 27001 standards, as well as ENISA's recommendations. The scope is to obtain the certification. However, the Albanian Transmission System Operator (OST) has started preparing some internal information protection rules, adopting guidelines as well as international laws. No specific standard or law has been mentioned as this initiative is at an initial stage of development. An in-depth investigation and audit of the OST is also being performed.

Participants agreed that the banking sector is heavily regulated, despite the fact that there is no specific standard promoted by the Bank of Albania. There is a combination of international standards, such as PCI DSS[110] for data security and others imposed by MasterCard[111] and Visa[112], which companies usually set out to follow strictly. Participants from the banking sector mentioned that it is not mandatory for Banks to follow standards, although they are part of CIIs and IIIs. Moreover, ISO 22301[113] for Business Continuity, COBIT[114] for IT governance, and GDPR for data protection are followed. The Financial Supervisory Authority AMF is in the process of selecting regional and EU best practices to follow. Usually advice and procedures are obtained from the Central Bank of Albania. The authority has various controls in place (e.g. BCP and Pen-testing) which are performed every four years. The authority provides its members with continuous risk assessments, awareness raising programs and general meetings with its members.

The private sector is improving slowly with the help of banks. Some service providers and security firms mentioned following ISO 27001, but they are not certified. Since the introduction of mandating ISO 27001 certification for any government bids, a substantial number of companies rushed to be certified. It is now mandatory to be certified from accredited entities and the companies has begun to realize the importance of security. The Electronic and Postal Communications Authority (AKEP) has rules for protecting the operators

[110] https://www.pcisecuritystandards.org
[111] http://www.mastercard.com/sea/consumer/standard-mastercard.html
[112] https://usa.visa.com/dam/VCOM/download/merchants/visa-global-acquirer-risk-standards.pdf
[113] https://www.bsigroup.com/en-GB/iso-22301-business-continuity/
[114] https://cobitonline.isaca.org/

and systems[115]. AKEP is protecting personal details of subscribers. However, AKEP cannot enforce different sectors to follow rules.

As such, initial identification of some minimum-security requirements based standards and good practices has been made by the public and private sectors, possibly in an ad-hoc manner. Initial steps have been taken to implement or change existing practice in a measurable way.

Focusing on the standards related to procurement, variant conclusions regarding the maturity of the public and private sectors can be drawn. There is no apparent attempt to provide a unified process to guide the identification of standards for procurement of hardware in the public sector and it is not standardised in every department. Instead, a more general framework based on procurement laws is provided and different ministries have different procedures and policies in place. Clearance from the justice system has to be granted for procurements. Considering the private sector, there are internal policies and procedures in place that participants characterised as varied and ranging. These are often evaluated and updated. In some cases, business-continuity requirements are included in tenders. It is worth noting that there is no mandatory procurement standard for any sector except the telecommunications sector. The legal department within Banks deals with procurement, as Banks are obliged to comply with different requirements such as ITIL and COBIT. The Transport authority follow ISO 27001 and have no-disclosure agreements with their suppliers. However, they do not audit suppliers. OST has a procurement department and they follow standards and define technical processes to adhere to. As such there is varied adaptation to standards and good practices in procurement processes by the public and private sector. For the ones that are recognised, implementation is *ad hoc* and uncoordinated.

Focusing on standards in software development, there are guidelines in place in the public sector, but the extent to which these guidelines are related to cybersecurity is not clear. The Government defines the standards that need to be adhered to for software development and for software use within public sector. The Law on Competition Law No. 9121 [116]defines that there cannot be only one company offering software unless it is very specific. There are some specific companies which are black listed, such as Kaspersky Lab, due to allegations from the USA and the EU about the lack of transparency. It was noted that the majority of the sectors in Albania do not rely on in-house software development. Most of the developers work in system integration and adaptation rather than software development. Energy and finance sectors procure software from abroad. However, there are technical specifications for other systems. With the exception of the Banking and Telecommunications sectors, as they have in-house software development capabilities, which vary in size and maturity, depending on the organization and its strategy. As such, there are no standards or good practices for software development that have been identified for use relating to integrity and resilience in public and private sectors.

[115] https://www.akep.al/en/legislation

[116] http://siteresources.worldbank.org/INTCOMPLEGALDB/Resources/Albania-en-new.pdf

D 5.2 INTERNET INFRASTRUCTURE RESILIENCE

This factor addresses the existence of reliable Internet services and infrastructure in the country as well as rigorous security processes across private and public sectors. Also, this aspect reviews the control that the government might have over its Internet infrastructure and the extent to which networks and systems are outsourced.

Stage: Formative to Established

Albania has experienced rapid development of telecommunications and of the information society in recent years. As a result, the usage of ICT has increased.

The nation's internet infrastructure is outsourced to the private sector and not maintained by the Albanian Government. According to AKEP, Telekom Albania is the largest telecom operator for mobile and broadband users in the country, followed by Vodafone Albania. Telekom Albania, formerly a state-owned telecom operator (known as Albanian Mobile Communications, or AMC), was privatised in 2000.[117] ALBtelecom is the third big player on the market. All three mobile network operators provide mobile broadband services using 4G technology. [118] As such, reliable Internet services and infrastructure have been established since the mid-90s. Technology and processes deployed for Internet infrastructure meet local and international laws, DCMs, and regulations managed by AKEP.[119]

Participants noted that there are two to three back-up lines in the country from different providers. They have highlighted that outages are minor in the country, with very sporadic cases of network power failures. Regarding internet use, there is an abundance of e-government and e-services offered and participants claimed that their uptake is increasing. E-government services are trusted because people are obliged to use them. There are also some functionality problems with some of the e-services. However, it was noted that users are afraid that they might become victims of scam, so they avoid using e-banking. Also, high commissions force businesses to avoid e-commerce. However, the youth are more risk taking when using internet services and are therefore starting to leverage e-commerce.

Focusing on servicing the finance sector, some banks are obtaining Internet services from Greece. Others have two or three different operators and private companies that provide them with network infrastructure.

It was not possible to determine during the CMM review, whether or not the national infrastructure is formally managed, with documented processes, roles and responsibilities, and limited redundancy.

117 Per information received from the Ministry of Infrastructure and Energy. [Email to the World Bank]. Date: September 14, 2018.
118 https://www.akep.al/images/stories/AKEP/statistika/2018/Treguesit_statistikor_per_vitin_2017.pdf
119 https://www.akep.al/en/legislation/regulation

D 5.3 SOFTWARE QUALITY

This factor examines the quality of software deployment and the functional requirements in public and private sectors. In addition, this factor reviews the existence and improvement of policies on and processes for software updates and maintenance based on risk assessments and the criticality of services.

Stage: Start-up

AKCESK has produced and published the 'Trusted List of Qualified Trust Service Providers (QTSP) [120] registered in Albania, which is in line with the European List of Trusted Lists (LOTL).[121] However, quality and performance of software used in the country is a concern, as functional requirements are not yet fully monitored. As catalogues of secure software platforms and applications within the public and private sectors do not exist. Although, there are examples of software that are not allowed to be used in Albania such as that by Kaspersky Lab, as noted by AKCESK. Participants mentioned that the quality of software is monitored by individual public entities on ad-hoc basis. It was noted that the private sector has a repository for which systems are allowed and which not. However, no evidence of such repository was presented during the review.

Focusing on the private sector, banks rely on an architecture standard, and every software needs to be reviewed. It was also noted that some organizations have a list of software packages and versions they would accept. The SMEs, however, do not follow standards as mentioned by participants. Maintenance and update of software is covered at an individual level. Each company has their own requirements. Some companies adopt the software quality ISO 25000 standard. To conclude, policies and processes regarding updates of software applications have not yet been formulated.

D 5.4 TECHNICAL SECURITY CONTROLS

This factor reviews evidence regarding the deployment of technical security controls by users, public and private sectors and whether the technical cybersecurity control set is based on established cybersecurity frameworks.

[120] http://akce.gov.al/publicAnglisht_html/regjistri/regjistri/index.html
[121] https://webgate.ec.europa.eu/tl-browser/#/

Stage: Start-up to Formative

The Government took measures and deployed various security technologies from an international security firm, as a result of Distributed Denial of Service (DDoS) attacks at the government infrastructure.

Focusing on the Banking sector, there are strict measures on maintaining automated updates and anti-virus. There are tools and procedures in place. Also, regular penetration testing vulnerability management is performed regularly to mitigate vulnerabilities.

For the private sector, participants reported that various tools are being deployed but not necessarily in a consistent manner. Solutions deployed include identity management, anti-virus, Network Introduction Detection Systems (NIDS) and Host Intrusion Detection Systems (HIDS). SMEs lack basic cyber hygiene and appropriate cybersecurity solutions.

There is no evidence at the time of this review of incentivizing the deployment of up-to-date technical security controls in the private and public sectors. The researchers were not able to determine whether ISPs are offering antimalware software as part of their services or if ISPs recognize the need to establish policies for technical security control deployment as part of their services, due to lack of participants from the ISPs at the review sessions.

It was noted by review participants that there is no established cybersecurity culture in Albania (see D2.1). It was mentioned that users would freely give their ID and credit cards to strangers when the ID card was introduced. Participants reiterated the lack of cybersecurity awareness among users, professionals, and SMEs. As such, technical security controls are neither deployed widely by users nor deployed inconsistently within the public and private sectors.

D 5.5 CRYPTOGRAPHIC CONTROL

This factor reviews the deployment of cryptographic techniques in all sectors and users for protection of data at rest or in transit, and the extent to which these cryptographic controls meet international standards and guidelines and are kept up-to-date.

Stage: Start-up to Formative

Cryptographic controls for protecting data at rest and in transit are recognised and deployed ad-hoc by multiple stakeholders and within various sectors. It was noted that encryption is being used for large organizations. Banks mandate two-factor authentication and laptop encryption. Servers are not encrypted but logging is enabled. Data Centers use strict rules that are followed, however bringing your own device (BYOD) is permissible. It is noted that RSA 1052 standards are being followed. Participants from the energy sector highlighted that the infrastructure is not exposed to the Internet, as they use private channels and Virtual Private Networks (VPNs). Participants mentioned that there is a law on money transfer (Law #.9917,

date 19.5.2008[122]) that defines which communication needs to be encrypted among different sectors.

State-of-the-art protocols, such as Secure Sockets Layer (SSL) or Transport Layer Security (TLS), are not deployed by web service providers to secure all communications between servers and web browsers for the majority of the government websites.[123] With the exception of the e-government portal[124], as it deploys encryption. It was noted that banks do deploy encryption on their web services and browsers. There are different ways to log in (e.g. ID card).

AKCESK leads the digital signatures, electronic identification and trusted services, initiatives in Albania. Among AKCESK core functions are registering and accrediting Trusted Service Providers and oversee their activity. AKCESK also inspects the methods of generating and managing public keys, and electronic certificates. Finally, AKCESK oversees the process of issuing qualified electronic certificates and the implementation of electronic signature, electronic identification and other trusted services.[125]

D 5.6 CYBERSECURITY MARKETPLACE

This factor addresses the availability and development of competitive cybersecurity technologies and insurance products.

Stage: Start-up

The domestic market provides limited cybersecurity technologies in Albania. No cybersecurity technologies are produced domestically, but international offerings are available. There are few partners from international organizations that provide cybersecurity technology and services. As such, the cybersecurity market is small.

Participants noted that there is a general lack of expertise. Retaining of talented and qualified IT and professionals is a great challenge as they usually leave Albania for better opportunities.

Banks and telecommunications firms usually pay for employees to be trained in cybersecurity but the Government does not have this capacity.

The Government has recognized its duty for education and awareness. The Government plans to have an environment with competitions so that everyone can do tests for security software in order to push professionals to produce software and technologies.

The need for a cyber insurance market has not been identified. There has yet to be a domestic market for cybercrime insurance products developed in the country.

[122] http://www.fint.gov.al/doc/Law%209917_Jan_2009.pdf
[123]Such as: http://cyberalbania.al; http://akshi.gov.al/; http://www.mod.gov.al/; http://akce.gov.al/publicAnglisht_html/index.html; http://www.cirt.gov.al/; http://cyberalbania.al/
[124] https://e-albania.al/
[125] http://akce.gov.al/publicAnglisht_html/rreth-nesh/index.html

D 5.7 RESPONSIBLE DISCLOSURE

This factor explores the establishment of a responsible-disclosure framework for the receipt and dissemination of vulnerability information across sectors and, if there is sufficient capacity, to continuously review and update this framework.

Stage: Start-up

No responsible-disclosure policy or framework has been established in the public sector. Participants acknowledged that there are unofficial agreements for sharing information. Experts might disclose information, but it does not mean that they will be protected from prosecution. As such, the need for a responsible-disclosure policy in public and private sector organisations is not yet acknowledged.

RECOMMENDATIONS

Following the information presented on the review of the maturity of cybersecurity Standards, Organisations, and Technologies, the following set of recommendations are provided to Albania. These recommendations aim to provide advice and steps to be followed for the enhancement of existing cybersecurity capacity, following the considerations of the GCSCC Cybersecurity Capacity Maturity Model.

ADHERENCE TO STANDARDS

R5.1 Enforce adaptation of a nationally agreed baseline of cybersecurity related standards and good practices across the public and private sectors (not only CIIs and IIIs), including standards in procurement and software development.

R5.2 Apply metrics to monitor compliance and establish periodic audits of the standards.

R5.3 Promote and adopt cybersecurity standards for procurement practices for the public sectors and private sectors.

R5.4 Establish a controls-review to assess the effectiveness of the current minimum security requirements and practices.

R5.5 Establish a framework to assess the effectiveness of standards for procurement and software development.

R5.6 Consider the implementation of best practices such as NIS and GDPR in consultation with all relevant stakeholders and regulators.

R5.7 Establish mandatory requirements for the adherence of standards by appointing security officers that will be held responsible for the implementation of these standards.

R5.8 Streamline clear guidance for the public sector for the procurement of hardware and software.

R5.9 Promote the awareness and implementation of standards among SMEs.

INTERNET INFRASTRUCTURE RESILIENCE

R5.10 Enhance coordination and collaboration regarding resilience of Internet infrastructure across public and private sectors.

R5.11 Conduct regular assessments of processes according to international standards and guidelines together with assessment of national information infrastructure security and critical services that drive investment in new technologies.

R5.12 Identify and map potential points of critical failure within the Internet infrastructure.

R5.13 Establish a system to formally manage the national infrastructure, with documented processes, roles and responsibilities, and adequate redundancy.

SOFTWARE QUALITY

R5.14 Develop a catalogue of secure software platforms and applications used within the public and private sectors, as well as critical infrastructure.

R5.15 Develop, implement and enforce policies and processes on software updates and maintenance.

R5.16 Gather and assess evidence of software quality deficiencies regarding their impact on usability and performance.

R5.17 Establish or assign an institution to elicit in a strategic manner common requirements for software quality and functionality across all public and private sectors.

R5.18 Promote the requirements for software quality and functionality across all public and private sectors and ensure that they are established.

TECHNICAL SECURITY CONTROLS

R5.19 Encourage ISPs and banks to offer anti-malware and anti-virus services for clients and ensure that their effectiveness is monitored and assessed.

R5.20 Establish metrics for measuring the effectiveness of technical controls across the public domain.

R5.21 Consider raising awareness of security controls by promoting cybersecurity best practices for users, such as strong passwords, secure back-ups, and use of antimalware on their devices.

R5.22 Develop processes for reasoning about the adoption of more technical controls based on risk assessment methodologies across the public domain.

R5.23 Provide citizens with certificates for authentication and digital signing and create pilot programmes within the public sector to boost the uptake of the new initiatives.

R5.24 Promote best practices in cybersecurity for users.

R5.25 Ensure that NIDS, HIDS, anti-DDoS, and Data Loss Prevention and other technologies are deployed across the public sector.

CRYPTOGRAPHIC CONTROLS

R5.26 Encourage the development and dissemination of cryptographic controls across all sectors and users for protection of data at rest and in transit, according to international standards and guidelines.

R5.27 Raise public awareness of secure communication services, such as encrypted/signed emails.

R5.28 Use SSL/TLS connections to secure communications all government, CIIs, and IIIs entities.

R5.29 Ensure that data are stored in an encrypted format in the data centres infrastructures.

R5.30 Establish or assign an institution responsible for designing a policy, aiming to assess the deployment of cryptographic controls according to their objectives and priorities within the public and private sector.

CYBERSECURITY MARKETPLACE

R5.31 Foster collaboration with the private sector and academia regarding research and development of cybersecurity technological products.

R5.32 Encourage and support local initiatives in partnership with businesses that aim at developing innovative cybersecurity technology, applications, services and solutions.

R5.33 Promote sharing of information and best practices among organisations to explore potential cybercrime insurance coverage.

RESPONSIBLE DISCLOSURE

R5.34 Develop a responsible vulnerability-disclosure framework or policy within the public sector and facilitate its adoption in the private sector, including a disclosure deadline, scheduled resolution and an acknowledgment report.

R5.35 Establish or assign an institution responsible for supervising the process of responsible-disclosure and ensure that organisations do not conceal vulnerability information.

R5.36 Develop a system to facilitate threat-intelligence sharing among the critical infrastructure partners. Promote sharing of threat-intelligence in the financial sector and incentivize companies to actively participate.

R5.37 Define thresholds and notification requirements for all sectors. These requirements should not only consider availability of services but the integrity and confidentiality of data.

R5.38 Agree on clear instructions on how to share information uniformly within EU in a formal and structured manner.

ADDITIONAL REFLECTIONS

Even though the duration of this review was shorter, the stakeholder engagement in the review, the representation and composition of stakeholder groups was, overall, balanced and broad.

This was the 27th country review that the GCSCC have supported directly.

The review was conducted in cooperation with the World Bank and the dissemination of this report was carried out in cooperation with Global Cybersecurity Center for Development (GCCD) under Korea Internet Security Agency (KISA) of Republic of Korea. The financing came from the Korea -- World Bank Group Partnership Facility (KWPF), which is administered by the World Bank for Korea's Ministry of Strategy and Finance.

Global Cyber Security Capacity Centre

Oxford Martin School, University of Oxford

Old Indian Institute, 34 Broad Street, Oxford OX1 3BD,

United Kingdom

Tel: +44 (0)1865 287430 • Fax: +44 (0) 1865 287435

Email: cybercapacity@oxfordmartin.ox.ac.uk

Web: www.oxfordmartin.ox.ac.uk

Cybersecurity Capacity Portal: www.sbs.ox.ac.uk/cybersecurity-capacity