Global Cyber Security Capacity Centre

Cybersecurity Capacity Assessment of the Republic of Kosovo

Global Cyber Security Capacity Centre
University of Oxford
18/6/2015

Document Administration

The author of this draft Dr. Maria Bada submits a draft to the academic board of the Global Cyber Security Capacity Centre, composed of Professors and experts from the Oxford Martin School, the Department of Computer Science of the University of Oxford, Said Business School, and the Oxford Internet Institute. Upon internal review, this report is submitted to the World Bank Group for their internal review process. Following completion of World Bank Group's review, the report is submitted to the host team (Ministry of Economic Development of the Republic of Kosovo) for their review. Once all edits have been agreed upon by all parties, and following government approval, the report is to be made available to the public and submitted to stakeholders who took part in the consultation.

Until this review process is complete, this document is not to be circulated outside of the aforementioned parties.

Version	Date
4.0	18.06.15

Global Cyber Security Capacity Centre

OXFORD MARTIN SCHOOL | UNIVERSITY OF OXFORD

Contents

Abbreviation List

ARKEP Regulatory Authority of Electronic and Postal Communications

SMEs Small and medium-sized enterprises

CISCO Computer Information System Company Organisation

CNI Critical National Infrastructure

CPD continuing professional development

EC TAIEX Technical Assistance and Information Exchange instrument of the European Commission

FP7 Seventh Framework Programme

GIZ Deutsche Gesellschaft für Internationale Zusammenarbeit

GoK Government of Kosovo

ISO International Organisation for Standardisation

KEK Kosovo Energy Corporation

KIPA Kosovo Institute of Public Administration

KJI Kosovo Judicial Institute

KPA Kosovo Property Agency

MED Ministry of Economic Development

NAPDP National Agency for Protection of Personal Data Protection

NRC The National Research Council

KPIs Key performance indicators

PTK Post and Telecom of Kosovo

STIKK Kosovo Association of Information and Communication Technology

UNCTAD United Nations Conference on Trade and Development

Cybersecurity Capacity Assessment of the Republic of Kosovo

Introduction

Through a Collaboration Agreement with *The World Bank*, The Global Cyber Security Capacity Centre has facilitated a self-assessment of cybersecurity capacity in the Republic of Kosovo (Kosovo). The objective of the self-assessment is to enable Kosovo to determine the areas of capacity the country might strategically invest in to become more cyber secure.

During February 9th-11th 2015, stakeholders from the following sectors participated in a three-day consultation to evaluate cybersecurity capacity in Kosovo:

- Ministries: Ministry of Economic Development, Ministry of Internal Affairs – Kosovo Police, Ministry of Internal Affairs – Agency of Civil Registration, Ministry of Public Administration – Agency for Information Society, Ministry of Trade and Industry, Ministry of Finance – Tax Administration of Kosovo, Ministry of Finance – Kosovo Customs, Ministry of Justice, Ministry of Education, Science, and Technology (hereinafter - Ministry of Education), Ministry for the Kosovo Security Forces, Regulatory Authority of Electronic And Postal Communications.
- Academia
- Internet governance representatives
- Internet Society chapters
- Criminal justice
- Intelligence community
- Legislators
- National security representatives
- CERT[1] teams
- Major commercial sectors and SMEs
- Finance sector
- Telecommunications companies

The consultations were premised on the Centre's Cybersecurity Capacity Maturity Model which is composed of five distinct areas of Cybersecurity Capacity, a) Cybersecurity policy and strategy; b) Cyber culture and society; c) Cybersecurity education, training and skills; d) Legal and regulatory frameworks; e) Standards, organisations, and technologies.

There are multiple factors in each dimension, which describe what it means to possess cybersecurity capacity. In each factor, there are indicators, which describe the five levels of maturity, whereby the lowest stage implies a rather ad-hoc level of capacity and the highest

[1] The name Computer Emergency Response Team is the historic designation for the first team (CERT/CC) at Carnegie Mellon University (CMU). CERT is now a registered service mark of Carnegie Mellon University that is licensed to other teams around the world. Throughout the report this term will be used.

stage both a strategic approach and an ability to dynamically adapt or change against environmental considerations. These are the following:

- **Start-up:** At this level either no cybersecurity maturity exists, or it is very embryonic in nature. It could also include initial discussions about cyber capacity building, but no concrete actions have been taken. It also includes a lack of observed evidence in this particular indicator.
- **Formative:** Some features of the indicators have begun to grow and be formulated, but may be ad-hoc, disorganized, poorly defined - or simply "new". However, evidence of this activity can be clearly demonstrated.
- **Established:** The elements of the sub-factor are in place, and working. There is not, however, well-thought-out consideration of the relative allocation of resources. Little trade-off decision-making has been made concerning the ''relative'' investment in the various elements of the sub-factor. But the indicator is functional and defined.
- **Strategic:** Choices have been made about which parts of the indicator are important, and which are less important for the particular organization or nation. Everything can't be as important as everything else due to finite resources, therefore certain choices must be made. The strategic level reflects the fact that these choices have been made. They should have been made contingent on the nation or organization's particular circumstances.
- **Dynamic:** At the Dynamic level, there are clear mechanisms in place to alter strategy depending on the prevailing circumstances: for example, the technology of the threat environment, global conflict, a significant change in one area of concern (e.g. Cybercrime or privacy). Dynamic organizations have developed methods for changing strategies in stride, in a "sense-and-respond" way. Rapid decision-making, reallocation of resources, and constant attention to the changing environment are feature of this level.

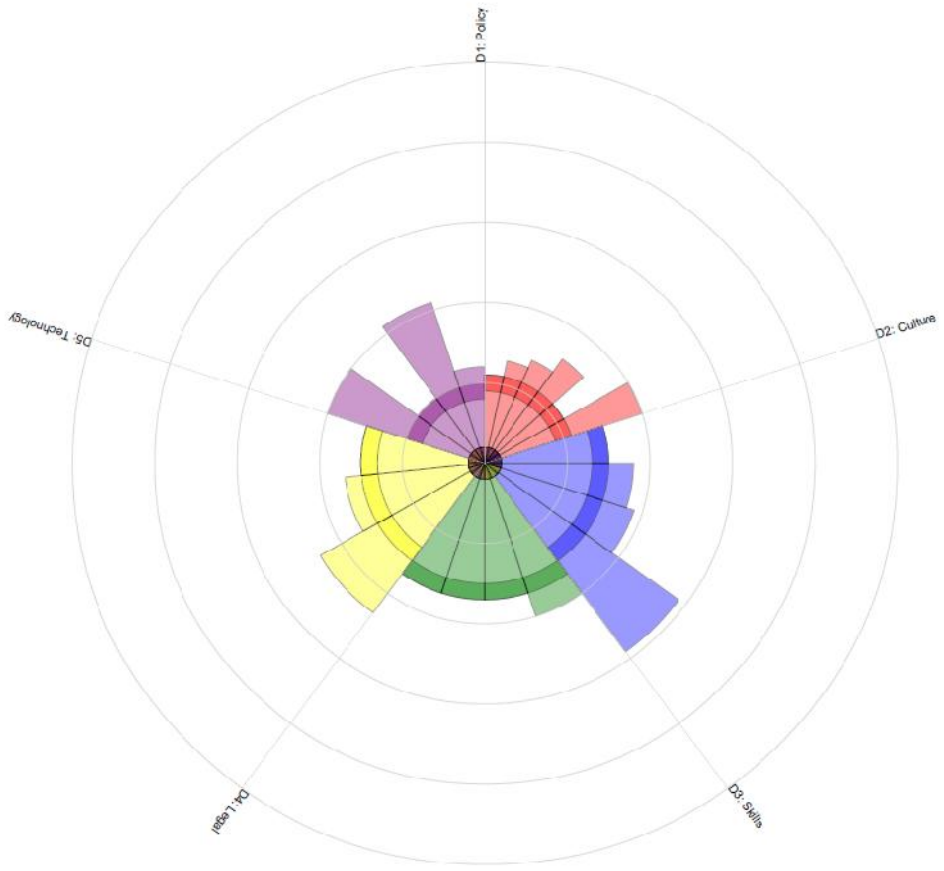
Following the self-assessment in Kosovo, results are being displayed in the present report, including recommendations on the next steps to be taken into consideration by the Government of Kosovo (hereinafter – GoK).

Assessment of Cybersecurity Maturity

In this section we provide an overall presentation of the cybersecurity capacity in Kosovo. First, the graphic below (Graphic I), presents the maturity estimates in each dimension. The stages of maturity for each factor extend out from the middle as an individual bar, and each dimension is a fifth of the graphic.

As seen in this graphic, for most factors cybersecurity capacity in Kosovo lies between an Initial and Formative stage of maturity, while for factor D2-4 (Privacy Online), maturity seems to be at a higher (Established) stage.

Graphic I: Assessment Results



The table below (Table I) presents a summary of the results on the stage of maturity for each factor, including a brief description of these results. In support of these, links of existing policies, strategies, laws and other additional information are provided.

Table I: Assessment Results

Dimension	Capacity Factor	Stage of Maturity	Brief Description	Links
Dimension 1 Cyber Security Policy and Strategy	**D1-1 National Cybersecurity Strategy**	Start-up	No national cybersecurity strategy exists, but some cybersecurity issues are covered by Electronic Communication Sector Policy – Digital Agenda for Kosovo 2013-2020 (hereinafter – Digital Agenda for Kosovo) and sublegal acts	Electronic Communication Sector Policy – Digital Agenda 2013-2020 http://mzhe.rks-gov.net/repository/docs/Electronic_Communication_Sector_Policy_2013-2020.pdf
	D1-2 Incident Response	Start-up	A governmental CERT exists but no national level incident response capacity exists. A national CERT, KOS-CERT is now being developed. According to the Digital Agenda for Kosovo, a national CERT has to be established and fully functional no later than in 2016	Electronic Communication Sector Policy – Digital Agenda 2013-2020 http://mzhe.rks-gov.net/repository/docs/Electronic_Communication_Sector_Policy_2013-2020.pdf
	D1-3 Critical National Infrastructure	Start-Up	No formal list of critical national infrastructure (CNI) assets has been developed by the government	Law on Electronic Communications No. 04/L-109 regulates social relations pertaining to electronic communications networks and services http://mzhe.rks-gov.net/repository/docs/Ligji_i_KE_i_Publikuar_%28Anglisht%29.pdf
	D1-4 Crisis Management	Start-up	Cybersecurity exercises at the national level have not been conducted, only planned within the Kosovo Police	
	D1-5 Cyber Defense Consideration	Start-up	A Strategy for Security of the Republic of Kosovo and The Action Plan of Strategy for Security of the Republic of Kosovo exist and are approved by the Government (Strategy - Decision No.01/129 of date: 15.06.2010 and Action Plan - DecisionNo.02/24 of date: 20.07.2011). According to The Plan of Strategic Documents for 2015 the development of a new security strategy (3rd row) and the Defence Strategy (41st row) is planned. No cyber-defence policy or strategy exists; no coordination in response to malicious attacks on military	http://www.kryeministri-ks.net/repository/docs/Analysis_of_Strategic_Security_Sector_Review_of_RKS_060314.pdf http://www.kryeministri-ks.net/?page=1,250 http://www.kryeministri-ks.net/repository/docs/Plani_Vjetor_i_Dokumenteve_Strategjike_2015.pdf

			information systems and defence network infrastructure has been established	
	D1-6 Digital Redundancy	Formative	Emergency-response assets are mapped and identified, including details on their location and their designated operators, but this list has not been formalised	
Dimension 2 Cyber Culture and Society	**D2-1 Cybersecurity Mind-Set**	Formative	There is increasing awareness of cyber risks in the public and private sector, but society-at-large is characterised by a general feeling of fear of cyber threats	
	D2-2 Cybersecurity Awareness	Formative	An awareness campaign programme has been developed at a national level by the National Agency for Personal Data Protection (NAPDP), the 'Privacy and Digital Age Awareness Programme'	Privacy and Digital Age Awareness Programme http://www.pda-ks.com/?page=1,5
	D2-3 Confidence and trust on the Internet	Formative	Trust in online services has been identified as a concern, with the banking sector promoting trust in online services. E-Government services are under development, provision of e-services is limited and e-commerce has not been fully developed	
	D2-4 Privacy Online	Established	There is adherence to the EU Declaration of Human Rights and the Strasbourg Convention. The Law on Data Privacy, which is now under development, is compliant with EU Law and the Budapest Convention	Law on Protection of Personal Data (03/L-172) http://www.kuvendikosoves.org/common/docs/ligjet/2010-172-eng.pdf The Annual Report (2013) of the Data Protection and Privacy National Agency http://www.amdp-rks.org/web/repository/docs/Final_ENG_ASHMDHP_Raporti_Vjetor_i_Pun_s_2013.pdf
Dimension 3 Cybersecurity Education, Training and Skills	**D3-1 National Availability of Cyber Education and Training**	Formative	There are educational offerings in information-security education and training as well as courses on cybersecurity. The University of Pristina is the only institution in the country providing PhD studies; it has courses on cybersecurity. Cybersecurity training is usually provided by Law Enforcement or by various private organisations	
	D3-2 National development of	Formative	The Ministry of Education has placed ICT and security issues as	National Background report on ICT research

	cybersecurity education		part of the curricula for all levels of education, and the National Research Council (NRC) has placed communication and technology as a priority research area. This is reflected in the efforts to build programmes in cybersecurity	for Kosovo http://wbc-inco.net/attach/KosovoICTReportFINAL_01_12_2009.pdf National Research Council (NRC) http://www.masht-gov.net/advCms/documents/NRP_%28Draft%29_English.pdf
	D3-3 Training and educational initiatives within public and private sector	Formative	The Kosovo Institute for Public Administration develops and implements training policies developed by the Ministry of Public Administration. The Ministry of Economic Development encourages the development of information technology training systems. See Appendix 18-XXIV.	http://www.kryeministri-ks.net/repository/docs/Rregullorja_02-2011-e_miratuar_nga_Qeveria-finale.pdf
	D3-4 Corporate Governance, Knowledge and Standards	Start-up	Boards and executives within private and state-owned companies have some minimal awareness of cybersecurity issues; however ICT and finance industry boards are more informed	
Dimension 4 Legal and Regulatory Frameworks	**D4-1 Cybersecurity Legal Frameworks**	Formative	There is no standalone cybersecurity law. But in the future (subject to EU legislative developments in cyber security), there may be sub-legislation developed. Kosovo Assembly has adopted the Law on Protection of Personal Data (03/L-172) and the agency responsible for its implementation is the National Agency for Personal Data Protection; The Substantive Law of Kosovo covers the prevention and combat of cybercrime; The Law on Information Society Services No. 04/L-094 aims to enable the legal use of electronic documentation, and to facilitate the implementation of e-commerce, e-signature and e-payments;	Law on Protection of Personal Data (03/L-172) http://www.kuvendikosoves.org/common/docs/ligjet/2010-172-eng.pdf Law on Prevention and Fight against Cyber Crime Law No.03/L–166 http://www.kuvendikosoves.org/common/docs/ligjet/2010-166-eng.pdf The Law on Information Society Services No. 04/L-094 http://mzhe.rks-gov.net/repository/docs/LIgji_i_SH_SH_I_(Anglisht).pdf The Law on Electronic Communications No. 04/L-109 http://www.art-

			Law on Electronic Communications No. 04/L-109, Article 85 imposes obligations on telecom operators among others (i) when requested to provide information about assessment of the security and/or integrity of the public electronic communications services and networks, including documented security policies; (ii) to take appropriate technical and organizational measures to appropriately manage the risks posed to security of networks and services; (iii) notify ARKEP in accordance with the regulation set by it of a breach of security or loss of integrity that has had a significant impact on the operation of networks or services; and (iv) provides ARKEP with competence to issue binding instructions aimed at increasing network integrity and security, e.g. to perform security audit carried out by the qualified independent body.	ks.org/repository/docs/Electronic%20communication.pdf
	D4-2 Legal investigation	Formative	The Cyber Crime Investigation Centre within the police force has the technical capacity and training to investigate computer-related crimes but this has not been transferred to prosecution or judicial services	The Kosovo Judicial Council's (KJC) Strategic Plan for the period 2007 – 2012 http://www.kgjk-ks.org/repository/docs/Kosovo-ICT-strategy_389023.pdf
	D4-3 Responsible Reporting	Start-up	No mechanism has been established for responsible reporting, on receiving and disseminating information on vulnerabilities.	
Dimension 5 Standards, organisations, and technologies	**D5-1 Adherence to standards**	Formative	The private sector implements internal ISO standards. Also GoK is using Microsoft Platform as a standard in developing software.	
	D5-2 Cybersecurity Coordinating Organisations	Start-up	No command-and-control agency has been established but a national incident-response organisation is now under development	
	D5-3 National Infrastructure Resilience	Formative	National technology infrastructure is managed informally, with no documented processes, roles and responsibilities outlined; Specifically for IPKO, networks and systems are outsourced mainly from Slovenia	

	D5-4 Cybersecurity Marketplace	Start-up	There are no cybersecurity products or cyber insurance marketplace in general (but well developed insurance market for banks provided from a foreign company)	

Dimension 1: Cybersecurity Policy and Strategy

Not every government has a national level cybersecurity policy and strategy or responsible body, for cybersecurity as a policy area is still evolving. However, importance of designating an overarching government body for cybersecurity coordination and having a national cybersecurity strategy and policy cannot be overemphasized. International experience shows that those governments better cope and mitigate against cyber incidents and attacks that do have a designated government body and cybersecurity strategy and policy in place. This dimension explores the capacity of the government to design, produce, coordinate and implement a cybersecurity strategy as well as policies upholding the strategy.

D1-1: Documented or Official National Cybersecurity Strategy

Cybersecurity policy and strategy are essential to mainstreaming cybersecurity agenda within government because they help prioritize cybersecurity against other important policy areas, determine areas of responsibility and mandate of different cybersecurity government actors, and direct allocation of resources to the emerging and existing cybersecurity issues and priority areas.

Start-up: There is no documented or official national cybersecurity strategy in Kosovo. The Ministry of Economic Development (MED) as the Ministry responsible for electronic communications, has responsibility and authority (under the Law on Electronic Communications, Article 7) to develop the policy and national strategies in the electronic communications field. It has undertaken, therefore, an initiative to draft a national Electronic Communication Sector Policy in consultation with multiple stakeholders. The Electronic Communication Sector Policy – Digital Agenda 2013-2020[2] includes cybersecurity and the development of ICT infrastructure as important components (national CERT capability, awareness raising, the development of broadband electronic communication networks throughout the national territory and promotion of the use of electronic communication services). This Policy is in compliance with the objectives set out in the Communication from the European Commission of 19th May 2010 to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "A Digital Agenda for Europe" (COM (2010) 245 final) and aligned with the Communication from the European Commission of 3rd March 2010 "A strategy for smart, sustainable and inclusive growth" (COM (2010) 2020 final). Ministry of Economic Development (MED) in coordination with Office of Strategic Planning –OSP (within The Office of Prime Minister), Ministry of Internal Affairs and Agency of Information Society (within Ministry of Public Administration) are in the process of consulting on how to proceed with the drafting of a national cybersecurity strategy.

Public administration entities and ministries have internal security policies that inform the operations of their internal independent networks. The Agency for Information Society is responsible for cybersecurity with regard to the government network. The agency is responsible for any security breach which occur using the states' network. The Law No. 04/L-

[2] http://mzhe.rks-gov.net/repository/docs/Electronic_Communication_Sector_Policy_2013-2020.pdf

145[3] recognised the establishment of the Agency for Information Society as a governmental executive agency within the Ministry of Public Administration. The Agency is the central administrative body for development and implementation of Information and Communication Technology for public institutions of Kosovo.

However, stakeholders express a high level of concern about security of their own networks. Although there is sufficient protection of national technological infrastructure, there is no comprehensive national cybersecurity strategy that drives and coordinates a centrally managed strategic approach to cyber security. There is consensus among various stakeholders for the establishment of an ICT Ministry which will be responsible also for cyber security, but this remains under discussion and has not been developed further.

D1-2: Incident Response

This sub-dimension speaks about the capacity of the government to identify and determine characteristics of national level incidents, events or threats in a systemic way - preferably, through a central registry. It also assesses the government's capacity to organize and coordinate an incident response.
US Department of Homeland Security defines[4] a cyber incident as the violation of an explicit or implied security policy. It can have many forms such as:

- *Attempts (either failed or successful) to gain unauthorized access to a system or its data;*
- *Unwanted disruption or denial of service;*
- *The unauthorized use of a system for processing or storing data; and*
- *Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.*

Start-up: It was generally agreed across all stakeholders that incidents are not categorised or listed at a national level. There is coordination between government stakeholders and Law Enforcement but coordination remains limited to the governmental network. With regards to the public electronic communications network, article 85 of the Law on Electronic Communications[5] obliges operators to notify national authority for electronic and postal communications (ARKEP)[6] of a breach of security or loss of integrity that has had a significant impact on the operation of networks or services. ARKEP in turn holds the right to communicate information about such breaches publicly. Relevant bylaw establishing the procedure of notification has not been established at the moment of drafting this report.

There are sublegal acts regarding incident response. The Incident Management Policy (Ref.: KC_DACP_07) aims at ensuring that Kosovo establishes a strategy for managing information security incidents resulting in a coordinated and orderly response and also at ensuring that

[3] http://www.kuvendikosoves.org/common/docs/ligjet/Law%20on%20information%20society%20government%20bodies.pdf
[4] http://www.dhs.gov/how-do-i/report-cyber-incidents
[5] http://www.art-ks.org/repository/docs/Electronic%20communication.pdf
[6] http://www.arkep-rks.org/?cid=2,1

security incidents are not only managed but also analysed with a view of learning from them and preventing their recurrence.

Within ministries there are teams for incident response: the Ministry for the Kosovo Security Force has built their own strategy based on that of NATO; the Ministry of Finance maintains two agencies with separate operational teams, and the Ministry of Public Administration owns a stand-alone system.

Kosovo Customs as part of the Ministry of Finance maintains a Security Information Event Management System, which is tested periodically. However, a central body has not been designated to collect emergency threat information and there is no specific mandate for a national cyber-response agency. Following ENISA guidelines for establishing a CERT, there is a security unit specifically set up to address and protect the systems of the government network maintained by the Ministry of Public Administration.

It must be noted that there is incident response capacity in Kosovo, since there is a governmental CERT, and a national CERT is now being developed under the ARKEP. Administrators of the governmental CERT are responsible for identification of incidents, which result in informing law enforcement. Law enforcement then coordinates activities for combating cybercrime. As far as coordination is concerned, the responsibility for incident response has been allocated within each public administration entity and ministry, and there is no clear cooperation yet between public and private sector.

D1-3: Critical National Infrastructure (CNI) Protection

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

Start-up:

Regarding Critical National Infrastructure (CNI), responses varied between the various public administration entities and ministries. At a national level, no list of CNI industries has been defined, nor a framework for collaboration between CNI has been identified during the consultations. It should be noted that for Law Enforcement, the Ministry of Justice, and the Forensic Agency, as well as the Ministry of Economic Development and Ministry of Public Administration, a general list of CNI assets has been created, but without any identified risk-based priorities. In general, telecommunication providers, energy providers, and the Civil Registration Agency are referred to as "critical service providers", however the breadth of CNI remains small for broader development reasons: CNI infrastructure is being still developed, and smart technologies have not yet been prevalent in this domain.

CNI is also mostly state-owned, and no reporting requirements for CNI operators are in place. The Electronic Communication Sector Policy – Digital Agenda for Kosovo 2013-2020 requires the assessment of services and their maintenance, but it was admitted by the interviewees that there is limited interaction between government ministries and owners of critical assets with regard to cyber security.

The Law on Electronic Communications, No. 04/L-109[7] regulates social relations pertaining to electronic communications networks and services, associated facilities and services; use of electronic communications resources as well as social relations pertaining to radio equipment; and terminal equipment and electromagnetic compatibility. This regulation is required to ensure an equivalent level of protection of rights concerning personal data, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector. The law addresses the issues related to reliability and security of the services provided over public electronic communications networks.

Response planning for an attack on critical assets is under discussion, but no formal plan exists as of yet and no protection processes or procedures have been agreed. Each public/private organisation has a business continuity plan. For the governmental network, there are no detailed procedures or instructions regarding response planning in the event of an attack. On the other hand, response planning has been established for the banking sector. Information-protection procedures and processes have been established within banks, supported by adequate technical security solutions.

As far as coordination is concerned, it is under discussions and the National Security Council brings together appropriate stakeholders (ARKEP, Ministries), but basically only telecommunication companies have some formal reporting procedures established under the Law on Electronic Communications. Dialogue between the public and private sector follows informal procedures while lacking parameters for information sharing: such procedures are generally on an individual or unstructured basis, or are non-existent.

Moreover, risk management is considered only if there is an ICT component to a specific industry. Usually telecommunication companies and energy organisations have basic capabilities to detect, identify, protect, respond and recover from cyber threats, but such capabilities are uncoordinated and vary in quality. In the banking sector security measures and guidelines for CNI cyber best practice have been established and incident-response procedures have been defined with insider-threat detection being accounted for. Within Ministries (e.g. the Ministry of Finance), cyber security is not yet taken into consideration as an operational risk.

D1-4: Crisis Management

Crisis management planning and evaluation capacity, bolstered by functional protocols and standards, is critical to implementing cybersecurity policies that are results-oriented and sustainable. Crisis management planning usually entails but is not limited to conduct of specialized 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 but also inform budgetary allocations.

[7] http://mzhe.rks-gov.net/repository/docs/Ligji_i_KE_i_Publikuar_%28Anglisht%29.pdf

Start-up: In Kosovo, there is some understanding that crisis management is necessary for national security. There are cyber exercises being planned, but only within the Police, not at a national level. Within the Police, there is a security IT Unit, a strategy regarding data loss and key performance indicators (KPIs) for internal affairs. Although there is some evaluation taking place after penetration testing at a local level (e.g. banks have an internal regulation on PIN testing), results from exercises do not inform overall crisis management at a national level.

Within GoK, there is a recovery centre and a strategy regarding data loss. There is a vulnerability-scanner application to scan systems for vulnerability issues, and based on this there is an effort to increase security according to its results. According to the vulnerability issues detected, there are measures being taken. But, no exercise has been conducted yet.

For the banking sector, realistic-high level scenarios inform plans to test information flows and decision-making, and new information is fed into the exercise at key points. There is as well an internal regulation on PIN-testing once a year.

D1-5: Cyber Defence Consideration

This sub-dimension 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 organization within executive branch. Among others, it also assesses the level of coordination among various public and private sector actors in response to malicious attacks on military information systems and critical national infrastructure.

Start-up: A national security policy exists and a national defence strategy is under preparation but no cyber-defence policy or strategy exists. The Ministry for the Kosovo Security Forces is under the governmental network but also maintains its own Command and Control Centre. While, there are Cyber Defence operation units incorporated into the different branches of the armed forces, no central command-and-control structure exists.

The Security Force in Kosovo is in transition and the majority of the employees at all levels of its units lack training. Kosovo, as a partially recognised state in Southeastern Europe, is required to follow European standards. It was commonly agreed that no coordination exists in response to malicious attacks on military information systems and defence network infrastructure.

Moreover, some implementation of standards and minimal acceptable practices has been carried out, but not in a coordinated manner.

D1-6: Digital Redundancy

Digital redundancy foresees such a design of a cybersecurity system in which duplication and failure of any component is safeguarded by the proper backup. This sub-dimension assesses government's capacity to plan and organize redundancy communication among stakeholders.

Formative: In Kosovo, emergency-response asset priorities and standard operating procedures are established in the event of a communications disruption in the emergency-response network. Moreover, stakeholders convene to identify gaps and overlaps in emergency-response asset communications and authority links.

Regarding digital redundancy, there is capacity within government and Law Enforcement. The majority of servers are on one network, where there are digital redundancy measures. Government data servers have routine backups. There is a business continuity plan and a recovery centre, in a location outside of Pristina, for both the Ministry of Finance and the Kosovo Customs as part of the Ministry of Finance.

Kosovo Law Enforcement also maintain physical back-up and own a disaster recovery centre in another city outside of Pristina. In the future there will be similar disaster recovery centres for the Security Forces established. Although emergency response assets are mapped and identified, including details on their location and their designated operators, this is not carried out in a formal manner but rather done informally and at a local level. Several United Nations Conference on Trade and Development (UNCTAD) documents specify the procedure in occurrence of an incident, and these have been implemented.

Dimension 2: Cyber Culture and Society

Even the most forward-thinking cybersecurity strategy and policy are of little help if nongovernment actors do not understand their roles and responsibilities in safeguarding sensitive data and protecting their personal and organizational resources as they interact with them daily through digital means. This dimension assesses important elements of a cyber culture on an individual and organizational level and their perception by various stakeholders. As well, it determines the level of trust in e-government and e-commerce services and adherence to privacy standards by the entities that engage in provision of these services.

D2-1: Cybersecurity Mind-set

This sub-dimension evaluates the level of recognition and priority attached to cybersecurity mind-set by government, private sector, and society at large. Cybersecurity mind-set is understood as a predisposition and, in certain cases, as a consistent behavioural model toward alignment of one's actions with cybersecurity priorities on an individual level or in an organizational setting. A cybersecurity mind-set consists of values, attitudes and practices, including habits, of individual users, experts, and other actors in the cybersecurity ecosystem.

Formative: Cybersecurity has been recognized as a priority across GoK, and therefore risks and threats have begun to be identified. At a governmental level, cyber security is a concern, there are some initiatives such as seminars, conferences and courses, organised by NAPDP as awareness initiatives, but these remain uncoordinated. Most strategies or policies contain a cyber-element.

After consultation with stakeholders from civil society and academia, it has been identified that large organisations such as banks or IT companies have begun to place priority on a cybersecurity mind-set by identifying high-risk practices, and they are characterised by a proactive cybersecurity mind-set as well as a higher degree of awareness of cyber threats than small and medium-sized enterprises (SMEs). A survey, conducted by the University of Pristina during 2014, also revealed that private companies are more aware of cyber security than organisations in the public sector[8].

Civil society is aware of cyber threats and privacy issues but takes no proactive steps to improve cybersecurity. It has also been noted that there is an important distinction in cybersecurity mind-set among different age groups. It is more common for young people to take proactive steps to improve their cyber security. Society-at-large is characterised by a general feeling of fear of cyber threats, but this is possibly because there is a lack of awareness and understanding of the benefits of digital citizenship.

D2-2: Cybersecurity Awareness

Formative: Awareness-raising across society-at-large remains at a low level, with the exception of young people. The Ministry of Education, National Agency for Personal Data Protection, and the Ministry of Local Government Administration developed a TV and radio awareness campaign programme at a national level, the 'Privacy and Digital Age Awareness

[8] Rexha, B., Halili, A., Rrmoku, K., Imeraj, D. Impact of secure programming on web application vulnerabilities. Faculty of Electrical and Computer Engineering, University of Prishtina, Kosovo, (Unpublished).

Programme'[9], aimed at informing the general public on their data protection rights. The National Agency for Personal Data Protection (NAPDP) has created a plan for increasing the awareness of citizens, a responsibility derived from the Law on Protection of Personal Data. Through the campaign, the Agency's aim is to further increase the knowledge of constitutionally guaranteed rights for protection of personal data, especially in the context of local and international legislation and conventions protecting these rights across key groups of citizens. The target groups in these cases are all citizens of Kosovo, with a special focus on youth and especially students, their teachers, state institutions and the private sector. The campaign uses various methods to spread its messages, such as printed, broadcast and electronic media, as well as organization of events. The campaign aims to make citizens aware of their right to complain whenever they consider that their private data are not being processed according to the relevant legislation.

NAPDP has based their practices on research on Internet usage in Kosovo. Research as indicated by NAPDP shows that Kosovo citizens are some of the most frequent users of Internet[10]. The group of users with the highest Internet usage are youth aged 16 to 18 years old. This group is also the most vulnerable one because, apart from frequent use of IT and Internet services, they represent a target group for data theft and mishandling of private data. Therefore the campaign organised by NAPDP ''Privacy in Digital Age'' aims to inform high-school youth, students, and generally users of Internet on data protection issues.

In cooperation with the Ministry of Education and experts from EU, NAPDP aims at creating a module for IT teachers called ''Safe usage of IT''. In this context, the campaign will target specifically those students who are studying IT related subjects and who aim to become IT professionals in the future. The Ministry of Education has already allocated a budget for this initiative.

Despite the ongoing implementation of cybersecurity awareness raising, it is not necessarily covering all of stakeholder groups. Moreover, there is no coordinated measurement framework to evaluate the effectiveness of this campaign.

D2-3: Confidence and Trust on the Internet

This sub-dimension assesses the level of stakeholders' trust in the use of online services, in general, and e-government and e-commerce services, in particular.

Formative: Trust in use of online services is identified as a concern. A few infrastructure operators and the banking sector consider measures to promote a higher level of trust in online services, however these have not yet been established.

E-government services are currently under development. The Ministry of Finance has developed online tax-form submission services, but no actual financial transactions take place online as of yet. These services do not necessarily recognise the need for the application of security measures to promote trust in e-services. Moreover, the private sector, specifically

[9] http://www.pda-ks.com/?page=1,5
[10] http://internetisigurte.org/home/wp-content/uploads/2013/09/Internet_Safety_Report_English.pdf

the banking sector, recognises the need for the application of security measures to promote citizens' trust in e-services. As a result, banks use a notification of a completed banking service transaction, which enhances the feeling of trust for their customers.

Some of the e-government services currently provided are government payments and budget management system, electronic register of property taxation, and a system for vehicle registration and drivers' licenses. Moreover, citizens and businesses use the online electronic bill payment program ''pay at the Bank'' for services provided by the Post and Telecom of Kosovo (PTK), Kosovo Energy Corporation (KEK), Kosovo Property Agency (KPA), the Kosovo Customs, and other billing organisations.

Mainly due to a limited number of e-government services provided online, no security breaches have been reported to date in Kosovo. With the expansion of e-government services, maintaining cybersecurity and promoting trust in their use will become more essential. Provision of e-services is currently limited and e-commerce is not fully developed. The need for security in e-services has been recognised by stakeholders and users and it was admitted that foreign websites are usually more trusted than the domestic ones.

D2-4: Privacy Online

This sub-dimension assesses the level of salience of privacy issues on the government agenda through enactment of relevant practices, laws, and regulations, and the level of engagement and advocacy around them by civil society. It also evaluates how national legislative norms adhere to regionally and internationally recognised standards for human rights.

Established: In support of UN Universal Declaration of Human Rights, the European Convention for the Protection of Fundamental Human Rights and Freedoms, the Convention 108 of 1981 on Personal Data Protection and Privacy during automatic processing of personal data and (of) Directive 95/46 of 1995, the right to protection of personal data and privacy is considered to be a fundamental human right, which is essential for the functioning of a democratic society. In Kosovo, this right is additionally protected by the Constitution and the Law on Protection of Personal Data.

The government adheres to the EU Declaration of Human Rights and the Strasbourg Convention. Concerning the Law No.03/L-172 on the Protection of Personal data there are regular workshops organised with participation of all relevant stakeholders. Moreover, the Law on Data Privacy, which is now under development, follows relevant EU Law. All relevant actors from civil society are actively driving changes in practice, law, and regulation that impinge on freedom of expression privacy issues.

Privacy in the workplace is recognised as an important component of cybersecurity and is beginning to be institutionalised in local employee programs, while employers maintain privacy policies that provide a minimum level of privacy for employees. Furthermore, there is a good understanding of data protection in the workplace both in public and private sector and employees are aware that their personal data is protected. Within public entities, the law and standards on privacy are followed more strictly than in the case of private entities.

Dimension 3: Cybersecurity Education, Training and Skills

This dimension assesses the availability and quality of cybersecurity education, training, and skills in Kosovo for various groups of government stakeholders, private sector, and population as a whole. In particular, it evaluates existing educational offerings and national development of cybersecurity education; training and educational initiatives within public and private sector; and corporate governance, knowledge, and standards.

D3-1: National Availability of Cyber Education and Training

This sub-dimension speaks to the importance of availability of high quality cybersecurity education and training options, their integration and synergies, in order to ensure adequate and sustainable supply of cybersecurity skills for the needs of public and private sectors. It takes stock of existing educational offerings in schools and universities and training offerings within private sector and beyond it in the field of information security and cyber security and provides a superficial evaluation of their structure and components.

Formative: There is an evident marketplace for information security education and training in Kosovo. There are educational offerings in information security. Courses on cybersecurity, (such as IT security, data security, information assurance and security, cryptography, technical issues, legal, ethical and social issues in ICT, forensics, e-commerce, etc.) are offered by universities within a number of bachelor and master degrees.

The University of Pristina provides teaching syllabi in the area of Internet and broadband technologies and is the only institution in the country providing PhD studies in the fields of secure mobile programming and cryptography. Also, the newly-established public University of Prizren offers academic programs in the field of ICT within its Faculty of Computer Science in two departments: Information and Telecommunication Technology, and Software Design. Besides, the American University in Kosovo, AAB-Riinvest College, Iliria College, and UBT College have also started offering study programs in the field of ICT.

Training in information security does take place, but is rather ad-hoc and uncoordinated. Training is usually provided by Law Enforcement and by various private organisations within the American University of Kosovo, such as The Computer Information System Company Organisation (CISCO), the International Organisation for Standardisation (ISO), CACTTUS Sh.a., and STIKK-Kosovo Association of Information and Communication Technology. Also, it is common practice for big private organisations to train their employees in other countries, such as the UK, Germany or the USA.

D3-2: National Development of Cyber Security Education

This sub-dimension explores what kind of incentive structure exists for the national development of cybersecurity education: for example, whether any education strategy for developing cybersecurity skills exists; whether cyber security as a discipline is given priority in educational curricula; whether adequate budget allocation is present.

Formative: There are incentives for training and education, while state budget for training, research and development have been allocated. The Ministry of Education has placed ICT and security issues as part of the curricula for all levels of education, and there is budgetary allocation for this effort. The National Research Council (NRC)[11] has placed communication and technology as a priority, and this is a reflected in the efforts to build programmes in cybersecurity.

In 2004, the Ministry of Education adopted a Strategy for Development of Higher Education in Kosovo 2005-2015. The main objectives determined in this strategy are advancing management and coordination in higher education, advancing capacity for research and scientific work, and development of a complete and functional infrastructure in higher education.

Kosovo followed the European practice of fostering research in ICT, which was one of the highest-priority themes of the EU's Seventh Framework Programme (FP7) for Research and Technological Development. Kosovo is entitled to participate in FP7 with the International Cooperation Partner Country status.

Research is among the main objectives of the higher education strategy. The research objectives include building of a common network infrastructure, a data-store centre, and a services repository for government; developing e-learning software, hardware and a legal policy infrastructure; securing resilient infrastructures; empowering the e-government portals with support for e-business to attract participation of business and customers; and to adopt standards of software engineering in the ICT industry and others.

In 2008, the Ministry of Education of Republic of Kosovo and the Federal Ministry of Science and Research of Austria signed a Memorandum of Understanding for Kosovo-Austria Institutional Partnership[12] in the field of Higher Education and Research including research in cybersecurity issues. The Partnership included the development of interfaces to research and innovation and interaction between universities and the local economy.

D3-3: Training and Educational Initiatives within the Public and Private Sector

Cyber security is a highly technical specialized field, and therefore strategic development and deployment of skillsets and tools to support them is central to maintaining organizations secure and mainstreaming cybersecurity culture within organizational structures. Apart from the question of strategic staffing, this sub-dimension assesses the scope of horizontal and vertical cybersecurity knowledge transfer within organizations and how it translates to continuous skills development.

Formative: Cybersecurity training programmes are executed in Kosovo but in an ad-hoc manner. Few trained IT personnel within public sector and private are designated to support cybersecurity issues as they occur. Although appropriate skillsets may exist within the workforce, experts with such skills are not easy to allocate.

[11] http://www.masht-gov.net/advCms/documents/NRP_%28Draft%29_English.pdf
[12] http://wbc-inco.net/attach/KosovoICTReportFINAL_01_12_2009.pdf

The Ministry of Economic Development encourages the development of information technology training systems (Appendix 18-XXIV)[13]. The Ministry of Public Administration has established an Executive Agency in order to support Kosovo Public Administration through staff training on Information Technology. Kosovo Institute for Public Administration (KIPA) develops and implements these training policies developed by the Ministry of Public Administration.

Training is usually provided by Law Enforcement and accredited training is provided by various private and educational organisations, such as The Computer Information System Company Organisation (CISCO) (within the American University of Kosovo), CACTTUS Sh.a., and STIKK-Kosovo Association of Information and Communication Technology, according to ISO 27000 series of standards that have been specifically reserved by the International Organization for Standardization (ISO) for information security matters. Private ICT companies are better organised in terms of cybersecurity training and education initiatives and overall they follow risk-management policies. Yet, the majority of them still lack specific cybersecurity training, and there is no organised knowledge-transfer to their peers in companies.

At the University of Pristina, a Centre of Cyber Information Security (Research & Development) is currently being established. The Centre will engage in research activities on cyber information security.

D3-4: Corporate Governance, Knowledge and Standards

Any organisation represents a dynamic environment, where needs should be continuously assessed and addressed for the realization of an organization's mission and strategic goals. This sub-dimension specifically looks into how private and state-owned companies', as represented by the highest executive level of senior management (C-level management), understand cyber security and react to changes related to the cybersecurity status quo.

Start-up: Awareness of cyber security at the C-level management remains limited. Boards and executives within private and state-owned companies have some awareness of cybersecurity issues but this has been appraised as minimal. Although board level members are usually not trained in cyber security, organisations are a dynamic environment, where needs are continuously assessed and addressed. As a result, even if board members might not recognise the need for a possible certification, they will be informed through internal communications and may take specific steps to meet this need.

The National Agency for Personal Data Protection (NAPDP), in cooperation with Ministry of Public Administration and the Kosovo Institute of Public Administration, has organized training for officials on personal data protection. The purpose of this activity was to provide officials with knowledge about the Law on Protection of Personal Data, its implementation, and the duties and responsibilities of NAPDP, as well as the relation of these officials with NAPDP.

[13] http://www.kryeministri-ks.net/repository/docs/Rregullorja_02-2011-e_miratuar_nga_Qeveria-finale.pdf

In the private sector, board members usually have an understanding of the risks associated with cyber security. However, in the case of state-owned companies, board members are usually not trained in cyber security and they are not therefore aware of how cybersecurity issues might affect their organisations, nor which direct threats they might face.

Dimension 4: Legal and Regulatory Frameworks

International experience attests to the crucial role legal and regulatory frameworks play in mainstreaming cyber security across sectors while presenting prevention, mitigation, and dispute mechanisms to individuals and organizations affected by cyber threats. This dimension looks into the government's capacity to design and enact national legislation and accompanying by-laws directly and indirectly relating to cybersecurity, with a particular emphasis placed on the topics of ICT security, privacy and data protection issues, cybercrime, and on the stakeholder groups represented by law enforcement, prosecution services, and courts.

D4-1: Cybersecurity Legal Frameworks

This sub-dimension assesses availability and comprehensiveness of ICT security and privacy and data protection legislation, its relation to human rights legislation, as well as country's status in relation to regional and international treaties directly or indirectly related to cyber security.

Formative: The Law on Electronic Communications, developed by the Ministry of Economic Development, includes references to ICT as well as more specific provisions addressing security and integrity of public electronic communication network and services, and is aligned with sectorial EU legislation. There is currently no stand-alone cybersecurity Law. But policy makers and the Ministry of Economic Development are considering of introducing in the future a proposed ICT legislation related to cyber security, depending on the changes in EU ICT legislation.

The Law on Electronic Communications foresees number of bylaws to be developed that should establish implementation procedures of the rights and obligations envisaged by the law. Such as, for instance, provision of the information about the major security breaches, performance of security audits. Those bylaws are pending to be developed. There are different pieces of legislation that speak to cybercrime (the Law on Electronic Communications, the Law on the Information Society Services chapter 14, the Law on Copyright and Related Rights, the Law on Protection of Personal Data, the Law on Prevention and Fight Against Cybercrime).

Comprehensive data protection legislation and regulatory procedures have been implemented, where domestic law provides for the individual's right to privacy, specifying notice, purpose, consent, security, disclosure, access and accountability of personal information. In 2010, Kosovo Assembly adopted the Law on Protection of Personal Data (03/L-172)[14] and the agency responsible for its implementation is the National Agency for Personal Data Protection (NAPDP). The Law defines the rights, responsibilities, principles and measures concerning the protection of personal data.

NAPDP reports directly to the Assembly of Kosovo and, as an independent institution, has legal responsibility for overseeing the implementation of the rules and regulations on

[14] http://www.kuvendikosoves.org/common/docs/ligjet/2010-172-eng.pdf

protection of personal data. Advising public and private bodies, deciding on complaints submitted, conducting inspections and audits, as well as providing support and promotion of the fundamental rights in the field of personal data protection, are the main functions of the Agency. In this way, NAPDP wants to ensure that the right of each individual to privacy is respected and protected during personal data processing. International cooperation in relation to protection of personal data is an important part of the permanent mission of the Agency, given the priority of the Government of Kosovo towards EU integration.

Data Protection Officers are established in each public administration entity and in private institutions, dealing with privacy issues. The Annual Report[15] (2013) of NAPDP includes all the details on the activities of the Agency in the area of personal data protection, the transfer of personal data as well as the assignment of data protection officers.

The Substantive Law on Cyber Crime of Kosovo covers the prevention and mitigation of cybercrime. The Law on Prevention and Fight against Cyber Crime No.03/L–166[16], which was developed with assistance from the Council of Europe, aims to prevent and combat cybercrime with concrete measures to prevent, discover and sanction violations through computer systems by providing observance of the human rights and safeguard of personal information. Article 16 of the Law refers to child pornography through computer systems, Article 9 refers to penal acts against confidentiality, integrity and availability of the computer systems, while Article 14 refers to computer-related penal acts.

Cybercrime is part of the Criminal Code in Kosovo. In addition to the above mentioned Criminal Law, partial legislation exists in Procedural Cybercrime Code. The International Law Enforcement Cooperation Unit (ILECU) is the coordinating body for investigation into cybercrimes.

D4-2: Legal Investigation

This sub-dimension studies the capacity of executive branch of government to prevent, combat, and investigate cyber incidents, attacks, and crimes, and of judiciary branch to prosecute cybercrime and electronic evidence cases. It also looks into the dynamic of formal and informal collaboration between different branches of government and between government and court system.

Formative: Some investigative capacity exists to investigate computer-related crimes, in accordance with domestic law, however it is minimal and lacks human resources. In particular, the Cyber Crime Investigation Unit within the Kosovo Police has the technical capacity and training to investigate computer-related crimes.

Prosecutors are not trained adequately, although the Council of Europe has provided some training on cybercrime matters. With the support of CyberCrime@IPA, two trainers from Kosovo Judicial Institute have attended a basic training for judges and prosecutors and an

[15] http://www.amdp-rks.org/web/repository/docs/Final_ENG_ASHMDHP_Raporti_Vjetor_i_Pun_s_2013.pdf
[16] http://www.kuvendikosoves.org/common/docs/ligjet/2010-166-eng.pdf

advanced training course in October 2012. They are able now to deliver training to other judges and prosecutors. One representative from Kosovo was funded to participate in the Master of Sciences (MSc) programme in Forensic Computing and Cybercrime Investigation offered by UCD. But, the majority of Judges do not have specialized training on cybercrime cases, electronic evidence or computer-related crimes, in general. Moreover, there is no formal mechanism for collaboration between judges concerning cybercrime cases.

There is support for continuing professional development (CPD) of the judiciary. Institutional development inputs are provided by the Kosovo Institute of Public Administration (KIPA), the leading institute for training members of the public service, and the Kosovo Judicial Institute (KJI), a training institute for judges and public prosecutors. The Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH also assists KIPA and KJI in developing new training modules and in training trainers to use modern teaching methods.

The Kosovo Judicial Council's (KJC) Strategic Plan[17] for the period of 2007–2012 marked introduction of ICT in the Kosovo Judiciary as one of critical preconditions for fulfilment of KJC's duties and responsibilities. In order to proceed in an organized and systematic way with its ICT efforts in the future, KJC requested technical assistance from the Technical Assistance and Information Exchange instrument of the European Commission (EC TAIEX) and the Government of Norway in preparation of the ICT Strategy for the period 2012–2017[18]. Through implementation of the ICT Strategy, KJC will work towards the following specific objectives: transformation of Kosovo courts into e-courts, which will use a central database environment; adequate ICT infrastructure and exchange of data and documents in e-form inside Kosovo judicial system, as well as with all other relevant ICT systems in Kosovo and abroad; availability of online services for citizens through creation of a judicial web portal; creation of KJC in-house human resources, who will possess knowledge and skills necessary for execution of this ICT strategy, as well as providing court staff with adequate training and hardware equipment for everyday and undisrupted usage of KJC's applications, e-mail and Internet. One of the main goals of "ICT strategy for judicial system" is to optimize secure IT services and recourses and establish cyber defence capabilities for Kosovo Judicial Council (KCL) web services.

D4-3: Responsible Reporting

This sub-dimension explores if the public and private sectors enact a responsible disclosure policy and if there is sufficient capacity on part of both to continuously review and update this policy and synchronise it with recognised international responsible disclosure mechanisms. It also analyses existing capacity of stakeholders to receive, analyse, and disseminate vulnerability information gleaned through the responsible disclosure mechanisms.

Start-up: The need for a responsible disclosure policy in public and private sector organisations is neither acknowledged nor understood, and therefore there is no formal disclosure framework. Internal and informal disclosure mechanisms for each public administration entity do exist, however nothing has been formalised. The Law on the

[17] http://www.kgjk-ks.org/repository/docs/Plani_strategjik_ANG_275311.pdf
[18] http://www.kgjk-ks.org/repository/docs/Kosovo-ICT-strategy_389023.pdf

Protection of Personal Data, (No.03/L–172) and the Law on Classification and Verification of Information (03/L-178)[19] refer specifically to the disclosure of personal data.

There are internal procedures for Regional Municipality Networks interactions and there are reporting requirements within government. Also, in case of a data breach in a telecommunication company, public disclosure is mandated according to the Law on Electronic Communications.

[19] http://www.assembly-kosova.org/common/docs/ligjet/2010-178-eng.pdf

Dimension 5: Standards, organisations, and technologies

This dimension brings forward the importance of implementation of cybersecurity standards and minimal acceptable practices; existence of well-functioning and high capacity organisations coordinating cyber security with formal authority over multiple stakeholders; and existence of a vibrant cybersecurity marketplace of technologies and cyber insurance services.

D5-1: Adherence to Standards

This sub-dimension assesses government's capacity to design or adapt from other jurisdictions and implement cybersecurity standards and minimal acceptable practices, especially those related to procurement procedures and software development. These standards and practices provide a minimum necessary baseline in the context of which strategic government decisions, especially organizational (resource) and financial (budgetary) ones, should take place.

Formative: Information-security standards have been identified for use. Generally, the private sector adheres to international standards such as ISO, and the Government of Kosovo is using Microsoft Platform as a standard for software development. It is the initiative of each public administration entity to adhere to standards in order to advance their investments.

Procurement, cyber-security standards, practices and procedures are currently under development nationally. The private sector already adheres to standards on procurement. Methodologies for software-development processes focused on integrity and resilience are promoted by government and professional communities. The Kosovo Business Registration Agency (KBRA), which falls under the responsibility of the Ministry of Trade and Industry, and Kosovo Customs use secure software and implement public key infrastructure (PKI).

Kosovo does not have a systematic method of software development as required by software engineering. Small and medium ICT companies (SMEs) have progressed to use CASE tools for certain phases of software development such as programming, but are not using fast tools for other phases such as analysis, design and testing. Moreover, they do not follow well-defined software methods and processes throughout the software cycle. Software development is usually external, but when software is developed locally SSL standards are implemented.

D5-2: Cybersecurity Coordinating Organisations

This sub-dimension assesses government's capacity to provide a comprehensive national situational awareness and adequate incident response and coordinate both of these functions with other relevant stakeholders through a formally established authority with strictly defined cybersecurity functions, enhanced automation, and sufficient resources.

Start-up: No Cybersecurity Command and Control Centre exists at a national level. Within the Kosovo Police and the Kosovo Security Force there is a Cybercrime Unit, but its capacity remains limited due to a lack of human resources. The Cybercrime Unit works in collaboration with telecommunication companies in order to address cyber incidents but cooperation between the actors remains rather informal.

Incident-response capacity is not coordinated and is performed in an ad-hoc manner. It has to be noted that the National CERT is now under development. According to the Law on Electronic Communications (no. 04/l-109), Article 10 Point 21[20] regarding the ARKEP, it is stated that *''a computer emergency response center functions with the aim to deal with threats to public electronic communication systems*''.

Incidents across government are reported to the Agency for Information Society (APA: Agency of Public Administration) whilst the private sector reports directly to Law Enforcement. The Agency of the Ministry of Public Administration serves as a governmental CERT, but it is not a national CERT. Moreover, there is no official communication framework and no official work-flow between different departments of government.

D5-3: National Infrastructure Resilience

This sub-dimension assesses how effectively the government deploys and manages infrastructure technologies (own government networks and systems) and how it performs monitoring and evaluation of the costs for infrastructure technologies and their resilience. In addition, it looks into existence and exercise of government's capacity to engage in strategic planning and maintain sufficient scientific, technical, industrial, and human capabilities.

Formative: Deployment of technology infrastructure and processes is performed in public and private sectors but not in a strategic manner. There are online government services offered, such as online submission of tax forms within the Ministry of Finance. Also, information and digital content are available online, but implementation and process are limited.

The Ministry of Public Administration provides network provision, network operation, but it is informally organised. The Internet-service infrastructure is reliable (in the case of IPKO, it follows Slovenian standards because of a parent company Telekom Slovenije), whereas e-commerce transactions follow more general international standards. National infrastructure regarding cybersecurity is managed informally, with no documented processes, roles and responsibilities. However, the government makes use of a state-owned network managed by the Ministry of Public Administration.

There are three major Internet service providers (ISPs) in Kosovo, all with licenses that allow them to connect directly to the international Internet backbone: IPKO Telecommunications LLC, Kujtesa, and the Post and Telecommunications Enterprise of Kosovo (PTK). The main telecommunication infrastructure provider is PTK, which is considered to be reliable. There are several other smaller ISPs that focus on extending Internet access beyond the service areas of these three ISPs. All three providers report relatively high Internet usage by businesses[21]. ISPs are continuing to expand and to upgrade their infrastructure but their presence is mostly limited to urban areas.

[20] http://mzhe.rks-gov.net/repository/docs/Ligji_i_KE_i_Publikuar_%28Anglisht%29.pdf

[21] http://pdf.usaid.gov/pdf_docs/PNADK675.pdf

D5-4: Cybersecurity Marketplace

This sub-dimension studies availability of competitive cybersecurity technologies and their strategic deployment and maintenance by public and private sectors. It also assesses the state cyber insurance marketplace and its offerings through the study of perception of financial risks by public and private sectors and perceived demand for cybercrime insurance.

Start-up: There are no cybersecurity technologies produced domestically. Specifically, some local companies provide services or produce software but they do not produce technology products. It is common practice for software-security firms to develop security mobile software applications, but the development of the software products is outsourced.

The need for a market in cybercrime insurance has not been identified in Kosovo through the assessment of financial risks for the public and private sectors. It has to be acknowledged, though, that cybercrime insurance is established specifically for the banking sector, covering unauthorised access and loss of data, and products suitable for SMEs are also on offer. Cybercrime insurance is available for the banking sector thanks to a foreign private company's offerings from Austria[22] and is not a development of the public or private sector in Kosovo as such. It was a common concern, however, that this market is overpriced and as a result there is limited take-up.

[22] Note: The information about existence of such an insurance was obtained during a field mission from local banking stakeholders however it was not confirmed through the desk research.

Recommendations

Following the information presented on the assessment of the cybersecurity maturity of the Republic of Kosovo, the Global Cyber Security Capacity Centre has produced a set of recommendations to be considered by the Government of Kosovo.

These recommendations refer to all five dimensions of cyber capacity and aim to provide advice and steps to be followed for the enhancement of existing cybersecurity capacity in Kosovo.

Dimension 1

Capacity Gap – develop a national cybersecurity strategy

As stated, there are plans in place to develop a comprehensive national Cybersecurity Strategy for Kosovo. Currently, the Ministry of Internal Affairs is responsible for collecting personal data for all citizens, so it is important for this Ministry to be involved in the effort of developing a national cybersecurity strategy.

It is recommended that a government entity with a mandate in ICT sector development (the Ministry of Economic Development) play the leading role in this process. It is as important that the development of the strategy be premised on multi-stakeholder consultation with such entities as the Agency for Information Society, the Regulatory Authority for Telecommunication (ARKEP), the National Agency for Personal Data Protection (NAPDP), as well as other Ministries.

Although there is some coordination between government stakeholders and Law Enforcement, this coordination remains limited to the governmental network. Therefore, it may be optimum for the country to draft regulations on this matter before the development of the national cybersecurity strategy.

Furthermore, there is no plan for a draft standalone ICT law related to cybersecurity. But in the future cybersecurity-focusing sub-legislation may be developed. The work in this area is expected to promote adoption of international standards and best practices, such as ISO, since it is now upon the decision of each public administration entity to adhere to standards in order to advance their investments.

A very critical point in well-established software provision is the availability, reliability and security level of data and services as well as the communication network. Security technologies serve to protect user privacy. All current technologies based on e-services depend heavily on secure data exchange. This aspect is an essential issue to be considered during the development of the Cybersecurity Strategy.

As far as coordination is concerned regarding Critical National Infrastructure (CNI), telecommunication companies have formal procedures established. The initiative of a formal

coordination between public and private sector and especially between different banks would be expected to provide the necessary parameters for information sharing.

Regarding crisis and risk management, conduct of exercises-simulations at a national level, at least once a year, would be expected to provide valuable insight and inform the overall crisis management.

Recommended Course of Action:

- Develop a National Cybersecurity Strategy.
- Assign the Ministry of Economic Development as a government entity responsible for the development and implementation of the National Cybersecurity Strategy.
- Prioritise drafting of regulations on incidents' listing and categorizing them at a national level before developing a national cybersecurity strategy
- Establish a national programme for promoting standards' adoption in procurement or software development.
- Conduct crisis and risk management exercises-simulations at a national level at least once a year.
- Strengthen formal coordination regarding Critical National Infrastructure (CNI) and information sharing between public and private sector and especially between different Banks.

Dimension 2

Capacity Gap – maintain and expand the national cybersecurity awareness campaign

The Ministry of Education, the National Agency on Personal Data Protection, and the Ministry of Local Government Administration have developed a cybersecurity awareness campaign programme at a national level. It is essential that this programme be not a standalone activity, be maintained to expand its reach to as many different target groups as possible, and be linked to the current planning process on development of a national cybersecurity strategy.

In addition, reinforcement of effective communication between government entities and civil society would lead to accomplishment of its maximum success. It is also extremely important that the awareness programme be evaluated for its effectiveness, thus leading to its further improvement according to the needs of cybersecurity stakeholders and beneficiaries, and the lessons learned during its implementation to date.

Use of online services requires a certain level of trust from users. Therefore, the efforts to promote the trust in online services, both e-government and e-commerce ones, are highly recommended, since only few infrastructure operators and the banking sector implement measures to promote trust in online services.

Recommended Course of Action:

- Maintain and expand the existing awareness programme to cover various target groups and link the programme to the national cybersecurity strategy development.
- Enact evaluation measurements to study effectiveness of the awareness programme.
- Promote trust in e-government and e-commerce services through regulation ensuring personal data privacy and adherence of e-government services to the highest cybersecurity protection standards.

Dimension 3

Capacity Gap – information security training and education need to be engrained through all stages of education

There are educational offerings in information security education and training. More deeply engrained information security training and education through all stages of education, from primary to secondary school, as well as from university to continuing professional development level, is expected to not only raise awareness of society at large on cyber threats and their prevention, but also enhance the ability of cybersecurity stakeholders to strategically locate experts on cybersecurity issues, and enhance supply of cybersecurity skills in workforce.

In addition, a national-level register of experts will facilitate their effective move to the market. It is imperative for the country to be able to identify and allocate expertise where needed.

Recommended Courses of Action:

- Engrain information security training and education through all stages of education.
- Allocate additional resources to cybersecurity education and training for public universities.
- Develop partnerships for the development of interfaces to research and innovation and interaction between universities and the local economy.
- Develop government-sponsored certification programs on cybersecurity.
- Introduce a regular mandatory cybersecurity training for public sector staff.
- Create a national-level register of cyber-security experts.
- Create obligatory cybersecurity modules for students and teachers in a new Strategy for Development of Higher Education in Kosovo for the period beyond 2015.
- Conduct cybersecurity trainings for public sector employees and board members of the state-owned enterprises in a regular manner and in a sufficient scope responding to emerging and existing cybersecurity issues encountered by the population of Kosovo.

Dimension 4

Capacity Gap – strengthen investigation capacity for computer-related crimes and develop a responsible disclosure policy

Some investigative capacity exists to investigate computer related crimes, in accordance with domestic law. In order for prosecutors to have the capacity to prosecute computer-related crimes, adequate training should be provided. Also, judges need to receive training on computer-related crimes and develop a formal collaboration mechanism to exchange information on computer related cases.

The need for a responsible disclosure policy in public and private sector organisations has to be enacted and a formal disclosure framework has to be developed.

Recommended Courses of Action:

- Provide training and education of prosecutors and judges on computer related crimes.
- Allocate additional resources to cybersecurity education & training for prosecutors and judges.
- Introduce regular mandatory cybersecurity training for prosecutors and judges.
- Ensure cybersecurity knowledge transfer from KIPA and KJI to public sector and maintain cybersecurity cooperation with international donors.
- Develop a responsible disclosure policy within public sector and facilitate its adoption in the private sector through targeted outreach.

Dimension 5

Capacity Gap – promote the adoption of international standards within the public sector, and establish cooperation between academia and research & development (R&D) industry to strengthen the software-engineering competencies of domestic ICT companies

Adherence to international standards such as ISO is common practice for the private sector. The establishment of a programme by the Government of Kosovo for the promotion of international standards and best practices could lead to their adoption not only in the private but also public sector. It is suggested that the Agency for Information Society, in collaboration with the Ministry of Economic Development, consider initiating such a programme while leveraging public funding. A national ICT strategy should include measures enabling promotion of adherence to international standards.

A Cybersecurity Command and Control Centre has been established within the Kosovo Police. The Cyber Crime Unit, also within the Kosovo Police, needs to advance its capacity through enhancement of human resources.

As far as incident-response capacity is concerned, it is essential for the national CERT that is being currently under development, to have enough resources and experts with sufficient and

accredited training, so that it can perform its functions in a coordinated and sufficient manner. It is also important to advance preparation of the relevant secondary legislation that will allow CERT to be operational from the regulatory framework standpoint.

Kosovo has recently improved its ICT performance. However, further investments are required to support R&D in ICT. A cooperation established between academia and research & development (R&D) industry can strengthen the software-engineering competence of domestic ICT companies. Updated curricula at universities, including software-engineering courses can contribute to building intellectual capacity in the field and promote adherence to standards in the public sector.

Recommended Courses of Action:

- Establish a programme to strengthen government's capacity to adapt or adopt international standards.
- A national ICT strategy should include measures enabling promotion of adherence to international best standards.
- Establish a national Command and Control Centre[23].
- Coordinate performance of the national CERT, currently under development, allocating sufficient resources and accredited training to its employees.
- Invest in ICT research and cooperation between academia, research and industry to strengthen the software-engineering competencies of domestic ICT companies.

Conclusion

The Republic of Kosovo is in the process of developing different aspects of cybersecurity capacity. Implementation of the national cybersecurity strategy, the preparation for which should be launched in 2015, and launch into operation of the national CERT, currently under development, are expected to set the foundations for an advanced capacity in the future. The recommendations presented above provide further guidance for increasing capacity in the different dimensions of cybersecurity maturity.

[23] The Command and Control Centre is established by the Government. A national Command and Control Centre, receives and correlates information from incident response capability organisations, public/private organisations, Layered Service Providers, Critical Information Infrastructure, defence and intelligence organisations, and provides advanced situational awareness.

Global
Cyber Security
Capacity Centre

OXFORD
MARTIN
SCHOOL

UNIVERSITY OF
OXFORD

DEPARTMENT OF
COMPUTER
SCIENCE

SAID
BUSINESS SCHOOL

The Global Cyber Security Capacity Centre is funded by the United Kingdom Foreign And Commonwealth Office and hosted by the 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