

Public Disclosure Authorized

Public Disclosure Authorized

Public Disclosure Authorized

Public Disclosure Authorized



Lessons Learned and Recommendations towards  
strengthening the Program

# Global Cybersecurity Capacity Program

© 2019 The World Bank  
1818 H Street NW, Washington DC 20433  
Telephone: 202-473-1000; Internet: [www.worldbank.org](http://www.worldbank.org)

### **Some rights reserved**

This work is a product of the staff of The World Bank with external contribution. Note that The World Bank does not necessarily own each component of the content included in the work. The World Bank therefore does not warrant that the use of the content contained in the work will not infringe on the rights of third parties. The risk of claims resulting from such infringement rests solely with you.

The findings, interpretations, and conclusions expressed in this work do not necessarily reflect the views of the Executive Directors of The World Bank or the governments they represent. The World Bank does not guarantee the accuracy of the data included in this work. The boundaries, colors, denominations, and other information shown on any map in this work do not imply any judgment on the part of The World Bank concerning the legal status of any territory or the endorsement or acceptance of such boundaries.

### **Rights and Permissions**

The material in this work is subject to copyright. Because The World Bank encourages dissemination of its knowledge, this work may be reproduced, in whole or in part, for noncommercial purposes as long as full attribution to this work is given.

Attribution – Please cite the work as follows: “World Bank. 2019. Global Cybersecurity Capacity Program. © World Bank.”

All queries on rights and licenses, including subsidiary rights, should be addressed to World Bank Publications, The World Bank Group, 1818 H Street NW, Washington, DC 20433, USA; fax: 202-522-2625; e-mail: [pubrights@worldbank.org](mailto:pubrights@worldbank.org).

# Contents

Acknowledgements	2
Executive Summary	4
Introduction	7
<b>Global Cybersecurity Capacity Program (2016-2019) overview</b>	<b>7</b>
Countries in scope	9
Key milestones	9
<b>Global Cybersecurity Capacity Program (2016-2019) major milestones timeline</b>	<b>10</b>
<b>Methodological approach</b>	<b>11</b>
Characterization of cybersecurity capacities	11
Measuring maturity	13
<b>Key objectives of the Program and Activities</b>	<b>14</b>
<b>General aspects</b>	<b>14</b>
<b>Kyrgyz Republic</b>	<b>17</b>
<b>Myanmar</b>	<b>26</b>
<b>Ghana</b>	<b>31</b>
<b>Western Balkans</b>	<b>38</b>
Republic of North Macedonia	38
Albania	47
Bosnia and Herzegovina	52
Regional level initiatives	59
Methodologies and practices	59
<b>Global Cybersecurity Capacity Building Program: Closing meeting</b>	<b>61</b>
<b>Results</b>	<b>64</b>
<b>Recommendations</b>	<b>66</b>

# Acknowledgements

This document summarizes the main results, lessons learned during completion of the Global Cybersecurity Capacity Program (hereinafter Program) conducted by the World Bank and related recommendations towards strengthening similar activities. Information contained in this material reflects the status of the Program as of May 31, 2019.

The Program team wish to extend its acknowledgements to the World Bank colleagues who tirelessly supported implementation of the Program, including: (from **Albania Country Office**) Ms. Odeta Buló, Senior Executive Assistant; Ms. Ana Gjakutaj, Senior Communications Officer; Ms. Elda Hafizi, Program Assistant; Ms. Enkelejda Karaj, Program Assistant; and Ms. Evis Sulko, Senior Country Operations Officer; (from **Bosnia and Herzegovina (BiH) Country Office**) Ms. Samra Bajramović, Program Assistant; Mr. Zoran Hadziahmetović, IT Officer; and Ms. Sanja Tanić, Program Assistant; (from **Ghana Country Office**) Mr. Stephen Tettevie, Team Assistant; (from **Kyrgyz Republic Country Office**) Ms. Zhanetta Baidolotova, Program Assistant; Mr. Uran Esengeldiev, Consultant; and Ms. Jyldyz Djakypova, Communications Officer; (from **Myanmar Country Office**) Mr. Aung Htun Lynn, IT Analyst; (from **Republic of North Macedonia Country Office**) Mr. Luan Aliu, Program Assistant; Ms. Anita Bozinovska, Communication Assistant; and Mr. Artan Saliu, IT Analyst; (from the **Digital Development Global Practice**) Ms. Irene Rubio Gonzalez, Consultant; Ms. Christine Howard, Program Assistant; Mr. Tim Kelly, Lead ICT Policy Specialist; Ms. Kaoru Kimura, ICT Policy Specialist; Mr. Siou Chew Kuek, Senior ICT Policy Specialist; Ms. Marisol Ruelas, Program Assistant; Mr. Juan Navas-Sabater, Lead ICT Policy Specialist; and Ms. Sandra Sargent, Senior Operations Officer. Country Managers Mr. Marco Mantovanelli (for Republic of North Macedonia), Mr. Emanuel Salinas (for BiH), and Ms. Maryam Salim (for Albania), together with Ms. Daria Lavrentieva, Senior Portfolio Coordinator for Western Balkans Regional Unit, were instrumental in supporting this Program and inspiring the team through their public presentations, which drove significant visibility to this cybersecurity work. Last but not least, the team extends its sincere gratitude to Ms. Boutheina Guerhazi, Senior Director, and Ms. Jane Treadwell, Practice Manager, from the Digital Development Global Practice who facilitated the work under the Program and supported its continuation under the Global Cyber Security Program II.

On the partner side, the World Bank team wish to acknowledge and cordially thank the Global Cybersecurity Center for Development of Korea Internet & Security Agency (KISA) and Oxford University's Global Cyber Security Capacity Centre (GCSCC) for their dedication to the Program and their crucial contributions to make it a success. In particular, the acknowledgement is extended to Mr. Jaeil Lee, Vice President of KISA; Ms. Junghee Kim, Director of KISA; Ms. Sinae Ryu, Manager of KISA; Ms. Soseon Her, Deputy General Researcher of KISA; and Ms. Junok Lim, Deputy General Researcher of KISA. Within the GCSCC, the Program team extends acknowledgments to Dr. Ioannis Agrafiotis, Research Fellow; Dr. Maria Bada, former Research Fellow; Dr. Ian Brown, former Associate Director; Prof. Paul Cornish, former Co-Director; Prof. Sadie Creese, Director; Prof. William Dutton, Oxford Martin Fellow; Dr. Marco Gercke, former Associate Director; Prof. Michael Goldsmith, Co-Director; Mr. Faisal Hameed, Researcher; Ms. Eva Ignatuschtschenko, former Research Fellow; Prof. Chris Mitchell, former Associate Director; Dr. Eva Nagyfejeo, Research Fellow; Ms. Lara Pace, former Head of Strategy and Engagement; Prof. Fred Piper, former Associate Director; Dr. Sarah Puello Alfonso, Project Officer; Prof. Angela Sasse, former Associate Director; Prof. Ivan Toft, former Associate Director; Prof. David Upton, former Co-Director; Prof. Basie von Solms, Oxford Martin Fellow; Ms. Carolin Weisser Harris, Lead International Operations. In Ghana and Myanmar the Norwegian Institute of International Affairs (NUPI) contributed financing to cover travel costs of GCSCC staff. Dr. Niels Nagelhus Schia, Senior Research Fellow at NUPI, contributed to the Myanmar report.

Last but not least, the Program team would like to thank the governments of participating countries for the leadership and dedication to Program’s objectives: (from **Albania**) Ms. Vilma Tomco, General Director, National Authority on Electronic Certification and Cyber Security; Mr. Rexhion Qafa, Cybersecurity Expert, National Authority on Electronic Certification and Cyber Security; Mr. Ibrahim Smoqi, Information Technologies Network Specialist of eGovernment Infrastructure Department, AKSHI; Ms. Irena Malolli, Director of Policies and Strategy Development of Telecommunications and Post, Ministry of Infrastructure and Energy; Mr. Fotjon Kosta, Head of ICT, Ministry of Infrastructure and Energy; Mr. Armando Qosja, Information Security Officer, Albcontrol; representatives of the banking sector Mr. Valsi Thomollari; Mr. Oerd Cukalla; Mr. Eni Nesturi; Ms. Eriketa Jolldashi; representatives of academia: Dr. Anni Dasho, Dr. Indrit Baholli; Mr. Sadi Matar, Political Advisor at European Union Special Representative in Bosnia and Herzegovina; (from **BiH**) Mr. Vlatko Drmić, Assistant Minister, Sector for Communications and Informatization, Ministry of Communications and Transport; Mr. Danko Lupi, Senior Associate for Informatization, Ministry of Communications and Transport; and Ms. Irida Varatanović, Head of Department for Informatization, Ministry of Communications and Transport; (from the **Kyrgyz Republic**) Mr. Sagymbaev Abdisamat, State Secretary of the State Committee for IT and Communications (SCITC); Mr. Kubanych Shatemirov, Vice-chairman, SCITC; Mr. Mirlan Omuraliev, former Vice-chairman, SCITC; Mr. Dastan Dogoev, Director of the Project Implementation Unit (PIU) of Digital CASA-Kyrgyz Republic Project; Mr. Bahtiar Djalikov, former Head of Information Security Department, SCITC; and Ms. Bibigul Bektenova, Chief specialist of ISD, SCITC; (from **Ghana**) Honourable Ursula Owusu-Ekufu, Minister for Communications; Honourable Vincent Sowah Odotei, Deputy Minister for Communications; Honourable George Andah, Deputy Minister for Communications; Mr Issah Yahaya, Former Chief Director of the Ministry for Communications; Dr. Albert Antwi-Boasiako, National Cyber Security Advisor/Team Lead, National Cyber Security Centre; Mr. Nelson Osae, Project Coordinator, e-Transform Unit, Ministry of Communications; Honourable David Gyewu, Director-General, National Information Technology Agency, Ministry of Communications; Mr Eric Akumiah, Data Expert, e-Transform Unit, Ministry of Communications; Mr Joseph Tetteh, Head of IT, Ministry of Communications; Mr Kofi Otchere, Chief Technology Officer, National Information Technology Agency, Ministry of Communications; Mr Kwadwo Osafo-Maafa, Director, Cybersecurity Division, National Communications Authority; (from **Myanmar**) Mr. U Ye Naing Moe, Director of IT and Cybersecurity Department, Ministry of Transport and Communications; (from **Republic of North Macedonia**) Mr. Aleksandar Acev, Head of National Centre for Computer Incident Response MKD-CIRT, Agency for Electronic Communications; Ms. Alenka Georgieva, Head of C-4 sector, Ministry of Defence; Ms. Ana Malceva, Legal Adviser of the Minister for Information Society and Administration; Mr. Dimitar Manchev, ICT Advisor, Ministry of Information Society and Administration; Ms. Elena Mancheva, ICT Advisor of the Minister for Information Society and Administration; Mr. Jane Stojanov, Head of sector for Telecommunications, Ministry of Interior; Ms. Jasmina Stojcheva, Senior Associate for Information Technologies, Agency for Electronic Communications; Ms. Jovana Gjorgjioska, Junior Associate for coordination and monitoring strategic plans, Ministry of Information Society and Administration; Mr. Marjan Stoilkovski, Head of Cyber Crime and Digital Forensics Unit, Ministry of Interior; Mr. Mitko Bogdanoski, Associate Professor and Vice Dean at the Military Academy “General Mihailo Apostolski” – Skopje, Ministry of Defence; Ms. Natalija Veljanoska, Head of Sector for Information Security, Ministry of Interior; Mr. Orhan Ismaili, IT / System Administrator, Ministry of Defence; and Ms. Solza Kovachevska, State Advisor for Information Systems and Technologies, Ministry of Information Society and Administration.



# Executive Summary

**O**ver three quarters of World Bank’s investment projects involve the financing of digital technologies<sup>1</sup> and it is reasonable to expect that this share will increase over time. The fourth Industrial Revolution is unfolding at full speed and is prompting governments to optimize current IT systems by adopting new technologies for the re-engineering of processes, as well as to provide new public services. Cloud computing, artificial intelligence, big data analytics, and new technologies are changing the modus operandi of government systems that are in charge of public finance management, human resources, and government service delivery. As “going digital” helps to increase efficiency and reduce costs, other government systems are also likely to follow suit.

**Yet, there is a caveat to rapid digitalization, which is often the result of public investment projects.** “Some of the perceived benefits of digital technologies are offset by emerging risks<sup>2</sup>”, according to the 2016 World Development Report on Digital Dividends. Cybersecurity risks, in particular, cannot be disregarded, as they may affect lives<sup>3</sup>, assets, trust, and social stability<sup>4</sup> if not prevented or effectively mitigated. Vulnerabilities of government IT systems that are exposed to the cyberspace even for a short period of time may lead to sizeable financial losses and malicious intrusions in the public governance system, with far-reaching consequences. The lack of government resources, awareness, and capacities worsens this issue and is often a major concern for policymakers.

**Conclusions can be easily drawn.** While promoting availability, affordability, and the adoption of digital technologies in its client countries, the World Bank as a financier and trusted partner should promote greater resilience of digital systems and infrastructures, as well as greater cybersecurity capacity and awareness among the governments and nations that the World Bank (WB) represents.

**The Global Cybersecurity Capacity Program**, which was generously financed by the Korea-World Bank Group Partnership (KWPF) between 2016 and 2019, is one of the first steps that the World Bank has taken in an attempt to bridge existing gaps in cybersecurity capacities, especially in the case of governments that have taken out loans from WB to cover the needs of their emerging digital economies. Thanks to tailored national and regional technical assistance schemes, this Program has helped to strengthen cybersecurity capacities and awareness in six countries, namely Albania, Bosnia and Herzegovina, Republic of North Macedonia in the Western Balkan region, Ghana in West Africa, the Kyrgyz Republic in Central Asia, and Myanmar in Southeast Asia. The objective was to benefit a selected sample of countries across geographical regions that prioritize cybersecurity assistance and have at least some capacity to design and implement digital

1 [https://siteresources.worldbank.org/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/Resources/WBG\\_ICT\\_Strategy-2012.pdf](https://siteresources.worldbank.org/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/Resources/WBG_ICT_Strategy-2012.pdf)

2 P. 3 <http://www.worldbank.org/en/publication/wdr2016>

3 This may refer to self-harm or suicide as a result of cyberbullying or participating in life-threatening online challenges.

4 [http://siteresources.worldbank.org/EXTNWDR2013/Resources/8258024-1352909193861/8936935-1356011448215/8986901-1380046989056/WDR\\_2014\\_Complete\\_Report.pdf](http://siteresources.worldbank.org/EXTNWDR2013/Resources/8258024-1352909193861/8936935-1356011448215/8986901-1380046989056/WDR_2014_Complete_Report.pdf)

investment projects that include elements of cybersecurity. The countries had to be classified based on their income levels for WB to be able to assess the ultimate Program effectiveness, which is the main subject of this Executive Summary.

**The effectiveness of the Program was measured based on the success of its implementation (“Were the planned activities delivered and how?”) and any intermediary outcomes (“Did the beneficiary governments take any steps toward strengthening cybersecurity?”).** The results of both indicators are described under country-specific chapters and also briefly summarized under a separate section.

**Each of the beneficiary countries underwent a Cybersecurity Maturity Model for Nations (CMM) assessment** conducted by the Global Cyber Security Capacity Centre (GCSCC) of Oxford University, which is also the creator of the flagship CMM methodology. Following the CMM exercise and delivery of analytical reports, another strategic partner on the Program—the Global Cyber security Center for Development (GCCD) under Korea Internet and Security Agency (KISA)—delivered a series of **in-country cybersecurity capacity-building workshops**. Finally, a selected set of countries received **country-specific or regional technical assistance** in the form of analytical studies and inputs related to cybersecurity.

The beneficiary governments have leveraged the newly-acquired knowledge and awareness of their cybersecurity capacities to address existing gaps through enhanced policies, legislative mechanisms, and cyber awareness media campaigns, as well as by fine-tuning the implementation of existing public investment projects or by designing new ones. Furthermore, the CMM assessments and workshops helped the countries to build multi-stakeholder cybersecurity coalitions that include the public and private sectors, academia, and the civil society. The safety and security of cyber space cannot be handled by a single individual; increased awareness and coordination on an inter-institutional level is of utmost importance for building trust and triggering the actions required to prevent and mitigate cyber incidents and attacks.

**A number of recommendations were put forward as a result of the Program.** The first recommendation is related to project management. Cybersecurity programs should be implemented by cross-functional teams, both on the financier’s (the World Bank) side and also, ideally, the contractor’s (consultants) side. The nature of the activities, their specific sequencing, and the need for high stakeholder involvement require an agile project management team that should be supported by a solid client-facing team in each beneficiary country. Otherwise, remote coordination may take a toll on the implementation process.

The second recommendation is to use these programs to target the countries in which representatives of governmental institutions are highly committed to cybersecurity donor programs. The Global Cybersecurity Capacity Program has achieved more robust results in the countries in which it was embraced by the counterparts that assumed “ownership” over the Program activities and regarded its deliverables as useful for the policymaking process from the outset.

The third recommendation highlighted in this Executive Summary (more can be found under the “Recommendations” section) is associated with the importance of adopting a regional approach whenever possible. As the Program implementation has shown in the Western Balkans, knowledge exchange is more beneficial when it is not “siloed”. As all Western Balkan countries aspire to become EU member states, similarities can be found in their digital development schemes, especially on the policy side. Therefore, a regional approach to strengthening their systems and institutional capacities through knowledge exchange is both appropriate and encouraged. In some parts of the region, public awareness campaigns could be synchronized in order to take advantage of linguistic and cultural similarities.

**The recommendations presented in this Executive Summary are strategic, as they feed into the follow-up Global Cybersecurity Capacity Program II, which is also financed by the KWPF.** This new Program will target six countries between 2019 and 2021 with a similar set of activities and implementation approach, which has generally proved to be effective and efficient. At the core of this approach is the power of international thought leadership and partnership in cybersecurity analytics, practice-oriented capacity building, and knowledge sharing. It is the hope of the authors of this Executive Summary that the recommendations generated by the Global Cybersecurity Capacity Program will outlive the previous program, thus enriching other similar programs of the World Bank, of other international financial institutions, and of governments themselves.

**The Global Cybersecurity Capacity Program is one of the first steps the World Bank has taken to meet client demand for cybersecurity on the analytical and advisory side.** However, the capacity building and financing needs of developing countries in this new area are growing, in parallel with the speed, scale, and sophistication of cyber incidents. This Executive Report has been prepared on the understanding that the demand for donor assistance in cybersecurity capacity and resilience building will continue. Hence, the knowledge that this Report provides will be of great interest to the Bank’s staff and management, client countries, and the development community at large.



# Introduction

## Global Cybersecurity Capacity Program (2016-2019) overview

---

The Global Cybersecurity Capacity Building Program was designed by the World Bank to assist selected developing countries in strengthening their national cybersecurity environment through customized, technical-assistance programs and/or capacity-building activities. The design of each country's program was based on the internationally-recognized, cybersecurity-capacity gap analysis and priority identification methodology. The grant aimed to directly benefit up to six developing countries and, while doing so, to operationalize the findings of Chapter 4 of the World Development Report 2016 that promotes open, affordable, and safe Internet for all.

The implementation the grant spanned across three of the World Bank's fiscal years: FY17-FY19. Its implementation was structured into four main elements: (i) Identification of the beneficiary countries and program setup; (ii) Gap analysis and identification of cybersecurity priorities, and dissemination of results; (iii) Delivery of capacity building and/or technical assistance based on the results of element 2; and (iv) Activity impact assessment.

In order to deliver the activities envisaged by the grant in the first two areas, WB launched a partnership with the Global Cybersecurity Center for Development of the Korea Internet & Security Agency and Oxford University's Global Cybersecurity Capacity Centre to support the Program. A brief overview of each partner has also been provided. Deloitte-Telecom Strategies Consulting (an implementing partner consortium) was contracted to support WB in implementation of the grant's remaining activities.



Originally Korea Internet & Security Agency (KISA), the subsidiary organization of the South Korean Ministry of Information was established in 1996 to handle all the necessary policies to protect the safe distribution of information. Later, in 2009, KISA merged with NIDA (National Internet Development Agency of Korea) and KIICA (Korea IT International Cooperation Agency). Korea Internet & Security Agency is devoted to “strengthen the competitiveness of Internet and information security industry by developing and spreading intelligent and convergence security technologies as the leading institution of the 4th industrial revolution, leading this trend of change in the times.”



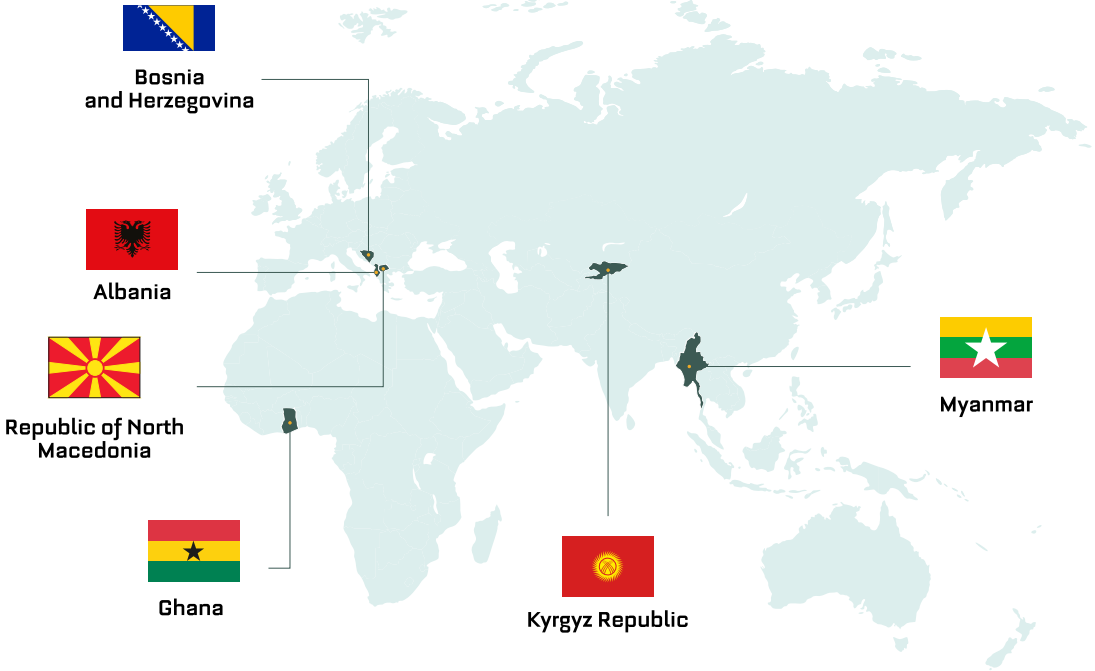
The Global Cybersecurity Center for Development (GCCD) was established in 2015. The main goal of the center is to disseminate practical knowledge and support capacity building in cybersecurity. These efforts help the member states to advance both their cybersecurity capacities and economic growth. The GCCD offers a series of programs, mainly for policymakers and experts in the public sector of developing countries, to build a trusted and secure environment. These programs consist in various topics spanning from policy establishment to technical skills on Internet incident responses. The GCCD is in partnership with the Korean government, universities, and international organizations, such as the World Bank, EBRD, and ENISA.



Oxford University's Global Cybersecurity Capacity Centre (GCSCC) is a leading multidisciplinary research Center focused on efficient and effective cybersecurity capacity building. It promotes an increase in the scale, pace, quality, and impact of cybersecurity capacity-building initiatives across the world. The GCSCC brings together international expertise from various sectors and disciplines to contribute to Center's outputs. It has created the CMM for Nations, a model used to review a country's cybersecurity capacity maturity that is the first of its kind. Through its various activities, the GCSCC aims to assist both governments and the private sector in the self-assessment, benchmarking, adoption and implementation of policies and practices in the area of cybersecurity.

In 2017, Deloitte joined in consortium with the Telecom Strategies Consulting Corp. (TSC) to provide technical assistance for the implementation of the Program.

**Countries in scope**



**Key milestones**



# Global Cybersecurity Capacity Program (2016-2019) major milestones timeline

November 2016 - March 2017	<b>World Bank</b>	Internal processing of the activity, country selection, preparation for the first CMM
April 2017	<b>Kyrgyz Republic</b>	CMM assessment in country review
August 2017	<b>Myanmar</b>	CMM assessment in country review
September 2017	<b>Kyrgyz Republic</b>	CMM Executive summary published (public disclosure)
November 2017	<b>Kyrgyz Republic</b>	GCCD/KISA workshop in Bishkek
January 2018	<b>Ghana</b>	CMM assessment in-country review
January - May 2018	<b>Kyrgyz Republic</b>	Cybersecurity technical assistance
February 2018	<b>Republic of North Macedonia</b>	CMM assessment in-country review
April 2018	<b>Republic of North Macedonia</b>	GCCD/KISA workshop in Skopje
June - September 2018	<b>Republic of North Macedonia</b>	Cybersecurity technical assistance
July 2018	<b>Republic of North Macedonia</b>	CMM report public disclosure
September 2018	<b>Albania</b>	CMM assessment in-country review
September - October 2018	<b>Albania</b>	Regional cybersecurity technical assistance
October 2018	<b>Bosnia and Herzegovina</b>	CMM assessment in-country review

December 2018	<b>Albania</b>
	GCCD/KISA workshop in Tirana
December 2018	<b>Bosnia and Herzegovina</b>
	GCCD/KISA workshop in Sarajevo
December 18-19, 2018	<b>World Bank</b>
	Global Cybersecurity Capacity Program: annual meeting in Washington, D.C.
February 2019	<b>Albania</b>
	CMM Review Report published (public disclosure)
May 2019	<b>Bosnia and Herzegovina</b>
	CMM Review Report disclosed to the public
July 2019	<b>World Bank</b>
	Internal closing of the activity

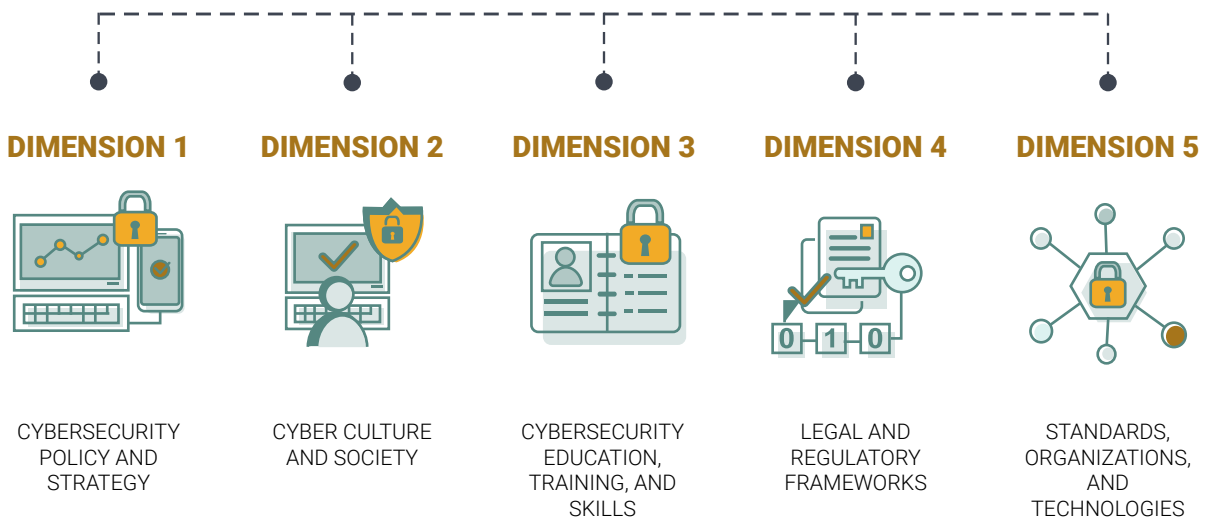
## Methodological approach

The Global Cybersecurity Capacity Centre’s CMM provided an analytical foundation for the Program. During the review process, the main stakeholders from the beneficiary countries were identified and invited to participate in the assessment and subsequent Program activities. As all of the Program’s major activities were built on the key findings and conclusions obtained from the model, it is therefore important to get familiar with its methodology and surrounding processes in order to better understanding of the Program itself.

### *Characterization of cybersecurity capacities*






The aim of the review was to enable the countries to grasp an understanding of their cybersecurity capacity in order to develop national cybersecurity strategies, and to strategically prioritize investments in cybersecurity capacities. The consultations took place using the CMM, which defines five dimensions of cybersecurity capacity as follows:

## DIMENSIONS OF CYBERSECURITY CAPACITY





These five dimensions describe what it means to possess a given cybersecurity capacity. They are broken down into different factors defining different cybersecurity capacities. Each capacity has different indicators, which specify the steps and actions that determine the level of maturity of that aspect.

DIMENSIONS	FACTORS	
<b>Dimension 1</b> 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 defense consideration D1.6 Communications redundancy	
<b>Dimension 2</b> 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 on the Internet D2.4 Reporting mechanisms D2.5 Media and social media	
<b>Dimension 3</b> Cybersecurity education, training, and skills	D3.1 Raising awareness D3.2 Framework for education D3.3 Framework for professional training	
<b>Dimension 4</b> Legal and regulatory frameworks	D4.1 Legal frameworks D4.2 Criminal justice system D4.3 Formal and informal cooperation frameworks to combat cybercrime	
<b>Dimension 5</b> Standards, organizations, 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	

There are five stages of maturity, ranging from the start-up stage to the dynamic stage. The start-up stage employs an ad-hoc approach to capacity, whereas the dynamic stage uses a strategic approach and the ability to adapt dynamically or change in response to environmental considerations.

## **Measuring maturity**

Relevant stakeholders were involved in each country-level CMM assessment. Depending on their background, each stakeholder, or group of stakeholders, was contacted to provide answers related to certain CMM dimensions.

According to the applied methodology, each aspect has a set of indicators consistent with the five stages of maturity. The so called “consensus method” was applied in order to determine the maturity level of each aspect of the CMM and to provide adequate proof of evidence for the stakeholders in connection with every indicator implemented at the country level.

Sessions were divided into focus groups and the researchers used semi-structured questions to keep the discussions on focused on the indicators. Information regarding the cybersecurity aspects falling under a given indicator was collected not only in a form of verbal discussions but also via email following the focus groups. Lack of the necessary evidence for all of the indicators at one stage resulted in a lower level of maturity.

The approach of the focus group mentioned previously allowed for a more comprehensive collection of information compared to other approaches, since a focus-group approach had the advantage of obtaining data, information, and evidence from diverse viewpoints. Contrary to the Q&A session, this approach provided an efficient way of merging the sessions into a valuable discussion among the participants. This research experience enabled relationship building among the participants that resulted in a better understanding of the cybersecurity practices and capacities of a given nation.

In agreement with the stakeholders, all sessions and meetings were recorded and supported with detailed meeting minutes. Data, information, and evidences received from the focus group underwent a content analysis process. This systematic research approach used for qualitative data analysis ensured that the research results were replicable for the purpose of their use.

The country review was followed by an analysis of the information gathered from the discussions with the stakeholders and from the meeting minutes recorded during the sessions. The maturity stages for all CMM factors were determined as a result of this work. A blended approach, premised on the use of inductive and deductive approaches, was used during the analysis of the information collected in the focus group discussions. The source material that was not aligned with the topics was further elaborated to identify additional challenges communicated by the participants or to adapt the recommendations of CMM.

During the preparation of the reports, additional desk searches were required to verify whether the results were valid. Therefore, the information received during the course of the interview process was complemented from additional official sources, such as the websites of government entities and universities, and the publications of international organizations.

Recommendations were formulated for each dimension. These recommendations covered the next steps that the country should take in order to improve its cybersecurity capacity. Findings and connected recommendations were derived from the sessions, meetings, and discussions with and among the stakeholders.

# Key objectives of the Program and Activities

## General aspects

---

From its outset, the Program pursued the following key objectives:



IMPROVE BENEFICIARY COUNTRIES' UNDERSTANDING OF CYBERSECURITY MATURITY STATUS QUO, EXISTING GAPS, AND PRIORITIES AT THE NATIONAL LEVEL.

---



IMPROVE BENEFICIARY COUNTRIES' AWARENESS AND CAPACITY TO IDENTIFY AND ENGAGE WITH RELEVANT STAKEHOLDERS AT THE NATIONAL LEVEL IN THE CONTEXT OF CYBERSECURITY.

---



STRENGTHEN BENEFICIARY COUNTRIES' CAPACITY IN AT LEAST ONE OF THE IDENTIFIED PRIORITIES (GAP) AND BROADEN CLIENT UNDERSTANDING ON HOW TO MOVE AHEAD WITH OTHER PRIORITIES (GAPS).

---



PERFORM A DONOR COORDINATION EFFORT AT THE NATIONAL LEVEL, MAP CYBERSECURITY ACTIVITIES UNDERTAKEN BY DIFFERENT DONORS, AND SECURE SYNERGIES.

---

To reach these objectives, the Program aimed to provide the following types of cybersecurity capacity-building support for each participating country: (a) CMM assessment review and report; (b) GCCD/KISA in-country workshop; and (c) Technical assistance. Close cooperation with GCCD/KISA and GCSCC ensured generally smooth Program delivery in each country.

The beneficiary country selection process was the first important component of the Program. The role of the partners involved in the Program cannot be overestimated. In the first component, a list was identified of beneficiary countries with strong demand for cybersecurity assistance and at least some capacity to design and implement cybersecurity interventions, which defined the setup and management of the entire program. The beneficiary country identification process was performed by taking into account a given set of criteria. These included, among others, the grant's alignment level with the on-going and planned in-country investment programs. A clear priority was given to the countries with existing national investment projects or those with at least prospects of such projects, i.e. countries that could potentially benefit from a wider incorporation of cybersecurity aspects into their national investments. This was deemed important to ensure the developmental impact on cybersecurity, which is characterized by the need of a long-term engagement, with subsequent appropriate financial resources and re-engineering of governance processes.

A considerable part of the first component was dedicated to the proper engagement with Governments and relevant agencies through policy dialogues. This part of work was particularly important, as the further implementation of the Program and the sustainability of its results depended on the governments of participating countries.

The second component included a Gap analysis, in addition to the identification of cybersecurity priorities and the dissemination of results. This Component was delivered by relying on the resources and expertise of GCSCC and GCCD/KISA. By using GCSCC, the Program applied the CMM for Nations to the assessment of the cybersecurity capacity of participating countries, and thus used it to reach objectives (I)-(IV). Throughout the Program's lifetime, GCSCC has performed several reviews and prepared CMM Review reports that were consulted nationally. CMM assessments included focus groups with all of the relevant stakeholders from beneficiary countries, including but not limited to: criminal justice and law enforcement, the defense intelligence community, policy owners, ministers and legislators, CSIRTs and leaders from both the government and the private sector, critical national infrastructure sectors, the international community, academia, civil society, Internet society representatives, etc. The CMM Review reports presented useful evidence of the cybersecurity status quo in beneficiary countries, along with recommendations to assist these nations in determining appropriate policies and investment priorities. In addition, CMM reports provided a good basis for benchmarking different countries from different cybersecurity perspectives. For example, the reports for Albania, BiH, and North Macedonia – all located in the Western Balkan region – allowed these countries and donors to assess their cybersecurity progress from a regional perspective. Publicly disclosed CMM reports were further disseminated to the general public through events (press conferences), press, and other external communication media (e.g. briefs, blogs, and social media posts). The knowledge, expertise, and experience brought by GCCD/KISA as a follow-up to the CMM were particularly valuable for the participating countries. This assistance came in support of objectives (iii) and (iv). Each GCCD/KISA seminar agenda tried to focus on the issue areas identified through the CMM, in order to help participating governments tackle existing cybersecurity capacity weaknesses/gaps.

**“We were glad to be part of this important Program developed by the World Bank. Among other activities, it allowed us to join the ranks of countries that have performed the CMM assessment, which we regard to be of great value not only from the standpoint of generating analytics, but also for building nationwide consensus on cybersecurity status quo and actions. As a result, the CMM report became a guide for us in the process of drafting Albania's new cybersecurity strategy and for other interventions in the cybersecurity field. We are now very much motivated to seize on the opportunities identified by the report, as well as tackle the weaknesses in order to achieve greater levels of cyber capacity to better serve our citizens.”**

Albania: Vilma Tomco, General Director, AKCESK

**“Over the course of several months we have completed a great number of analytical and capacity-building activities in the domain of cybersecurity, and every aspect of cooperation with the World Bank and its partners – the GCSCC and GCCD of KISA – proved to be more than satisfactory. Seizing upon this occasion, we would like to express our gratitude for being included into the Global Cybersecurity Capacity Building Program, as its findings and recommendations will greatly help us in enhancing the cybersecurity capacity of our country for years to come.”**

Bosnia and Herzegovina: Danko Lupi, Senior Associate for Informatization, MOCT

The third component included the Delivery of technical assistance/capacity building is based on the results of component number two. To address modern governmental cybersecurity challenges, technical assistance/capacity building activities have provided consolidated experience in government relations around technological and digital economic challenges, promotion, dissemination, and training of ICT solutions for strategic nation-wide sectors in support of objectives (i)-(iii). The activities were focused on the processes and instruments necessary for successful funding and articulation of national initiatives in the field of cybersecurity. Seasoned cybersecurity experts tailored advice in the form of written reports and face-to-face consultations to selected lead government counterpart institutions in the beneficiary countries. For instance, WB accompanied by TSC & Deloitte held meetings with selected stakeholders, validated the preliminary findings of the CMM review, collected stakeholders’ points of view, as well as national cybersecurity-related ongoing projects, motivations, needs, and concerns, among other aspects. These meetings were aimed at understanding the countries’ assessments and needs in greater depth and at detecting the key gaps and potential improvement areas for their governments in cybersecurity.

The results of the CMM review report were closely supported and complemented by four on-site workshops delivered by GCCD/KISA: in Albania, BiH, Kyrgyz Republic, and North Macedonia. Notably, the GCCD/KISA tailored each workshop to the specific needs of beneficiary countries; the lead government counterparts of these countries were consulted in the process of the workshop preparation. Each workshop featured topics around the cybersecurity gaps/weaknesses/issue areas identified through the CMM assessments with the aim of narrowing down specific capacity gaps, as identified through the CMM. In-country workshops convened various stakeholders from the government, academia, the private sector, and civil society, typically those who had participated in the CMM review process. As part of these workshops, CMM key findings and conclusions were also disseminated.

The fourth component included an Impact assessment of the activity. The aim was to assess the overall implementation of the grant and its early impact, as well as arrive at a set of conclusions regarding the activities’ potential for replication and scale-up under WB activities in developing countries.

The key findings and conclusions of the impact assessment were validated with select lead government counterparts from beneficiary countries and grant Program partners during a dissemination event in Washington, D.C. in December 2018.

The World Bank’s approach to the overall Program, based on multiple deliverables and several avenues for providing support to beneficiary governments (e.g. analytical, knowledge sharing, and capacity building), ensured a high degree of adaptability and flexibility, when it came to establishing the exact mode of cooperation, depending on the operating environment. Also, such a comprehensive approach enabled WB to tailor and focus the required support to the current needs of participating countries. In addition, it has been concluded that the involvement of international cybersecurity expertise was a major contribution alone to the success of this Program.





The Kyrgyz Republic, a multi-ethnic population of some 6.1 million people, is located in Central Asia. Despite the recent economic tremors affecting the region, the country’s economy showed resilience. However, its GDP per capita (\$1,130 in 2017) remained low. In order to transform into a digital economy, the Kyrgyz Republic requires significant investments, as well as policy and regulatory reforms. Its Internet penetration is still in the early stages. Also, e-government services available to citizens are limited and e-commerce development is at a preliminary phase. The situation is mostly driven by the high costs of international Internet access in this landlocked and largely mountainous country.<sup>5</sup>

In order to achieve more affordable Internet access, by crowding in private investments in the ICT sector and improving the public sector’s capacity to deliver digital government services, the Government of the Kyrgyz Republic has engaged in the Digital Central Asia and South Asia (Digital CASA) Project financed by the World Bank. In parallel, through the State Committee on Information Technology and Communications of the Kyrgyz Republic (SCITC), the Government became a beneficiary under the Global Cybersecurity Capacity Building Program, in order to strengthen its capacity to enable secure transformation of the country into a Central Asian digital hub.

To impulse ICT development in the Kyrgyz Republic, the State Committee on Information Technology and Communications of the Kyrgyz Republic (SCITC) was established in mid-2016. This entity is responsible for improving national cybersecurity capacities, among other things.

The Global Cybersecurity Capacity Building Program kicked off with the CMM assessment. The CMM in-country assessment review was conducted during 4-6 April 2017, with the [Executive summary published in September 2017](#). Stakeholders representing the following sectors participated in the consultations to review the Kyrgyz Republic’s cybersecurity capacity:

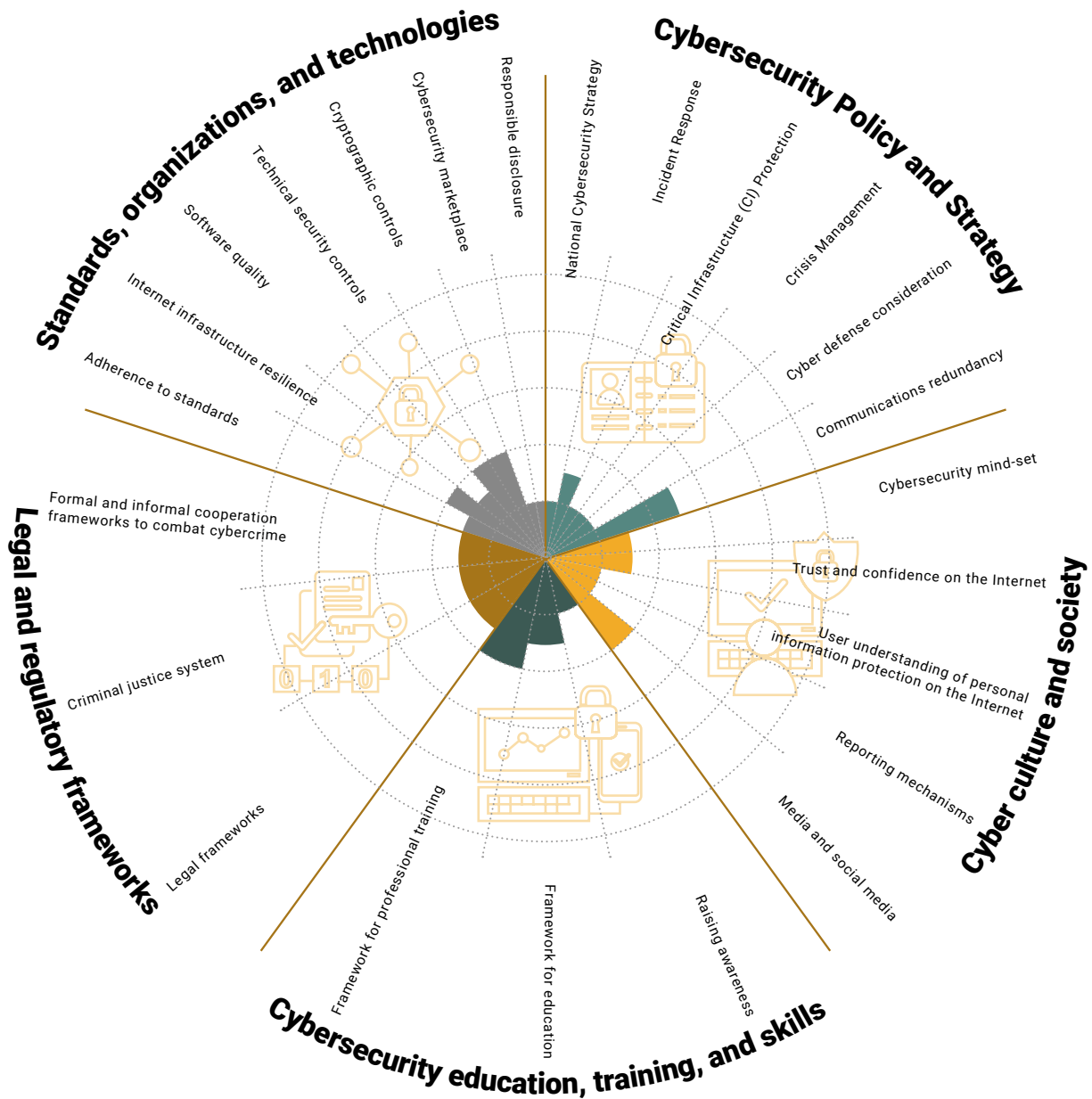
### Public sector entities:

- State Committee on Information Technology and Communications of the Kyrgyz Republic
- State Committee for National Security of the Kyrgyz Republic
- State Committee for Defense Affairs of the Kyrgyz Republic
- National Statistical Committee of the Kyrgyz Republic
- Ministry of Education and Science of the Kyrgyz Republic
- Ministry of Internal Affairs of the Kyrgyz Republic
- Ministry of Finance of the Kyrgyz Republic
- Ministry of Foreign Affairs of the Kyrgyz Republic
- Ministry of Justice of the Kyrgyz Republic
- Ministry of Health of the Kyrgyz Republic
- Ministry of Transport and Roads of the Kyrgyz Republic
- Centre for Standardisation and Metrology under the Ministry of Economy of the Kyrgyz Republic
- State Service for Combating Economic Crimes under the Government of the Kyrgyz Republic
- State Financial Intelligence Service under the Government of the Kyrgyz Republic
- State Registration Service under the Government of the Kyrgyz Republic
- State Customs Service under the Government of the Kyrgyz Republic
- State Tax Service of the Kyrgyz Republic
- Local government representatives

5 <http://documents.worldbank.org/curated/en/233891521770539859/pdf/Kyrgyz-Digital-PAD-03012018.pdf>

- Criminal justice sector
- Defense sector
- Private sector
- Telecommunications companies
- Finance sector
- Academia
- Civil society organizations
- International organizations and embassies

# OVERALL REPRESENTATION OF THE CYBERSECURITY CAPACITY IN THE KYRGYZ REPUBLIC



According to the finalized CMM Review Report, the following key findings were identified across the five dimensions of cybersecurity capacity:

### **Cybersecurity policy and strategy**



- Missing official national cybersecurity strategy framework.
- No national IT-incident response organization.
- The concept of cybersecurity in critical infrastructures (CI) was still in the early stages.
- Cyber defense was not yet a priority in the national cybersecurity posture, with no cyber defense strategy or dedicated unit.

### **Cyber culture and society**



- Cybersecurity has not yet become a priority across the public and private sectors.
- In contrast to the development of e-government services, the national e-commerce sector was still in the early stages.
- An understanding of how to protect personal information online was at the initial stage of development.
- The role of mass media and social media in cybersecurity reporting and raising awareness was ad-hoc.

### **Cybersecurity education, training, and skills**



- A general lack of cybersecurity awareness in the Kyrgyz Republic was acknowledged across the various stakeholder discussions.
- Both in the public and private sectors, cybersecurity awareness was very limited among executive managers.
- The development of cybersecurity educational initiatives was still in the early stages.
- Training courses were provided in a largely uncoordinated manner by different organizations and vary in depth and coverage, leading to a gap between the supply and demand of cybersecurity training programs.

### **Legal and regulatory frameworks**



- The development of a legal framework to regulate the full scope of cybersecurity and cybercrime was in the early stages.
- The protection of children using the Internet was not yet addressed in legislation.
- Existing cybersecurity related legislation was not yet sufficiently enforced due to a lack of legislation and dedicated enforcement authorities.
- Across the criminal justice system there were no regular training courses for law enforcement officers, financial and human resources were insufficient, and specialized knowledge was not yet developed.
- The need to establish informal and formal cooperation mechanisms, both domestically and across borders, has not yet been widely-recognized.

### **Standards, organizations, and technologies**



- Standards regulating cybersecurity and information security were in the preliminary stages.
- Internet penetration was fairly limited, especially in rural areas.
- Internet downtime and interruptions, often caused by power outages, were frequent.
- No inventory of software used in the public and private sectors.
- No catalog of secure software.
- The adoption of technical security controls varied across different sectors and organizations.
- No mechanisms in place to assess the effectiveness of security controls.
- No market for cybersecurity technologies and cybercrime insurance products.
- No responsible disclosure policy or framework in the public or private sectors.
- No information on detected issues and vulnerabilities was shared formally between organizations, either within or across sectors.

The World Bank has facilitated, in cooperation with the SCITC and the Global Cybersecurity Center for Development (GCCD) of Korea Internet & Security Agency (KISA), the GCCD-the Kyrgyzstan Cybersecurity CMM Seminar in Bishkek on 29-30 November 2017. The following topics were covered by GCCD/KISA, selected in coordination with SCITC and the World Bank:

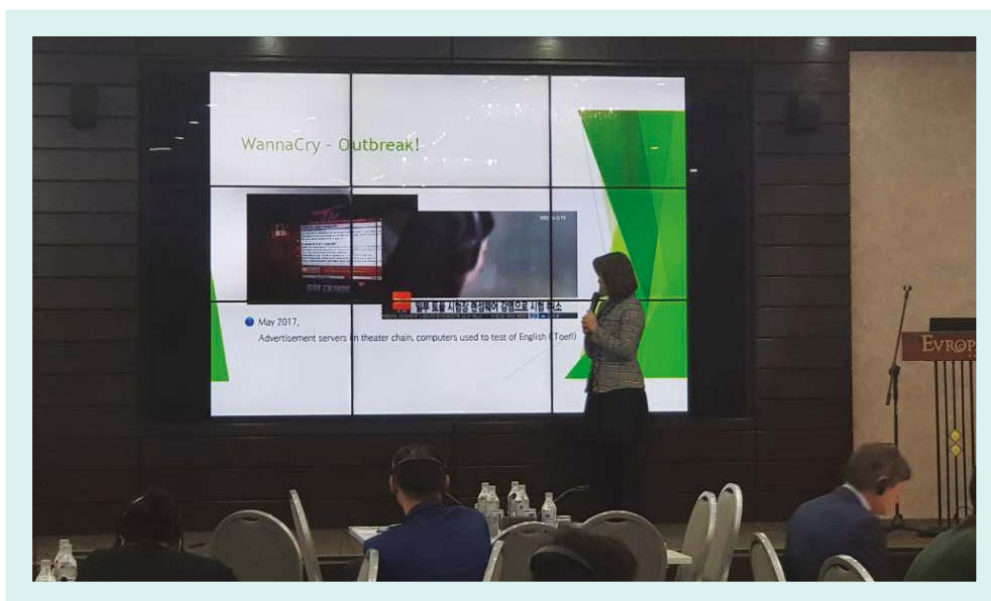
- “Introduction of KISA & Global cooperation” by Ms. You Jin Moon, Researcher, International Intelligence Team, Korea Internet & Security Center, KISA
- “Cybersecurity Framework in Republic of Korea (ROK)” by Mr. Kwang Jin Park, Chief Researcher, Cybersecurity Planning Team, Korea Internet & Security Center, KISA
- “KrCERT/CC Operation and Activities” by Mr. Sangwon Han, Researcher, Detection Team 1, Korea Internet & Security Center, KISA
- “Cyber Incident Trend in Republic of Korea (ROK)” by Mr. Ahn Changyong, Principal Researcher, ASEC Response team, Ahnlab
- “Global Cyber Threats Analysis” by Ms. Song Jihwon, Deputy general researcher, Analysis team 1, Korea Internet & Security Center, KISA
- “E-government Security” by Mr. Cho Eun-Lae, General Researcher, Public information Security Team, Korea Internet & Security Center, KISA

### Photos from the GCCD-the Kyrgyz Republic Cybersecurity CMM Seminar



From left to right: **Mr. Uran Esengeldiev** (ICT Consultant, the World Bank), **Ms. YouJin Moon** (Researcher, KISA), **Mr. Mirlan Omuraliev** (Deputy Chairman of SCITC), **Mr. Kwangjin Park** (Chief Researcher, KISA), **Mr. Kim** (seconded from Korea Information Society Development Institute (KISDI) to SCITC), **Ms. Junok Lim** (Researcher, GCCD/KISA)

Photo credit: KISA



**Ms. Jihwon Song** (Deputy general researcher, KISA)

Photo credit: KISA

The GCCD/KISA seminar provided an opportunity to disseminate and discuss the results of the CMM analysis. The event participants representing 40 different institutions, including the government, the private sector, academia, and donors, received an overview of the CMM report. In addition, the Korean delegation shared details of the cybersecurity framework and e-government security implemented in ROK, the operations of the country's incident response and security teams, global cyber incident trends, and cyber incidents in the finance sector.

#### 2017 GCCD-Kyrgyz Republic Cybersecurity CMM Seminar banner



Further Program activities in the Kyrgyz Republic included technical assistance revolving around three key components of the Digital CASA-Kyrgyz Republic Project (Digital Connectivity Infrastructure, Digital Platforms and Smart Solutions, and Enabling Environment for Digital Economy). These components could be briefly summarized through their key objectives:

- **Digital connectivity infrastructure:** improving regional connectivity by increasing the security capacity and reach of the government network (G-Net).
- **Digital platforms and smart solutions:** Eurasia cloud regional data center and G-Cloud, digital platforms, and shared services and smart solutions.
- **Enabling environment for a digital economy:** legal, regulatory, and institutional foundations for a digital economy, partnerships for digital leadership and strategic communications, ICT skills development, and digital innovations.

The technical assistance teams provided expert support on fundamental questions derived from the development of the Digital CASA-Kyrgyz Republic Project and the results of the CMM output. The following topics were agreed upon with the local stakeholders as priority in the context of this work:

1. Relevant CSIRT/CERT capability models.
2. Relevant SOC models and capabilities.
3. Threat modeling and threat landscape strategies.
4. Cloud on-boarding and security validation.
5. Protection of national critical infrastructures.
6. National cyber laboratory (CyberLab).
7. Third-party collaboration models.
8. Cybersecurity education program models.



They took part in a two-day, on-site mission in Bishkek on 25-26 April 2018. Experts held a series of meetings with the representatives from the Digital CASA-Kyrgyz Republic project's the Project Implementation Unit (PIU) and SCITC. The following topics were covered during the work sessions with the stakeholders:

## DAY 1

Ongoing and planned cyber components of the Digital CASA-Kyrgyz Republic project.

Work session on CSIRT/CERT and SOC capability models.

Some aspects of threat landscape and risk management processes.

On this day, Digital CASA project components were discussed in detail with the stakeholders from the SCITC. Deloitte presented applicable strategies, organizational CSIRT/CERT and SOC models, and their authority models and capabilities, along with a general planning approach with relevant milestones to steer the discussion.

## DAY 2

Work session on third-party collaboration models and strategies.

Work session on threat modeling, threat landscape strategies, and protection of national critical infrastructures.

Closing session: a wrap-up of the topics presented during the previous two days, additional topics, and later actions were discussed with the stakeholders from the SCITC and PIU.

On this day, information sharing and collaboration models, applicable risk management frameworks, threat taxonomies, and critical infrastructure protection considerations were presented and discussed with the stakeholders.

The consultancy output in relation to this in-country model was compiled into a document addressing the questions described earlier. The goal of this approach was to provide an initial alignment with CMM recommendations, introduce cybersecurity-related tasks for Digital CASA-Kyrgyz Republic Project component development, and provide general guidelines on relevant practices and standards.

As part of the delivery of the Kyrgyz Republic's technical assistance, additional supporting information and documentation have been shared with the local stakeholders following the mission at the request of SCITC and PIU.

The final package of in-country assistance consisted of:

### Relevant CSIRT/CERT capability models

The role and the purpose of a national computer emergency response team or a computer security incident response team (CSIRT) were explained, including an initial framework for a CSIRT establishment roadmap, based on the recommended industry practices and notes from prominent cybersecurity agencies. The importance of the establishment of clear and well-defined project goals and a dedicated support plan were presented, including a process plan for the establishment of a Governmental/National CSIRT capability. In addition, the document provided a general description of the more common authority models, outlined the required staff, their general skill-set, and a clear definition of their responsibilities and tasks within the organization required for CSIRT operations. In addition, the taxonomic organization of typical service categories provided by a CSIRT were discussed.

## **Relevant SOC models and capabilities**

The organizational and functional models of a security operations Center (SOC) were presented. Different authorization models required for a SOC to regulate a specific constituency were also described. Six SOC models offering different capabilities were presented, alongside a summary of typical capability offerings for each of the aggregated SOC models. The definition of the required staff roles, responsibilities, and base-skillset profiles, including the duties recommended for a typical SOC, were discussed with the on-site mission participants. TSC & Deloitte emphasized core technologies of a successful SOC, such as data collection, correlation, monitoring and real-time analysis, and the importance of having the right combination of these elements.

## **Threat modeling and threat landscape strategies**

Understanding the associated threats and risks of cybersecurity-related initiatives is critically important for the Digital CASA-Kyrgyz Republic Project. The technical assistance provided SCITC and PIU with a guideline to support decisions around risk-related inputs and a knowledge base for risk assessment and management methodologies and processes. The importance of the threat classification taxonomy was emphasized, i.e. the use of a strong foundation in the form of definitions and classification schemes. An overview and a short comparison analysis between the most relevant methodologies available was provided. In addition, examples of risk case evaluations were discussed, including threats, optical links, and backbone infrastructures.

## **Protection of national critical infrastructures**

Protection of critical infrastructure means ensuring that assets, systems and services vital to the country and its society continue to function as required. Key functions and related categories that describe specific cybersecurity activities that are common across all critical infrastructure sectors were presented to Kyrgyz stakeholders. As part of this, attributes of a typical a critical infrastructure inventory were discussed. As requested by the mission participants, the key aspects of the reporting process of an appropriately designed and maintained inventory were summarized. In order to combat the threats and risks connected to each element of the critical infrastructure, the importance of defining and implementing measures to aid infrastructure protection was described. The design and implementation of a protection framework at the country and industry level was also emphasized. Furthermore, the documentation listed the profiles for the governance of critical infrastructure protection depending on the needs, requirements, and current structures in a given country.

## **Third-party collaboration models**

The importance of effective information sharing for organizations in the public and private sectors was discussed with the stakeholders. As part of the this collaboration, various members of the process usually exchange information about threats, incidents, vulnerabilities, mitigating measures, situational awareness, strategic analysis, best practices, and tools. Technical assistance teams briefly described a system applied for evaluating the reliability and credibility of the both the information and items collected. The experts similarly presented a simple and intuitive schema for indicating when and how sensitive information can be shared, by facilitating a more frequent and effective collaboration. They also focused on cyber information-sharing approaches that can be applied to enable participants to develop tailored strategies for layering defenses across different steps of the kill-chain. Collaboration models were provided – Public Private Partnerships (PPP) and Information Sharing and Analysis Centers (ISAC) – to enhance cybersecurity at all different levels, i.e. information on threat sharing and awareness raising. Finally, the experts provided a list of challenges and recommendations that can be considered during the establishment of the presented collaboration models.

## CSA-CCM and CSA-STAR certification framework

The Cloud Controls Matrix (CCM) and the Consensus Assessments Initiative Questionnaire (CAIQ) of the Cloud Security Alliance (CSA) are the two documents that are most often used by companies to assess a cloud provider's controls and risk model, and it is a good starting point to determine which controls it needs from its cloud provider. The Security, Trust and Assurance Registry (STAR) was therefore presented to Kyrgyz stakeholders, along with a brief overview of the CSA Consensus Assessments Initiative Questionnaire (CSA-CAIQ) and the CSA Cloud Controls Matrix (CSA-CCM). Requirements and the three levels of assurance of the STAR Certification framework were discussed, as well.

## National Cybersecurity Strategy

The purpose and the need for a National Cybersecurity Strategy in order to maintain the security and resilience of national infrastructures and services was presented to local stakeholders. The experts also provided an overview of a general life cycle for strategy development and listed a set of concrete actions for a typical approach for developing, executing, and maintaining a national cybersecurity strategy. Key consideration points for the SCITC, together with the list of recommendations of the short analysis of the current status of cybersecurity strategies within the European Union (EU) and selected non-European countries conducted by ENISA, were enumerated separately.

## Applicability of the OWASP ASVS and Legal Project to COTS software evaluation

The operations and use of secure and reliable applications that meet the needs and requirements of an organization are key to cybersecurity. It is also vital that security features of commercially available, off-the-shelf (COTS) software meet the standards and requirements set by the SCITC and PIU. Therefore, the experts summarized for the Kyrgyz stakeholders the importance of an adequately documented procurement and testing of commercially available COTS software. Open Web Application Security Project (OWASP) is an open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted. OWASP Application Security Verification Standard (ASVS) provides a basis for testing application technical security controls, as well as any technical security controls in the environment, that are relied on to protect against vulnerabilities. The Application Security Verification Standard's three security verification levels were thus discussed in detail. The OWASP Legal Project supplementing the OWASP ASVS was also thoroughly covered. The Secure Software Development Contract Annex provided an initial overview on the different types of requirements or aspects that could be considered during software procurement or when outsourcing negotiations.

It is important to note that each section of the consulting package concluded with additional relevant references and resources so that SCITC and PIU could further independently research the topics of their interest.

Finally, the World Bank commissioned a [cybersecurity awareness video](#) targeting the general public to help spread information on the scope of the assistance provided to the Kyrgyz Republic throughout the Program.

## **Impact of the Kyrgyz Republic's participation in the Global Cybersecurity Capacity Building Program**

The objective of the Kyrgyz work program was to enable the country to gain an understanding of its cybersecurity capacity, form a well-known roadmap for further actions – specifically under the Digital CASA-Kyrgyz Republic Project – and by doing so, increase cybersecurity financing. As a result, specific steps were proposed to the Government, the main of which include: the development of a comprehensive legal and regulatory framework, a national cybersecurity strategy, and a national Computer Security Incident Response Team (CSIRT).

Following the implementation of the Global Cybersecurity Capacity Building Program in the Kyrgyz Republic, the Security Council of the Kyrgyz Republic issued a document “On measures for digital development of the Kyrgyz Republic”, which was signed by the President of the Kyrgyz Republic on 18 December 2018. This document outlined a list of measures to be undertaken by the country in the field of cybersecurity:

**“...by February 1, 2019, finalize and adopt the Cybersecurity Strategy of the Kyrgyz Republic, defining the approaches and vision for the implementation of the following issues:**

- **creation of clearly demarcated organizational structures, such as computer incident response teams to ensure the cybersecurity of banking, telecommunications and other service infrastructures, monitoring and response centers to cyber threats;**
- **formation of a legal and methodological basis for countering computer crimes;**
- **formation of a national information security system, including a cryptographic security system;**
- **formation of a security system for the critical information infrastructure of the Kyrgyz Republic, cybersecurity of state structures and organizations of the non-state sector;**
- **technical standardization and international cooperation in the field of cybersecurity;**
- **building, and strengthening human capabilities in the field of cybersecurity.”**

The Government of the Kyrgyz Republic is now working towards implementing the measures mentioned earlier, including through the implementation of the Digital CASA-Kyrgyz Republic Project, effective since January 2019.



Myanmar is the largest country in mainland Southeast Asia. Despite its abundant natural resources and strategic location between India, China, and Thailand, Myanmar remains one of the least developed countries in Asia, with a population of 53 million and GDP (per capita) of US\$1,190 (2017). In 2011, Myanmar embarked on a momentous transition: from a planned economy to an open-market economy. One of the main drivers of the country's reform agenda since then has been the development of ICT infrastructures. Along with it, the Government started to pay attention to cybersecurity mainstreaming.<sup>6</sup>

The World Bank Group is working with both the government and the local authorities on several projects to help develop and implement country-level strategies. Some of these programs are targeting ICT-related investments. For example, the World Bank's pipeline Digital Myanmar Project (P167978) pursues the following objectives: (i) increase integration and efficiency of digital investments for targeted public sector agencies using a shared digital government platform, and (ii) increase availability and transparency of selected digital services for Myanmar people, businesses and government employees. The Global Cybersecurity Capacity Building Program supported the scoping of cybersecurity activities for this important Project through the CMM assessment.



Ministry of Transport and Communications, is in charge of ICT/Digital Development in Myanmar. The department of Information Technology and Cyber Security (ITCSD) is responsible for national cyber security.

The CMM in-country assessment review was conducted in Myanmar during 29-31 August 2017. The CMM review was conducted by the GCSCC in cooperation with the World Bank. At the same time, for this CMM the GCSCC received additional support from the Norwegian Institute of International Affairs (NUPI) as part of its project "Cybersecurity capacity building 2.0 - Bridging the digital divide and strengthening sustainable development through cybersecurity capacity building". The assessment was hosted by the Ministry of Transport and Communications (MOTC). Stakeholders representing the following institutions participated in the consultations to review Myanmar's cybersecurity capacity:

#### Public sector entities:

- Central Bank of Myanmar
- IT and Cybersecurity Department of the MOTC
- Ministry of Border Affairs
- Ministry of Commerce
- Ministry of Transport and Communications
- Ministry of Construction
- Ministry of Defence
- Ministry of Education
- Ministry of Electricity and Energy
- Ministry of Foreign Affairs
- Ministry of Health and Sports
- Ministry of Home Affairs
- Ministry of Industry
- Ministry of Information
- Ministry of Labor, Immigration and Population

<sup>6</sup> <http://documents.worldbank.org/curated/en/393851542862936421/pdf/Concept-Project-Information-Documents-Integrated-Safeguards-Data-Sheet-MM-Digital-Myanmar-Project-P167978.pdf>



- Ministry of Planning and Finance
- Myanmar Computer Emergency Response Team (mmCERT)
- Pyithu Hluttaw Transportation, Communications and Construction Committee (Lower House of Parliament)
- Legal Affairs and Special Cases Assessment Commission

#### Criminal justice sector:

- Myanmar Police Force
- Cybercrime Division of the Criminal Investigation Department
- Inspector General of the Myanmar Police Force
- Union Attorney General's Office
- Union Supreme Court
- Rule of Law Centers

#### Technology and telecommunications sector:

- US ICT Council, MPT – KDDI, Telenor, Ooredoo, MyTel, Yatanarpon Teleport, Third Eye, and Myanmar Survey Research.

#### Finance sector:

- Myanmar Payment Union, Myanmar Economic Bank, Myanmar Foreign Trade Bank, Myanmar Investment and Commercial Bank, and Commercial Private Banks (KBZ, AYA, CB Bank, MAB, AGD).

Critical infrastructure owners, including hospitals, transportation, electricity, and water.

#### Academia:

- University of Computer Studies (Yangon), University of Information Technology (Yangon), University of Computer Studies (Mandalay), University of Technology (Yatanarpon Cyber City), and Myanmar Institute of Information Technology (Mandalay).

#### Professional societies:

- Union of Myanmar Federation of Chambers of Commerce and Industry, Myanmar Computer Federation, Myanmar Computer Professional Association, and Myanmar Computer Industrial Association.

#### Non-governmental organizations (NGOs) and the international community:

- World Food Programme, Japan International Cooperation Agency (JICA), Myanmar ICT for Development Organization (MIDO), and Myanmar Centre for Responsible Business.

#### Photos from the CMM assessment in Myanmar



Representatives from the Government of Myanmar, GCSCC, World Bank, and NUPI

Photo credit: WBG

# OVERALL REPRESENTATION OF THE CYBERSECURITY CAPACITY IN MYANMAR





**MOTC, GCSCC, World Bank and other CMM participants**

Photo credit: WBG

The CMM Review Report was finalized and accepted by the lead government counterpart – the Ministry of Transport and Communications (MOTC). When this document was drafted, the report was not yet published. According to the finalized Report, the following key findings were identified across the five dimensions of cybersecurity capacity at the time of the assessment.

### **Cybersecurity policy and strategy**



- Missing official national cybersecurity strategy document.
- The majority of the public departments did not have a cybersecurity unit and there was no uniform set of policies across all departments.
- Critical infrastructures, as a term, were not understood and a national risk assessment had never been executed.
- No list of CI stakeholders nor mandatory security controls to adhere to.
- No cyber defense strategy in place.

### **Cyber culture and society**



- Cybersecurity has not yet become a priority for the public and private sectors or for end-users.
- General lack of awareness of the risks and threats in cyberspace at all governmental levels.
- Generally, cybersecurity capacities in the private sector (with the exception of the major domestic and international telecommunications providers and international ICT companies) were weak.
- Internet users generally had minimal levels of awareness of cybersecurity risks and safe online practices.
- Internet users were not aware of the vulnerabilities women and children face online.
- Public trust in e-government services was limited.
- E-commerce services were only offered on a minimal scale.
- Levels of awareness of personal information protection and personal data security were low.
- No central dedicated reporting framework to enable users to report on computer-related or online incidents and crimes.
- Both traditional and online mass media, were incorrectly reporting about cyber threats in an insufficient manner.

### **Cybersecurity education, training, and skills**



- Lack of political commitment to implement practical and pragmatic awareness-raising efforts and initiatives was therefore ad-hoc and uncoordinated.
- Cybersecurity awareness-raising was not yet perceived to be a priority, there were no efforts to raise the awareness of cybersecurity among executive staff in any sector
- Cybersecurity was not part of the national school curriculum
- Professional training in cybersecurity was offered in an ad-hoc manner and not at a national level
- Knowledge transfer from IT staff to other personnel was occasional and not systematic.

## Legal and regulatory frameworks



- No adequate legislation regarding ICT security.
- No specific legislation on digital rights.
- No data protection legislation.
- Protection of internet use by children was rudimentary.
- No provisions in the legislation for protecting consumers online.
- General intellectual-property legislation in place was outdated and not applicable to online content
- Criminal procedural law did not specify investigative powers for law enforcement in cybercrime cases.
- Across the criminal-justice system, the capacity was limited due to the lack of experts, budget, and technical equipment needed to tackle cybercrime cases.
- The capacity of prosecutors to handle cybercrime cases and cases involving digital evidence was considered limited by the stakeholders.
- The ability of courts to handle cybercrime cases was perceived as low, with no specialized training available to judges.
- Both domestically and abroad, informal and formal cooperation mechanisms were ad-hoc and only in the initial stages.
- Despite the formal cooperation mechanisms, cooperation between the police and ISPs was challenging.

## Standards, organizations, and technologies



- No uniform set of standards and policies in the public sector.
- Lack of any centralized institution responsible for the implementation of standards and the execution of audits.
- No mandatory controls for critical infrastructure stakeholders.
- No controls on the specification and implementation of procurement and software development standards.
- Investments focused mainly on the mobile market, whereas fixed broadband and network infrastructures were neglected.
- There were occasions in which Government allegedly shut down mobile and fixed Internet connections without a clear legislation in place.
- An inventory of software used in the public and private sectors, as well as a catalog of secure software is absent.
- The quality and performance of the deployed software was a major issue due to the fact that pirated versions of software are frequently used and installed throughout the public sector. This is becoming increasingly common in the private sector as well.
- The effective monitoring and quality assessment of software was conducted ad-hoc only in a few private institutions.
- There were no mechanisms in place to assess the effectiveness of technical security controls.
- The use of pirated software and unofficial media for sharing sensitive data rendered the existing limited controls ineffective in the newly constructed network and data centers throughout the public sector.
- In the public sector, the transmission of data – stored in data centers in encrypted format – was not encrypted.
- No market for cybersecurity technologies and cybercrime insurance products.
- No responsible disclosure policy or framework in the public or private sectors.
- The reporting mechanism in place in the public sector was not used.
- No formal sharing of threat intelligence information with other institutions, either within the same sector or across different sectors.

Due to operating environment constraints at the time of Program implementation, Myanmar could not fully benefit from the full package of technical assistance, initially included in the Program<sup>7</sup>. Thus, no further activities were undertaken in the country.

<sup>7</sup> It should be noted that Myanmar is the only country in the Program reflected on the harmonized list of fragile situations in FY17-FY19: <http://www.worldbank.org/en/topic/fragilityconflictviolence/brief/harmonized-list-of-fragile-situations>



Ghana is one of the fastest-growing economies in West Africa, with a GDP (per capita) of US\$1,880 (2017) and a population of 26.9 million. This economic growth created demand for wider availability and adoption of ICTs. The World Bank and the Government of Ghana are working together to help meet this demand. To this end, one of the joint projects is the eTransform Ghana Project (P144140). Its main objective is to improve the efficiency and coverage of government service delivery using ICT.<sup>8</sup>



The Ministry of Communications (MoC) of Ghana aims to shift the transition of Ghana to a knowledge-based society through the mainstreaming of ICT. MoC has the responsibility of developing and implementing national policies and ICT infrastructures, in order to achieve a cost-effective system for growth. The economic competitiveness and knowledge-based environment for Ghana could not come without laying down the foundation of an information security strategy.

The Global Cybersecurity Capacity Building Program supported the eTransform Ghana Project implementation. As part of this Program, the CMM in-country assessment review was conducted during 15-17 January 2018. The cybersecurity capacity review was conducted by the GCSCC, in cooperation with the World Bank. In addition, for this CMM the GCSCC received additional support from the Norwegian Institute of International Affairs (NUPI). The review was hosted by the MoC, with representatives of the U.S. Department of State and the MITRE Corporation participating in the review as observers. Stakeholders representing the following institutions participated in the consultations to review cybersecurity capacity in Ghana:

#### Public sector entities:

- Data Protection Commission
- Africa Cert
- Bank of Ghana
- GC Net
- Ghana Armed Forces
- Ghana National Petroleum Corporation
- Ghana Railway Development Authority
- Ministry of Communications (MoC)
- Ministry of Defense
- Ministry of Education
- Ministry of Environment, Science and Technology
- Ministry of Finance
- Ministry of Foreign Affairs
- Ministry of Gender, Children and Social Protection
- Ministry of Health
- Ministry of Information
- Ministry of Interior
- Ministry of Justice
- Ministry of Transport
- Attorney General's Department
- National Communications Authority (NCA)
- National Identification Authority
- National Information Technology Agency (NITA)

8 <https://www.worldbank.org/en/country/ghana/overview#1>

#### Criminal justice sector:

- Bureau of National Investigations
- Criminal Investigations Department
- Economic and Organized Crime Office
- Financial Intelligence Centre
- Judicial Service
- National Security
- Research Department

#### Technology and telecommunications sector:

- Vodafone Ghana
- AirtelTigo Ghana
- Busy Internet Ghana

#### Finance sector:

- Barclays Bank
- Cal Bank
- Ecobank
- Fidelity Bank Ghana Limited
- Ghana Commercial Bank
- Omni Bank

#### Critical Infrastructure owners:

- Agricultural Development Bank
- Driver and Vehicle Licensing Authority
- Electricity Company of Ghana
- Ghana Interbank Payment and Settlement Systems
- Ghana Internet Exchange
- Ghana Maritime Authority
- Ghana Post
- Ghana Water Company Limited
- GRIDCO
- Ministry of Aviation
- Ministry of Health
- Ministry of Transport
- National Communications Authority
- National Health Insurance Authority
- National Information Technology Agency
- National Investment Bank
- National Road Safety Commission
- Volta River Authority
- Zipnet

#### Academia:

- Accra Technical University
- Ashesi University
- Central University College
- Ghana Technology University College
- KNUST
- Legon Centre for International Affairs (LECIAD)
- University of Cape Coast
- University of Development Studies
- University of Ghana



#### Professional societies:

- Ghana Telecoms Chamber

#### Private Sector

- Association of Ghana Industries
- Deloitte
- e-Crime Bureau
- Enterprise Group
- e-Transact
- GC Net
- Ghana National Chamber of Commerce
- GHASALC
- Google
- IBM Ghana Limited
- Innovare
- ISACA
- KPMG
- Margins Id
- Microsoft
- Newmont Gold
- Tonaton
- Tullow Oil
- Vodacom Ghana Ltd

#### Non-governmental organizations (NGOs) and international community:

- Adventist Development and Relieve Agency
- British High Commission
- Internet Society Ghana Chapter
- J Initiative
- Media Foundation for West Africa
- Plan International Ghana
- US Embassy
- World Vision Ghana

#### Photos from the CMM assessment in Ghana

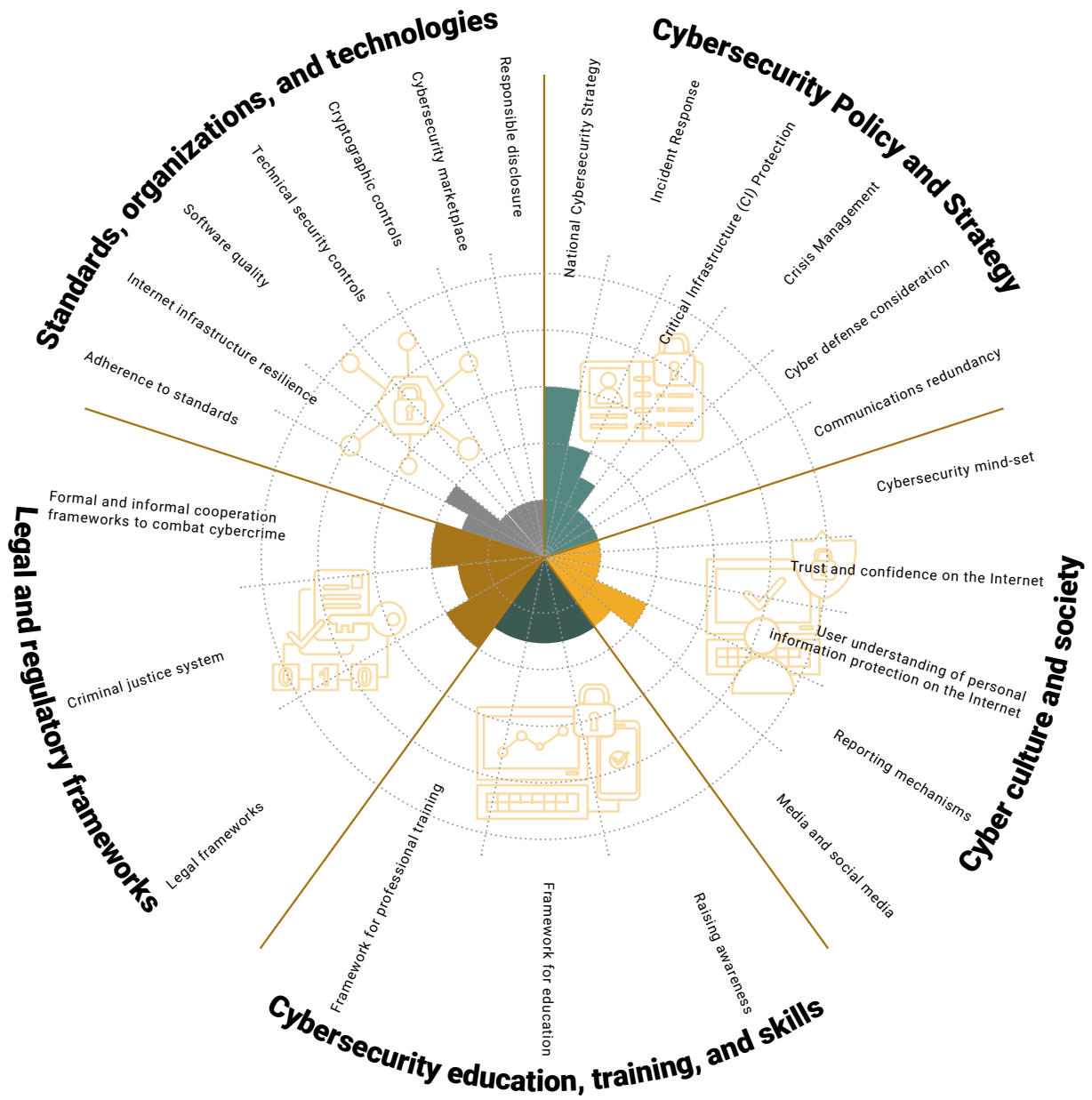


Honourable Minister for Communications **Ursula Owusu-Ekufu**, Deputy Minister **Vincent Sowah Odotei**, and other representatives from Ghanaian government institutions, together with representatives from the World Bank, GCSCC, US Department of State, and MITRE.

Photo credit: GCSCC



# OVERALL REPRESENTATION OF THE CYBERSECURITY CAPACITY IN GHANA





During the focus group break at the CMM assessment review in Ghana.

Photo credit: GCSCC

The CMM Review Report was finalized and disseminated. When this document was drafted, the report was not yet published. According to the finalized CMM Review Report, the following key findings were identified across the five dimensions of cybersecurity capacity at the time of the assessment.

### **Cybersecurity policy and strategy**



- The implementation of the National Cybersecurity Policy and Strategy is at a very early stage.
- More frequent consultations with stakeholders and dedicated budgets for cybersecurity were mentioned as improvement areas.
- The national computer-related incident response organization (CERT-GH) at the National Communications Authority (NCA) did not have a legal basis. In addition, certain restrictions impeded the CERT's operational ability, such as budgets and human resources.
- Reporting of cyber incidents to the Bank of Ghana and the Financial Intelligence Centre, despite being mandatory, happened only on an ad-hoc basis.
- Although the Data Protection Act (DPA) requires that organizations report cybersecurity incidents to the Data Protection Commission, there were no clear processes and chains of responsibility setting out what had to be reported, to whom it needed to be reported, and how it needed to be reported.
- Development of capabilities in most organizations was ad-hoc and dependent on the organization's own structures.
- No mechanisms for threat and vulnerability disclosure and for interaction on cybersecurity issues between CI owners and between CI owners and the government.
- Information-sharing among organizations and sectors was very ad-hoc and informal.
- The need to integrate cybersecurity in the national crisis management was identified.
- Cybersecurity was not part of the national defense strategy and there was no specific cyber defense strategy.
- Digital redundancy measures were considered (ad-hoc) only by some individual institutions (in both the private and public sectors), but these engagements were not formally coordinated at the national level.

## Cyber culture and society



- Users were not well aware of the risks associated with Internet use.
- Government agencies generally had a minimal understanding of the risks and threats originating from cyberspace.
- SMEs did not have the human capacity nor the resources to invest sufficiently in cybersecurity.
- For larger international NGOs, cybersecurity was not considered a priority.
- The majority of the Ghanaian society was not aware that e-government services existed.
- E-commerce services were provided to a limited extent and were in the early stages of development.
- Awareness of personal data protection and security was low.
- Channels in place to report incidents or crimes, either computer-related or only, were not coordinated.
- Cybersecurity issues overall were insufficiently reported by online or traditional mass media.

## Cybersecurity education, training, and skills



- A national program for cybersecurity awareness raising, led by a designated organization (from any sector) that addresses a wide range of demographics was not established.
- Awareness-raising efforts initiated by some organizations and institutions were uncoordinated at the national level.
- Except for major international organizations, financial institutions, and telecommunication companies, there was limited awareness of cybersecurity threats and risks in the private sector.
- It was deemed necessary to enhance cybersecurity education in schools and universities, as well as strengthening research and development activities in order to protect critical infrastructures and to nurture the growth of their cybersecurity industry.
- Educators in cybersecurity were not sufficiently available.
- Cooperation between the private sector and universities was mainly ad-hoc.
- No comprehensive approach to cybersecurity education and training was in place.
- A cybersecurity framework for certification and accreditation of public sector professionals did not exist

## Legal and regulatory frameworks



- The legislation adopted or amended did not cover all aspects of cybersecurity, such as human rights protection on the Internet, consumer protection on the Internet, internet safety for children, and comprehensive digital evidence regulations.
- Across the criminal justice system, it was not clear how the cybercrime unit of the Ghanaian Police is set up, how it operates, and what kind of training it provides.
- Law-enforcement community faced with the lack of evidence to proceed with the prosecution, the lack of forensic tools and laboratories that could help to analyze the data from devices, and the lack of an adequate level of training and certifications needed to carry out prosecutions.
- Generally, law-enforcement officers used their discretion when prosecuting cybercrime.
- Many cybercrime cases could not be solved, since the majority of Ghana's Internet infrastructure was in the hands of private stakeholders and service providers, they might have felt reluctant to share their subscribers' information with the police.
- Lack of law-enforcement agencies capable of solving cybercrime boosted the confidence of criminals, as well as victims' reluctance to report crimes.

- Lack of current, reliable and accurate cybercrime statistics from the Ghanaian Police Service made it difficult to quantify the level of threat posed by cybercrime in order to support investigations and better inform strategic decisions of policy makers and regulators.
- The ability of prosecutors and judges to handle cybercrime cases and cases involving digital evidence was considered to be limited by the stakeholders.
- Limited budget and the absence of technical equipment was a reason for not following the procedures for handling cybercrime cases and cases involving digital evidence
- Formal training covered about 10% of the total prosecutors and judges.
- Informal and formal cooperation mechanisms were ad-hoc, both domestically and abroad.

### **Standards, organizations, and technologies**



- No baseline for national ICT security standards, or a government-led initiative to promote exchange of best practices, or to foster the implementation of cybersecurity standards.
- Efforts for identifying and implementing standards are made within the sector rather than across different sectors.
- No evidence for the adoption of ICT standards by SMEs.
- No mandatory standards for the procurement of software implemented in the public sector.
- No clear degree of authentication processes implemented by the private and public sectors.
- No inventory of secure software to be used in the public and private sectors.
- Ad-hoc adoption of technical security controls varied across sectors and organizations.
- Common use of personal email accounts (e.g. Yahoo and Gmail) for official email correspondence was observed.
- No regulations in place to require the implementation of controls and auditing for compliance purposes.
- No domestic market for cybercrime insurance products.
- No responsible disclosure policy or framework.

Strong political backing helps drive forward the ongoing World Bank e-Transform Project for Ghana, which provides support for cybersecurity. In parallel, the country benefits from a complementary World Bank Advisory Services and Analytics Activity “Support for Cybersecurity Capacity Building” (P162839). As a result, the parties agreed that there was no need for additional, cybersecurity-focused technical assistance under the Global Cybersecurity Capacity Building Program. Thus, the Program’s resources initially earmarked for the Ghana work program were subsequently reallocated.

It should be also noted that Ghana has benefited from GCCD’s KISA capacity-building activities outside this Program.

## Western Balkans

The Western Balkan region comprises the following countries: Albania, Bosnia and Herzegovina, Kosovo, Montenegro, North Macedonia, and Serbia. The EU accession prospects motivate the region-wide digital transformation, which requires not only the development of the future-proof ICT infrastructure, but also strengthening their cybersecurity infrastructures.

Among other digital activities, cybersecurity became part of the regional priorities endorsed by the Prime Ministers of all six Western Balkan states in 2017 as part of their [Multi-annual Action Plan \(MAP\) for the Regional Economic Area](#). MAP underlines regional collaboration in the area of cybersecurity. To support the region with this task and in coordination with the participating countries from the region, the Program was adjusted to provide regional technical assistance to support countries in their efforts toward the implementation of some of the established regional priorities. Additionally, the Program has supported participating countries in their thinking of potential regional activities that could strengthen cybersecurity at the regional level. For more details, please refer to Regional Training Center and Information Sharing and Analysis Center (ISAC) sections in Regional level initiatives chapter later in this document.



### Republic of North Macedonia

North Macedonia, a landlocked country of 2.1 million people, is located in the south-eastern part of the Western Balkan region. It is an upper middle-income country, with a GDP (per capita) of \$6,100 (2018) that has made great strides in reforming its economy over the last decade. However, the transition to a well-functioning and inclusive market economy is not yet complete. To take advantage of new opportunities, North Macedonia will need to implement reforms to close the income gap with Europe.<sup>9</sup>



The Ministry of Society and Administration (MISA) is responsible for the development and promotion of the information society. It supports the state administration bodies with implementing and maintaining communication systems and information technology equipment. Furthermore, MISA stands as a backbone organization for the country's integrated information and communication network, national large volume databases, and the development and information security services provided to state bodies, legal entities and other persons entrusted with the law.

In order to achieve the country's information security goals, the MISA joined the Global Cybersecurity Capacity Building Program. As in other countries, the main activities kicked off with the CMM assessment. The in-country assessment review was conducted from 30 January - 1 February 2018. The cybersecurity capacity review was conducted by the GCSCC in cooperation with the World Bank. The assessment was hosted by the MISA jointly with the Ministry of Defense and the Ministry of Interior. Representatives from those three ministries comprise the core of the national Cybersecurity Working Group. When this document was drafted and ahead of establishment of dedicated national bodies, the Group was responsible for the development of and, in some cases, the implementation of the major national initiatives in the area of cybersecurity. Stakeholders representing the following institutions participated in the consultation to review North Macedonia's cybersecurity capacity:

<sup>9</sup> <https://www.worldbank.org/en/country/northmacedonia/overview>

#### Public sector entities:

- Agency for Electronic Communication (AEC)
- Agency for Promotion of Entrepreneurship
- Agency for Real Estate Cadaster
- Cabinet of the President of the Republic of North Macedonia
- Central Registry (of companies)
- Customs administration
- Department of Cybercrime and Digital Forensics
- Directorate for Personal Data Protection
- Directorate for Security of Classified Information
- Financial Intelligence Office
- Financial Police
- Food and Veterinary Agency
- Health Insurance Fund
- Institute for Public Health
- Insurance Supervision Agency
- Ministry of Defense
- Ministry of Education and Science
- Ministry of Finance
- Ministry of Foreign Affairs
- Ministry of Health
- Ministry of Information Society and Administration
- Ministry of Interior
- Ministry of Justice
- Ministry of Labor and Social Policy
- Ministry of Transport and Communications
- National Centre for Computer Incidents Response (MKD-CIRT)
- Office of Security and Counter Intelligence
- Public Revenue Office
- State Audit Office
- The Association of the Units of Local Self-Government of RM
- The Intelligence Agency

#### Criminal justice sector:

- Financial Police Office
- Public Prosecutor's Office for Prosecuting Criminal Offences Related to and Arising from the Content of the Illegally Intercepted Communications
- The Public Prosecutor's Office

#### Technology and telecommunications sector:

- INFIGO
- INTEGRA SOLUTIONS
- MAX HOSTING
- NEXT-EM
- Nextsense
- TELECOM

#### Finance sector:

- Clearing House KIBS AD Skopje
- Halk Bank AD Skopje
- Komercijalna Banka AD Skopje
- KPMG (in North Macedonia)
- Ohridska Banka AD Skopje
- ProCredit Bank (in North Macedonia)
- SPARCASSE BANK (in North Macedonia)
- Stopanska Banka AD Bitola
- Triglav Osiguruvanje AD
- TTK BANKA AD Skopje



### Critical infrastructure owners:

- Civil Aviation Agency
- Crisis Management Centre
- EVN
- Macedonian Railway Infrastructure
- MEPSO
- MNAV
- National Bank of the Republic of North Macedonia
- Public enterprise for state roads

### Academia:

- Faculty of Computer Science and Engineering – Ss. Cyril and Methodius University in Skopje
- Faculty of Electrical Engineering and Information Technologies FEIT – Ss. Cyril and Methodius University in Skopje
- Goce Delcev University – Stip
- MARNET – Macedonian Academic Research Network
- Military Academy “General Mihailo Apostolski”
- University of Information Science and Technology “St. Paul the Apostle” Ohrid – UIST

### Professional societies/non-governmental organizations (NGOs):

- Internet Hotline Provider Macedonia Association
- RE2020

### International community:

- Croatian Embassy Skopje
- Albanian Embassy in Skopje
- International Republic Institute

### Photos from the CMM assessment in North Macedonia



From left to right: **Marco Mantovanelli** (Country Manager for North Macedonia of the World Bank), **His Excellency Damjan Manchevski** (Minister of Information Society and Administration), **Carolyn Weisser Harris** (Lead International Operations GCSCC), **Dr. Eva Nagyfejeo** (Researcher, GCSCC), **Jeb Webb** (Oceania Cybersecurity Centre), **James Boorman** (Oceania Cybersecurity Centre), **Jovana Gjorgjioska** (Junior Associate for strategic planning, EU integration and international cooperation division, Ministry of Information Society and Administration), **Artan Saliu** (IT Analyst, the World Bank)

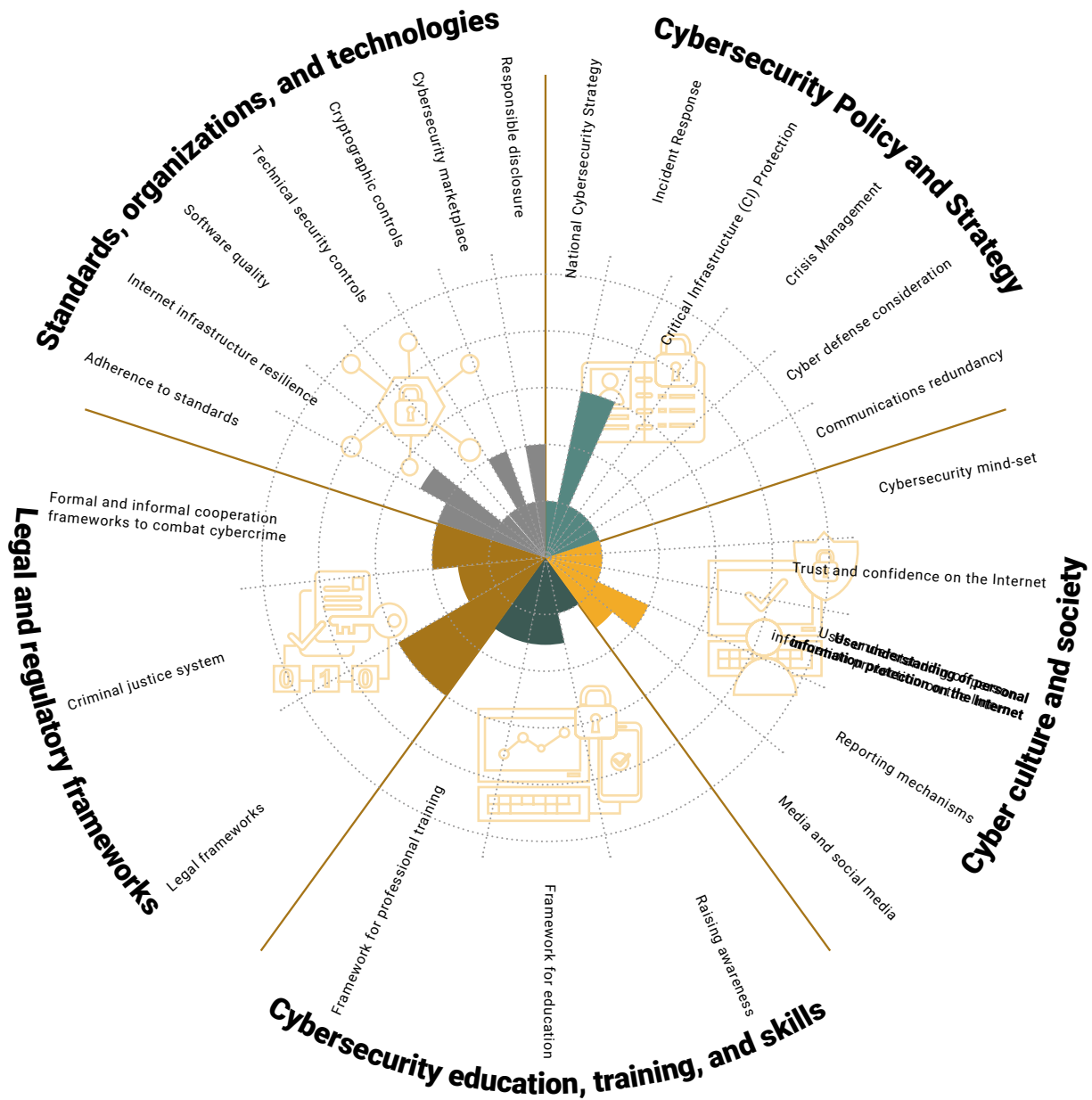
Photo credit: GCSCC



**MISA, GCSCC, Oceania Cybersecurity Centre, World Bank, and other participants from the CMM in North Macedonia**

Photo credit: GCSCC

# OVERALL REPRESENTATION OF THE CYBERSECURITY CAPACITY IN THE REPUBLIC OF NORTH MACEDONIA



The CMM Review Report was published in July 2018. According to the Report, the following key findings were identified across the five dimensions of cybersecurity capacity:

### **Cybersecurity policy and strategy**



- No official national cybersecurity document existed.
- No overarching national cybersecurity program was available.
- Limited availability of financial and human resources.
- No accepted definition of CI and no formal categorization of CI assets.
- General crisis management is necessary for national security, however cybersecurity was not yet considered as a critical component.
- Cybersecurity was not part of the national defense strategy and there was no specific cyber defense strategy.
- Ministry of Defense is responsible for defense within different government organizations, however there was no central cyber command or control structure.
- No coordinated and systematic communications redundancy at the national level.

### **Cyber culture and society**



- Cybersecurity culture was generally not very advanced and often users were not aware of the risks associated with Internet use.
- Awareness of and familiarity with personal data protection was generally low.
- Users were generally not aware of the channels available for computer-related or online incidents and crimes.
- Cybersecurity issues were insufficiently reported in the media, both online and offline.

### **Cybersecurity education, training, and skills**



- A national program for cybersecurity awareness raising led by a designated organization did not exist.
- Within public institutions, limited training in cybersecurity issues both for IT and general staff.

### **Legal and regulatory frameworks**



- No all-encompassing legal framework that deals explicitly with cybersecurity.
- There was no decentralization of digital forensics among the different institutions.
- Not able to tackle serious cybercrime cases due to the lack of staff with adequate knowledge and skills for such investigations.
- Limited budget and insufficient availability of technical equipment.
- No special courts for handling cybercrime cases.
- No specialized training for judges on informal and formal cybercrime.
- Cooperation mechanisms needed improvement, both domestically and abroad.

### **Standards, organizations, and technologies**



- No obligation to implement any national (or sector-specific) ICT security standard was observed.
- No government-led initiative to promote the exchange of best practices or to foster the implementation of cybersecurity standards.
- No mandatory standard for any sector related to the procurement of hardware and software.
- The extent to which software development guidelines in both the public and private sectors are related to cybersecurity was not clear.
- No inventory of secure software for use in public and private sectors.
- No full monitoring of functional security requirements of the software used in the public sector.
- Ad-hoc adoption of technical security controls varied across sectors and organizations.
- Cryptographic controls for protecting data at rest and in transit were deployed ad hoc.
- No domestic market for cybercrime insurance products.

The CMM assessment proved to be beneficial for the country, since more than two thirds of the CMM assessment activities were prioritized in the National Cybersecurity Strategy and the rest became part of the related Action Plan. According to MISA, the majority of the CMM recommendations were combined and grouped into 5 key areas as 5C Goals of the Cybersecurity Strategy and the Action Plan.

**“The combination of strong political will and prioritization of cybersecurity capacity building with the support from our strategic partners, resulted in momentous results in the past year. The cooperation with the World Bank came to light at the right time, providing support in the crucial phases of capacity building: assessment, developing strategic documents, as well as awareness raising and education. I am sure that just like other participating nations, the Republic of North Macedonia benefited significantly from the support and expertise acquired through the World Bank’s Global Cybersecurity Capacity Building Program.”**

His Excellency Damjan Manchevski, Minister of Information Society and Administration of Republic of North Macedonia

#### 2018 GCCD-Republic Of North Macedonia Cybersecurity CMM Seminar banner



The World Bank then facilitated, in cooperation with the MISA and the Global Cybersecurity Center for Development (GCCD) of Korea Internet & Security Agency (KISA), a capacity-building workshop in Skopje on 2-3 April 2018. The main focus of the workshop was the National Cybersecurity Policy and Framework & National CERT/CSIRT Operation. The following topics were covered by GCCD/ KISA and selected in coordination with the MISA and the World Bank:

- “KISA Introduction & Global Cooperation” by Dr. Jeong Min Lee, Manager, KISA
- “Strategies for developing an Information Protection Law” by Mr. Jaemyung Lim, Head of delegation and Chief Researcher, GCCD, KISA
- “KrcERT/CC Operation & Activities” by Ms. You Jin Moon, Researcher, KISA
- “Recent attacks of APT group” by Mr. Youngjoon Jang, External expert
- “Cyber Incident Response Cases in Korea” by Dr. Jeong Min Lee, Manager, KISA
- “Cyber Threat Analysis Cases in Korea” by Ms. Hyeon Jin Lee, KISA
- “Information Infrastructure Protection Policy & Technology” by Mr. Jin Woo Choi, KISA
- “Cyber Threat Analysis Sharing System in Korea. New Emerging Cybersecurity Trends”, by Mr. Shin Woo Sung, KISA

Following the seminar Mr. Dimitar Manchev, ICT Advisor, Unit for E-infrastructure and IT Standards, Sector for Information Society Development at MISA summarized his and his colleagues’ impressions: “We would like to express our profound gratitude for the successful Cybersecurity seminar, which was very helpful for the Government IT employees from the standpoint of increasing their awareness of Cybersecurity. In this regard, we would like to continue this cooperation in the future, concerning Cybersecurity issues and other relevant IT topics.”

TSC & Deloitte’s technical assistance teams supported the country in the preparation of the National Cybersecurity Strategy and the related Action Plan by providing just-in-time consulting support.



Photos from 2018 GCCD workshop in North Macedonia



**Mr. Youngjoon Jang** (NSHC)

Photo credit: KISA



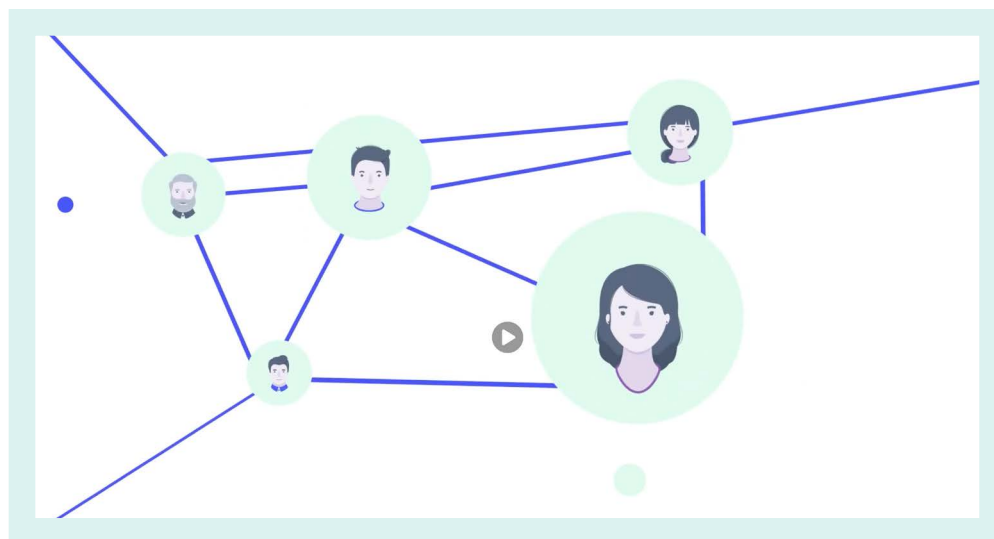
From left to right: **Mr. Luan Aliu** (Program Assistant, the World Bank), **Ms. Youjin Moon** (Researcher, GCCD, KISA), **Mr. Artan Saliu** (IT Analyst, the World Bank), **Mr. Dimitar Manchev** (ICT Advisor, Unit for E-infrastructure and IT Standards, Sector for Information Society Development, MISA), **His Excellency Damjan Manchevski** (Minister of Information Society and Administration), **Mr. Jaemyung Lim** (Chief Researcher and Head of GCCD, KISA Delegation), **Ms. Solza Kovachevska** (State Advisor for Information Systems and Technologies, MISA), **Dr. Jeong Min Lee** (Manager, KISA), **Ms. Junok Lim** (Researcher, GCCD, KISA)

Photo credit: KISA

## Key cybersecurity policy documents on MISA's website: National Cybersecurity Strategy and Action Plan 2018 - 2022.



## Security on the Internet Starts with Me video



In addition, the World Bank financed a [cybersecurity awareness video](#) to help spread information among the general public about the importance of cybersecurity for every citizen.

## **Impact of North Macedonia's participation in the Global Cybersecurity Capacity Building Program**

The Global Cybersecurity Capacity Building Program provided support to key cybersecurity initiatives in North Macedonia.

First, the CMM assessment process facilitated the formation of the **National Cybersecurity Working Group** consisting of the Ministry of Information Society and Administration, Ministry of Interior, and Ministry of Defense, and which is supported by national MKD-CIRT team.



Second, the CMM assessment significantly presented the **National Cybersecurity Strategy 2018 – 2022**, which pursues the following main goals:

### **GOAL 1: Cyber resilience**

“Cyber resilience provides confidentiality, integrity, and availability through identification, protection and establishment of pre-incident state of cyberspace.”

### **GOAL 2: Cyber capacities and cyber culture**

“Rather than solely focusing on raising the awareness of cyber threats, this goal also refers to the commitment towards building the necessary cybersecurity capacities by all affected stakeholders with relevant activities in this field. Promoting cybersecurity culture induces responsibility and an understanding of cyber-related risks by all actors, developing a learned level of trust in e-services, and user’s understanding of how to protect personal information online.”

### **GOAL 3: Combating cyber crime**

“The development and utilization of information and operational technologies leads to the occurrence of different forms of abuse characterized as cyber-crime. ... Given the widespread range of cybercrime and scope of institutions and organizations in charge of cybercrime management and handling, this goal requires the establishment of a specialized, detailed national plan for cybercrime management, including cyberspace enabled crime.”

### **GOAL 4: Cyber defense**

“Establishing a cyber component in the national security sector in all working groups and bodies focused on cybercrime.

One of the conditions for the establishment of efficient national cyber defense is for all organizations that offer services in cyberspace to continuously update and adjust operational plans in accordance with national scenarios (in order to protect CII and IIS).

The civil-military cooperation at the international level is based on state-owned resources, which are also in operation in cyberspace and regard warning, prevention, protection, distraction, detection, and active defense.”

### **GOAL 5: Cooperation and exchange of information**

“Every organization and every individual should take responsibility for the use of new technologies. In order to enjoy a safe cyberspace and a transparent and safe use of ICT at the national level, it is essential to define efficient and effective procedures for the cooperation and exchange of information for all stakeholders. Furthermore, it is vital to strengthen the capacities, procedures, and processes between participating stakeholders through continuous cooperation.”

Then, the Program consultants supported the development of the National Cybersecurity Action Plan 2018 – 2022, which details the activities required to achieve the goals set forth in the National Cybersecurity Strategy:

- Priority activities
  - Establishing a National Cybersecurity Council
  - Establishing a Body with operational cybersecurity capacities
  - Conducting a study to identify the Critical Information Infrastructure (CII) and other Important Information Systems (IIS).
- Activities implementing the 5C Goals of the Strategy

For more details regarding the provided technical assistance, please refer to Regional Training Center and Information Sharing and Analysis Center (ISAC) sections in the Regional level initiatives chapters, which can be found later in this document.

The Program has also triggered inter-Ministerial collaboration between Bosnia and Herzegovina and North Macedonia. Both countries plan to sign a Memorandum of Understanding that would advance bilateral collaboration in the area of cybersecurity.



Albania, home to 2.87 million inhabitants, is situated in the southwestern part of the Western Balkan region bordering on the Ionian and Adriatic seas. During the past three decades, the country has made remarkable economic progress, evolving from one of the poorest nations in Europe to a middle-income country, with GDP per capita of \$4,544 in 2018.<sup>10</sup>



The National Authority for Electronic Certification and Cybersecurity (AKCESK) took a mission to oversee the implementation of Albania’s Electronic Signature, Electronic Identification, and Cybersecurity laws. Within this mission AKCESK works to ensure the security for trusted services and the reliability and security of transactions between citizens, businesses, and public authorities. Their goal is to increase the overall security level of the information system networks of Albania.

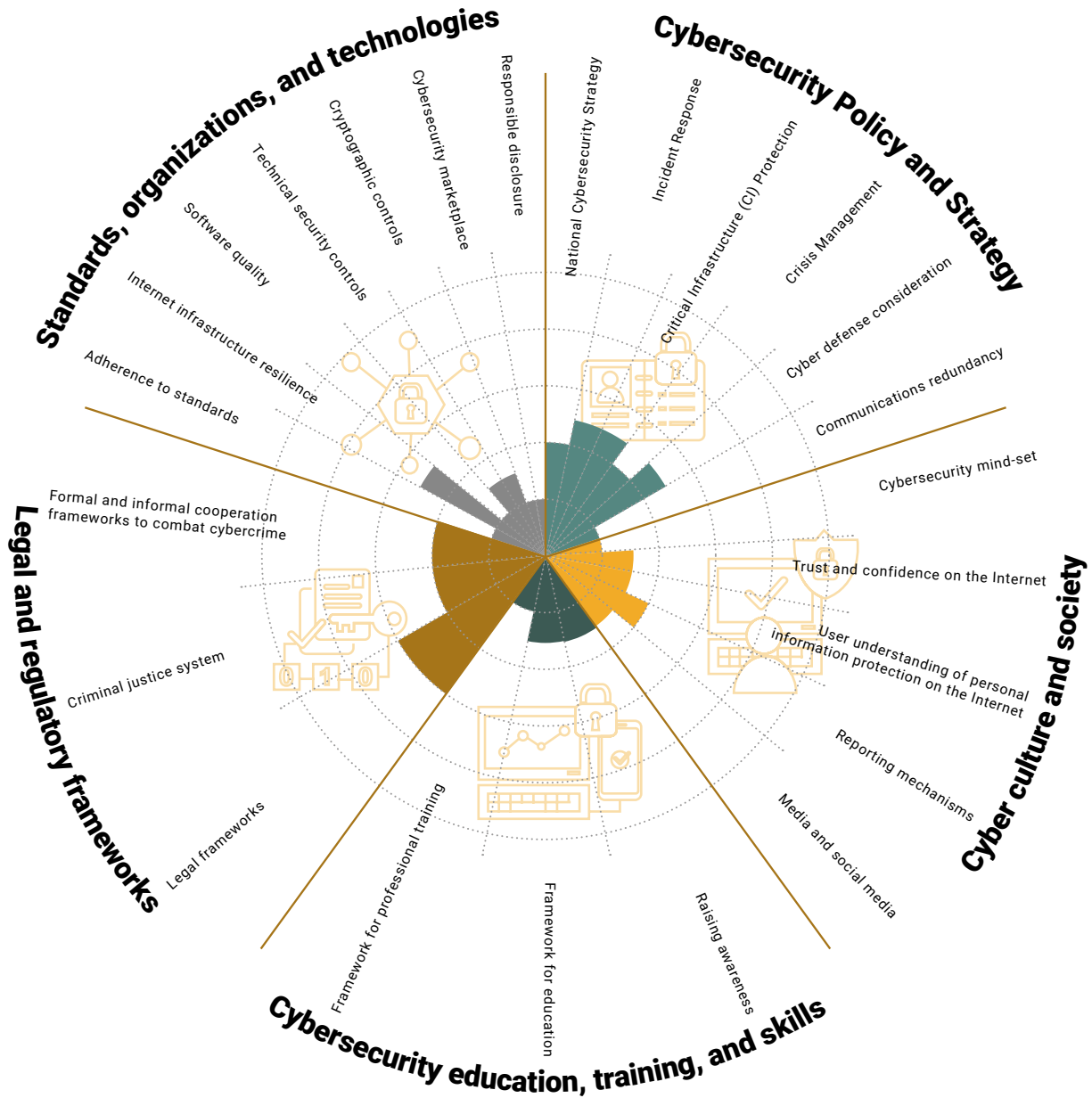
In order to accelerate the pace of equitable growth, Albania is implementing structural reforms that will raise productivity and competitiveness in the economy, create more jobs, and improve governance and public service delivery.

To support its reform agenda in the ICT sector, Albania joined the Global Cybersecurity Capacity Building Program in 2018. As a result, the CMM in-country assessment review was conducted during 3-4 September 2018. The review was conducted by the GCSCC in cooperation with the World Bank. The CMM was hosted by the AKCESK. Stakeholders representing the following sectors participated in the consultation to review Albania’s cybersecurity capacity:

- Universities
- Internet Society representatives
- Internet registries
- 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 Defense
- 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

<sup>10</sup> <https://www.worldbank.org/en/country/albania/overview#1>

# OVERALL REPRESENTATION OF THE CYBERSECURITY CAPACITY IN ALBANIA



The CMM Review Report was published in February 2019. According to the Report, the following key findings were identified across the five dimensions of cybersecurity capacity:

### **Cybersecurity policy and strategy**



- CMM review was not able to determine the maturity of the threat and vulnerability disclosure among CII owners, as well as between CI and the government.
- General crisis management is necessary for national security, however cybersecurity was not yet considered a crucial component.
- Digital redundancy measures were considered (ad-hoc) by private companies and other organizations, but these measures were not systematically coordinated at the national level.

### **Cyber culture and society**



- Lack of a cybersecurity mindset at the local level or for small and medium enterprises (SMEs).
- Limited access to the Internet, as well as limited levels of digital illiteracy in rural areas.
- Existing cybersecurity awareness efforts were too limited in scale to provide a sufficient level of knowledge across society as a whole.
- Due to a relative lack of e-service delivery in the past, there was a lack of trust in the Internet for providing certain services.
- A small proportion of the population was using e-commerce services.
- Users and stakeholders in the public and private sectors had general but limited knowledge about how personal information is handled online.
- Ad-hoc media coverage on cybersecurity.
- Limited discussion on social media about cybersecurity.

### **Cybersecurity education, training, and skills**



- A national program for cybersecurity awareness raising, led by a designated organization (from any sector) that addresses a wide range of demographics was not established.
- Cybersecurity-specific courses were not yet offered by public and private universities and colleges.
- There were not enough professors specialized in cybersecurity because according to the Ministry of Education, Sport, and Youth only doctorate (PhD) holders were allowed to teach such courses.
- The need for training professionals in cybersecurity has been recognized by the Government but has not been documented at the national level.
- There were no certified government and public-sector agencies under internationally recognized standards in cybersecurity.
- Training on cybersecurity issues both for IT staff and general staff was very limited in the public institutions.
- The perception of the private sector's management and CEOs regarding cybersecurity needed significant improvement.
- Retaining security professionals is an issue in Albania as they often leave the country to seek better opportunities in the EU or North America.

### **Legal and regulatory frameworks**



- No all-encompassing regulation that deals explicitly with cybersecurity.
- Insufficient resources and continuous training for the employees of the Cybercrime Unit.
- No separate court structure or specialized judges for cybercrime cases and cases involving electronic evidence.

### **Standards, organizations, and technologies**



- No obligation to implement national (or sector-specific) ICT security standards.

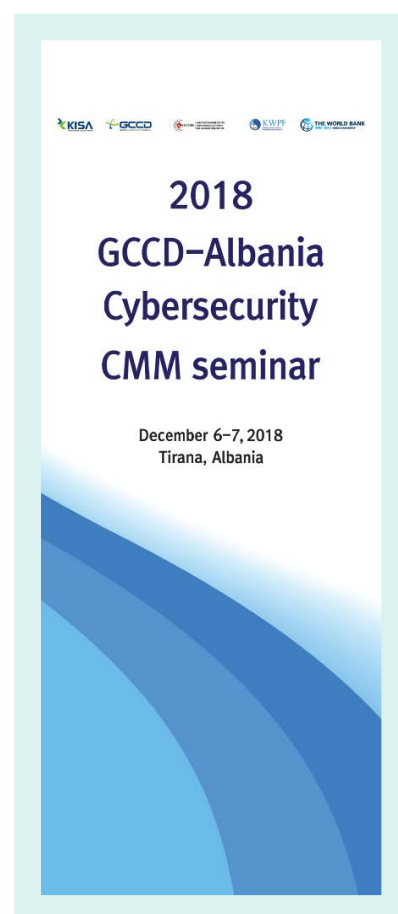
- No mandatory standards for the procurement of hardware and software.
- The extent to which software development guidelines in both the public and private sectors are related to cybersecurity was not clear.
- No inventory of secure software for the use in public and private sectors.
- Ad-hoc adoption of technical security controls varied across sectors and organizations.
- Cryptographic controls for protecting data at rest and in transit were deployed ad hoc.
- Domestic market provided limited cybersecurity technologies.
- No domestic market for cybercrime insurance products.
- No policy for responsible information disclosure (except for the classified information handled by the Albanian NSA).

Following the CMM, the World Bank facilitated, in cooperation with the AKCESK and Global Cybersecurity Center for Development of Korea Internet & Security Agency, the 2018 GCCD-Albania Cybersecurity CMM Seminar in Tirana on 6-7 December 2018. This seminar provided the opportunity to share the experience, expertise, and knowledge in the field of cybersecurity of the experts from the Korean delegation with the local stakeholders. While the main focus of the workshop was on the National Cybersecurity Framework & CERT/CSIRT Operations, other important topics were also covered by GCCD/KISA with prior coordination with AKCESK and the World Bank:

- “KISA introduction & International Cooperation” by Mr. Seunggu Ji, Manager, GCCD, KISA
- “Cybersecurity Framework Development” by Mr. Jaemyung Lim, Chief researcher, GCCD, KISA
- “KrCERT/CC Structure” by Mr. Youngwook Park, General researcher, GCCD, KISA
- “KrCERT/CC Operation and Activities” by Mr. Sangwon Han, Researcher, GCCD, KISA
- “Communication between KrCERT/CC and other CERT organizations in Korea” by Mr. Hansaem Park, Researcher, GCCD, KISA
- “Recent Cybersecurity in IoT Devices in Korea” by Ms. Yoonsun Choi, Deputy Senior Researcher, GCCD, KISA
- “E-government Security” by Ms. Daeun Yoo, Researcher, GCCD, KISA

For more details regarding the technical assistance provided, please refer to the Regional Training Center and Information Sharing and Analysis Center (ISAC) sections in the Regional level initiatives chapter later in this document.

**2018 GCCD-Albania Cybersecurity CMM Seminar banner**



## **The Impact of Albania's of participation in the Global Cybersecurity Capacity Building Program**

### **Photos from the 2018 GCCD-Albania Cybersecurity CMM Seminar**



AKCESK, GCSCC, and other CMM participants in Albania

Photo credit: KISA



**Mr. Sangwon Han**, Researcher, GCCD of KISA

Photo credit: KISA

Although the Program in Albania lasted for only a few months, the initial results were immediately visible. When this document was drafted, AKCESK was leading the preparation of the very first Cybersecurity Strategy and Subsequent Action Plan. The preparation of both is presented in the CMM Review report. According to AKCESK, the national cybersecurity environment has been strengthened with help of the stakeholder mobilization and the capacity building conducted during the CMM deployment. These efforts were further supported by a capacity-building seminar on the identified gaps (by GCCD of KISA). All of the factors contributed to a more informed, active, and better-coordinated process with all the relevant parties involved.

Furthermore, as the Chair of Cybersecurity Alliance for Mutual Progress (CAMP), KISA invited three representatives from AKCESK to CAMP's 3rd Annual Meeting in Seoul, Republic of Korea on 12-14 September 2018. Albania's participation in the Global Cybersecurity Capacity Building Program enabled representatives from AKCESK to participate in the CAMP 2018.

CAMP serves as the networking platform for 55 organizations from 41 different countries to enhance cybersecurity capacity building, as well as promote information sharing. CAMP contributes to facilitating stronger and effective collaboration at the global level to maintain peaceful cyberspace.





## Bosnia and Herzegovina

Bosnia and Herzegovina is a largely landlocked country with a population of 3.8 million inhabitants that is located in the northwestern part of the Western Balkan region. It is an upper middle-income country with a GDP (per capita) of \$4,409 that has made many accomplishments since the mid-1990s, despite having a complex government system including two entities and one district (the Federation of Bosnia and Herzegovina, the Republic of Srpska, and the Brčko District). Today, it is an EU potential candidate country and is now embarking on a new growth model amid a period of slow growth and the global financial crisis.<sup>11</sup>



The organization responsible for the transport and communication competencies, including the country's cyber strategy in Bosnia and Herzegovina is the Ministry of Communications and Transport (MOCT). The ministry's responsibilities cover most of the country's critical infrastructures. Such infrastructures includes road, air and sea traffic, and critical resource traffic like pipelines. When it comes to critical digital assets, the ministry is also the regulator of telecommunication systems. The Cabinet of Ministers assure the internal controls and audit processes. Through this procedure it is ensured that the National Cyber Strategy is harmonically incorporated into the country's legal system.

The country is working to strengthen its state-level cybersecurity. The Global Cybersecurity Capacity Building Program included it as one of its beneficiaries in September 2018, with the first major activity—the CMM assessment—starting a month later, on 23-25 October 2018. The cybersecurity capacity review was conducted by the GCSCC in cooperation with the World Bank and the review was hosted by the MOCT of BiH. Stakeholders representing the following institutions participated in the consultations to review cybersecurity capacity in Bosnia and Herzegovina:

Faculty of Electrical Engineering - University of Sarajevo  
Faculty of Criminology and Security Studies - University of Sarajevo  
Faculty of Electrical Engineering - University of Banja Luka  
Faculty of Security Science - University of Banja Luka  
Faculty of Information Technology - University "Džemal Bijedić" of Mostar  
Faculty of Mechanical Engineering and Computing - University of Mostar  
Federal Ministry of Education and Science  
Ministry of Science and Technology of Republika Srpska  
University Tel-Informatic Centre  
Ministry of Security of Bosnia and Herzegovina  
Federal Police Administration  
Ministry of the Interior of Republika Srpska  
Ministry of Justice of Bosnia and Herzegovina  
The Prosecutor's Office of Bosnia and Herzegovina

11 <https://www.worldbank.org/en/country/bosniaandherzegovina/overview>

State Investigation and Protection Agency  
 Ministry of Defense of Bosnia and Herzegovina  
 Intelligence – Security Agency of Bosnia and Herzegovina  
 Directorate for Coordination of Police Bodies of Bosnia and Herzegovina  
 Ministry of Communications and Transport of Bosnia and Herzegovina  
 Department for maintenance and development of electronic business and e-government system -  
 General Secretariat of the Council of Ministers of Bosnia and Herzegovina  
 Communications Regulatory Agency of Bosnia and Herzegovina  
 The Information Society Agency of Republika Srpska  
 Microsoft Bosnia and Herzegovina  
 BH Telecom  
 Eronet  
 Mtel  
 Central Bank of Bosnia and Herzegovina  
 Elektroprenos Bosnia and Herzegovina  
 The State Electricity Regulatory Commission of Bosnia and Herzegovina  
 BIT Alianse  
 ICT Association of Foreign Trade Chamber of Bosnia and Herzegovina  
 OSCE Bosnia and Herzegovina  
 Regional Cooperation Council (RCC)  
 World Bank - Bosnia and Herzegovina  
 Parliament Bosnia and Herzegovina - Information Technology Sector  
 Ministry of Civil Affairs of Bosnia and Herzegovina  
 Ministry of Finance/Finance and Treasury of Bosnia and Herzegovina  
 Ministry of Foreign Affairs of Bosnia and Herzegovina  
 Ministry of Foreign Trade and Economic Relations of Bosnia and Herzegovina  
 Agency for Identification Documents, Registers and Data Exchange of Bosnia and Herzegovina

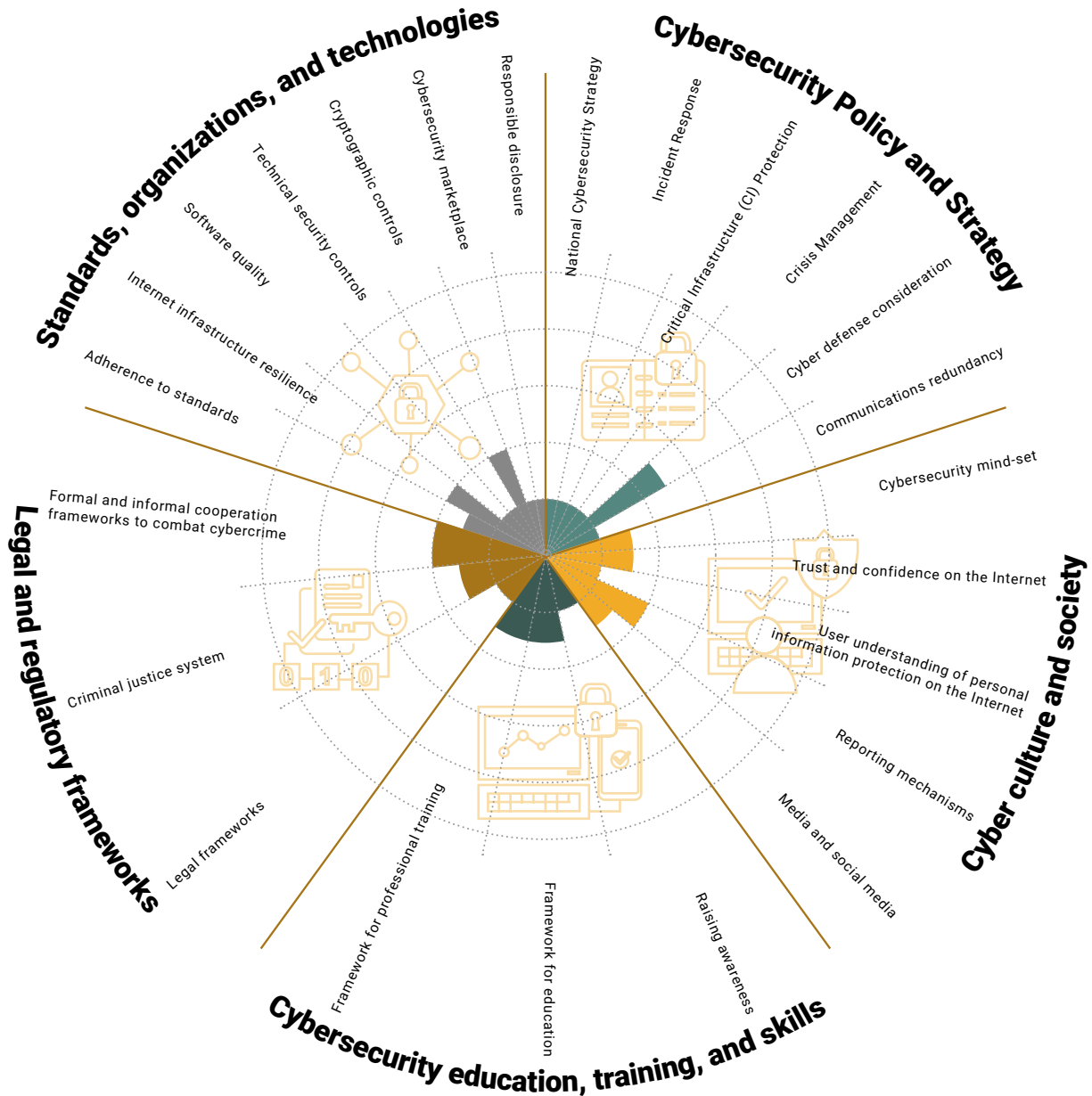
**Photo from the CMM assessment in BiH**



From left to right: **Danko Lupi** (Senior Associate for Informatization, MOCT), **Dr. Eva Nagyfejeo** (Researcher, GCSCC), **Dr. Sarah Puello Alfonso** (Researcher, GCSCC), **Dr. Maria Bada** (Researcher, GCSCC), and **Vlatko Drmić** (Assistant Minister, MOCT)

Photo credit: GCSCC

# OVERALL REPRESENTATION OF THE CYBERSECURITY CAPACITY IN BOSNIA AND HERZEGOVINA



The CMM Review Report was published in May 2019. According to the CMM Review Report, the following key findings were identified across the five dimensions of cybersecurity capacity:

### **Cybersecurity policy and strategy**



- No overarching national cybersecurity program.
- No official national cybersecurity document detailing how to establish coordination between governmental and non-governmental, key cybersecurity actors.
- No registry or catalog of national-level incidents centrally managed by the government.
- No national coordinating body (such as CSIRT or CERT) in order to effectively coordinate cybersecurity incident response and management.
- No mandatory reporting requirements for cyber incidents.
- No accepted definition of national CI and no formal categorization of CI assets at the state level.
- Limited and ad-hoc interaction between government ministries and owners of CI assets.
- Risk management exercises and cyber drills at the state level have not been formalized.
- The cyber defense strategy of the Ministry of Defence was developed without the adoption of an official national cybersecurity strategy.
- Digital redundancy measures were considered (ad-hoc) by private telecommunication companies and other organizations, but these measures were not systematically coordinated at the state level.
- No exercises or drills were conducted at the state level to test emergency response under circumstances with disrupted communications.

### **Cyber culture and society**



- Low level of awareness of the values, attitudes, and practices necessary for a healthy cybersecurity ecosystem resulting from limited knowledge of existing cyber threats, lack of harmonization in the legislation, in established mechanisms for awareness-raising.
- Users did not trust in the limited e-government services available.
- Lack of awareness and understanding of the possible threats (lack of ICT literacy).
- E-commerce services were often offered in an unsecure environment.
- No systematic user understanding of online personal information protection.
- Most people were unaware of the degree to which sensitive personal information should be kept private.
- Existing channels of reporting, particularly between entities and regions were not coordinated and were used in an ad-hoc manner.
- Cybersecurity issues overall were insufficiently reported across mainstream media, both online and offline.

### **Cybersecurity education, training, and skills**



- Awareness raising was not a priority for government institutions partially due to the lack of knowledge about possible risks and threats.
- Awareness-raising programs were mostly presented by international initiatives.
- Awareness raising on cybersecurity issues for executives was limited.
- At primary and secondary levels of education cybersecurity-related topics included less than a year of lessons.
- At higher education level no cybersecurity-related courses were offered.
- Cybersecurity training programs offered to professionals in different sectors appeared to be ad-hoc and not readily-recognized by the government.
- Low number of experts in cybersecurity.

## Legal and regulatory frameworks



- Due to complex system of government in the country, cybersecurity and cybercrime are dispersed under four Criminal Codes and Laws on Criminal Procedure (one at the state level and three at the entity level).
- Existing legislations at the state level were only partially harmonized and had not fully implemented the provisions of the Budapest Convention on Cybercrime.
- Legislation did not cover all aspects of cybersecurity, such as human rights protection and consumer and intellectual property protection on the Internet.
- Institutional capacities to tackle cybercrime issues remained at the entity level. At the state level, there was no specialized cybercrime unit for combating cybercrime.
- Stakeholders suggested that the judiciary, prosecutors and the police did not have adequate knowledge and skills to investigate cybercrime cases.
- Working-level cooperation between the judiciary, law enforcement, government, and private sector was described by stakeholders as informal and weak.

## Standards, organizations, and technologies



- Participants from both the public and private sectors were not aware of any ICT standards promoted by the government.
- At the state level, there was no mandatory standard for any sector related to the procurement of hardware and software.
- In software development there were different guidelines in both the public and the private sectors
- No identified centrally managed catalogue of secure software platforms and applications at the state level
- Adoption of technical security controls varied across sectors and organizations
- Cryptographic controls for protecting data at rest and in transit were deployed ad hoc at state level
- The country did not produce cybersecurity technologies but relied on international offerings
- No policy in place for responsible information disclosure within the public or the private sectors
- Training on cybersecurity issues both for IT staff and general staff was limited within the public institutions

**“This Cybersecurity Maturity Model (CMM) Assessment Report is very important for us, because the drafting process of the Law on Cybersecurity in Bosnia and Herzegovina is planned for 2019. We hope that the CMM Assessment Report will help us get a much clearer picture of the cybersecurity situation in Bosnia and Herzegovina.”**

Bosnia and Herzegovina: Danko Lupi, Senior Associate for Informatization, MOCT



The World Bank then facilitated, in cooperation with the MOCT and the Global Cybersecurity Center for Development (GCCD) of Korea Internet & Security Agency (KISA), the 2018 GCCD-Bosnia and Herzegovina Cybersecurity CMM workshop, organized in Sarajevo on 3-4 December 2018. Around 70 - 80 participants from 52 institutions attended the event. The main focus of the workshop was National Cybersecurity Policy, Legal Framework & CERT/CSIRT Operation. The following topics were covered by GCCD/KISA, selected in coordination with the Ministry of Communication and Transport of Bosnia and Herzegovina, and the World Bank:

- “KISA introduction & International Cooperation” by Mr. Seunggu Ji, Manager, GCCD, KISA
- “Cybersecurity Framework Development” by Mr. Jaemyung Lim, Chief researcher, GCCD, KISA
- “KrCERT/CC and Cybersecurity in the Republic of Korea” by Mr. Sangwon Han, Researcher, GCCD, KISA
- “Cybersecurity Domestic Cooperation of KrCERT/CC” by Mr. Youngwook Park, General researcher, GCCD, KISA
- “E-government Security (Secure Software Development)” by Ms. Daeun Yoo, Researcher, GCCD, KISA
- “Cyber Attack Response (Phishing and Smishing)” by Mr. Hansaem Park, Researcher, GCCD, KISA
- “Recent Cybersecurity in IoT Devices in Korea” by Ms. Yoonsun Choi, Deputy senior researcher, GCCD, KISA

### 2018 GCCD-Bosnia and Herzegovina Cybersecurity CMM seminar banner



### Photos from the 2018 GCCD-Bosnia and Herzegovina Cybersecurity CMM workshop



Ministry of Communication and Transport of Bosnia and Herzegovina, GCCD of KISA, and other workshop participants

Photo credit: KISA





Mr. Seunggu Ji, Manager, KISA  
Photo credit: KISA

### ***Impact of Bosnia and Herzegovina's participation in the Global Cybersecurity Capacity Building Program***

Bosnia and Herzegovina was the last beneficiary country of the Global Cybersecurity Capacity Building Program. Despite the restrictive timeline, the country demonstrated considerable ownership and initiative.

The successful CMM assessment and subsequent workshop facilitated both nationwide and international cooperation to support the efficient planning of the initiatives concerning the state-level cybersecurity-related legislation and policy documents in this area. More precisely, the Program presented the drafting process of the Strategic Cybersecurity Framework in Bosnia and Herzegovina and of the drafting of the Law on Cybersecurity in Bosnia and Herzegovina (both ongoing when this document was drafted).

The Program has also triggered inter-Ministerial collaboration between Bosnia and Herzegovina and North Macedonia. Both countries plan to sign a Memorandum of Understanding that would advance bilateral collaboration in the field of cybersecurity.

## Regional level initiatives

---

In addition to the country-level technical assistance described earlier, the Program has provided regional-level technical assistance for the planning and establishment of a Regional Training Center, and an Information Sharing and Analysis Center (ISAC). It also included summary of the potential regional activities in the area of cybersecurity.

### **Regional Training Center**

#### **Establishment of the Regional Training Center**

The reasons for cybersecurity training programs and the establishment of a Regional Training Center were presented. The design of the Regional Training Center and its programs were based on pedagogical foundations that aimed to equip policymakers and public sector agencies with the knowledge and skills to create a sustainable environment for the adoption, acceleration, and utilization of cybersecurity culture in the beneficiary countries to achieve national development goals. In support of the activities in relation to the goals already mentioned, the main courses of action are described in detail.

#### **Key objectives**

Key objectives to fulfill the mission of the Regional Training Center to strengthen cybersecurity, trust, and data and privacy protection in the services of the information society, providing value to citizens, companies, administration, academic, research, and strategic sectors were discussed in this section of the document.

#### **Organizational aspects**

Functions assigned to training centers at the organizational level were listed. The actions proposed in order to achieve the goal of offering services and resources on the topics of awareness and education in cybersecurity were outlined, together with the personnel's requirements.

## Methodologies and practices

---

An awareness-raising methodology for the Regional Training Center that should be based on the knowledge of the current awareness situation and the practices that must be followed in order to achieve the objectives set forth to fulfill the mission of the Regional Training Center were detailed.

#### **Operation model**

- **Target Audience.** Specific target audiences that must be identified and contacted to be able to start discussions with specific stakeholders and communication were emphasized in this section.
- **Delivery methods and structure.** Different methods and supporting infrastructures for delivering training and awareness in various capacities, including onsite actions and online initiatives, were elaborated in detail.
- **Facilitators and educational team.** An important part of the success of a Regional Training Center are the facilitators, professors, and speakers involved in the actual delivery of the courses and sessions. The activities that the team of professionals working for the Regional Training Center must be able to perform were discussed.
- **Training catalog and descriptions.** The importance of a detailed and up-to-date training catalog to support the activities and training plan of the Regional Training Center was highlighted. The implementation of a typologies course considering the delivery methods and structure were summarized in brief.

#### **Case studies**

The report presented number of examples of cyber training centers:

- INCIBE (Instituto Nacional de Ciberseguridad/Spanish national Cybersecurity Institute), Spain
- NIST (National Institute of Standards and Technology), United States
- SANS Institute, United States)
- ASEAN-Japan Cybersecurity Capacity Building Center (AJCCBC)
- ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE)

## Deployment plan example

The points to consider when implementing a regional training center were described, which include the project description and proposed activities, methodology, expected schedule, and finance.

## **Information Sharing and Analysis Center (ISAC)**

The Information Sharing and Analysis Center (ISAC) establishment support documentation consisted of:

### ISAC implementation aspects

- Information Sharing and Analysis Centers
- Key reasons for creating and be part of an ISAC
- Categorization of ISAC models
- ISAC participant roles
- Governance and funding
- Capabilities

### Collaboration models

- Information sharing models
- Information analysis
- Interoperability in information exchange

### Challenges and recommendations

Key consideration points, along with the list of recommendations of the short analysis of the current status of cybersecurity strategies within the European Union (EU) and selected non-European countries conducted by ENISA were enumerated in this section.

### Selected ISACs organized by model

- Country-focused model
- Sector-specific ISAC model
- International ISACs

### Case studies

This section presented several examples of ISACs:

- MS-ISAC (Multi-State Information Sharing & Analysis Center), United States
- X-ISAC, Luxembourg
- N-ISAC (National ISAC), Taiwan
- KISA, South Korea

## **Summary of the potential regional activities in the area of cybersecurity**

Presentation of concrete topics on regional collaboration and their potential implementation. This deliverable identified different cybersecurity initiatives, including:

- Cooperation in fighting against cybercrime
- Coordinated awareness campaigns
- Joint cybersecurity academic research programs
- Regional training programs for public sector personnel and cybersecurity experts
- Cooperation of incident response teams and ISACs
- Consultation on harmonized legal frameworks
- Critical infrastructure management
- Participation in global and European support programs
- Sectorial cross country cooperation
- Participation in global and European cybersecurity organizations

# Global Cybersecurity Capacity Building Program: Closing meeting

**O**n 18-19 December 2018, the Global Cybersecurity Capacity Building Program Closing Meeting took place at the headquarters of the World Bank in Washington D.C. The event was organized around the:

- Regional cybersecurity Approach for the Western Balkans; and
- Review of the Global Cybersecurity Capacity Building Program, Results and Lessons Learned.

Representatives from the organizations and the partners involved in the Program were convened by the World Bank. The following organizations were represented during the event:

- Department of Construction, Transport and Communication (Government Office of the Kyrgyz Republic)
- Ministry of Transport and Telecommunications (Bosnia and Herzegovina)
- Ministry of Information Society and Administration (Republic of North Macedonia)
- Global Cybersecurity Capacity Centre (University of Oxford)
- Korea Internet and Security Agency (KISA)
- Digital Development Global Practice of the World Bank
- Western Balkans Country Management Unit of the World Bank
- Telecom Strategies Consulting
- Deloitte

## DAY 1

The first day of the event (18 December) was devoted to discussing the theme of the Regional Cybersecurity Approach for the Western Balkans. On this day, the discussion was organized around the following:

<b>Session I:</b> Strengthening cybersecurity at the regional level in the Western Balkans	<p>This session discussed a regional approach and potential regional cybersecurity priorities for the Western Balkan region. Specifically, the session presented ideas on what regional collaboration could entail and invited participants to discuss those ideas:</p> <ul style="list-style-type: none"><li>• Opening of the session and snapshot of the World Bank's regional priorities in the Western Balkans was presented by the World Bank's Western Balkans Country Management Unit.</li><li>• Status of the Regional collaboration in the area of cybersecurity in the Western Balkans was introduced by representatives from the Ministry of Information Society and Administration in the Republic of North Macedonia, and the Ministry of Communications and Transport in Bosnia and Herzegovina.</li><li>• A potential regional approach towards cybersecurity in the Western Balkans was discussed among the participants of the session facilitated by TSC &amp; Deloitte representatives.</li></ul>
<b>Session II:</b> Defining concrete actions that could be implemented at the regional level	<p>This session continued with the presentation of specific ideas for regional collaboration and their potential implementation:</p> <ul style="list-style-type: none"><li>• Regional cybersecurity initiatives that could be developed in the Western Balkans, including ISACs and the Regional Training Center, were presented by TSC &amp; Deloitte.</li></ul>

## DAY 2

The second day (December 19) of the event was dedicated to the Review of the Program, results and lessons learned. The agenda included four sessions:

### Session I

Cybersecurity at the World Bank, review of the Program

This session presented the World Bank's major initiatives, partnerships, and technical assistance in cybersecurity. Afterwards, the session reviewed the implementation circle of the Global Cybersecurity Capacity Building Program and presented its objectives, as well as some of the results:

- Opening of the session and presentation "The World Bank: Initiatives and Partnerships in Cybersecurity" by the Digital Development Global Practice (the World Bank).
- Global Cybersecurity Capacity Building Program: Implementation process and results from the Digital Development Global Practice (the World Bank).

### Session II

Implementation of the Program in North Macedonia, Bosnia and Herzegovina, and the Kyrgyz Republic

This session discussed the implementation of the Program in North Macedonia, Bosnia and Herzegovina, and in the Kyrgyz Republic:

- Opening of the session by the World Bank's Western Balkans Country Management Unit.
- Implementation of the Program and its anticipated results in the Kyrgyz Republic (State Committee on IT and Communications).
- Implementation of the Program and its anticipated results in North Macedonia (Ministry of Information Society and Administration).
- Implementation of the Program and its anticipated results in Bosnia and Herzegovina (Ministry of Communications and Transport).

### Session III

Implementation of the Program: Experience and recommendations from partners

This session provided the floor for the implementation of the Program's Partners – The Global Cybersecurity Center for Development (GCCD) of Korea Internet & Security Agency (KISA) and the Global Cybersecurity Capacity Center (University of Oxford). Both reflected on their respective activities and engagements:

- Implementation of GCCS's experience by Korea Internet & Security Agency (KISA).
- Implementation of GCSCC's experience by GCSCC (University of Oxford).

### Session IV

Discussion on the lessons learned and next steps

This session provided a review of the lessons learned from the Program and advice on how potential future programs might be strengthened. The session invited the participants to share their views on how the design of the Program could be improved and how its implementation could be more efficient:

- Lessons learned and recommendations towards strengthening the Program and its implementation moving forward by Deloitte.



Both days concluded with open discussions about different topics covered at the event. Participants shared their views on the activities performed throughout the Program, summarized key findings and lessons learned, and formulated recommendations towards further improving similar programs. In addition, the discussion ended with brainstorming about the potential next steps that could result from the Program's activities. The recommendations discussed and validated by the participants are detailed in the Results chapter later in this document.

### Photo from the Global Cybersecurity Capacity Building Program Annual Meeting participants



From left to right (front row)

**Dr. Jeong Min Lee** (Manager, KISA), **Dr. Michael Goldsmith** (Director, GCSCC, University of Oxford), **Natalija Gelvanovska-Garcia** (Senior Regulatory Specialist, the World Bank), **Dimitar Manchev** (ICT Advisor, Ministry of Information Society and Administration of the Republic of Macedonia), **Zhenia Viatchaninova Dalphond** (ICT Consultant, the World Bank), **Solza Kovachevska** (State Advisor for Information Systems and Technologies, Ministry of Information Society and Administration of the Republic of Macedonia), **Sandra Sargent** (Senior Operations Officer, Digital Development Department Global Practice, the World Bank)

From left to right (back row)

**Talgatbek Sulaimanov** (Cybersecurity Expert, State Committee on Information and Communication Technologies, the Kyrgyz Republic), **Inkyung Jeon** (Senior Researcher, KISA), **Attila Duka-Zólyomi** (Manager, Deloitte), **Marcos Saco** (Senior Manager, Deloitte), **Javier Marín** (Senior Partner, TSC), **Lina Rainiene** (Deputy Director General of Communications Regulatory Authority of Lithuania), **Danko Lupi** (Senior Associate for Informatization, Ministry of Communications and Transport, Bosnia and Herzegovina), **Branislav Zimonjic** (Senior Advisor, Ministry of Communications and Transport, Bosnia and Herzegovina), **Bakyt Berdaliev** (Deputy Head of the Department of Construction, Transport and Communication, Government Office of the Kyrgyz Republic), **Uran Esengeldiev** (ICT Consultant, the World Bank)

Photo credit: The World Bank



# Results

The key outcomes resulting from the completion of the Global Cybersecurity Capacity Building Program could be summarized as follows:

- It strengthened the **Kyrgyz Republic's** national cybersecurity environment through an analytical study (CMM), i.e. through both cybersecurity stakeholder and donor mobilization and their capacity building during the CMM assessment; through a capacity-building seminar on the identified gaps (by GCCD), and through a customized technical assistance program to support Digital CASA-Kyrgyz Republic Project's cybersecurity component.
- It strengthened the national cybersecurity environment of **Myanmar** through an analytical study (CMM), i.e. through cybersecurity stakeholder mobilization and their capacity building during the CMM assessment. The study's findings were reviewed and validated by the line Ministry. The CMM assessment will inform of the preparation of the cybersecurity strategy.
- It strengthened the **Ghana's** national cybersecurity environment using an analytical study (CMM), i.e. through cybersecurity stakeholder mobilization and their capacity building during the CMM assessment and dissemination events highlighting the identified gaps. The study was reviewed and validated by the line Ministry. This work fed into e-Transform Ghana Project implementation.
- It strengthened **North Macedonia's** national cybersecurity environment through an analytical study (CMM), i.e. through cybersecurity stakeholder mobilization and their capacity building during the CMM assessment; through a capacity-building seminar on the identified gaps (by GCCD), and a through customized technical assistance program to support the cybersecurity development in the country. As a result of technical assistance, North Macedonia has prepared and adopted the National Cybersecurity Strategy and subsequent Action Plan.
- It strengthened **Albania's** national cybersecurity environment through an analytical study (CMM), i.e. through cybersecurity stakeholder mobilization and their capacity building during the CMM assessment; through a capacity-building seminar on the identified gaps (by GCCD). This work led to the preparation of the National Cybersecurity Strategy and subsequent Action Plan (ongoing).
- It strengthened **Bosnia and Herzegovina's** national cybersecurity environment by conducting an analytical study (CMM), i.e. through cybersecurity stakeholder mobilization and their capacity building during the CMM assessment; a capacity-building seminar on the identified gaps (by GCCD). This work led to the preparation of the National Cybersecurity Law (ongoing when this document was drafted).

In the case of three Western Balkan countries, the technical assistance has contributed to the strengthening of the cyber ties between the participating countries. For instance, the line ministries in BiH and North Macedonia have agreed to sign a Memorandum of Understanding in the area of cyber security to better coordinate activities in this area and exchange relevant experiences.

### **Other Outcomes and Impacts**

The implementation of the Program strengthened the relationships between the participating countries. For instance, BiH and North Macedonia have agreed to sign a memorandum of understanding in the area of cybersecurity to better coordinate activities in this area and exchange relevant experiences.

The countries participating in the Program have established bilateral relationships with the relevant Korean institutions and some have since benefited from the Program's training activities in cybersecurity Republic of Korea, including those falling under the CAMP program.

The analytics prepared throughout the Program presented the preparation of the donor programs in cybersecurity. For instance, the European Commission is currently designing its regional technical assistance program in the Western Balkans, by considering of the CMM Review reports prepared under the Program. Similarly, the cybersecurity program for the region of the UK's Foreign and Commonwealth Office is benefitting from the analytical insights provided by the Program. North Macedonia plans to organize a donor conference to solicit funding for its Cybersecurity Action Plan supported by the Program.

Technical assistance provided to the Kyrgyz Republic resulted in the elevation of the national cybersecurity agenda and in greater attention paid on cybersecurity under the Digital-CASA Project. As a result, the Government has taken the decision to complement the cybersecurity financing for this Project, which could provide additional investment support for cybersecurity activities in the country.

# Recommendations

**B**ased on the experience, results, and the lessons learned from the completion of the Global Cybersecurity Capacity Building Program conducted by the World Bank, the following recommendations are presented in this section for strengthening similar activities under the follow-up programs.

## Higher stakeholder involvement

Improvement of the stakeholders' involvement from the country in the Program and its activities for the entire duration of the Program.

*Those countries, where local stakeholders and representatives of institutions devoted a high level of attention and commitment to the Program, have achieved more robust results, as evidenced by the fact that these results have been incorporated into other government-related activities and therefore have a higher potential for sustainability. Also, such involvement resulted in the improved planning of Program-related tasks, activities, and final deliverables. This commitment led to quicker and smoother achievement of the stated policy goals and the completion of related activities. Notably, a high-level of government commitment for the entire duration of the Program required less demanding efforts from the Program managers, in addition to involved experts and partners (GCSCC and GCCD/KISA).*

Involvement of local consultancy firms for a more effective and efficient follow-up and completion of the Program.

*Consultancy firms with presence on the local market have more comprehensive and deeper knowledge about the needs and current circumstances of the given country. Global expertise combined with local knowledge is key to providing professional high-quality services to governmental institutions. This outlined advantage can result in a more successful and efficient achievement of Program goals. Programs similar to the Global Cybersecurity Capacity Building Program might benefit from the identification of such consultancy firms by already implementing partners at early stages of the Program planning. Timely and regular involvement of consultancy firms from the very first steps of the Program activities can lead to a higher utilization of the local knowledge and expertise of the parties involved.*

## Multistage approach to CMM assessment

Regional kick-off workshop prior to the CMM assessment or before the implementation of the CMM recommendations could be beneficial for a more comprehensive approach to cybersecurity-related activities.

*Information sharing is key for a successful management of cybersecurity-related matters. Therefore, in order to achieve the best possible results and utilize a CMM assessment in the most effective and beneficial way, workshops or other information sharing forums could provide the means for an improved planning and preparation of any activities related to the CMM assessment and its subsequent follow-up. These events can take place in the form of regional or local workshops, meetings providing the opportunity for the stakeholders involved and participating institutions to harmonize their activities, and future actions the regional or country level.*

As the CMM assessment explores the Critical National Infrastructure and its cybersecurity competency, it could be useful to link the CMM reviews to the National Risk Assessments.

*As mentioned earlier, the coordination of cybersecurity-related activities is important for the management of country or regional-level priority tasks. One of these priority areas is the national cybersecurity risk assessment and, more specifically, the identification and assessment of the Critical National Infrastructure. The harmonization of the CMM review activities and timing might help to achieve results in a more effective and efficient way, e.g. by reducing the load on participants involved.*

In order to further improve the transparency and accuracy of the CMM assessment's findings, a validation process involving CMM domain area key experts could be considered .

*The five dimensions of the CMM cover the entire spectrum of critical cybersecurity-related areas and seeing that the recommendations presented in the CMM Review Report can have a significant influence on the future cybersecurity of a given country, it might be important to involve a wide range of affected parties into the CMM results validation process, as much as possible. Therefore, involving key experts that could not participate in the initial assessment, but might have valuable comments to improve the accuracy of the CMM assessment findings and thus any related recommendations, could result in a more comprehensive CMM review Report. It can be stated that CMM is a good tool for soliciting expert input and the further engagement of experts.*

Integration of the CMM assessment into the National Cybersecurity Strategy (NCS) development activities.

*Some countries might be in the early phases of establishing their cybersecurity legal and regulatory framework. These initial activities might specifically signify the development of the National Cybersecurity Strategy. Since a CMM assessment can have findings and recommendations that might influence the strategic vision and goals set forth in the National Cybersecurity Strategy, harmonizing the CMM review activities with the tasks of the National Cybersecurity Strategy development process can significantly improve the quality of the resulting National Cybersecurity Strategy. This approach could also provide nations with a rich and broad set of findings that can be used to optimize NCS development. Furthermore, the CMM-based NCS development motivates leveraging synergies among national stakeholders and creating formalized national cyber coalitions.*

Improvement of the CMM final report approval process in order to decrease the lead time.

*One of the most rapidly changing fields is ICT, including its subset – cybersecurity. CMM under the Program followed a rigorous internal review process prior to its publication. This review was conducted by GCSCC, the World Bank, and country stakeholders, in addition to the other participants involved in the CMM assessment. This approach sometimes resulted the review process taking longer than expected (months instead of weeks). A significantly increased lead time of the approval of the final CMM report might result in a situation where the findings and recommendations of the CMM Review Report might become outdated and/or obsolete. In order to avoid such situations and to benefit from the assessment results as much as possible, it is important to strictly plan and follow this plan for the CMM Review Report finalization and approval process.*

## Capacity building and enhancing

It is recommended to consider “study visits” for cybersecurity experts from the assessed country to countries that had already completed the assessment or to countries that are far ahead in the implementation of cybersecurity mechanisms (e.g. the EU, ROK, the US, etc.).

*In order to facilitate an effective completion of the CMM assessment in a given country, professionals that will be involved in the review can benefit from “study visits” to countries with more experience in such activities. This approach could be even more valuable for visits to countries from the same region or to countries with similar cybersecurity maturity levels. This could also be a good source of experience and knowledge exchange among the countries. In addition, such preliminary preparation can have valuable impact on the preparation and planning of the activities for the upcoming CMM assessment and after its completion (follow-up activities).*

Organization and attendance of internationally accredited IT Security and Governance trainings and certification courses for Program beneficiaries.

*Participation in international cooperation programs can facilitate the wider and deeper understanding and appropriation of international standards, terminology and taxonomy, which is vital to achieving the goals set in the National Cybersecurity Strategy. Also, such trainings will enable establishment of cross border collaboration between the participants of these events through building personal relations and trust among them. Typically, these training sessions are expensive, as some are provided by private sector, which prevents many developing countries from benefiting from them. Therefore, donor support is critical in order to achieve adequate attendance.*

Considering the knowledge, skills, and experience obtained from the current Program it would be highly beneficial for the World Bank’s future donor programs to continue their cooperation with the renowned public sector-driven centers of excellence (e.g. KISA’s GCCD) and academic research institutions (e.g. GCSCC).

*During the cooperation with the Global Cybersecurity Capacity Centre (GCSCC) at the University of Oxford and Global Cybersecurity Center of Korea Internet and Security Agency, the methodology and approach applied for the cybersecurity maturity assessment of the countries involved has been tailored and improved in order to meet specific client needs. In the future, this knowledge and experience will help to improve the efficiency of the execution of similar projects and the dissemination of the results, which will in turn benefit the participating countries.*

Leveraging technical assistance and participation in country-level activities from the onset of the Program.

*Similar programs could leverage further types of technical assistance activities for the benefit of the clients of participating developing countries. These activities could be dedicated to:*

- *Cybersecurity-related consultancy services.*
- *Drafting and finalization of National Cybersecurity Strategy.*
- *Development of a related Implementation/Action Plan.*
- *Establishment of training centers at the local or regional level.*

*Such programs could help the stakeholders receive technical assistance support from global experts with broad theoretical and practical knowledge.*







**WORLD BANK GROUP**