CYBERSECURITY CAPACITY REVIEW

Former Yugoslav Republic of Macedonia (FYR Macedonia)

July 2018

Global Cyber Security Capacity Centre

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

KWPF
KOREA-WORLD BANK PARTNERSHIP FACILITY

KISA Korea Internet & Security Agency

GCCD
Global Cybersecurity Center for Development

THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP

CONTENTS

DOCUMENT ADMINISTRATION

Lead researchers: Dr Eva Nagyfejeo, Ms Carolin Weisser, Mr Matthew Griffin

Reviewed by: Professor Paul Cornish, Professor William Dutton, Professor Michael Goldsmith, Professor Basie Von Solms

Approved by: Professor Michael Goldsmith

Version	*Date*	*Notes*
1	*25 March 2018*	*First draft to Technical Board*
2	*24 April 2018*	*Second draft to MISA and World Bank*
3	*13 June 2018*	*Third draft to World Bank*
4	*20 June 2018*	*Fourth draft to MISA*
5	*9 July 2018*	*Fifth draft to World Bank and MISA*
6	*13 August 2018*	*Final report to World Bank and MISA*

LIST OF ABBREVIATIONS

AEC	Agency for Electronic Communications
BSI	British Standards Institution
CAF	Common Assessment Framework
CEH	Certified Ethical Hacker
CERT	Computer Emergency Response Team
CFCE	Certified Forensic Computer Examiner
CI	Critical Infrastructure
CIRT	Computer Incident Response Team
CISSP	Certified Information Systems Security Professional
CMM	Cybersecurity Capacity Maturity Model for Nations
CoE	Council of Europe
DSCI	Directorate for Security of Classified Information
ECTEG	European Cybercrime Training and Education Group
EU	European Union
FYR	Former Yugoslav Republic (of Macedonia)
GCSCC	Global Cyber Security Capacity Centre
GDPR	General Data Protection Regulation
HIDS	Host Intrusion Detection Systems
ICT	Information and communication technologies
IPA	Instrument for Pre-Accession Assistance (of the European Union)
ISP	Internet Service Provider
MISP	Malware Information Sharing Platform
MISA	Ministry of Information Society and Administration
MKD-CIRT	Macedonian Computer Incident Response Team
MoD	Ministry of Defence
MoF	Ministry of Finance
MoI	Ministry of Interior
MoU	Memorandum of Understanding
NATO	The North Atlantic Treaty Organization
NBRM	National Bank of the Republic of Macedonia
NGO	Non-Governmental Organisation
NIDS	Network Introduction Detection Systems
NIS	The Directive on security of network and information systems (of the EU)

NIST	National Institute of Standards and Technology
NOS	The NATO Office of Security
OSCE	Organization for Security and Co-operation in Europe
PfP	Partnership for Peace (programme)
PIN	Personal identification number
SIENA	Secure Information Exchange Network Application
SME	Small and medium enterprises
TETRA	Terrestrial Trunked Radio (standard)
UNDP	United Nations Development Programme
WB	World Bank

EXECUTIVE SUMMARY

In collaboration with the World Bank (WB), the Global Cyber Security Capacity Centre (GCSCC, or 'the Centre') undertook a review of the maturity of cybersecurity capacity in the former Yugoslav Republic of Macedonia (FYR Macedonia) at the invitation of the Ministry of Information Society and Administration (MISA). The objective of this review was to enable the Government to gain an understanding of its cybersecurity capacity in order to develop the country's national cybersecurity strategy, and to strategically prioritise investments in cybersecurity capacities.

Over the period 30 January–1 February 2018, the following stakeholders participated in roundtable consultations: academia, civil society, criminal justice, law enforcement, the defence community, information technology officers and representatives from public sector entities, critical infrastructure owners, policy makers, computer emergency response teams, information technology officers from the private sector (including telecommunications companies and financial institutions), as well as international partners.

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

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

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

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

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

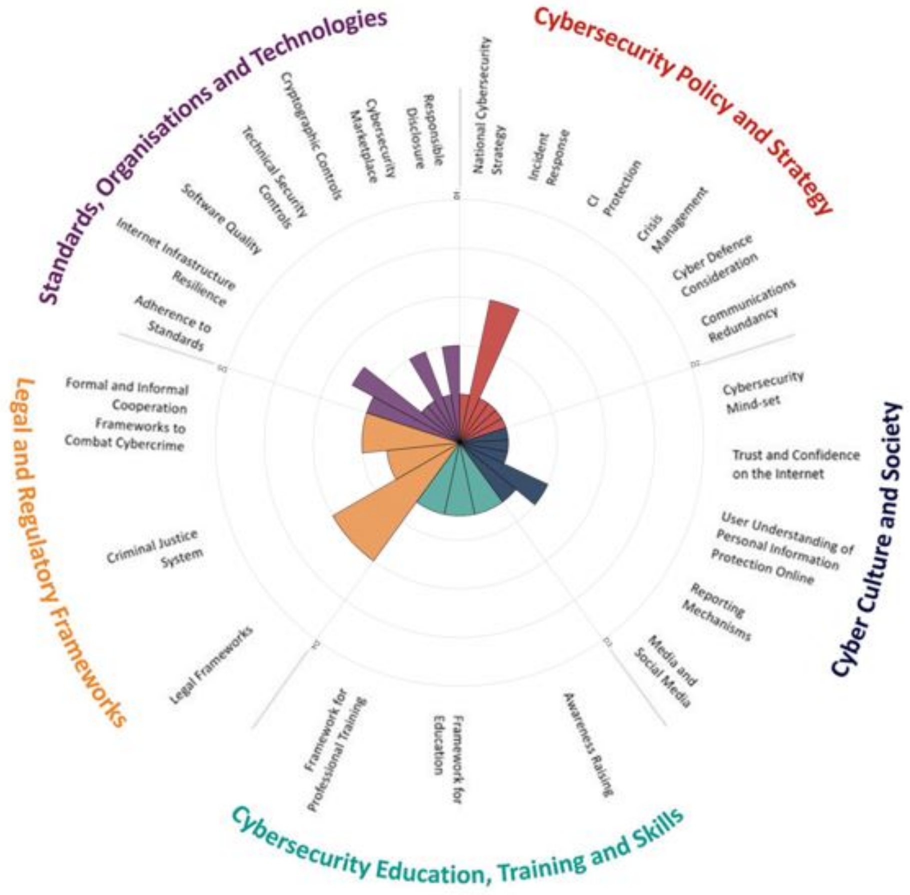

Figure 1: Overall representation of the cybersecurity capacity in FYR Macedonia.

Cybersecurity Policy and Strategy

Currently, there is no official national cybersecurity document in FYR Macedonia detailing how to establish coordination between key cybersecurity governmental and non-governmental actors, nor is there an overarching national cybersecurity programme. However, consultation processes for strategy development have been initiated. The development of the cybersecurity strategy was announced in November 2017 during a high-level public debate on cybersecurity policies. For all participants in that debate one area of concern was the limited availability of financial and human resources. For instance, MISA has no cybersecurity budget available to develop the strategy. Currently, MISA, the Ministry of Defence (MoD), the Ministry of the Interior (MoI), the Agency for Electronic Communications (AEC), the Directorate for Personal Data Protection, and the Directorate for Security of Classified Information are collectively the driving force to improve the cybersecurity environment.[2] The plan is to develop a national cybersecurity strategy. Additionally, the MoD will develop a cyber defence strategy.

[2] Government of the Republic of Macedonia (2017) Annual National Programme of the Republic of Macedonia for NATO membership 2017/2018. *http://www.mfa.gov.mk/images/stories/GNP/GNP-2017-2018-MNR-web.pdf*

The Macedonian Computer Incident Response Team (MKD-CIRT) serves as the national coordinating body for the reporting and management of cybersecurity incidents for the authorities and public sector institutions. In 2015, the MKD-CIRT was set up within the AEC as the 'official national point of contact and coordination in dealing with security incidents in networks and information systems' pursuant to the Law on Electronic Communications.[3]

The concept of cybersecurity in critical infrastructure (CI) is in its infancy in FYR Macedonia. There is as yet no accepted definition of CI and no formal categorisation of CI assets.

It was not possible to obtain a clear picture regarding crisis management in the course of the CMM review. The extent to which organisations consider cyber threats as part of crisis situations is uncertain. It is understood that general crisis management is necessary for national security, however cybersecurity is not yet considered as a component.

Cyber defence capacity in FYR Macedonia is at a start-up stage, as cybersecurity is not currently part of the national defence strategy and there is no specific cyber defence strategy. The MoD is responsible for defence within different government organisations, however there is no central cyber command or control structure. Participants acknowledged the need to create a new unit specifically for cyber defence.

It was not possible to obtain a clear picture regarding communications redundancy during the review. Digital redundancy measures are considered (in an ad-hoc manner) by private telecommunication companies and other organisations, but there is nothing coordinated and systematic at the national level.

Cyber Culture and Society

The cyber ecosystem in FYR Macedonia is still in its early stages. Participants explained that in some government agencies and leading companies a cybersecurity mind-set has started to develop. However, the cybersecurity culture is generally not very advanced and often users are not aware of the risks associated with the use of Internet.

The majority of Internet users 'blindly' trust information and communication technologies (ICT) and Internet services. Participants indicated that users are mostly unaware of any risks when using the Internet and assume that they are safe to use online services. Most users do not have the ability to critically assess the content they see and receive online, nor the applications they use. Among the concerns raised by the participants were also those cases where users were aware of the risks – in the cases of cybercrime, cyberbullying and data breaches, for example – but they did not undertake the necessary security measures out of convenience.

Awareness of the need to protect personal information and familiarity with security concerns regarding personal data is generally low.

Participants mentioned that there are some channels for users in place in order to report computer-related or online incidents and crimes: (1) reporting the matter to a police station in person or by phone; (2) contacting the cybercrime unit at the MoI; and (3) contacting the Directorate of Personal Data Protection in the case of a data abuse. Participants noted,

[3] Agency for Electronic Communications. MKD-CIRT. *https://mkd-cirt.mk/?lang=en*

however, that users are generally not aware of these reporting channels or that they face challenges providing evidence when they report incidents at police stations.

Overall, cybersecurity issues are insufficiently reported in the media both online and offline. If reporting is taking place, then it is done mostly in the case of major international events.

Cybersecurity Education, Training and Skills

A national programme for cybersecurity awareness raising is yet to be established, led by a designated organisation (from any sector) addressing a wide range of demographics.

Currently, cybersecurity awareness raising efforts are sporadic and mostly done on a voluntarily basis and with limited resources by non-governmental organisations (NGOs) and with ad hoc support from the government. However, FYR Macedonia has been active in promoting a safer Internet and has had a regular engagement with the EU's Safer Internet Day initiative since 2010. Leading these activities are the NGOs from the Insafe / INHOPE network, universities, such as the University of Skopje (Faculty of Computer Science and Engineering), as well as line ministries.[4]

The need for enhancing cybersecurity education in schools and universities has been identified by the Government, in particular by the line Ministry, industry, and academic stakeholders. Currently, two universities accomplished the accreditation for undergraduate and master's programmes specialising in cybersecurity. In particular one university which attracts most of the students in IT related subjects is also highly engaged in research and cooperating on the international level.

The need to train professionals in cybersecurity has been recognized by the Government but has not been documented on the national level. Within public institutions, training in cybersecurity issues both for IT staff and general staff is very limited, and it is often at the discretion of management whether a member of staff is permitted to attend a general cybersecurity training or certification course. In the private sector, training is more integrated and sometimes mandatory for IT staff and, in some companies, for non-IT staff.

Legal and Regulatory Frameworks

Comprehensive ICT legislative and regulatory frameworks addressing cybersecurity have been implemented and legislation protecting the rights of individuals and organisations in the digital environment has been adopted in FYR Macedonia.

FYR Macedonia does not have an all-encompassing legal framework that deals explicitly with cybersecurity.[5] However, several legal instruments refer to cybersecurity-related issues such as the Law on Personal Data Protection, the Law on Electronic Commerce, the Law on

[4] Netsafe.finki.ukim.mk. (2018). Ден на безбеден интернет. [online] Available at: http://netsafe.finki.ukim.mk/ [Accessed 19 Mar. 2018].

[5] DiploFoundation (2016) Cybersecurity in the Western Balkans: Policy gaps and cooperation opportunities. *https://www.diplomacy.edu/sites/default/files/Cybersecurity%20in%20Western%20Balkans.pdf*

Electronic Communications, the Law on Interception of Communications, and the Law on Electronic Data and Electronic Signature.[6]

Across the criminal justice system, capacities are between start-up and formative stages of maturity in FYR Macedonia.

Currently, the Cybercrime and Digital Forensic Department within the MoI is the only unit in the country that has the capacity to investigate cybercrime cases (e.g. in mobile and computer forensics). Participants acknowledged the need to decentralise the digital forensics capacity among the different institutions; there is, however, currently no capacity to do so.

Concerning serious cybercrime cases, FYR Macedonia has no capacity to tackle those due to the lack of staff with the knowledge and skills for such investigations. As a result, the MoI has to rely on the private sector, academia and the MKD-CIRT. There is, however, some capacity to deal with less serious cybercrime cases.

The capacity of prosecutors and judges to handle cybercrime cases and cases involving digital evidence was considered by review participants to be limited and ad-hoc. Participants referred to the limited budget and the insufficient availability of technical equipment. There are no special courts for handling cybercrime cases and no specialised training for judges on cybercrime. There is, however, some ad hoc training on electronic evidence provided by the Academy for Judges and Public Prosecutors of Macedonia.

The authorities in FYR Macedonia have recognised the need to improve informal and formal cooperation mechanisms, both domestically and across borders, but these mechanisms remain ad hoc.

Standards, Organisations, and Technologies

The CMM review found no obligation to implement any national (or sector specific) ICT security standard. In addition, there is no government-led initiative to promote the exchange of good practices or to foster the implementation of cybersecurity standards.

Similarly, there is no mandatory standard for any sector related to the procurement of hardware and software. The public procurement system used to be decentralized, with each government body having its own procurement procedure,[7] however the new draft legislation on public procurement will ensure that it is centralised and executed through the e-government portal.[8] It is expected to be adopted by the end of 2018.

Focusing on standards in software development, there are guidelines in place in both the public and private sectors, but the extent to which these guidelines are related to

[6] Ibid.

[7] US Department of Commerce, Export.gov https://www.export.gov/article?id=Macedonia-Selling-to-the-Government

[8] Single National Electronic Register of Regulations of the Republic of Macedonia. Draft Law on Public Procurement.
https://ener.gov.mk/Default.aspx?item=pub_regulation&subitem=view_reg_detail&itemid=Xp2x6ms4eMDvLz1aB8J7aA==

cybersecurity is not clear. It was noted that the ICT Department at the MoI has an in-house software development team that delivers the most critical software solutions.

The country has experienced a very rapid development of telecommunications and of the information society in recent years.[9] The usage of ICT has increased significantly. Based on data provided by the State Statistical Office for 2016, 72.2 percent of the population were Internet users and 75.3 percent of households had Internet access, while the figure for enterprises with ten or more employees was 93.8 percent.[10]

There is no inventory of secure software for use in public and private sectors in FYR Macedonia. The quality and performance of software in the public sector is a concern, but functional requirements are not yet fully monitored. Users are advised to install patches, and organisations generally ensure quality of existing software.

The adoption of technical security controls in the country varies across sectors and organisations, but they are mostly ad hoc and not consistently deployed.

Cryptographic controls for protecting data at rest and in transit are recognised and deployed ad hoc by multiple stakeholders and within various sectors. Protecting data in transit is regulated under the Law on Personal Data Protection for websites/portals that contain personal data and/or require the user to log in Also, the Law on Classified Information regulates and ensures full control for protecting classified information.[11] Currently, the Directorate for Security of Classified Information (DSCI) is coordinating with a working group that is tasked with the drafting of the proposal text of the Decree on Crypto Protection.[12]

The domestic market provides limited cybersecurity technologies. No domestic market for cybercrime insurance products has yet been developed in the country.

Currently, there is a policy in place for responsible information disclosure[13] that falls under the process for incident handling. According to the policy, ‘sensitive information can be received in the MKD-CIRT through an incident report submitted by a constituent or another party that is participating in the process of incident management.’[14] A more detailed process of disclosing vulnerabilities responsibly is under development with regard to the reporting, handling and dissemination of information to other parties or to the public if a vulnerability is detected in software or on a website.

[9] Tasevski, P. (2015) Macedonian path towards cybersecurity. Information & Security, 32(2), 1.

[10] State Statistical Office. Information Society. *http://www.stat.gov.mk/OblastOpsto_en.aspx?id=27*

[11] Law on Classified Information. Directorate for Security of Classified Information. Official Gazette of the Republic of Macedonia no. 113/07.

[12] Government of the Republic of Macedonia (2017) Annual National Programme of the Republic of Macedonia for NATO membership 2017/2018. *http://www.mfa.gov.mk/images/stories/GNP/GNP-2017-2018-MNR-web.pdf*

[13] MKD-CIRT (2016) Information Disclosure Policy. Version 1.0 – 16.03.2016. https://mkd-cirt.mk/wp-content/uploads/2018/03/4-INFORMATION-DISCLOSURE-POLICY-_web.pdf

[14] Ibid.

INTRODUCTION

In collaboration with the World Bank (WB), the Global Cyber Security Capacity Centre (GCSCC, or 'the Centre') undertook a review of the maturity of cybersecurity capacity in the former Yugoslav Republic of Macedonia (FYR Macedonia) at the invitation of the Ministry of Information Society and Administration (MISA). The objective of this review was to enable the Government to gain an understanding of its cybersecurity capacity in order to provide insights for the development of the country's national cybersecurity strategy, and to strategically prioritise investment in cybersecurity capacities.

Over the period 30 January–1 February 2018, stakeholders from the following institutions participated in a three-day consultation process:

Public sector entities:

- *A*gency for Electronic Communication (AEC)
- Agency for Promotion of Entrepreneurship (APPRM)
- Agency for Real Estate Cadaster
- Cabinet of the President of the Republic of Macedonia
- Central Registry (of companies) (CRM)
- Customs administration
- Department of Cybercrime and Digital Forensics (MoI)
- Directorate for Personal Data Protection (DZLP)
- Directorate for Security of Classified Information (DBKI)
- Financial Intelligence Office (UFR)
- Financial Police (FPO)
- Food and Veterinary Agency
- Health Insurance Fund (FZO)
- Institute for Public Health (IPH)
- Insurance Supervision Agency (ISA)
- Ministry of Defence (MoD)
- Ministry of Education and Science
- Ministry of Finance (MoF)
- Ministry of Foreign Affairs
- Ministry of Health (ZDRAVSTVO)
- Ministry of Information Society and Administration (MISA)
- Ministry of Interior (MoI)
- Ministry of Justice
- Ministry of Labor and Social Policy (MTSP)
- Ministry of Transport and Communications
- National Centre for Computer Incidents Response (MKD-CIRT)
- Office of Security and Counter Intelligence (UBK)
- Public Revenue Office (UJP)
- State Audit Office (DZR)

- The Association of the Units of Local Self-Government of RM (ZELS)
- The Intelligence Agency (IA)

Criminal justice sector:

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

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 Macedonia
- Ohridska Banka AD Skopje
- ProCredit Bank Macedonia
- SPARCASSE BANK Macedonia AD
- Stopanska Banka AD Bitola
- Triglav Osiguruvanje AD
- TTK BANKA AD Skopje

Critical infrastructure owners:

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

Academia:

- Faculty of Computer Science and Engineering (FCSE) – 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 (UGD)
- 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 organisations (NGOs):

- Internet Hotline Provider Macedonia Association
- RE2020

International community:

- Croatian Embassy Skopje
- Albanian Embassy in Skopje
- International Republic Institute (IRI)

DIMENSIONS OF CYBERSECURITY CAPACITY

Consultations were premised on the GCSCC Cybersecurity Capacity Maturity Model (CMM)[15] which is composed of five distinct *dimensions* of cybersecurity capacity.

Each dimension consists of a set of factors, which describe and define what it means to possess cybersecurity capacity therein. The table below shows the five dimensions with the five dimensions together with the factors of which they are comprised:

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

[15] Global Cyber Security Capacity Centre, Cybersecurity Capacity Maturity Model for Nations (CMM) *https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cmm-revised-edition* (accessed 25 February 2018)

STAGES OF CYBERSECURITY CAPACITY MATURITY

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

Start-up: at this stage either no cybersecurity maturity exists, or it is very embryonic in nature. There might be initial discussions about cybersecurity capacity building, but no concrete actions have been taken. There is an absence of observable evidence of cybersecurity capacity at this stage.

Formative: some aspects have begun to grow and be formulated, but may be ad-hoc, disorganised, poorly defined – or simply new However, evidence of this aspect can be clearly demonstrated.

Established: the indicators of the aspect are in place, and functioning. However, there is not well thought-out consideration of the relative allocation of resources. Little trade-off decision-making has been made concerning the relative investment in this aspect. But the aspect is functional and defined.

Strategic: at this stage, choices have been made about which indicators of the aspect are important, and which are less important for the particular organisation or state. The strategic stage reflects the fact that these choices have been made, conditional upon the state’s or organisation's particular circumstances.

Dynamic: At this stage, there are clear mechanisms in place to alter strategy depending on the prevailing circumstances such as the technological sophistication of the threat environment, global conflict or a significant change in one area of concern (e.g. cybercrime or privacy). Dynamic organisations have developed methods for changing strategies in-stride. Rapid decision-making, reallocation of resources, and constant attention to the changing environment are features of this stage.

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

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

METHODOLOGY - MEASURING MATURITY

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

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

The CMM uses a focus group methodology since it offers a richer set of data compared to other qualitative approaches.[16] Like interviews, focus groups are an interactive methodology with the advantage that during the process of collecting data and information diverse viewpoints and conceptions can emerge. It is a fundamental part of the method that rather than posing questions to every interviewee, the researcher(s) should facilitate a discussion between the participants, encouraging them to adopt, defend or criticise different perspectives. [17] It is this interaction and tension that offers advantage over other methodologies, making it possible for a level of consensus to be reached among participants and for a better understanding of cybersecurity practices and capacities to be obtained.[18]

With the prior consent of participants, all sessions are recorded and transcribed. Content analysis – a systematic research methodology used to analyse qualitative data – is applied to

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

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

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

the data generated by focus groups.[19] The purpose of content analysis is to design "replicable and valid inferences from texts to the context of their use".[20]

There are three approaches to content analysis. The first is the inductive approach which is based on "open coding", meaning that the categories or themes are freely created by the researcher. In open coding, headings and notes are written in the transcripts while reading them and different categories are created to include similar notes that capture the same aspect of the phenomenon under study.[21] The process is repeated and the notes and headings are read again. The next step is to classify the categories into groups. The aim is to merge possible categories that share the same meaning.[22] Dey explains that this process categorises data as "belonging together".[23]

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

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

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

In several cases while drafting a report, desk research is necessary in order to validate and verify the results. For example, stakeholders might not be always aware of recent developments in their country, such as whether the country has signed a convention on personal data protection. The sources that can provide further information can be the official government or ministry websites, annual reports of international organisations, university websites, etc.

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

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

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

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

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

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

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

CYBERSECURITY CONTEXT IN FYR MACEDONIA

The percentage of individuals using the Internet in FYR Macedonia has grown rapidly over the past decade with 70.38 percent adoption in 2015, compared to 26.45 percent in 2005[24]. This compares to growth from 46.3 percent to 75.3 percent over the same period for the European average[25]. Such increases in adoption has led to FYR Macedonia being ranked 69th on the International Telecommunications Union (ITU) Global ICT Development Index ranking, which indicated that in 2017 there were 17.88 percent fixed (wired)-broadband subscriptions per 100 inhabitants, compared to 58.98 percent active mobile-broadband subscriptions per 100 inhabitants.[26] According to the World Economic Forum's Global Information Technology report[27], FYR Macedonia ranks 39th in the world on Affordability (including the cost of accessing ICT, either via mobile telephony or fixed broadband Internet, as well as the level of competition in the Internet and telephony sectors that determine this cost). Despite this, a recent study of the Digital Transformation of thew Western Balkans[28] found that network readiness in FYR Macedonia is below the EU average and confirms that "infrastructure, regulatory and political environment, among weakest points of digital transformation of the Western Balkans."

The Government has been active in trying to grow its internal ICT industry and attract foreign direct investment. Efforts have been made to adapt and update its telecoms legislation as part of wider plans for integration in the EU. Previous communications law (adopted in March 2005) was designed to end the monopoly of Makedonski Telekom, while also paving the way for the creation of an independent regulator, the Agency for Electronic Communications (Agencija za Elektronski Komunikacii, AEK).[29] Such attempts at opening up the market has contributed to the share of the workforce in FYR Macedonia that is employed in knowledge intensive activities to reach 26.3 percent, ranking 51st in the world.[30]

FYR Macedonia has bilateral agreements with more than ten European countries and around 20 non-European countries. Also, the country has been an aspiring member of the North

[24] ITU ICT Statistics Database http://bit.ly/2GbVuYN (what is the actual link?) https://www.google.com/publicdata/explore?ds=emi9ik86jcuic_#!ctype=l&strail=false&bcs=d&nselm=h&met_y=i99H&scale_y=lin&ind_y=false&rdim=country&idim=country:MK&ifdim=country&tstart=1108252800000&tend=1423785600000&hl=en_US&dl=en_US&ind=false

[25] ITU ICT Data for the World Time Series - https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

[26] http://www.itu.int/net4/ITU-D/idi/2017/index.html#idi2017economycard-tab&MKD

[27] WEF Global Information Technology Report 2016 http://www3.weforum.org/docs/GITR2016/WEF_GITR_Full_Report.pdf

[28] The Impact of Digital Transformation on the Western Balkans – Tackling the Challenges towards Political Stability and Economic Prosperity 2018 - https://digitalsummitwb6.com/wp-content/uploads/2018/04/Layout-Study-final-.pdf

[29] TeleGeography, GlobalComms Database – Macedonia, March 2018

[30] WEF, Networked Readiness Index. Global Information Technology Report (2016) http://reports.weforum.org/global-information-technology-report-2016/networked-readiness-index/#indicatorId=NRI.D.09

Atlantic Treaty Organization (NATO) since 2002 and taken part in International Peace Keeping missions,[31] such as joint planning, training and military exercises within the framework of the Partnership for Peace (PfP) programme and in cooperation with the NATO accredited cyber defence hub, the CCD COE.[32] Also, Macedonian representatives organised several cyber defence related workshops and trainings in Ohrid and Skopje, which were sponsored/funded by the EU and NATO. During the 2008 Bucharest Summit it was agreed that NATO will grant FYR Macedonia a membership status, once a mutually acceptable solution regarding the name issue is reached with Greece.[33] Furthermore, FYR Macedonia is currently a candidate for accession to the European Union (EU). Should FYR Macedonia be successful in this process, its accession will have significant cybersecurity implications, such as adhering to the forthcoming General Data Protection Regulation and the NIS Directive that are both pre-requisites to boosting the European Digital Single Market.[34]

[31] ITU Global Cybersecurity Index 2017 Europe *https://www.itu.int/en/ITU-D/Cybersecurity/Documents/EUR_GCIv2_report.pdf*

[32] Tasevski, P. (2015) Macedonian path towards cybersecurity. Information & Security, 32(2)/ 1.

[33] NATO (2018) Relations with the former Yugoslav Republic of Macedonia. *https://www.nato.int/cps/en/natohq/topics_48830.htm*

[34] European Comission Digital Single Market https://ec.europa.eu/commission/priorities/digital-single-market_en

REVIEW REPORT

OVERVIEW

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

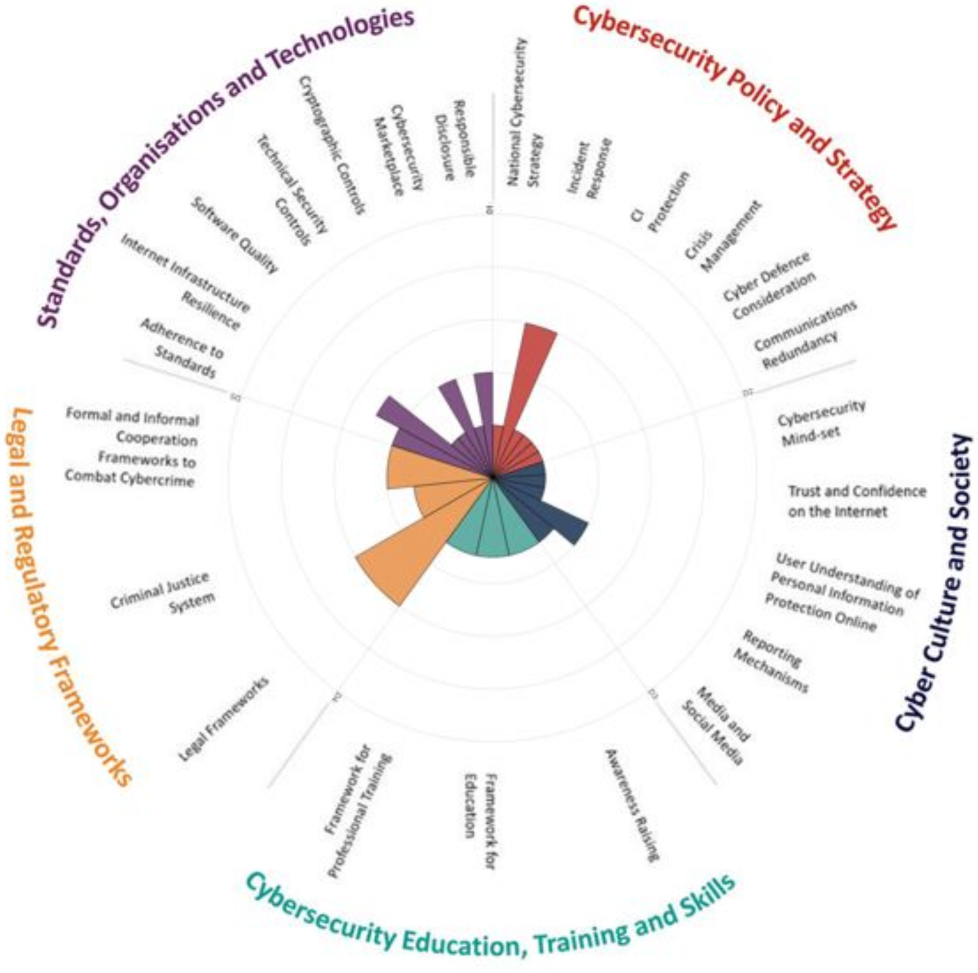

Figure 2: Overall representation of the cybersecurity capacity in FYR Macedonia

DIMENSION 1

CYBERSECURITY POLICY AND STRATEGY

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

D 1.1 NATIONAL CYBERSECURITY STRATEGY

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

Stage: Start-up

Currently, there is no official national cybersecurity document in FYR Macedonia detailing how to establish coordination between key governmental and non-governmental cybersecurity actors, nor is there an overarching national cybersecurity programme. However, consultation processes for strategy development have been initiated. The development of the cybersecurity strategy was announced in November 2017 during a high-level public debate on cybersecurity policies.

For all participants in that debate one area of concern was the limited availability of financial and human resources. Participants suggested that there is currently only a limited pool of people, both professionals and civil servants, with IT and in particular cybersecurity expertise. Moreover, the lack of financial incentives within the public sector complicates the ability to retain personnel (see also D3). For instance, MISA has no cybersecurity budget available for developing the strategy. One participant suggested allocating a small budget to host a multi-stakeholder event during the first phase of the development of the strategy, as that could drive the discussion in the right way.

National policies referring to cybersecurity are absent and ministries act in silos when identifying risks and threats. Participants acknowledged that a cybersecurity strategy tailored to the needs of FYR Macedonia is long overdue.

It is important to note that in light of the introduction of the European Union Cybersecurity Strategy (2013), the United Nations Development Programme (UNDP) offered an assessment study in preparation of the National Cybersecurity Strategy in FYR Macedonia[35] in 2014. Based on the UNDP proposal, the strategy would cover four main areas: (1) Developing and promoting the cyber defence concept; (2) Measures and activities for cybercrime suppression; (3) Establishing and improving a system for preventing cyber-attacks; (4) Managing incidents caused by cybercrime.[36] The UNDP-initiated proposal might be valuable when developing the national cybersecurity strategy in line with the EU Cybersecurity Strategy.

Currently, MISA, the Ministry of Defence (MoD), the Ministry of the Interior (MoI), the Agency for Electronic Communications (AEC), the Directorate for Personal Data Protection, and the Directorate for Security of Classified Information are collectively the driving force to improve the cybersecurity environment.[37] The plan is to develop a national cybersecurity strategy. The MoD will develop a cyber defence strategy.

Additional information: Parallel to the CMM Assessment, an informal working group consisting from members of MISA, MoI and MoD was formed. On 22 March 2018, MISA issued a formal decision to establish a national cybersecurity strategy working group, tasked to create strategic documents in the field of national cybersecurity and action plans.

In July 2018, a National Cyber Security Strategy was developed and adopted, following a public stakeholder consultation process, thereby demonstrating the country's willingness and efforts to act upon key priorities and recommendations stemming from the assessment.

These are developments after the assessment in January 2018 and are recognised as process and added here for information but do not have impact on the identified maturity stage at the time of the CMM review.

D 1.2 INCIDENT RESPONSE

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

[35] UNDP (2014) International Expert for Preparation of an Assessment Study for the Requirements for Preparation of a National Cyber Security Strategy. *https://jobs.undp.org/cj_view_job.cfm?cur_job_id=43974*

[36] Ibid.

[37] Government of the Republic of Macedonia (2017) Annual National Programme of the Republic of Macedonia for NATO membership 2017/2018. *http://www.mfa.gov.mk/images/stories/GNP/GNP-2017-2018-MNR-web.pdf*

Stage: Established

The Macedonian Computer Incident Response Team (MKD-CIRT) serves as the official national coordinating body for the reporting and management of cybersecurity incidents for the authorities and public sector institutions. In 2015, the MKD-CIRT was set up within AEC as the 'official national point of contact and coordination in dealing with security incidents in networks and information systems' pursuant to the Law on Electronic Communications.[38] The AEC (an independent regulatory body) has been responsible for regulating the electronic communications market since 2005.[39] According to the Rules on the Organisational Structure for the host organisation – the AEC – the MKD-CIRT functions as a department within AEC and has five members (one head of the department and four advisers- incident handlers and analysts).

In 2017, a Malware Information Sharing Platform (MISP) was set up by the MKD-CIRT that serves as a platform 'to share, store and correlate the indicators of compromises of targeted attacks, threats and vulnerabilities' for all public institutions, operators of critical infrastructures and large financial companies (e.g. financial, transportation, energy, communications).[40] In the same year, the website of MKD-CIRT was launched; it offers various options for reporting incidents securely via an online incident reporting form (https://mkd-cirt.mk/incident-reporting/?lang=en), fax, written correspondence or email (soc@mkd-cirt.mk).[41]

MKD-CIRT as a National CIRT maintains a registry of all reported incidents from its constituency. Constituents of MKD-CIRT include the Government of FYR Macedonia, its ministries and the state-owned and private companies that operate the critical infrastructure in the country. MKD-CIRT has an incident-classification scheme as well as incident handling and response procedures which jointly with the reporter, determine the criticality of the assets involved in the incident. Also, it is the role of MKD-CIRT to identify the level of classification of the incident. There is no obligation for mandatory reporting of incidents, but MKD-CIRT expects this to be implemented by the Government through its commitment to transpose the obligations from the EU Directive on security of network and information systems (the NIS Directive) into national legislation (e.g. amendments to existing laws or enacting a new law and subsequent bylaws or regulations).

Also, there is a newly-established FINKI-CIRT at the Faculty of Computer Science and Engineering at the Saints Cyril and Methodius University of Skopje. The FINKI-CIRT currently serves the students of the Faculty, with the plans to extend its reach toward the whole University. Currently, the point of contact with FINKI-CIRT is the official email cirt@finki.ukim.mk. The web presence and the web reporting form is in the final phase of publication.

Despite efforts by MKD-CIRT to encourage organisations to report incidents to MKD-CIRT, e.g. by conducting meetings specifically designed to explain the ways of reporting incidents and by offering tools, the review findings seem to indicate that informal channels for information

[38] Agency for Electronic Communications. MKD-CIRT. *https://mkd-cirt.mk/?lang=en*

[39] Central and Eastern European Working Group (CEERWG). Republic of Macedonia, Agency for Electronic Communications. *https://www.ceerwg.net/macedonia*

[40] Government of the Republic of Macedonia (2017) Annual National Programme of the Republic of Macedonia for NATO membership 2017/2018. *http://www.mfa.gov.mk/images/stories/GNP/GNP-2017-2018-MNR-web.pdf*

[41] Agency for Electronic Communications. MKD-CIRT. *https://mkd-cirt.mk/incident-reporting/?lang=en*

sharing between various sectors predominate. According to participants, it is faster to escalate events, request information or act on incidents through personal contacts, due to time-consuming bureaucratic processes that act to delay formal channels of communication. MKD-CIRT cooperates fully and shares information with state institutions responsible for law enforcement, such as the MoI.[42] However, participants expressed the need to improve communication channels between MKD-CIRT and the MoI and to share statistics, since often the same incidents are reported to them both. Also, participants highlighted that the private sector often prefer not to report incidents, either because they are not aware of the availability of reporting channels or because there is a lack of trust in the capability of the institutions. There is also a plan to sign an agreement in the form of a Memorandum of Understanding (MoU), between the MoI and the MKD-CIRT that will facilitate data exchange on the regularity of incidents.

Participants noted that theoretically, every incident associated with cybercrime has to be reported to the police. However, in practice, the private sector conduct a thorough analysis of these incidents before reporting them to MKD-CIRT or rarely to the MoI. In the meantime, MKD-CIRT can contact the MoI for information-sharing purposes and statistics, and can use the official channels for communication to report possible criminal activities to the MoI.

D 1.3 CRITICAL INFRASTRUCTURE (CI) PROTECTION

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

Stage: Start-up

The concept of cybersecurity in critical infrastructure (CI) is in its infancy in FYR Macedonia. National infrastructure operators have been recognised and contacted by the MKD-CIRT team, and they subsequently became constituents of MKD-CIRT (see D1.2). However, as there is no accepted definition of CI and no formal categorisation of CI assets it was not clear if these include all the relevant organisations. Therefore, the mechanisms for threat and vulnerability disclosure established by MKD-CERT, which enables interaction on cybersecurity issues with CI owners and the Government may be limited. The evidence also suggested that interaction between CI owners is not existing. According to participants, information-sharing is very ad-hoc and informal, if it takes place at all. For other sectors, such as finance, there are mainly informal channels of communication with scarce reporting of vulnerabilities and incidents.

[42] Agency for Electronic Communications. MKD-CIRT. International Regulatory Conference, 2016, Ohrid.

D 1.4 CRISIS MANAGEMENT

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

Stage: Start-up

It was not possible to obtain a clear picture regarding crisis management in the course of this CMM review. The extent to which organisations in FYR Macedonia consider cyber-threats as part of a crisis situation is therefore uncertain.

Participants noted that certain CI stakeholders, as well as organisations from the finance sector maintain business-continuity plans depending on the criticality of the system. The desk research suggests that current legislative frameworks addressing crisis management systems in FYR Macedonia are centred on the MoI, MoD, Protection and Rescue Directorate, Crisis Management Centre, Ministry of Transport and Communication, Directorate for Security of Classified Information (DSCI), Ministry of Environment and Spatial Planning, and Ministry of Administration and Information Society, when it comes to cybersecurity.[43] However, considering the complex nature of cyber threats, the lack of strategic guidelines in the documents might easily create confusion when national stakeholders have to respond and act together.[44] It is understood that general crisis management is necessary for national security, however cybersecurity is not yet considered as a component. Partially, this may be because FYR Macedonia has not experienced a major cyber-attack yet. Participants noted that the NATO Cooperative Cyber Defence Centre of Excellence provides support on an ad-hoc basis (to individual agencies) but not at the national level. However, there has been a high-level table-top exercise between MoD and MoI practicing crisis communications using systems specially designed for this.

D 1.5 CYBER DEFENCE

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

[43] Hadji-Janev, M. (2014). Toward Effective National Cyber Security Strategy: The Path Forward For Macedonia. Cyber Security and Resiliency Policy Framework. http://www.c3initiative.com/en/2016/10/12/english-toward-effective-national-cyber-security-strategy-the-path-that-macedonia-must-consider-metodi-hadji-janev/

[44] Ibid.

Stage: Start-up

Cyber defence capacity in FYR Macedonia is at a start-up stage, as cybersecurity is not currently part of the national defence strategy and there is no specific cyber defence strategy. The MoD is responsible for defence, however there is no central cyber command or control structure. Participants of the review acknowledged the need to create a new unit specifically for cyber defence.

However, there is no cybersecurity information sharing agreement with the Army of the Republic of Macedonia (Armija na Republika Makedonija: ARM). Currently, the Army's role covers a broad range of fields including to support and organize network and communication operations in military or crisis situations (by special demand from from the President of FYR Macedonia)to implement and follow NATO standards, requirements and best practices in the area of cybersecurity to protect the Army's systems. In 2017, on the 25th anniversary of the formation of the modern ARM, President Gjorgji Ivanov announced that one of the tasks of the ARM will also be 'cyber defence and electronic warfare to prevent and protect the nation's critical infrastructure in close coordination with other state institutions'[45], but these tasks have not been officially confirmed.

At the operational level, the NATO Office of Security (NOS, a NATO competent body) liaises with the Directorate for Security of Classified Information (DSCI) regarding the 'exchange and protection of classified information between the FYR Macedonia and NATO.'[46] For instance, NOS representatives perform regular inspection visits to the DSCI and registries located within ministries.[47] However, because the country is not NATO member yet, the exchange and the cooperation with NATO is limited to this extent as FYR Macedonia has no access to the NATO system nor any responsibilities to protect it.

D 1.6 COMMUNICATIONS REDUNDANCY

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

Stage: Start-up

It was not possible to obtain a clear picture regarding communications redundancy in FYR Macedonia during the review. Digital redundancy measures are considered (in an ad-hoc

[45] Bozinovski, I. (2017) 'Macedonian Army transforms for new tasks', IHS Jane's Defence Weekly *http://www.janes.com/article/73416/macedonian-army-transforms-for-new-tasks*
[46] Government of the Republic of Macedonia. Directorate for Security of Classified Information. NATO Office of Security. *http://www.dbki.gov.mk/?q=node/166*
[47] Ibid.

manner) by private telecommunication companies and other organisations, but there is nothing coordinated and systematic at the national level. Participants gave divergent views, some acknowledged that FYR Macedonia's emergency-response capabilities are inadequate, whilst others disagreed stating that a network failure does not mean that the entire infrastructure goes down. Also, there have been no exercises or drills conducted to test emergency response under circumstances with disrupted communications. Some institutions such as the MoI and MoD have Terrestrial Trunked Radio (TETRA) radio communication systems in place.

RECOMMENDATIONS

Following the information presented during the review of the maturity of *Cybersecurity Policy and Strategy*, the GCSCC has developed the following set of recommendations for consideration by the Government of FYR Macedonia. These recommendations provide advice and steps aimed to increase existing cybersecurity capacity as per the considerations of the Centre's CMM assessment. The recommendations are provided specifically for each factor.

NATIONAL CYBERSECURITY STRATEGY

R1.1 Ensure that multi-stakeholder processes are followed consistently during the development processes of the two strategies for cyber security.

R1.2 Identify and involve key stakeholder groups, including international partners, and, at minimum, the organisations which participated in the CMM review.

R1.3 Allocate budget to ensure the development and implementation of cybersecurity strategic plans. Consider including international best practices (e.g. NIS and GDPR Directives).

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

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

R1.6 Consider scenario and real-time cyber exercises to achieve a concurrent picture of national cyber resilience.

R1.7 Expand the key stakeholder group (steering committee), which is involved in the development of the national cybersecurity strategy, to include the financial sector, the private sector (including SMEs) that might be considered part of CI in the near future, as well as international partners.

INCIDENT RESPONSE

R1.8 Ensure that MKD-CIRT has the necessary financial and human resources to fulfil its existing mandate for a national cyber incident response with clear processes and defined roles and responsibilities, including:

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

R1.9 Identify and document key incident response processes[48] highlighting when and how different Ministries should be involved.

R1.10 Establish metrics to monitor and evaluate the effectiveness of MKD-CIRT.

R1.11 Establish regular training for the employees of the MKD-CIRT and design metrics to assess the results of this training.

CRITICAL INFRASTRUCTURE (CI) PROTECTION

R1.12 Develop and conduct a national risk assessment aiming to identify CI stakeholders.

R1.13 Perform regular, detailed audits of CII assets with regards to cybersecurity and disseminate CII asset audit lists to relevant stakeholders. Inform CII stakeholders of their responsibilities.

R1.14 Establish a mechanism for regular vulnerability disclosure and information sharing between CI asset owners and the government. Establish regular dialogue

[48] A collection of procedures aimed at identifying, investigating and responding to potential security incidents in a way that minimizes impact and supports rapid recovery.

between tactical and executive strategic levels regarding cyber risk practices and encourage communication among CI operators.

R1.15 Identify internal and external CI communication strategies with clear points of contact.

R1.16 Establish information protection and risk management procedures and processes within CI, supported by adequate technical security solutions, which inform the development of an incident response plan for cyber incidents.

R1.17 Establish common processes to measure and assess the capability of CI asset owners to detect, identify, respond to and recover from cyber threats.

R1.18 Task regulators for every sector to mandate disclosure of incidents. Set thresholds for the incident disclosure upon consultations with private and public organisations from the respective sectors.

CRISIS MANAGEMENT

R1.19 Design a cybersecurity needs assessment of measures and techniques for crisis management. The involvement of key stakeholders and other experts, such as think tanks, academics and civil society leaders should be sought.

R1.20 Develop a national business continuity / disaster recovery / contingency plan.

R1.21 Organise national cyber security exercises, identify metrics to evaluate the success of the exercises and ensure that lessons will inform the decision-making process for future exercises. Plan the exercises by engaging relevant participants, outlining their role in the exercise, and articulating the benefits of, and incentives for, participation.

CYBER DEFENCE

R1.22 Ensure the development of a cyber defence component in the national security strategy. This component should consider the threats to national security that might emerge from cyberspace.

R1.23 Establish cyber operation units in different branches of government and armed forces as appropriate.

R1.24 Develop a communication and coordination framework for cyber defence in response to malicious cyber-attacks on military information systems and critical infrastructure.

R1.25 Assess and determine cyber defence capability requirements, involving public and private sector stakeholders. Conduct continuous reviews of the evolving threat landscape in cybersecurity to ensure that cyber defence policies continue to meet national security objectives.

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

COMMUNICATIONS REDUNDANCY

R1.27 Allocate appropriate resources, not exclusively to activities such as hardware integration, technology stress testing, personnel training and crisis simulation drills, but also to ensuring that redundancy efforts are appropriately communicated to relevant stakeholders

R1.28 Establish a process, involving all relevant stakeholders, to identify gaps and overlaps in emergency response asset communications and authority links.

R1.29 Link all emergency response assets into a national emergency communication network with isolated but accessible backup systems.

R1.30 Establish communication channels across emergency response functions, geographic areas of responsibility, public and private responders, and command authorities. Create outreach and education activities of redundant communications protocols tailored to the roles and responsibilities of each organisation in the emergency response plan.

R1.31 Allocate cybersecurity exercise planning to a relevant authority. Conduct and test a needs assessment of measures with consideration of a simple exercise scenario. Since emergency exercises exist, as a first step include cyber elements within one of these scenarios.

R1.32 Identify metrics to evaluate the success of the exercise. Evaluate the exercises and feed the findings back into the decision-making process.

DIMENSION 2

CYBERSECURITY CULTURE AND SOCIETY

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

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

D 2.1 CYBERSECURITY MIND-SET

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

Stage: Start-up

The cyber ecosystem in FYR Macedonia is still in its early stages. Participants described that in some government agencies and leading companies a cybersecurity mind-set has started to develop but the cybersecurity culture is generally not very advanced and users are often not aware of the risks associated with the use of Internet.

The Government has recognised the need to prioritise cybersecurity across the public sector. Leading government agencies such as MISA and the other Ministries involved in the informal working group that is drafting a national cybersecurity strategy (see D1.1), have advocated a cybersecurity mind-set. Participants also noted that there is an increased level of awareness and efforts to tackle cybersecurity, data protection, and critical national infrastructure protection. However, it has not yet become a high priority despite the requirements of the EU and NATO membership processes and their legal and regulatory requirements. Participants noted that the country faces problems regarding cybersecurity that are similar to other European countries, but they also acknowledged that the implementation of initiatives has been a major challenge and that the political will to implement change across the Government is often missing. The assessment was seen as very useful element to create awareness for cybersecurity on the political agenda.

Overall, the general awareness for cybersecurity within government agencies remains still very low. Participants noted that it also varies across hierarchical levels: whereas the IT departments and those employees with responsibilities regarding cybersecurity have already developed a cybersecurity mind-set, there has been a lack of awareness for the risks and threats originating from cyber space at the top executive levels. A general concern was expressed that there is a lack of cybersecurity knowledge at the highest levels of government. This is seen as an obstacle for the implementation of initiatives in this regard and of cybersecurity capacity-building efforts overall. In line with this, participants mentioned that top management perceives cybersecurity expenditures most often as a cost rather than as a necessary investment to ensure network and data security. Concerns were raised over the routine use of private emails by staff across public institutions for official correspondence. IT experts are generally available in the country but they tend not to move into the public sector due to the lack of financial incentives and often seek employment opportunities in other European countries. Hence, the national, relatively low level of a cybersecurity mind-set is in large part also an institutional problem.

The public sector is not well prepared to establish secure networks and only a few institutions have the necessary know-how to secure their own websites. It was not clear from the consultations of any specific incidents against government networks or services. However, in 2017, the government server was hacked by Yemenite *Rxr*, which defaced the websites of major government agencies and a municipality that are hosted on the server. It was not clear how the incident was solved and what impact it had on the security of the government server and the services running on it but participants brought it up as an example of an cyber incident.

In contrast, most participants agreed that in the private sector (especially major telecommunication providers and international ICT companies, as well as financial institutions) the general understanding of cybersecurity risks and protective measures is further advanced than in public sector institutions. Also, in the ICT sector, which is a growing sector in FYR Macedonia and which has attracted a number of international companies to do business in the country, there is a stronger mind-set regarding cybersecurity. However, domestic small and medium enterprises (SMEs) often do not have a cybersecurity mind-set or do not have the human capacity or the resources to invest sufficiently into cybersecurity, even if they are aware of the risks and threats for their businesses. Participants mentioned that a study (which was not available to the researchers) found that many businesses' websites – as in the public sector – are not secured and represent a risk to the companies itself.

Much like most of the public and private sector entities, Internet users have generally low levels of awareness of cybersecurity risks and best practices for secure online behaviour. Cybersecurity has not yet filtered into the daily lives of citizens who engage with Internet routinely via computer from home (69.5 percent) or smart phone applications[49] and social media (according to Internet World Stats, almost 50 percent of the population use Facebook[50]*)*. According to participants, the majority of users do not understand the risks associated with being online. The result is that users generally, including those with more technical knowledge, higher level of education or younger age, do not handle passwords and personal identification numbers (PINs) securely, but as a matter of convenience (e.g. using the same password for different purposes or sharing the PINs and passwords). Users also tend to share their personal information online via social media. The result is that not only children, who are generally vulnerable to cybercrime, but women, in particular, are regularly exposed to online safety challenges (e.g. cyberbullying, harassment, cyberstalking, body shaming, rape threats and revenge pornography). Participants attributed this to a general lack of security consciousness and awareness among Internet users that have not been developed yet. On the other it is a problem, that users are either not aware that they have become a victim of cybercrime or do not perceive the event as a crime, such as in the case of cyberbullying.

However, people in FYR Macedonia place a high priority on security when using online banking and credit cards for online shopping. Participants attributed this discrepancy to the materials that banks provide customers when they start online banking, which makes them aware of the risk. However, these efforts were sector-specific and not deployed across the private sector as a whole.

The current Government was formed after the election of 2016. This change in government was the result of a political crisis[51] that emerged after it had become public that the Macedonian Administration for Security and Counterintelligence and senior government ministers were associated in illegal telephone and Internet surveillance of journalists, NGOs, politicians, and other individuals in the country, and that government officials were also involved in financial crimes. It was not possible to obtain a clear picture how the scandal had an impact on public opinion and the use of Internet services by users. But participants suggested that this most likely has an impact on the stakeholders' online behaviour of those who were the targets of surveillance as well as having an impact on citizens' perceptions of, and trust in, e-governance services (see below).

[49] IPA.sa. (2018). Country Profile Macedonia [online] Available at: https://beta.iph.sa/country-profile/MK [Accessed 4 Mar. 2018].

[50] Internetworldstats.com. (2018). Internet in Europe Stats [online] Available at: https://www.internetworldstats.com/stats4.htm#europe [Accessed 4 Mar. 2018].

[51] ComputerWeekly.com. (2018). The Macedonian surveillance scandal that brought down a government. [online] Available at: http://www.computerweekly.com/feature/The-Macedonian-surveillance-scandal-that-brought-down-a-government [Accessed 4 Mar. 2018].

D 2.2 TRUST AND CONFIDENCE ON THE INTERNET

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

Stage: Start-up

The majority of Internet users in FYR Macedonia tend to 'blindly' trust ICT and Internet services. Participants believed that users are largely unaware of cybersecurity risks when using Internet and assume that they have the confidence to use online services without undue risk. However, most users are perceived not to have the ability to critically assess content they see and receive online, nor the applications they use. Among the concerns raised by the participants were some cases when users were aware of the risks, because of cases of cybercrime, cyberbullying, or data breaches, but they nevertheless failed to take the necessary security measures to protect themselves, largely due to such actions being seen as inconvenient.

Moreover, Internet service providers (ISPs) are not seen by the participants to be taking adequate measures in a strategic way to promote trust in online services known to the participants.

E-government services for citizens and businesses have been partially implemented for about ten years but they are still limited relative to the policy ambitions. A regional study indicates that there are many individual government projects, but there is a lack of effective strategies and coordination activities among government agencies to build capacity from these initiatives.[52] According to the participants, the majority of Macedonians are not even aware that e-government services exist.

The trust levels around existing services still need to be assessed, but some assume that there is a general trust in those services as suppliers from the private sector need to go through certification. However, the authors found that in a comparative analysis of e-government and open government services in the Western Balkan region that was published in 2015 [53], FYR Macedonia performed below the average on e-government, compared to its neighbours. The authors noted that there is resistance among citizens to use the services due to the lack of trust in their security.[54]

[52] E-Government Analysis; From E- to Open Government. (2015). [ebook] Danilovgrad: Regional School of Public Administratio. Available at: https://respaweb.eu/download/doc/eGov+-+From+E-Government+to+Open+Government.pdf/d3ab1cd43fa4cd3071be9cea7e4b0cd3.pdf [Accessed 15 Mar. 2018].

[53] Adriana Minović , Adel Abusara, Eranda Begaj, Vladimir Erceg, Predrag Tasevski, Vladimir Radunović, Franziska Klopfer (2016). Cybersecurity in the Western Balkans: Policy gaps and cooperation opportunities. [online] Geneva: DiploFoundation. Available at: https://www.diplomacy.edu/sites/default/files/Cybersecurity%20in%20Western%20Balkans.pdf [Accessed 7 Mar. 2018].

[54] E-Government Analysis; From E- to Open Government. (2015). [ebook] Danilovgrad: Regional School of Public Administratio. Available at: https://respaweb.eu/download/doc/eGov+-+From+E-Government+to+Open+Government.pdf/d3ab1cd43fa4cd3071be9cea7e4b0cd3.pdf [Accessed 15 Mar. 2018].

Some e-government services for businesses have been established, such as the portal https://e-presudi.finance.gov.mk provided by the MoF. This portal is a database of court decisions in the field of taxes and customs. The main goal is to provide information in a simple and friendly manner regarding court decisions and opinions. The MoF's Customs Administration which provides, among other services, a system to process declarations, to exchange information between the European Commission and EU Member States, and a single window system for import, export and transit licenses and tariff quota (http://www.customs.gov.mk/index.php/en/e-carina-2). The Agency for Real Estate Cadastre offers a detailed online map of properties in the country (https://ossp.katastar.gov.mk/OSSP/faces/public/customMaps/parcelSearch.xhtml). [55] Also the Public Procurement Bureau under the MoF offers an online system (https://e-nabavki.gov.mk/PublicAccess/Home.aspx#/home), which enables conducting public procurements in an electronic form and electronic trading between contracting authorities in FYR Macedonia and domestic and foreign economic operators.

The citizen-oriented e-government services are more limited. A national e-health service called *MojTermin* (My Time; http://mojtermin.mk/) is a key part of public and private health care allowing patients to book appointments online and receive text message reminders. Medical staff can see referrals, prescriptions and requests in real time. *MojTermin* also integrates electronic health records and health cards.[56] According to participants, citizens will be able to submit their tax declaration online via a portal created by the MoF.

Beyond that, 27 institutions publish data sets on MISA's Open Government Data Portal (http://www.otvorenipodatoci.gov.mk/Templates/Pages/StartPage.aspx?page=13), which makes the country the most advanced in the region.

In contrast, e-commerce services, both from international and domestic vendors are provided and used at a larger scale. International companies such as eBay and Amazon[57] offer their services and there are also popular domestic e-commerce companies. One of the most successful start-up companies in FYR Macedonia is an online shopping website. However, participants noted that consumers still prefer seeing the products they buy in person or only trust specific platforms, such as the international platforms and brands. This assumption is confirmed in the Macedonia Country Commercial Guide (https://www.export.gov/article?id=Macedonia-ECommerce). A slightly different situation exists for e-banking services, which are more widely used. Participants suggested that the security settings/processes, like authentication steps and double/triple check contributed to their use, rather trust in those services. Participants mentioned that banks inform new customers about security solutions and the terms and conditions at the beginning of their relationship.

[55] Katastar.gov.mk. (2018). Agency for Real Estate Cadastre. [online] Available at: http://www.katastar.gov.mk/en/home/# [Accessed 4 Mar. 2018].

[56] Euro.who.int. (2018). E-health in practice. [online] Available at: http://www.euro.who.int/en/countries/the-former-yugoslav-republic-of-macedonia/news/news/2016/03/e-health-in-practice [Accessed 4 Mar. 2018].

[57] Amazon.co.uk. (2018). Amazon.co.uk Help: International Delivery Rates & Times. [online] Available at: https://www.amazon.co.uk/gp/help/customer/display.html?nodeId=11072981#GUID-4B07A895-53A8-4B77-97A4-D950DC206246__SECTION_081DCDC3ABFA40E79AEA07A853F85713 [Accessed 4 Mar. 2018].

D 2.3 USER UNDERSTANDING OF PERSONAL INFORMATION PROTECTION ONLINE

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

Stage: Start-up

Awareness around the protection of personal information and security concerns regarding personal data is generally low. As mentioned above, participants noted that personal information is often shared through social media, in particular Facebook, and users are not aware to which degree that sensitive personal information should be kept private, such as images of children or themselves which they share publically or with their partners. Therefore, only a minority of users employ what are deemed to be good cybersecurity practices when using social media and online services. On the other hand, a study found that lack of trust in privacy and data protection is one of the barriers to the use of e-government services (see above). Participants attributed this to the increasing consciousness among users and stakeholders in the public and private sectors of cyber risks regarding personal data. An increasing proportion of users have started to employ cybersecurity practices in response to the increase in reporting in the media and awareness campaigns, according to participants. There is no public debate over the issue, but the discussions take place among those who are generally well informed.

D 2.4 REPORTING MECHANISMS

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

Stage: Formative

Participants mentioned that there are some channels for users in place in order to report computer-related or online incidents and crimes: e.g. (1) every police station in person or via phone, (2) the cybercrime unit at the MoI, and (3) the Directorate of Personal Data Protection in the case of a data abuse. On its website the Directorate informs citizens about protection of personal rights they have. For instance, they can make a “Request for confirming violation of the right of the right of personal data protection”.[58]

[58] Dzlp.mk. (2018). Your rights | Дирекција за заштита на личните податоци. [online] Available at: https://dzlp.mk/en/node/2201 [Accessed 19 Mar. 2018].

The MoI offers phone numbers for the citizens to report any computer crime directly to the Department of Cybercrime and Digital Forensics and also to any police station. The MoI has set up the Red Button (http://redbutton.mvr.gov.mk/) reporting scheme on its website, however it has limitations because citizens can only report crimes related to online child sexual abuse and hate speech online (http://www.govornaomraza.mk/). Also, there is the possibility to report cybercrime to the MoI via email (cybercrime@moi.gov.mk). However, if the perpetrator is not from FYR Macedonia, the MoI cannot prosecute them, but they can be detected and the MOI can inform the authorities of the foreign country where the criminal is based.[59] In 2017, the Computer Crime and Digital Forensics Unit within the MoI received five requests and eight requests until April 2018. Statistics are available regarding the usage of the Red Button reporting scheme, and also regarding how many cases were reported directly to the Department of Cybercrime and Digital Forensics. Also, on the website of MKD-CIRT (https://mkd-cirt.mk/incident-reporting/?lang=en) there is a possibility to report incidents.

Participants noted, however, that users are not aware of these channels or they face challenges providing evidence. Due to the nature and characteristics of cybercrime cases, in most cases it is important for electronic evidence to be delivered fast, so that no loss or damage would occur. Therefore, current legislation requires that material evidence or electronic evidence be provided the same day. However, this is often not possible and victims, often women, are thwarted to report because of this requirement. Also, there is no online reporting systems which allow users in all parts of the country to report incidents. A participant also mentioned that victims tend to contact NGOs if they are aware of the latter working in the field of cybersecurity. A website with support from the European Commission's Safer Internet Initiative for awareness raising but also for reporting incidents is pending for implementation, as it requires the formal agreement by the Government to receive the required funding from the initiative. However, this is an informal channel and not a nation-wide way to report cybercrimes. Discussions around establishing of such mechanisms on the national level have taken place, e.g. as part of the MC4 cybercrime centre, but so far, the discussions have been ad-hoc and the issues have not been prioritised on the political level.

Within the private sector, banks usually have a reporting mechanism in place as part of their customer service. But not one was specifically identified by participants.

[59] Akademik (2014) 'МВР апелира до граѓаните: Ако забележите педофилија на интернет – пријавете на cybercrime@ moi.gov.mk', *https://www.akademik.mk/mvr-apelira-do-graganite-ako-zabelezhite-pedofilija-na-internet-prijavete-na-cybercrime-moi-gov-mk-4/*

D 2.5 MEDIA AND SOCIAL MEDIA

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

Stage: Start-up – Formative

In FYR Macedonia, cybersecurity issues overall are insufficiently reported in media both online and offline. If reporting is taking place, then it is completed mostly in the case of major international events. Traditional media more seldom provide coverage on cybersecurity compared to social media where issues around cybersecurity are discussed more frequently. One university organises faked phishing attacks on a regular basis to raise awareness among students. These incidents are usually picked up by the students and discussed on social media platforms. Participants considered the lack of knowledge and interest in cybersecurity among the general public to be one of the main reasons for minimal media coverage of the topic. There was consensus that media and social media should play a major role in raising cybersecurity awareness.

RECOMMENDATIONS

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

CYBERSECURITY MIND-SET

R2.1 Intensify efforts in leading government agencies to prioritise cybersecurity and enhance efforts at all levels of government and across ministries to promote understanding of cyber risks and threats.

R2.2 Design coordinated training programmes for employees in the public organisations in cooperation with the private sector. Trainings should include:

a) web security (e.g. protection of personal information online, social media, social engineering, secure web browsing, malware, passwords)
b) email security (e.g. identify a phishing email, sending an email securely)
c) data security (e.g. handling and classifying sensitive information, back-up and recovery)

d) mobile device security (e.g. portable data storage)
e) remote access security (e.g. working from home/while travelling)

R2.3 Consider educating the public on the nature and consequences of cybercrime in FYR Macedonia.

R2.4 Consider in collaboration with the NGOs providing youth social programmes (e.g. in schools and universities) that will teach them about the safe and responsible behaviour online (e.g. the risks of using social media) and how to prevent any uncompromising behaviour.

R2.5 Consider setting up a multi-stakeholder group (including business, government, law enforcement agencies, and academia) to run joint projects and initiatives as well as facilitate ongoing discussions on cybercrime and cybersecurity issues.

R2.6 Design online programmes and training materials (e.g. cybersecurity best practices, cyber threat landscape in FYR Macedonia, risk management) in consultation with the multi-stakeholder group and make them freely accessible for the public in order to equip them with the right skills needed for their everyday use of the Internet and online services.

R2.7 Identify vulnerable groups and high-risk behaviour across the public, in particular children and women, to inform targeted, coordinated awareness campaigns, as recommended in R3.1.

R2.8 Promote prioritisation of risk and threat understanding for private sector entities by identifying high-risk practices.

R2.9 Enhance efforts in the private sector, in particular telecommunication and e-commerce services to employ cybersecurity good (proactive) practices.

R2.10 Consider designing a guide book specifically for SMEs in cooperation with leading firms in order to help become less vulnerable to cybercrime, given that budgets are often tight (e.g. application of certain restrictions, strong passwords, installation of latest security patches, back up data).

R2.11 Promote the sharing of information on incidents and best practices among organisations and across sectors to promote a proactive cybersecurity mind-set.

TRUST AND CONFIDENCE ON THE INTERNET

R2.12 Consider involving celebrities to educate the public via social media about the safe and responsible use of Internet and online services (e.g. sharing videos of celebrities -actors, singers, football players- on social media platforms demonstrating how they protect their information/privacy online).

Content of the video could be, for instance, telling a story about how the celebrity became a victim of online fraud and cybercrime, what were the consequences and what protective measure she/he takes in order to prevent this from happening again.

R2.13 When introducing e-government services for citizens, implement security measures from the beginning to build trust and uptake by citizens, companies, and other users.

R2.14 When introducing e-government services for citizens promote their use through a coordinated programme, including the compliance to web standards that protect the anonymity of users.

R2.15 Employ processes for gathering user feedback within government agencies in order to ensure efficient management of online content.

R2.16 Ensure that security measures are in place for existing e-government services for businesses and public organisations.

R2.17 Encourage government leaders to use social media (e.g. Facebook, Twitter, YouTube, Instagram) and promote the use of e-government services on their social media profiles in a fun and creative way, such as through videos and infographics. Users are more likely to use e-government services if politicians/leaders use social media responsibly.

R2.18 Encourage government leaders to engage with the public via social media channels in order to create trust and show that they act in public interest. These platforms can be used in an efficient way to communicate their message and demonstrate their commitment to giving back to the communities.

R2.19 Consider educating the public by developing an effective Cybersecurity Communication Strategy/Plan (e.g. strategic approach to cyber crises, promoting the benefits of using e-government services and suggesting deadlines to register).

R2.20 Promote the implementation of user-consent policies by Internet operators.

R2.21 Encourage ISPs to establish programmes that promote trust in their services based on measures of effectiveness of these programmes.

R2.22 To promote trust of users in e-services inform users about the utility of deployed security solutions.

R2.23 Encourage the development of e-commerce services with emphasising the need for a security (e.g. use of SSL encryption, post trust certificates/logos of third-party authentication services on the homepage).

R2.24 Encourage chief executive officers (CEOs) of companies to use social media platforms in order to create trust with their customers and increase transparency. Customers are more likely to use e-commerce services and products if the CEO of their preferred brand uses social media.

R2.25 Ensure that the private sector apply security measures to establish trust in e-commerce services, including informing users of the utility of deployed security solutions.

R2.26 Encourage users to access the terms and conditions for using e-commerce services.

R2.27 To promote trust of customers in e-commerce services post customer reviews (both good and bad) and testimonials.

USER UNDERSTANDING OF PERSONAL INFORMATION PROTECTION ONLINE

R2.28 Continue programmes in cooperation with NGOs and support existing efforts by stakeholders to raise user awareness of online risks. Promote measures available to protect privacy and enable users to make informed decisions when and how they share their personal information online.

R2.29 Encourage a public debate on social media platforms and in the traditional media (TV and print) regarding the protection of personal information and about the balance between security and privacy to inform policymaking.

R2.30 Develop a Code of Practice on Protecting Personal Information Online in consultation with multiple stakeholders that can be distributed within the public (e.g. in primary and secondary schools).

REPORTING MECHANISMS

R2.31 Establish coordinated mechanisms within the public and the private sector allowing citizens to report cybercrime cases, including online fraud, cyberbullying, child abuse online, identify theft, privacy and security breaches, and other incidents, in particular affecting women and other vulnerable groups.

R2.32 Provide manuals to educate the public, teachers and parents about the types of cybercrime that can be reported, how to exercise their rights when falling victim to such crimes and how to report it.

R2.33 Raise awareness about new and existing reporting channels among the wider public and across stakeholder groups and cooperate with the private sector in this regard.

R2.34 Set up a website for the Cybercrime Unit at the MoI where victims of cybercrime would be able to report to the police by choosing different options: 1) dialling a number in case it is an emergency or the crime is in progress 2) completing an online form for non-emergency crimes or reporting via email. It is important that all reporting channels should offer the victim the option to report anonymously (e.g. anonymous online forms).

R2.35 Consider establishing the Cybercrime Unit of the MoI as the national fraud and cybercrime reporting centre, providing a central point of contact for citizens and businesses.

R2.36 Consider establishing secure two-way information sharing between the Cybercrime Unit and the commanders in different regions/municipalities.

MEDIA AND SOCIAL MEDIA

R2.37 In cooperation with civil society and media organisations develop programmes and campaigns to raise awareness among media providers and leading social media actors, for instance during the dedicated Safer Internet Day or the Cybersecurity Awareness Month (October) or dedicated web or social media sites on this topic (see also R3.1).

R2.38 Enhance the understanding of cybersecurity among media providers (e.g. journalists and editors) and facilitate a more active role of media in conveying information about cybersecurity to the public.

R2.39 Encourage media content providers to disseminate information on good (proactive) cybersecurity practices that users can pursue to protect themselves or to respond to cyber incidents. This could stimulate social media discussions on the topic.

DIMENSION 3
CYBERSECURITY EDUCATION, TRAINING AND SKILLS

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

D 3.1 AWARENESS RAISING

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

Stage: Start-up - formative

A national programme for cybersecurity awareness raising, led by a designated organisation (from any sector) which addresses a wide range of demographics is yet to be established. A proposal by a civil society organisation for the establishment of a Cybersecurity Centre with such a respective mandate was proposed to the previous and current government but has not been implemented, according to a participant.

According to the participants, cybersecurity awareness raising efforts are mostly sporadic and not centrally coordinated. However, FYR Macedonia has been engaged in the EU's Safer Internet Day initiative since 2010. The initiative, which is driven by the European Commission, aims to increase awareness of the problems that can arise when using Internet; the initiative organises various events and activities that promote proper use of Internet. The activities are mostly led by NGOs such as the Insafe / INHOPE network, but also universities like the University of Skopje (Faculty of Computer Science and Engineering). The line ministries have done awareness raising, too.[60] A participant mentioned that the engagement by the Government has not reached in recent years the higher levels of public sector decision makers; the efforts are mostly done on a voluntarily basis and with limited resources. However, it is also possible that due to the lack of a national awareness programme, initiatives are not known across stakeholder groups. The private sector offered free cybersecurity courses for personnel in public institutions, which was perceived as very useful by participants. MISA cooperated with UNICEF and universities to conduct campaigns, which targeted school children, but this was a one-off effort. Everyone agreed that this kind of campaign should be repeated on an annual basis.

Another stakeholder in cybersecurity awareness raising is the Metamorphosis Foundation, which conducts awareness raising efforts around personal data protection, in cooperation with the Directorate for Personal Data Protection and with support of the European Union (http://www.crisp.org.mk).

According to the participants, telecommunications companies and banks integrate cybersecurity messages in the contract documents for customers and also offer free trials of security software. Several banks also ran cybersecurity awareness campaigns in their major branches across the country throughout 2017.

Regarding cybersecurity awareness raising efforts for executives, some international companies, mostly informed by their headquarters, undertake some initiatives across all hierarchy levels, but it is not a strategic approach. In 2016, some banks started annual trainings aimed at CEOs, as these banks' leadership is perceived to be most likely be a target of a cyber-attack (e.g. through spear phishing).

Overall, there was a consensus among the participants that current awareness raising efforts in the country are not sufficient and that their outreach is too small. To raise the awareness of cybersecurity to a significant extent, a national approach is needed.

D 3.2 FRAMEWORK FOR EDUCATION

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

Stage: Start-up - Formative

The need for enhancing cybersecurity education in schools and universities has been identified by the Government, in particular in the line Ministry (MISA), industry, and academic

[60] Netsafe.finki.ukim.mk. (2018). Ден на безбеден интернет. [online] Available at: http://netsafe.finki.ukim.mk/ [Accessed 19 Mar. 2018].

stakeholders. On the university level, the University Ss. Cyril and Methodius (UKIM) offers cybersecurity related mandatory and elective courses (e.g. in Computer Security and Protection, Security and Cryptography, Computer Systems Security, and Network Security) on 3 levels of education (ie. undergraduate, graduate, and post-graduate/doctoral). In addition, FCSE is part of regional and pan-European projects tackling the topics in cybersecurity, such as GEANT (https://www.geant.org/), Enhancing Cyber Security (https://www.observatoire-fic.com/contribution-enhancing-cyber-security-the-challenges-in-fyrom-kosovo-and-moldova/), etc.

Overall, the uptake of these courses is relatively good among computer science students (up to 50% of all) and also students in related subjects such as engineering show some interest in the subject matter. Several doctoral students have dedicated their theses to cybersecurity topics. Additionally, the Macedonian Military Academy has offered a multi-disciplinary cybersecurity programme since 2013, in cooperation with a university in the U.S.[61] It is in discussion with other universities to extend their current programme. Beyond that, the Academy offers courses on a doctoral level focusing on cybersecurity and critical infrastructure protection, and cybersecurity courses for non-IT experts.

The participants of different sessions of the review were either not aware of the above offerings, despite their existence, or thought that a coherent government approach to cybersecurity education is missing. The latter was explained as arising from insufficient autonomy of the universities, which affects their ability to plan and disburse financial allocations.

There is a regular information exchange between education institutions and the private sector in order to respond to market needs. However, it is mainly driven by a requirement imposed by the law, according to which involve government and private sector should be involved in the accreditation process of a course.

The review participants expressed a concern that there is a lack of cybersecurity education at the primary and secondary level, while there is increase in school children accessing Internet frequently. However, despite IT courses being offered, cybersecurity has not been integrated in the curricula of primary and secondary school yet. A problem is that although the Ministry of Education has the authority for education, there are separate departments for primary, secondary and tertiary education with separate curricula policy development. There is no horizontal coordination regarding ICT and IS nor any dedicated budget.

It was not clear from the review whether there are enough cybersecurity educators in the country or which qualification programmes are in place for them. On the university level, there are several professors in the cybersecurity field who publish research on cybersecurity issues and present their work at international events. Experts from the industry are regularly invited as visiting lecturers. However, on a school level there is notable lack of educators to teach school children the basics of cybersecurity.

[61] Macedonian News Agency | Kurir.mk. (2018). Macedonia first in SEE introduced platform for cyber defense of the Military Academy - Macedonian News Agency | Kurir.mk. [online] Available at: http://kurir.mk/en/?p=13338 [Accessed 19 Mar. 2018].

D 3.3 FRAMEWORK FOR PROFESSIONAL TRAINING

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

Stage: Start-up to Formative

The need for training professionals in cybersecurity has been recognised by the Government but has not been documented on the national level. Within public institutions, training on cybersecurity issues both for IT staff and general staff is quite limited and it often depends on the respective management in the institution whether a specific member of staff can attend a general cybersecurity training or certification course. Also, many IT positions do not require specific professional certificates that would validate the ability of a job-seeker to perform the job. Participants suggested that this might change with the adoption of the EU NIS Directive.

In the private sector, training is more integrated and sometimes mandatory for IT staff and also general staff in some companies. The review participants mentioned that mechanisms are in place to ensure that the knowledge gained in such courses is transferred within the organisation. However, they noted that it is challenging for many companies to convince the decision makers that training and certification is a continuous task. According to them, a driver for more regular trainings regarding cybersecurity is regulation, as it increases the awareness on the management levels. Insurances were given as an example where regulation asks for bottom-up information chains. The regulation resulted in better communication and trust between management and IT personnel and also contributed to an attitude that it is important to be more cybersecure.

The high costs for training courses are seen as a major obstacle for both institutions and individuals to pursue cybersecurity certifications, and the incentives are lacking as certifications are not a requirement or part of the job description expected by some sectors, such as the banking sector. Often the training is ad-hoc, when a new project is implemented.

Cooperation of universities with the private sector, e.g. ISP and vendors such as Microsoft and Cisco, does take place in the form of certification courses for students and of establishment of labs to allow hands-on exercise for students. However, to receive the actual certification students have to complete and pay for the actual exam. The additional fees became a reason to discontinue a cooperation with Semos education, a private organisation which offers ethical hacking training. Cooperation with the public sector exists to the extent that members share their experiences in lectures organized at the university level.

The participants assumed that the transposition of the General Data Protection Regulation (GDPR), which requires Data Protection Officers in every institution, and of the EU NIS Directive will have a large impact on the training offerings, not only related to data protection but also to cybersecurity, in general, as certification will become a requirement.

A general problem, as mentioned earlier, is that qualified IT staff often leave for other European countries because of the better job prospects, which hollows out the supply in qualified IT staff, both with general IT knowledge and also those with cybersecurity expertise.

RECOMMENDATIONS

Following the information presented on the review of the maturity of *cybersecurity education, training and skills*, the following set of recommendations are provided to the Government of FYR Macedonia. These recommendations aim to provide advice and steps to be followed for the enhancement of existing cybersecurity capacity, following the considerations of the GCSCC CMM assessment.

AWARENESS RAISING

R3.1 Appoint a dedicated organisation with a mandate to develop and implement a planned national cybersecurity awareness-raising programme. Coordinate and cooperate with key stakeholders, in particular those who participated in the review, representing private sector, civil society, and international partners.

R3.2 Implement a national portal to disseminate materials for various target groups. Ensure aligning of this effort with existing platforms to avoid duplication.

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

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

R3.5 Establish metrics and ensure that evidence of application and lessons learnt feed into existing and newly-developed programmes.

R3.6 Develop a dedicated awareness-raising programme for executive managers within the public and private sectors, as this group is usually the final arbiters on investments into security.

R3.7 It is suggested that the one-off campaign by MISA, UNICEF and universities targeting school children, be repeated annually.

FRAMEWORK FOR EDUCATION

R3.8 Develop qualification programmes for cybersecurity educators and start building a cadre of existing and new professional educators to ensure that skilled staff are available to teach newly-formed and existing cybersecurity courses.

R3.9 Integrate specialised cybersecurity courses in all computer science degrees at universities and offer specialised cybersecurity courses in universities and other higher education bodies.

R3.10 Create cybersecurity education programmes for non-cybersecurity experts and make them available at universities and other higher education bodies.

R3.11 Collect and evaluate feedback from existing students for further development and enhancement of cybersecurity course offerings.

R3.12 Develop partnerships for the development of interfaces for research, innovation and interaction between universities and the private sector.

R3.13 Create initiatives to advance cybersecurity education in the primary and secondary school curricula.

FRAMEWORK FOR PROFESSIONAL TRAINING

R3.14 Identify training needs and develop training courses, seminars and online resources for targeted demographics, including non-IT professionals. Cooperate with the private sector to develop those offerings.

R3.15 Provide training for experts on various aspects of cybersecurity, such as technical training in data systems, tools, models, and operation of these tools.

R3.16 Create a knowledge exchange programme targeted at enhanced cooperation between training providers and academia.

R3.17 Establish continuous training for IT employees and general employees regarding cybersecurity issues.

R3.18 Advance the role and importance of cybersecurity certification in IT job categories, including possible regulation to this effect such as requirements for specific job roles.

R3.19 Consider subsidizing the high cost of training and certification courses for trainees.

R3.20 Create incentives for cybersecurity experts to stay in the country and get more involved in cybersecurity matters, including creating a business environment which fosters innovation and entrepreneurship.

DIMENSION 4
LEGAL AND REGULATORY FRAMEWORKS

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

D 4.1 LEGAL FRAMEWORKS

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

Stage: Established

Comprehensive ICT legislative and regulatory frameworks addressing cybersecurity have been implemented and legislation protecting the rights of individuals and organisations in the digital environment has been adopted in FYR Macedonia.

The first step was taken in 2004 when FYR Macedonia ratified the Budapest Convention on Cybercrime. [62] The following year, the country ratified an Additional Protocol to the Convention on Cybercrime concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems.[63]

The most relevant legislative frameworks related to FYR Macedonia's Internet landscape are:

[62] Council of Europe (2001) Convention on Cybercrime, 23 November 2001. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

[63] Council of Europe (2006) Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189

- the Criminal Code[64] (1996, last time amended in 2013)
- the Law on Criminal Procedure[65] (Criminal Procedure Code)
- the Law on Electronic Communications[66]
- the Law on Communications Monitoring[67]
- the Law on Electronic Commerce[68]
- the Law on Electronic Management[69]
- the Code of Civil Procedure[70]
- the Law on Electronic Data Form and Electronic Signature[71]
- the Law on Personal Data Protection[72]
- the Law on Interception of Communications[73]
- the Law on Litigation[74]
- the Law on Classified Information[75]

FYR Macedonia does not have an all-encompassing legal framework that deals explicitly with cybersecurity.[76] However, several legal instruments refer to cybersecurity-related issues such as the Law on Personal Data Protection, the Law on Electronic Commerce, the Law on Electronic Communications, the Law on Interception of Communications and the Law on Electronic Data and Electronic Signature.[77]

The Law on Electronic Management adopted in 2009 provides standards and norms for information systems security in the public sector (including legal entities).[78]In 2011 MISA adopted two additional guidelines: 1) to monitor and manage information security related incidents; and 2) risk management.[79] The Law on Classified Information covers both foreign and national classified information and also requests regular inspections of all state bodies and legal entities with regard to the strict implementation of the law.[80]

The Constitution guarantees basic human rights and freedom of speech under:

- ‘Article 16 – Freedom of expression and free access to information

[64] Law on Criminal Code, Official Gazette No .37/1996, 80/1999, 4/2002, 43/2003, 19/2004, 81/2005, 50/2006, 60/2006, 73/2006, 87/2007, 7/2008, 139/2008, 114/2009, 51/2011, 51/2011, 135/2011, 185/2011, 142/2012, 143/2012, 166/2012, 55/2013, 82/2013.

[65] Law on Criminal Procedure, Official Gazette No. 150/2010 and 100/2012.

[66] Law on Electronic Communications. The Official Gazette of R.M no. 13/2005, 14/2007, 55/2007, 98/2008, 83/2010, 13/2012, 59/2012, 123/2012, 23/2013.

[67] Law on Communications Monitoring. The Official Gazette of R.M no. 121/2006, 110/2008, 4/2009, 116/2012.

[68] Law on e-Commerce. The Official Gazette of R.M no. 133/2007, 17/2011, 188/2014.

[69] Law on Electronic Management. The Official Gazette of R.M no. 105/2009, 47/2011.

[70] Code of Civil Procedure. The Official Gazette of R.M no. 79/2005, 110/2008, 83/2009, 116/2010.

[71] Law on Electronic Data Form and Electronic Signature. The Official Gazette of R.M no. 34/2001, 98/2008.

[72] Law on Personal Data Protection, Official Gazette No. 7/2005, 103/2008, 124/2008, 124/2010, 135/2011, 43/2014, 153/2015 and 99/2016.

[73] Law on Interception of Communications, Official Gazette No.121/2006, 110/2008, 4/2009, 116/2012.

[74] Law on Litigation, Official Gazette No. 79/2005, 110/2008, 83/2009, 116/2010.

[75] Law on Classified Information. Directorate for Security of Classified Information. Official Gazette of the Republic of Macedonia no. 113/07.

[76] DiploFoundation (2016) Cybersecurity in the Western Balkans: Policy gaps and cooperation opportunities. *https://www.diplomacy.edu/sites/default/files/Cybersecurity%20in%20Western%20Balkans.pdf*

[77] Ibid.

[78] Law on Electronic Management. The Official Gazette of R.M no. 105/2009, 47/2011.

[79] Ministry of Information Society and Administration. Information security – legislative for data protection in information systems. *http://www.mioa.gov.mk/?q=node/2660*

[80] Government of the Republic of Macedonia. Directorate for Security of Classified Information. *http://www.dbki.gov.mk/?q=node/130*

- Article 17 - Freedom and confidentiality of correspondence and other forms of communication
- Article 18 - Security and confidentiality of personal information
- Article 25 – Right to privacy of his/her personal and family life
- Article 26 - Right to the in violability of the home'[81]

While FYR Macedonia has not adopted specific legislation on human rights online, it is a signatory to international instruments on human rights such as the European Convention on Human Rights and the U.N. Geneva Convention relating to the Status of Refugees and Convention against Torture. According to the Human Rights Report provided by the U.S. Department of State there was no violation of Internet freedom by the government.[82] However, in the wake of the illegal mass wiretapping scandal in 2015, many people switched to using messaging applications that offer end-to-end encryption such as Viber and WhatsApp.[83]

Comprehensive legislation on protection of children online has been adopted and enforced under Articles 193 and 193a of the Criminal Code.[84] It adheres to Article 9 of the Budapest Convention that regulates the distribution of child abuse materials online. Since 2010, new amendments have been added to the Criminal Law that include the legal provisions on online child pornography and online sexual grooming.

Similarly, following the ratification of the Budapest Convention in 2004, FYR Macedonia had to make changes in the Criminal Code to fulfil obligations related to consumer protection and intellectual property online. In 2016 new legal provisions were added to the Law on Consumer Protection (2004) to align it with consumer protection legislation in the EU. The Ministry of Economy was in charge of drafting this legislation.

Article 286 of the Criminal Code regulates intellectual property in the country.

> **Unauthorized use of another's invention**
>
> Article 286
> (1) A person who without authorization uses, publishes, cedes or transfers another's registered or protected invention, shall be punished with a fine, or with imprisonment of up to three years.
> (2) The objects shall be confiscated.
> (3) Prosecution is undertaken on indictment.[85]

The MoI was involved in drafting of the legal provisions in the Criminal Code and is in charge of the Code implementation. At the national level, the Macedonian Customs Office and the

[81] Constitution of the Republic of Macedonia (2011)
http://www.wipo.int/edocs/lexdocs/laws/en/mk/mk014en.pdf

[82] US Department of State (2016) Macedonia 2016 human rights report.
https://www.state.gov/documents/organization/265658.pdf

[83] Ibid.

[84] Law on Criminal Code, Official Gazette No .37/1996, 80/1999, 4/2002, 43/2003, 19/2004, 81/2005, 50/2006, 60/2006, 73/2006, 87/2007, 7/2008, 139/2008, 114/2009, 51/2011, 51/2011, 135/2011, 185/2011, 142/2012, 143/2012, 166/2012, 55/2013, 82/2013.
http://unpan1.un.org/intradoc/groups/public/documents/untc/unpan016120.pdf

[85] Ibid.

Coordinating Body for Intellectual Property are the responsible institutions regulating intellectual property of online products and services.

The provisions of the Budapest Convention were transferred into the Criminal Code and the Law on Criminal Procedure, which are considered to be the most important pieces of legislation addressing cybercrime.

The Criminal Code covers the following substantive provisions related to cybercrime:

- Article 122 - Definition of payment card, **child pornography**, computer system and computer data
- Article 144 - Endangering security
- Article 147 - Violation of confidentiality of letters or other parcels
- Article 149 - **Misuse of personal data**
- Article 149-a - Prevention of access to a public information system
- Article 157 - **Violation of an author's right** and related rights
- Article 157a- Violation of the right of the technical specially of protected satellite signal
- Article 157 b- Piracy of audiovisual products
- Article 157c- Piracy of phonograms
- Article 193- **Showing pornographic materials to a child**
- Article 193 a – **Production and distribution of child pornography**
- Article 193 b – Enticement to intercourse or other sexual acts on a minor under 14 years
- Article 251 - Damage and unauthorized entering in a computer system
- Article 251a - Production and spreading of computer viruses
- Article 251b- Computer fraud
- Article 271 - Making, procuring or selling counterfeiting means
- Article 274 b- Issuing a bad check and abuse of a credit card
- Article 286 - **Violation of the right of registered or protected invention and topography of integrated circuits**
- Article 379 a – Computer forgery
- Article 394 D - Dissemination of racist and xenophobic material through computer systems

(Adapted from Council of Europe, Octopus Cybercrime Community, Country Wiki [86]*)*

Similarly, procedural cybercrime legal provisions are fully implemented in the Law on Criminal Procedure in Chapter XIX under Article 184 (search of a computer system and computer data), Article 198 (Temporary seizure of computer data), and Article 252, which refers to special investigative measures such as the monitoring, recording and inspection of telephone or other electronic communications.[87] It is worth mentioning that the Law on Criminal Procedure provides safeguards to the exercise of procedural powers, such as specifying that special investigative measures should be only used as a last resort measure.[88] For instance, Article 256 sanctions secret access to computer systems only 'after an explained request from the public prosecutor shall be ordered by the judge of previous procedure with a written order.'[89]

[86] Council of Europe (2017) Octopus Cybercrime Community, Country Wiki. *https://www.coe.int/en/web/octopus/country-wiki/-/asset_publisher/hFPA5fbKjyCJ/content/-the-former-yugoslav-republic-of-macedonia-/pop_up?_101_INSTANCE_hFPA5fbKjyCJ_viewMode=print&_101_INSTANCE_hFPA5fbKjyCJ_languageId=en_GB*

[87] Ibid.

[88] Ibid.

[89] Law on Criminal Procedure, Official Gazette No. 150/2010 and 100/2012.

Also, the amendments adopted in 2013 refer to the collection of digital evidence by law enforcement authorities. [90]

The public consultation E-portal ENER-Single National Electronic Registry of legislation (www.ener.gov.mk) plays a vital role in enhancing the government's transparency and inclusiveness in the legislative process.[91] ENER is considered to be the most advanced public consultation mechanism in the region. The length of the consultation process is 20 days for both new and amended laws. All the comments are reviewed by the government prior to the final adoption of a law.

After the adoption of the Budapest Convention in 2004, the approach changed in 2011 with less focus on cybercrime investigations and more on the collection of electronic evidence, in general. The MoI supports all investigations that are related to electronic evidence. Currently, the Ministry is in the process of building capacities to conduct and support all kinds of investigations related to cybercrime.

One participant suggested for consideration a proposal to amend and add a new article in the Criminal Procedural Code regarding the implementation of Article 32 of the Budapest Convention, which refers to trans-border access to stored computer data with consent, because the current legislation is not sufficient when obtaining electronic evidence from companies and ISPs that are located outside of the country.

D 4.2 CRIMINAL JUSTICE SYSTEM

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

Stage: Start-up – Formative

Across the criminal justice system, capacities are between start-up and formative stages of maturity in FYR Macedonia.

Regarding institutional capacities to tackle cybercrime issues, 'the Cybercrime Unit located within the Department for Suppression of Organised and Serious Crime and the Forensic

[90] DiploFoundation (2016) Cybersecurity in the Western Balkans: Policy gaps and cooperation opportunities. *https://www.diplomacy.edu/sites/default/files/Cybersecurity%20in%20Western%20Balkans.pdf*

[91] Public-Private Dialogue 2015 Workshop. Macedonian E-Gov Solution For Public Consultation In The Legislative Process-A National Platform For Sustainable PPD Based On Regulatory Impact Assessment Transparency Principles. Copenhagen, March 10-13, 2015. *http://www.publicprivatedialogue.org/workshop%202015/2015%20-%20Public%20Private%20Dialogue%20in%20Macedonia.pdf* (accessed 7 March 2018).

Department of the MoI merged into a single Cybercrime and Digital Forensic Department, thus forming a more efficient and effective investigative unit.'[92]

According to the Law on Criminal Procedure, the MoI cooperates with the prosecutor who has the main role in the cybercrime investigation. Law enforcement acts only as a facilitator to obtain electronic evidence during an investigation and at a trial. However, according to a representative from the MoI, there is a new approach under way. The new standard operating procedure will be published in 2018. Also, the Cybercrime Unit is in the process of implementing the action plan of the Cybercrime Strategy that was developed at the end of 2017.

Until now the MoI has retained the responsibility to investigate and collect electronic evidence not only from storage devices (e.g. mobile phone, hard disk and computers) but also from third parties (e.g. multi-national and national ISPs and also from ISPs that offer cloud services abroad).

Regarding capacities, the Cybercrime and Digital Forensic Department within the MoI has 22 staff members who are certified professionals; namely, they have received the Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH) provided by EC-Council, and the Certified Forensic Computer Examiner (CFCE) certifications. Currently, the MoI is in the process of re-certifying its employees together with other police officers who are working in the Cybercrime and Digital Forensic Department. In order to improve investigation procedures, the MoI is developing the MC4 (Macedonian Cybercrime Platform/Complaint Centre) that is planned to be in operation by the end of 2018. MC4 will provide citizens with information and updates on cybercrime issues, such as news about offenders' modus operandi on Internet, and will also offer means to report anonymously any cybercrime-related activities (e.g. suspicious activities on the Darknet or forums).

Concerning serious cybercrime cases, FYR Macedonia has no capacity due to the lack of staff with the knowledge and skills to investigate. As a result, the MoI has to rely on the private sector, academia and MKD-CIRT. There is, however, some capacity to deal with less serious cybercrime cases.

According to participants, at the national level there is no appropriate cybercrime training available for law enforcement officers, prosecutors or judges. However, FYR Macedonia regularly participates in cybercrime trainings abroad, cooperating with the Council of Europe (CoE), the European Commission, the Organization for Security and Co-operation in Europe (OSCE), the United Nations, being part of European Cybercrime Training and Education Group (ECTEG), Europol, and also undertaking some of the training organised by EC3. For instance, in September 2017 official trainers of ECTEG were invited to Skopje, where two training courses on digital evidence-gathering were completed by first responders. This event was organised by the MoI that provided training for 18 police officers who are now appointed as first responders to collect evidence related to cybercrime in the country. Also, several courses are offered by the Instrument for Pre-Accession (IPA) fund (providing training and equipment)

[92] DiploFoundation (2016) Cybersecurity in the Western Balkans: Policy gaps and cooperation opportunities. *https://www.diplomacy.edu/sites/default/files/Cybersecurity%20in%20Western%20Balkans.pdf*

and the OSCE. For instance, OSCE provides training for law-enforcement officers to combat cybercrime through the use of open-source digital forensic tools.[93]

One participant expressed concern regarding the small capacity of the Financial Police Office compared to the MoI. The one person in charge of cybercrime cases has already left the Office which is now waiting for three additional staff members to join.

Similarly, the Special Public Prosecutors Office has small capacity, because it does not have a jurisdiction to investigate cybercrime cases, only to prosecute special cases regarding unlawful interception of communications. Also, most of these cases are related to financial crime. The Special Public Prosecutor's Office has 22 investigators coming from the Financial Police Office, but most of them are financial-crime investigators and only one has experience with cybercrime cases.

Currently, the Cybercrime and Digital Forensic Department within the MoI is the only unit in the country that has the capacity to investigate cybercrime cases (e.g. mobile and computer forensics). In the near future, the MoI plans to build this capacity within the different institutions such as the MoF and the Financial Police Office, which has only one cybercrime investigator at the moment. The participants acknowledged the need to decentralise the digital-forensics capacity among several institutions, but currently there is no capacity to do so. It was suggested that investigating financial cybercrime cases related to Bitcoin and money-laundering should be carried out by the Financial Police, which would be the most suitable investigative authority, together with the Revenue Office or the Special Prosecutor's Office. The MoI is unable to support all the prosecutors in the country regarding the collection of digital evidence from the electronic devices. The MoI has two forensic laboratories (one for mobile devices and the other for computer forensics). The National Police also have a forensic laboratory, but it was not clear to what extent it has been fully operationalized.

The capacity of prosecutors and judges to handle cybercrime cases and cases involving digital evidence was considered by review participants to be limited and ad-hoc. Participants referred to the limited budget and the insufficient availability of technical equipment. There are no special courts for handling cybercrime cases, nor specialised trainings for judges on cybercrime. There is, however, some ad hoc training on electronic evidence provided by the Academy for Judges and Public Prosecutors of Macedonia.

Judges and prosecutors are eligible to participate in those trainings but these are available only four times a year. This has a negative impact on the effectiveness of law enforcement to handle cybercrime cases. If these are brought to court, it potentially leads to ineffective investigations and prosecutions, and, subsequently, lack of convictions. However, prosecutors and judges receive ad-hoc trainings sponsored by international and regional bodies such as CoE through the iPROCEEDS project. For instance, in 2017 three new prosecutors received training in Montenegro on cybercrime, electronic evidence and proceeds of online crime.[94] In February 2018 the three newly-trained prosecutors shared their knowledge and equipped their peers with the skills required to carry out cybercrime investigations more efficiently.

[93] OSCE (2016) 'OSCE trains law enforcement officers from South East Europe to combat cybercrime through use of open source digital forensic tools', *https://www.osce.org/secretariat/268036*

[94] Council of Europe (2017) 'iPROCEEDS: Regional Training of Trainers on cybercrime, electronic evidence and online crime proceeds', *https://www.coe.int/en/web/cybercrime/-/iproceeds-regional-training-of-trainers-on-cybercrime-electronic-evidence-and-online-crime-proceeds*

D 4.3 FORMAL AND INFORMAL COOPERATION FRAMEWORKS TO COMBAT CYBERCRIME

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

Stage: Formative

The authorities in FYR Macedonia have recognised the need to improve informal and formal cooperation mechanisms, both domestically and across borders, but these mechanisms remain ad hoc.

One example for formal cooperation is part of EC3's specialised Focal Points (FPs); for instance, FP CYBORG focuses on cybercrime that affects critical infrastructure and information systems.[95] In 2017 FYR Macedonia joined CYBORG and TWINS focal points but it is not part of the investigation committee. FYR Macedonia initiates regional or international cases that are led by EC3. The country has operational (since 2014) and strategic agreement (since 2010) with Europol. A strategic agreement means that FYR Macedonia can submit requests but is not able to receive information from Europol, in other words, it is 'limited to the exchange of general intelligence as well as strategic and technical information'.[96] An operative agreement allows the exchange of information including personal data[97] through the Secure Information Exchange Network Application (SIENA) platform, which has been in operation since 2014.

Informal cooperation exists with multinational ISPs on a voluntary basis, since they have no legal responsibility and are not obliged to answer requests coming from law enforcement. However, the cooperation does have formal elements. For example, law enforcement can send a formal request that is a copy of the prosecutor's order when requesting data from ISPs.

At the national level, cooperation between the prosecutor and the Department of Cybercrime and Digital Forensics is completely formal. The only exception is provision of support during investigations concerning electronic evidence. The cooperation with industry and academia is formal. Also, the MoI has both formal and informal cooperation mechanisms with the national MKD-CIRT. In 2017 the MoI developed a recommendation and a flowchart regarding the cooperation mechanisms with MKD-CIRT. The recommendation refers to cases that should be handled by the MoI only (in criminal cases), by the national CERT only (without criminal intent), and by both (where there is an overlap). The MoU signed between the MoI and MKD-CIRT also helps to implement the recommendation.

FYR Macedonia is part of iPROCEEDS – Cooperation on Cybercrime project under the IPA; earlier called Cybercrime@IPA. The iPROCEEDS project that started in 2016 covers seven

[95] Europol (2014) EC3. EC3: a look back at the first year. https://www.europol.europa.eu/newsroom/news/ec3-look-back-first-year

[96] Europol. Partners and agreements. *https://www.europol.europa.eu/partners-agreements*

[97] Ibid.

countries in the region and eight institutions from FYR Macedonia at the national level.[98] The project targets money laundering connected with cybercrime and virtual currency. The MoI is leading the project, which will be finished by June 2019.

Among the various international cooperation channels available, the engagement with Europol and INTERPOL Skopje were described as the most important channels to facilitate cross-border cooperation and information-sharing. INTERPOL Skopje has access to INTERPOL's secure communication linkage, I-24/7, which is a restricted-access Internet portal, providing police across the country instant and automated access to INTERPOL's criminal databases. The I-24/7 network is considered to be an informal cooperation because it is used only to share information for intelligence purposes, and not for evidence-gathering.

The Data retention policy in FYR Macedonia sets a period of 12 months by law. However, data-preservation policy depends on the case. When collecting digital evidence, it is mandatory to obtain an order from the court or the prosecutor that guarantees the integrity for the data that is collected as evidence in court. Prosecutors often have to rely on the MoI's digital forensics laboratory and capacity to a great extent.

Under the EU umbrella, an action plan for the establishment of a Safer Internet Center as a basic structure on a national level for child and youth online protection was developed and coordinated by the MISA Advisory Board (members are the cybercrime unit at the MoI, the AEC, the Directorate for Personal Data Protection, the Macedonian Chamber of ICT, and a civil society organisation the Internet Hotline Provider Macedonia) and submitted to the previous government. The action plan was adopted but the implementation was not prioritised. With the new Government in place, meetings have taken place to proceed with this initiative but it was not clear from the consultations if implementation will take place. According to participants, there is a lack of awareness of the issue.

RECOMMENDATIONS

LEGAL FRAMEWORKS

R4.1 Consider harmonising the Law on Personal Data Protection with the GDPR and ensure that legal mechanisms are in place which enable strategic decision-making and determine the timeframe after which personal data are no longer required as evidence for investigation and must be deleted. Identify international and regional trends and good practices to inform the assessment and amendment of data protection laws and associated resource planning.

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

[98] Council of Europe. iPROCEEDS – Targeting crime proceeds on the Internet in South Eastern Europe and Turkey. *https://www.coe.int/en/web/cybercrime/iproceeds*

R4.3 Review the Criminal Procedural Code concerning the requirement for consent to cross-border access to stored computer data.

R4.4 Develop new legislative provisions through multi-stakeholder consultation processes on consumer protection online and human rights online.

R4.5 Ensure that in the case of cross-border investigation, procedural law stipulates what actions need to be conducted in order to successfully investigate cybercrime.

R4.6 Consider developing a separate strategy covering cybercrime specifically that would also clarify the roles and responsibilities of the actors (CIRTs, law enforcement, Ministries) involved in handling computer security incident response and cybercrime investigations.

R4.7 Dedicate resources to ensure full enforcement of existing and new cybersecurity laws and monitor implementation.

R4.8 Ensure that in the case of cross-border investigation, procedural law stipulates what actions need to be conducted in order to successfully investigate cybercrime.

R4.9 Adapt and implement legal provisions on e-commerce, regarding cybercrime incidents such as online fraud, spam, and phishing sites.

R4.10 Consider developing a platform for sharing electronic evidence between regional cybercrime forces.

R4.11 Enhance the existing cooperation between ISPs and law-enforcement agencies for removal of copyright-infringing content from websites.

R4.12 Foster research on human rights on Internet and ensure that measures are in place to exceed minimal baselines specified in international agreements.

R4.13 Revise and enforce legislative provisions that obliges ISPs to provide technical assistance for law enforcement when they conduct lawful electronic surveillance.

CRIMINAL JUSTICE SYSTEM

R4.14 Invest in advanced investigative capabilities in order to allow for the investigation of complex cybercrime cases, supported by regular testing and training of investigators.

R4.15 Allocate resources dedicated to fully operational cybercrime units based on strategic decision-making in order to support investigations, especially at a local level.

R4.16 Strengthen national investigation capacity for computer-related crimes, including human, procedural and technological resources, full investigative measures and digital chain of custody.

R4.17 Develop and institutionalise specialised training programmes for police, prosecutors and judges on cybercrime and electronic evidence through EC3 or other organisations.

R4.18 Consider turning the Cybercrime and Digital Forensic Department within the MoI into FYR Macedonia's central point of contact to carry out cybercrime investigations both domestically and internationally.

R4.19 Consider establishing institutional capacity building programmes for judges, prosecutors and police personnel from security agencies to acquire new ICT skills needed for cybercrime investigations (e.g. digital evidence gathering) and effective ways of enforcing cyber laws.

R4.20 Consider establishing standards for the training of law enforcement officers on cybercrime.

R4.21 Dedicate sufficient human and technological resources in order to ensure effective legal proceedings regarding cybercrime cases.

R4.22 Consider requesting reliable and accurate cybercrime statistics from the MoI and MKD-CIRT in order to better inform decision-makers about the current cybercrime threat landscape in FYR Macedonia when developing policies and legislations to address this matter.

R4.23 Build a cadre of specialist prosecutors and judges to handle cybercrime cases and cases involving electronic evidence.

R4.24 Establish a formal mechanism to enable the exchange of information and good practices between prosecutors and judges in order to ensure efficient and effective prosecution of cybercrime cases.

R4.25 Work on building on the cooperation between the MKD-CIRT and other sectors on collecting and analysing cyber-incidents through an information-sharing platform.

R4.26 Collect and analyse statistics and trends regularly on cybercrime investigations, on cybercrime prosecutions and on cybercrime convictions.

FORMAL AND INFORMAL COOPERATION FRAMEWORKS

R4.27 Strengthen international cooperation to combat cybercrime based on existing legal assistance frameworks and enter further bilateral or international agreements.

R4.28 Consider setting up a Threat Intelligence Platform for real-time information sharing between the MoI and the MKD-CIRT.

R4.29 Allocate resources to support the exchange of information between public and private sectors domestically and to enhance the legislative framework and communication mechanisms.

R4.30 Enhance cooperation between the public sector and banks and other financial institutions regarding the sharing of incidents, in order to increase the level of cybersecurity awareness in FYR Macedonia.

R4.31 Facilitate informal cooperation mechanisms within the police and criminal justice system, and between police and third parties, both domestically and across borders, in particular ISPs.

R4.32 Consider establishing a 24/7 point of contact within the Cybercrime Unit of the MoI in order to provide instant assistance for mutual legal assistance requests.

R4.33 Strengthen informal cooperation mechanisms within the police and criminal-justice system, and between police and third parties, both domestically and across borders. Consider know-hows from other areas, such as anti-corruption cooperation.

R4.34 Consider revising the data retention period, according to international best practices, for instance GDPR.

R4.35 Consider implementing the EU child protection project through multi-stakeholder consultation processes.

DIMENSION 5
STANDARDS, ORGANISATIONS AND TECHNOLOGIES

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

D 5.1 ADHERENCE TO STANDARDS

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

Stage: Formative

According to the Public Administration Reform Strategy 2018-2022[99], the 'Law on Introduction of Quality Management System[100] and the Common Assessment Framework (CAF) adopted in May 2013 have laid the foundation for introducing international and national quality management standards (minimum ISO 9001 and CAF)', however, only for the public administration bodies.[101] The strategy states that '51 institutions have so far introduced ISO 9001 Quality Management Standard, and 29 institutions have introduced CAF'.[102] While ISO

[99] Ministry of Information Society and Administration (2017) 'Public Administration Reform Strategy 2018-2022', http://mioa.gov.mk/files/pdf/dokumenti/Draft_PAR_STRATEGY201-2022_16122017_final_en.pdf

[100]Law on Introduction of Quality Management System (2013) http://www.mio.gov.mk/files/pdf/caf/Zakon%20za%20voveduvanje%20na%20sistem%20za%20upravuvanje%20i%20zaednicka%20ramka%20za%20procenka%20na%20rabotenjeto%20i%20davanjeto%20uslugi%20vo%20drzavnata%20sluzba.pdf

[101] Ministry of Information Society and Administration (2017) 'Public Administration Reform Strategy 2018-2022', http://mioa.gov.mk/files/pdf/dokumenti/Draft_PAR_STRATEGY201-2022_16122017_final_en.pdf

[102] Ibid.

certification for private companies is not required by law, it is sometimes listed by contracting authorities in the tender documentation as a requirement for the economic operator in order to participate in the tender process (e.g. proving professional ability). An action plan has been developed on a national level for the implementation of acceptance criteria to meet minimum security baselines for information security defined in ISO 27002 for relevant institutions in the IPA2 structure. This initiative is supported by DG NEAR.

Regarding public institutions, the CMM review found that the participants were not fully aware of the aforementioned requirements. Some mentioned that the Law on Electronic Management[103], which was adopted in 2009 (with changes in 2011, 2015 and 2016) and which regulates the work of public institutions regarding the exchange of electronic data and documents. It is based on the ISO 27000 series of standards and requires certain technical and organisational security requirements, loosely based on ISO 27001, that public institutions must comply with in order to connect to the National Interoperability Platform managed by MISA. However, the Law does not cover electronic documents that contain classified information, personal information, and information related to the protection of national security.[104]

It is the Law on Classified Information (2004)[105] that has full control over both foreign and national classified information, as well as requiring inspection and supervisions of all state and legal entities[106] (see D4.1.) Also, the Law empowers the Directorate for Security of Classified Information to ensure that international standards and norms are in place when handling classified information. Nevertheless, one participant mentioned that some institutions have identified and implemented information risk-management standards such as ISO 9001:2015 or ISO 20000-1:2011 based on their own internal policies. In the system for producing biometric passports, a security profiling is taking place in terms of accessing the data on the chip (BAC, EAC & SAC), as well as ICAO for MRTD in the area. This suggests that there is no national guideline or policy which applies across government institutions.

Large organisations and the banking setor are more advanced regarding the design, adoption and auditing of standards for cybersecurity. According to the Banking Law,[107] all financial institutions shall adhere to information security standards stated in the bylaw 'Decision on the bank's information system security (2008)'.[108] This decision was first introduced in 2003, then revised in 2008 and lately in April 2018. All financial institutions are required to follow the information security standards prescribed in the decision introduced by the National Bank of the Republic of Macedonia (NBRM). Therefore, there is no voluntary adoption for information security standards but a formal, structured process annually assessed by a special IT supervision unit in the Supervision Department unit in NBRM (e.g. if the financial institutions do not follow some standards they are sanctioned). The information security

[103] Assembly of the Republic of Macedonia (2009) 'The Law on Electronic Management', Official Gazette of RM, Official Gazette No.105/2009, 47/2011 *http://mioa.gov.mk/files/pdf/en/Law_on_Electronic_Management.pdf*

[104] Ibid.

[105] Government of the Republic of Macedonia. Directorate for Security and Classified Information. *http://www.dbki.gov.mk/files/pdf_files/Law_on_Classified_Information.pdf*

[106] Government of the Republic of Macedonia. Directorate for Security and Classified Information. *http://www.dbki.gov.mk/?q=node/130*

[107] Constitutional Court of the Republic of Macedonia. Banking Law (2008) http://www.nbrm.mk/content/Regulativa/Banking_Law_Unofficial%2007-06-2017.pdf

[108] National Bank of the Republic of Macedonia. Decision on the bank's information system security (2008). Official Gazette of the Republic of Macedonia" No. 31/2008. *http://www.nbrm.mk/WBStorage/Files/IT%20security.pdf*

standards stated in the decision are carefully tailored and based on ISO 27001, the Principles for the Sound Management of Operational Risk[109] issued by the Basel Committee on Banking Supervision (2011), the National Institute of Standards and Technology (NIST) Cybersecurity Framework (2014) and Cyber resilience in financial market infrastructure[110] issued by the Bank for International Settlements (2014). Furthermore, the NBRM introduced a cyber-security tool in 2016 in order to help the banks to measure their inherent level of cyber risk and to identify the cyber maturity level of resilience that they should achieve.[111]

Nevertheless, financial institutions are allowed to follow any international standard which is not in collision with the standards prescribed in the decision on the bank's information system security (2008). For instance, a bank implemented ISO 20000 which was not part of the regulation but a voluntary pursuit of the bank. Also, the implementation of best practices and informal standards is up to the institutions to decide. However, in case if an outsourcing company is used for processing or keeping financial information, the NBRM requires them to be compliant with ISO 27001, in addition to ISO 20000. Similarly, the insurance market adopted ISO 27001:2013 regulation that defines the minimum information technology standards for IT undertakings; but it was decided not to adopt the full standard, only the parts that lacked the enforcement of the governance of IT systems.

Several concerns were raised by the participants regarding ICT security standards. For instance, the USAID Organizational Performance Improvement Program certified six judicial institutions for ISO 9001:2015.[112] In reality however, most of that certification process was only to get certified without changing the organisational mind-set. It was noted that the size of IT teams in SMEs are too small (e.g. only three employees) that makes the implementation of ISO 9001:2015 challenging. Also, public institutions face similar problems. ICT standards evolve continuously and getting re-certified is expensive, requiring paperwork and change in the procedures that is difficult to implement. Therefore, finding a balance where some companies have to be certified whilst others have the option to opt in and opt out might be a solution.

In contrast, an auditor certified by the British Standards Institution (BSI) argued that the problem is not the small size of the IT team but rather the extent to which the organisation takes the ICT standards seriously. Reference was given to the allocation of sufficient budget and the actions taken by the government or management of the institution. Certifications are considered essential for the organisation to be recognised.

Some participants added that ICT certification requirement (e.g. ISO 27001:2013) is often the only way to get budget for cybersecurity (e.g. asking for specific software) from the management. Another concern is that after the initial phase of the implementation process, ICT standards are not monitored and maintained consistently until they need to be re-certified. Therefore, the mind-set of the organisation needs to be changed first in order to increase competence and commitment from ICT technicians and not vice versa.

[109] Bank for International Settlements (2011) Principles for the Sound Management of Operational Risk by the Basel Committee on Banking Supervision. *https://www.bis.org/publ/bcbs195.pdf*

[110] Bank for International Settlements (2014) Cyber resilience in financial market infrastructure. *https://www.bis.org/cpmi/publ/d122.pdf*

[111] 17th Regional payment Systems Workshop 8-11 May 2018 Antalya. Thematic investigation- Cyber Resilience of the banking sector in Macedonia.

[112] USAID (2017) 'Six judicial institutions certified in ISO 9001:2015 with USAID support', *https://www.usaid.gov/macedonia/macedonia/press-releases/six-judicial-institutions-certified-iso-90012015-usaid-0*

Based on the review, there is no mandatory standard for any sector related to the procurement of hardware and software. The public procurement system used to be decentralized, with each government body having its own procurement procedure, [113] however the new draft legislation on public procurement will ensure that it is centralised and executed through the e-government portal.[114] It is expexted to be adopted by the end of 2018. Currently, the Law of Public Procurement[115] (adopted in 2007) regulates public procurement such as electronic auctions on the basis of the lowest price criterion.[116] In the law, the quality management systems are regulated in Articles 155-158, but only in terms that if the contracting authority requires certificates for quality management, they must be based on the relevant European or international standards.

In January 2018, the government established a National ICT Council, consisted of members at the ministerial level.[117] The role of the National ICT Council includes the development and implementation of a National ICT strategy and advising on yearly plans for public procurement of ICT hardware and software, including tender documentation for all public institutions. [118]

One participant expressed concern that the 'cheapest price wins' approach is detrimental for the computers' security system within the public sector. Another participant referred to 'state interference' as another challenge when implementing ICT-related procurement at the national level (e.g. budget allocation for the procurement of software and hardware was not approved by the government because of financial incentives). When it comes to the private sector, there are internal policies and procedures in place that participants characterized as thorough.

Focusing on standards in software development, there are guidelines in place in both public and private sectors, but the extent to which these guidelines are related to cybersecurity is not clear. It was noted that the ICT Department at the MoI has an in-house software development team that delivers the most critical software solutions. Due to the limited capacity of the team, in-house software development is not present at the institutional level. Participants in the private sector were not aware of any required standard for software development in the insurance and banking industry.

Participants referred to an incident that happened in 2013 when a piece of software was developed for a government institution. The software to be installed was not verified to ensure that it does not leak information via error messages or does not contain any corrupt files. During the evaluation process it was discovered that the software communicates with a foreign country and shares information. Fortunately, this was detected before the product went into production, however these incidents supposedly happen on a regular basis.

[113] US Department of Commerce, Export.gov https://www.export.gov/article?id=Macedonia-Selling-to-the-Government

[114] Single National Electronic Register of Regulations of the Republic of Macedonia. Draft Law on Public Procurement. https://ener.gov.mk/Default.aspx?item=pub_regulation&subitem=view_reg_detail&itemid=Xp2x6ms4eMDvLz1aB8J7aA==

[115] Law of Public Procurement (2007) *http://www.bjn.gov.mk/content/Legislativa/ZJN_precisten%20tekst_Fevruari%202018.docx*

[116] Ibid.

[117] Government of the Republic of Macedonia. ВЛАДА НА РЕПУБЛИКА МАКЕДОНИЈА. Official Gazette of the Republic of Macedonia (number: 22/2018)

[118] Ibid.

Furthermore, software companies offer services to international customers who are obliged to apply certain standards in their respective countries. In that case, according to one participant, software development companies have to perform a compliance audit in accordance with at least ten ICT standards in the ISO 27000 family (of standards) that focus on network, communication and application security. Therefore, it is essential to distinguish whether software is developed for international or local customers, since the local market has no regulatory requirements.

5.2 INTERNET INFRASTRUCTURE RESILIENCE

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

Stage: Formative - Established

FYR Macedonia has experienced rapid development of telecommunications and of the information society in recent years.[119] As a result, the usage of ICT has increased. Based on data provided by the State Statistical Office for 2016, 72.2 percent of the population were Internet users and 75.3 percent of households had Internet access, while the figure for enterprises with ten or more employees was 93.8 percent.[120]

The broadband market in FYR Macedonia is experiencing steady, if unspectacular, growth, and reached 385,000 subscribers at end-March 2017, up 4.6 percent from 367,970 a year earlier and 357,383 at 31 March 2015 – with a household penetration of nearly 69 percent at the most recent date, putting it some way ahead of the regional average of 50 percent. Between them, the country's two mobile network operators counted a total of 2.26 million subscribers at 31 March 2017, down marginally from 2.29 million at the start of the year, and 2.30 million at end-March 2016, with cellular population penetration standing at around 109 percent at the most recent date. [121]

Participants generally agreed that Internet services are reliable and noted that the majority of Internet infrastructure is privatised. However, they were not aware of the situation within the Ministries or the Government and whether they have their own infrastructure or not.

Also, participants mentioned that incidents have no impact on cyber defence, because the crucial IT networks (like defence and MoI) have their own separate networks and ISP connections, which are used in case Internet infrastructure breaks down.

[119] Tasevski, P. (2015) Macedonian path towards cybersecurity. Information & Security, 32(2), 1.

[120] State Statistical Office. Information Society. *http://www.stat.gov.mk/OblastOpsto_en.aspx?id=27*

[121] TeleGeography, GlobalComms Database – Macedonia, March 2018

One participant added that in 2017 there was a major outage of one of the biggest ISPs for a couple of hours. It was not a specific cybersecurity incident (rather an international connection problem with the equipment), but it disrupted mobile Internet connections.

Furthermore, in 2014 IT security researchers accidentally discovered that there was no AP/client isolation on 3G communication on either of the two mobile operators. Anyone from 3G connected device could access another device directly and there was no filter on it. This was raised with the operator and was resolved in the end.

Redundant Internet connection is configured among all ISPs to prevent Internet from going down. This is regulated by the AEC responsible for monitoring of the quality of service provided by the operators.[122] In 2017 the Agency adopted the *QoS Regulation* that requires the operators to provide a minimum level of quality of service that has to be reported to the Agency regularly.[123] The ISPs need to comply with that law in order to get a license to operate.

For the financial sector there is a requirement from the National Bank that all outsourcing service providers should offer SLE and ISO 20000 for the financial sector, such as banks and saving banks.

Also, there is no regional support to secure Internet infrastructure in the country.

D 5.3 SOFTWARE QUALITY

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

Stage: Start-up

There is no inventory of secure software for use in public and private sectors in FYR Macedonia. The quality and performance of software in the public sector is a concern, but functional requirements are not yet fully monitored. Users are advised to install patches and organisations generally ensure quality of existing software. Policies for updating software products or monitoring the functionality of applications may exist but are not necessarily enforced or formulated - each organisation has its own requirements defined at the corporate level. Participants acknowledged the need for a catalogue of secure software platforms and applications within the private and public sectors. One participant noted that a hardware or software catalogue with recommendations in the public sector is forbidden by law.

[122] Getting the Deal Through (2017) Macedonia – Telecoms and Media. *https://gettingthedealthrough.com/area/39/jurisdiction/108/telecoms-media-macedonia/*

[123] Ibid.

Others argued that the lack of mobile device management within the public sector (as well as possibly in the private sector) is a bigger issue, since there is no IT department that would monitor and secure the employees' company mobile devices.

Participants were not aware of guidelines or policies in place for patch management concerning software and security updates. However, system administrators can authorise the installation of software updates by a given date. At the MoI there is a procedure in place for administrators to control patching, software upgrades and back-ups for the ICT systems and end-user (employee's) workstations using a domain policy.

Some mentioned that penetration testing projects are carried out to monitor software quality but not all companies are conducting it. Regarding the financial sector, the National Bank requires penetration testing on new applications and proper secure coding practices in place. For the insurance sector there is no demand for penetration testing, however this is likely to be in place when the EU's General GDPR will be applied from late May 2018.

One participant referred to an incident that happened during the development phase of a software. The new version of the software that was delivered by the development company fulfilled all the requirements. However, additional small changes made in the software were neglected causing financial loss until it was detected. The software verification test failed because the software was tested based on the requirements only. There was no comprehensive framework for verification and validation.

Also, there are requirements for insurance companies to report any major change in the software and to conduct internal risk assessments before carrying out the adjustments. However, the dynamics of business processes require continuous software updates and if organisations fail to maintain continuous testing in order to deliver quality software, there is a higher risk of flaws in the application and hence the risk of incidents increases. During the CMM assessment one participant pointed out that the accreditation process for Communication Information Systems implies creation of documented Risk Assessment for the Information System. The DSCI issued a "Manual for Evaluation and Managing Security Risk for Communication Information Systems"[124]. Moreover, in 2017, with the support of OSCE, a methodology for IT security risk assessment was created, based on ISO 27005:2011.

One participant suggested introducing the process of continuous testing, including testing of properly configured systems, setting up test environments, and also consumer acceptance tests.

[124] Directorate for Security of Classified Information issued a "Manual for evaluation and managing security risk for Communication Information Systems"
http://www.dbki.gov.mk/files/pdf_files/metodologija/Metodologija_za_procena_na_rizik_signed.pdf

D 5.4 TECHNICAL SECURITY CONTROLS

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

Stage: Start-up

The adoption of technical security controls in FYR Macedonia varies across sectors and organisations, but they are mostly ad-hoc and not consistently deployed.

At the private sector level, the National Bank has a Decision in place relating to the established standards concerning the bank's information system security (No. 31/2008) such as security testing, monitoring, and upgrading the bank's information system assets.[125] Participants agreed that banks employ a much higher level of technical cybersecurity controls compared to other sectors in the region.

ISPs both provide and promote anti-malware software as part of their services, however it depends on the customer and the product. Some products go free-of-charge and some are payable. Also, there are different packages with certain security controls that are offered to customers (e.g. end-user protection).

Participants mentioned that there is a substantial level of technical security controls in place (such as firewalls, business continuity planning), however they are not tested regularly. There were some interesting findings during the penetration testing projects including:

1) physical controls are sometimes not in place; or
2) technical measures are in place but not properly configured (e.g. if the system is transferred into a secondary location the security control/technical measure that was purchased in the primary location is not available after the transferral, thus making the system weak)
3) when the systems are transferred to a different location problems arise
4) generally, companies have no compliance issues since they have disaster recovery site, however full technical measures are absent

[125] National Bank of the Republic of Macedonia (2008) 'Decision on the bank's information system security', Official Gazette of the Republic of Macedonia No. 31/2008. http://www.nbrm.mk/WBStorage/Files/IT%20security.pdf

D 5.5 CRYPTOGRAPHIC CONTROLS

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

Stage: Formative

Cryptographic controls for protecting data at rest and in transit are recognised and deployed in an ad-hoc manner by multiple stakeholders and within various sectors. Protecting data in transit is regulated under the Law on Personal Data Protection for websites/portals that contain personal data and/or require the user to log in Also, the Law on Classified Information regulates and ensures full control for protecting classified information.[126] Currently, the Directorate for Security of Classified Information (DSCI) is coordinating with a working group that is tasked with the drafting of the proposal text of the Decree on Crypto Protection.[127]

At the national level, the MoI is responsible for the provision of standards for cryptographic protection but only for systems that process classified information. A representative from the MoI also confirmed using cryptography for classified information in transit. Regarding encryption of personal data, the Ministry deploys state-of-the-art algorithms and standards at the institutional level. The encryption of personal data at rest is covered under the Law on Personal Data Protection[128].

Within the private sector, participants noted that accession to online banking services is HTTPS mandatory in FYR Macedonia. The Insurance Supervision Agency provides one central portal/website without cryptographic controls https://www.asoportal.mk/isaportal/default.aspx, incorporated security standards). According to a participant, the Law on Personal Data Protection requires all companies that transfer personal data outside of their perimeters to be encrypted, whether the personal data are at rest or in transit. Database encryption is not common.

[126] Law on Classified Information. Directorate for Security of Classified Information. Official Gazette of the Republic of Macedonia no. 113/07.

[127] Government of the Republic of Macedonia (2017) Annual National Programme of the Republic of Macedonia for NATO membership 2017/2018. *http://www.mfa.gov.mk/images/stories/GNP/GNP-2017-2018-MNR-web.pdf*

[128] Parliament of the Republic of Macedonia. Law on Personal Data Protection. Official Gazette No. 7/2005, 103/2008, 124/2008, 124/2010, 135/2011, 43/2014, 153/2015 and 99/2016. *http://www.ceecprivacy.org/pdf/Law%20on%20Personal%20Data%20Protection.pdf*

D 5.6 CYBERSECURITY MARKETPLACE

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

Stage: Start-up

The domestic market provides limited cybersecurity technologies in FYR Macedonia. There has yet to be a domestic market for cybercrime insurance products developed in the country. It was however noted by participants during the review that firms provide, for instance, penetration testing services.

D 5.7 RESPONSIBLE DISCLOSURE

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

Stage: Formative

In FYR Macedonia there is a policy in place for responsible information disclosure[129] that falls under the process for incident handling. According to the policy, 'sensitive information can be received in the MKD-CIRT through an incident report submitted by a constituent or another party that is participating in the process of incident management.'[130] According to the policy, the MKD-CIRT follows the 'need to know' principle that means that information not publicly available must not be shared with the public, only with the entities that need to know about it.[131] Sensitive information will be disclosed only if it is necessary to resolve the incident.[132] Furthermore, MKD-CIRT will share the requested sensitive information with public institutions and third parties only after all legal requirements are fulfilled (e.g. delivery of a court order). MKD-CIRT also has an informal malware information sharing platform that could be used as a tool to exchange information on known vulnerabilities, however, this is not commonly used.

Currently, a more detailed process of disclosing vulnerabilities responsibly is under development with regard to the reporting, handling and dissemination of information to other parties or to the public if a vulnerability is detected in software or on a website. Reporting

[129] MKD-CIRT (2016) Information Disclosure Policy. Version 1.0 – 16.03.2016. https://mkd-cirt.mk/wp-content/uploads/2018/03/4-INFORMATION-DISCLOSURE-POLICY-_web.pdf

[130] Ibid.

[131] Ibid.

[132] Ibid.

vulnerabilities among critical infrastructure owners does not exist. Participants noted that organisations believe that disclosure of incidents will lead to reputational damages, especially in the telecommunications and finance sector.

RECOMMENDATIONS

ADHERENCE TO STANDARDS

R5.1 Adopt a nationally agreed baseline of cybersecurity related standards and good practices across the public and private sectors, including ICT security standards in procurement and software development. Consult with existing working groups and experts from all sectors, but in particular the banking sector, as well as audit companies and professional associations.

R5.2 Establish or assign an institution responsible for the implementation, auditing and measurement of the success of standards across public and private sectors. Apply metrics to monitor compliance and establish periodic audits.

R5.3 Promote discussions on how standards and good practices can be used to address risk within critical infrastructure supply chains by both government and infrastructure organisations. Identify and mandate standards to which CIIs should adhere to.

R5.4 Identify a minimum set of controls for all governmental departments based on annual assessments and establish a controls-review to assess the effectiveness of the current controls and practices.

R5.5 Establish frequent training for IT employees.

R5.6 Establish a framework to assess the effectiveness of standards for procurement and software development.

R5.7 Consider the implementation of best practices such as NIS and GDPR in consultation with all relevant stakeholders and regulators.

R5.8 Establish mandatory requirements for the adherence of standards by appointing security officers that will be held responsible for the implementation of these standards.

R5.9 Streamline clear guidance for the public sector for the procurement of hardware and software.

R5.10 Promote the awareness and implementation of standards among SMEs.

INTERNET INFRASTRUCTURE RESILIENCE

R5.11 Establish or assign an institution responsible for enhancing coordination and collaboration regarding the resilience of Internet infrastructure across the public and private sectors.

R5.12 Increase reliability of Internet infrastructure and expand the national programme for infrastructure development.

R5.13 Establish or assign an institution to identify, implement and perform auditing on technology and processes deployed for Internet infrastructure.

R5.14 Identify and map points of critical failure across the Internet infrastructure.

R5.15 Conduct regular assessments of processes according to international standards and guidelines together with assessment of national information infrastructure security and critical services that drive investment in new technologies.

SOFTWARE QUALITY

R5.16 Develop a catalogue of secure software platforms and applications used within the public and private sectors, as well as critical infrastructure.

R5.17 Develop, implement and enforce policies and processes on software updates and maintenance.

R5.18 Gather and assess evidence of software quality deficiencies regarding their impact on usability and performance.

R5.19 Establish or assign an institution to elicit in a strategic manner common requirements for software quality and functionality across all public and private sectors.

R5.20 Promote the requirements for software quality and functionality across all public and private sectors and ensure that they are established.

TECHNICAL SECURITY CONTROLS

R5.21 Encourage ISPs and banks to offer anti-malware and anti-virus services for clients and ensure that their effectiveness is monitored and assessed.

R5.22 Establish metrics for measuring the effectiveness of technical controls across the public domain.

R5.23 Develop processes for reasoning about the adoption of more technical controls based on risk assessment methodologies suitable for the public domain.

R5.24 Ensure that Network Introduction Detection Systems (NIDS) and Host Intrusion Detection Systems (HIDS) are deployed in across the public sector.

R5.25 Consider raising awareness of security controls by promoting cybersecurity best practices for users, such as strong passwords, secure back-ups, and use of anti-malware on their devices.

R5.26 Designate an authority to be responsible for the strategic decisions on technical controls that will supervise end-to-end all networks and will promote the adoption of a unified framework for security controls.

R5.27 Keep technical security controls up-to-date within the public and private sector, monitor their effectiveness and review on a regular basis.

R5.28 Conduct penetration testing for the private/public sector, the results of which should inform the implementation of technical controls.

R5.29 Create authentication processes for users before signing in to critical networks.

CRYPTOGRAPHIC CONTROLS

R5.30 Encourage the development and dissemination of cryptographic controls across all sectors and users for protection of data at rest and in transit, according to international standards and guidelines.

R5.31 Raise public awareness of secure communication services, such as encrypted/signed emails.

R5.32 Consider requiring all cloud services that share data to automatically encrypt data before it is uploaded. This will help the process of buying certain cloud services easier for companies.

R5.33 Use SSL/TLS connections to secure communications between government bodies and data centres.

R5.34 Establish or assign an institution to design a policy, aiming to assess the deployment of cryptographic controls, according to their objectives and priorities within the public and private sector.

CYBERSECURITY MARKETPLACE

R5.35 Foster collaboration with the private sector and academia regarding research and development of cybersecurity technological products.

R5.36 Encourage and support local initiatives in partnership with businesses that aim at developing innovative cybersecurity technology, applications, services and solutions.

R5.37 Promote sharing of information and best practices among organisations to explore potential cybercrime insurance coverage.

RESPONSIBLE DISCLOSURE

R5.38 Develop a responsible vulnerability disclosure framework or policy within the public sector and facilitate its adoption in the private sector, including a disclosure deadline, scheduled resolution, and an acknowledgement report.

R5.39 Assign MKD-CIRT responsibility for supervising the process of responsible disclosure and ensure that organisations do not conceal this information.

R5.40 Develop a system to facilitate threat-intelligence sharing within the critical infrastructure partners and ISPs. Promote sharing of threat-intelligence in the financial sector and incentivise companies to actively participate.

R5.41 Encourage sharing of technical details of vulnerabilities among critical infrastructure and ISPs and deploy existing informal information-sharing groups and platforms to build trust.

R5.42 Promote the existing methods for incident report in the public sector.

R5.43 Define thresholds and notification requirements for all sectors. These requirements should not only consider availability of services but the integrity and confidentiality of data.

R5.44 Promote the hotline and mobile application for incident report in the public sector.

ADDITIONAL REFLECTIONS

The representation and composition of stakeholders was sufficient as representatives of each stakeholder group were present in one or more sessions of the review. However, certain stakeholder groups were underrepresented such as law enforcement (in particular from the local/regional level) and the private sector (in particular domestic companies and SMEs).

The level of stakeholder engagement during the consultations was sometimes limited, which limits the completeness of evidence in some areas. However, overall the contribution of many participants and the willingness of the hosting organisations to share information before, during and after the consultations provided sufficient evidence to draw conclusions on the maturity of cybersecurity capacity based on the CMM.

This was the 22nd country review that the GCSCC has supported directly.

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

Global Cyber Security Capacity Centre

Oxford Martin School, University of Oxford

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

United Kingdom

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

Email: cybercapacity@oxfordmartin.ox.ac.uk

Web: www.oxfordmartin.ox.ac.uk

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