Replublic of Macedonia

National Cyber Security Strategy 2018-2022

Action Plan 2018-2022

December 2018

Preface

The purpose of this document is to define in more detil the activities set in the first National Cyber Security Strategy 2018-2022. Following a cyber security capacity assesment, a working group has been created, tasked to develop strategic documents in the field of cyber securitym, consisting of representatives from the institutions in charge of this Strategy - the Ministry of Information Society and Administration, the Ministry of Defence and the Ministry of Interior. The responsibilities of this working group will be extended in order to include the implementation of the activities of the Body with operational cyber security capacities.

This Action Plan outlines the major activities needed to strengthen our cyber secuirty capacities. However, it should be taken into account that most activities to be done by the Body are subject to change, as they may be further asessed and defined.

The structure of this Action Plan consists of three activities with highest priority - the basis of this Action Plan. These activities set the ground for further development of all other activiites, divided according to the 5C Goals defined in the Strategy. Activities with intermediate and low priority are listed under each of these goals. Tasks, preconditions, priority, institution in charge, cooperation institutions, financial source and timeline are listed for every activity.

The Action Plan is developed for the period 2018-2022. However, it is envisioned that a yearly review of the activities will be conducted.

Implementation

National ICT Council - to be transformed into National ICT and Security Council

The ICT Council consists of Ministers, thereby ensuring compliance of strategic-level decisions across state institutions. Extending this Council to be in charge of cyber security would result in systematic changes:
1. changing the name to a National Council for ICT and Security
2. changing the authority (IS would not fall under ICT, but coexist as an equally important field governed by this body).
3. adding new memebrs to the Council, among which the future Director of the Body with operational cyber security capacities.

The **Body with operational cyber security capacities*** (to be established within an existing state authority) will be in charge of the implementation of the activities defined in this Action Plan, thereby establishing a cyber security operational plan.

Note

*Untill the Body with operational cyber security capacities is established, this activity will be be conducted by the working group tasked to conduct the activities steming from the strategic documents in the field of cyber security.

Abreviations

AEC - Agency for Electronic Communications
AQAHE - Agency for quality assurance in higher education
AJPP - Academy of Judges and Public Prosecutors
ARM - Army of the Republic of Macedonia
BDE - Bureau for Development of Education
CDPMEA - Cabinet of the Deputy Prime Minister of the Government of the Republic of Macedonia, in charge for economic affairs and coordination of economic departments
CERT - Computer Emergency Readiness Team
CII - Critical Information Infrastructure
CIRT - Computer Incident Response Team
CMC - Crisis Management Center
CSIRT - Computer Security Incident Response Team
CSDFI - National Cyber Security and Digital Forensics Institute
DPDP - Directorate for Personal Data Protection
DSCI - Directorate for Security of Classified Information
EU - European Union
GRM - Government of the Republic of Macedonia
IIS - Important Information Systems
MASIT - ICT Chamber of commerce
MD - Ministry of Defence
MES - Ministry of Education and Science
ME - Ministry of Economy
MF - Ministry of Finance
MFA - Ministry of Foreign Affairs

MSSI - Military Service for Security and Intelligence
MISA - Ministry of Information Society and Administration
MJ - Ministry of Justice
MKD - CIRT - National Centre for Computer Incident Response
MoI - Ministry of Interior
NATO - North Atlantic Treaty Organization
NBRM - National Bank of the Republic of Macedonia
NCSC - National Cyber Security Council
OBCS - Body with operational cyber security capacities
PRDM - Protection and Rescue Directorate of Macedonia
PP - Public Prosecution
SEP - Secretariat for European Affairs
SL - Secretariat for Legislation
SSO - State Statistical Office of the Republic of Macedonia
FITD - Fund for Innovations and Technology Development
WB6 - Western Balkans 6

Number of activities	Activity	Code	Manner of implementation (Tasks)	Precondition	Priority	Leading institution	Collaborators	Financial source	Start date	End date
PRIORITY ACTIVITIES										
P1	Establishing a National Cyber Security Council	P1.1	Defining the authority and competences of the National Cyber Security Council according to the National Cyber Security Strategy.		highest	MISA	Cyber Security working group	/	November 2018	December 2018
		P1.2	Identification of a president and members of the National Cyber Security Council.							
		P1.3	Adopting a decision to establish a National Cyber Security Council (or extending the authority of the National ICT Council).							
P2	Establishing a Body with operational cyber security capacities (either as a newly formed, independent body (agency, directory) or as a new organizational unit within existing state authority.	P2.1	Analysis of existing institutional cyber security capacities in order to identify the best infrastructure for the Body with operational cyber security capacities	P1	highest	NCSC	MF, line ministries	Budget of RM	January 2019	June 2019
		P2.2	Establishing a Body with operational cyber security capacities and dividing activities with MKD-CIRT							
		P2.3	Identifying the required budget, infrastructure and human resources for the formation of the Body, as well as the means to provide the aforementioned resources.							
		P2.4	Assessment of the required legal changes and proposed amendment text							
		P2.5	Securing the necessary financial resources for the establishment of the Body.							
		P2.6	Deliver a proposal to the Government of RM for the establishment of the Body with operational cyber security capacities.						June 2019	January 2020
		P2.7	Adopting a legal framework supporting the establishment of the Body with operational cyber security capacities							
P3	Conducting a Study to identify the Critical Information Infrastructure (CII) and other Important Information Systems (IIS).	P3.1	Conducting a Study in order to be able to identify the Critical Information Infrastructure and Important Information Systems, and address the needs for transposition of EU regulation in this area. The study outputs should include: 1. identification of CII sectors 2. identification of authorities/ regulators for each sector 3. identification of operators for each sector 4. assessing the need to amend existing sector laws (lex generalis) for each of the identified sectors and provide recommendations.	P1	highest	MISA, MKD-CIRT	line ministries, Owners of the CII and IIS, Universities	Budget of RM and donor help	January 2019	April 2019

Number of activities	Activity	Code	Manner of implementation (Tasks)	Precondition	Priority	Leading institution	Collaborators	Financial source	Start date	End date
GOAL 1: CYBER RESILIENCE										
1.1	Advancing the capacities and capabilities of the National Centre for Computer Incident Response MKD-CIRT and facilitating growth and development of other CSIRT/CERT/CIRT teams.	1.1.1	Increasing the number of employees in the center by means of recruitment, filling in positions and continuous staff training in dealing with incidents, malware analysis, security checks and forensics.	P3	high	MKD-CIRT	line ministries and other sectors, including owners of the CII.	Budget of MKD-CIRT	2018	2022
		1.1.2	Expanding the services portfolio pursuant to the NIS Directive	P3	high	MKD-CIRT, OBCS*	all relevant stakeholders	Budget of MKD-CIRT	2018	2022
		1.1.3	Developing a national cyber incident taxonomy		high	MKD-CIRT	Universities, MISA	Budget of MKD-CIRT	January 2019	June 2019
		1.1.4	Developing additional CSIRT/CERT/CIRT teams on different levels divisional, institutional, academic, etc.).		high	organizations and institutions that require and have the capacities to develop CSIRT/CERT/CIRT teams	MKD-CIRT, OBCS*, line ministries and other sectors, including owners of the CII	organizational and institutional budgets	2019	continous
1.2	Establishing a single and comprehensive legal framework for cyber resilience, taking into account the legal regulatory framework in the Republic of Macedonia and the EU.	1.2.1	Preparation and adoption of a Law on security of network and information systems, thereby transposing the European Directive on security of network and information systems (NIS Directive 2016/1148).		highest	MISA	all stakeholders	Budget of RM or donor help	2019	2020
		1.2.2	Aligning the national legislation with the NIS Directive		high	MISA	line ministries, and all other relevant stakeholders	Budget of RM or donor help	2020	2021
		1.2.3	Aligning the Crisis Management Law, taking into consideration the cyber security risks.	P3	high	CMC, MD	MKD-CIRT, line ministries	Budget of RM	2019	2020
		1.3.1	Defining a list of CII and IIS based on Study results (P3).	P3	high	MISA	MKD-CIRT, Universities and all other relevant stakeholders, including CII and IIS owners	Budget of RM or donor help	2019	2019
		1.3.2	Propositions for relevant law amendments in order to define competences and responsibilities regarding CII.	P3, 1.3.1	high	MISA	MKD-CIRT and all other relevant stakeholders	Budget of RM	2019	2020

Number of activities	Activity	Code	Manner of implementation (Tasks)	Precondition	Priority	Leading institution	Collaborators	Financial source	Start date	End date
1.3	Identification and protection of CII (Critical information infrastructure) and IIS (Other important systems)	1.3.3	Propositions for minimal technical and organizational measures for information security for each identified sector.	P3, 1.3.1	high	OBCS*, MISA	MKD-CIRT and all other relevant stakeholders	Budget of RM	2020	2021
		1.3.4	Harmonization and adoption of Sectoral Acts (material laws) with the new law on information security.	1.2, P3, 1.3.1	high	MISA	line ministries	Budget of RM	2020	2021
		1.3.5	Harmonization of internal Acts of CII operators	1.3.1, 1,3,4	high	CII operators	line ministries	organizational and institutional budgets	2020	continuous
		1.3.6	Conducting continuous analysis, perceiving the real state and defining measures and recommendations for raising the level of cyber security for institutions in charge of CII and IIS management.	P3, 1.3.1, 1.3.4, 1.3.5	high	OBCS*	MKD-CIRT, line ministries, Universities, owners of the CII and IIS	Budget of RM	2020	2022
		1.3.7	Continuous improvement of resilience, integrity and reliability of CII and IIS.	P1, 1.3.6	high	NCSC, OBCS*	line ministries, Universities and the owners of the CII and IIS	Budget of RM	2020	2022
		1.3.8	Defining precise procedures for data storage and protection, processed in CII and IIS systems and conducting continuous analysis and audit on the effectiveness of the defined procedures.	P2, P3, 1.3.1	high	OBCS*	MKD-CIRT, DPDP, line ministries and the owners of the CII and IIS	Budget of RM	2020	2022
		1.3.9	Conducting regular audits in order to detect threats and risks of information systems and networks that are part of CII and IIS.	P2, P3	high	OBCS*	MKD-CIRT, Universitites, line ministries and the owners of the CII and IIS	Budget of RM	2020	2022
		1.3.10	Development and periodic testing of cyber attacks and cyber defence plans/scenarios	P2,P3	high	OBCS*	all stakeholders constituting the national defence	Budget of RM	2020	2022
1.4	Utilization of the best solutions for cyber incident prevention and response with the purpose of protecting the national security interests.	1.4.1	Monitoring the latest cyber security threats.	P2	high	MKD-CIRT, OBCS*	all stakeholders	Budget of RM	2019	continuous
		1.4.2	Monitoring and implementing the latest and best hardware and software solutions in response to cyber incidents.	P2	high	OBCS*	all stakeholders	Budget of RM	2020	continuous
		1.4.3	Continuous advancement of technological and organizational measures in order to effectively handle cyber threats.	P2	high	MKD-CIRT, OBCS*	all stakeholders	Budget of RM	2019	continuous
		1.4.4	Development of a methodology for cyber threats risk assessment at national level.	P1	high	NCSC	MKD-CIRT, all stakeholders	Budget of RM	2019	2022

Number of activities	Activity	Code	Manner of implementation (Tasks)	Precondition	Priority	Leading institution	Collaborators	Financial source	Start date	End date
		1.4.5	Continuous monitoring, adoption and implementation of internationally recognized standards and procedures in the field of cyber security.	P2	high	NCSC	all stakeholders	Budget of RM	2019	continuous
1.5	Taking measures and activities to handle cyber incidents of large scale and scope.	1.5.1	Defining a state of cyber crisis, a state of emergency and a state of war at national level in relation to cyber security.	P3, 1.2.3	high	CMC, MoD , MKD-CIRT	OBCS*, line ministries	Budget of RM	2019	2020
		1.5.2	Including a Cyber Security Representative in the Steering Committee in charge of proposing crisis response measures (CMC)	P3, 1.2.3	high	CMC	NCSC	Budget of RM	2019	2020
1.6	Providing/developing and implementing national capacities for redundant operational and communication systems available in case of large-scale cyber incidents	1.6.1	Identification of relevant entities and analysis of their competencies and coordination for conducting critical operations in state of crisis	P2	high	OBCS*	NCSC, line ministries and MKD-CIRT	Budget of RM or donor help	2020	2021
		1.6.2	Analysis on the current redundant operational and communication capacities and the interoperability of communication-information systems.							
		1.6.3	Project implementation for provision of redundant operational and communication capacities (isolated from public communication networks)							
		1.6.4	Adoption of procedures (standard, security) for establishing communication protocols between crisis management competent entities.							
		1.6.5	Conducting regular trainings and exercises for redundant operational and communication protocols, adapted to the roles and competences of each entity in the crisis management plan.							

Number of activities	Activity	Code	Manner of implementation (Tasks)	Precondition	Priority	Leading institution	Collaborators	Financial source	Start date	End date
GOAL 2: CYBER CAPACITIES AND CYBER SECURITY CULTURE										
2.1	Establishing a Cyber Security and Digital Forensics Institute (CSDFI)	2.1.1	Establishing a National Cyber Security and Digital Forensics Institute, in cooperation with all universities that have capacities in the field of cyber security		high	MoD/Military academy	Universities	Budget of RM	2019	continuous
		2.1.2	Establishing a Regional Cyber Security Center	2.1.1	high	OBCS*, CSDFI	FITD, MKD-CIRT, FA, MISA, MoD, MoI, regional cooperation WB6, Universities	Donor help	2020	continuous
		2.1.3	Implementation of a cyber security Centre of Excellence, as a model for capacity strengthening		high	OBCS*, CSDFI	FITD, MKD-CIRT, Universitites	Donor help	2021	continuous
2.2	Development and promotion of study programs and trainings in the area of cyber security at all levels of education	2.2.1	Improving the existing and developing a new curricula in primary and secondary schools and including elements in the field of cyber security in new university study programs.	2.1.1	high	MSE	CSDFI, Universities, AQUE, BDE	Budget of RM	2019	continuous
		2.2.2	Education and training of academic staff in primary and secondary schools in the field of cyber security and providing adequate and regularly updated resources for students.	2.1.1	high	MSE	CSDFI, Universities, AQUE, BDE	Budget of RM	2019	continuous
2.3	Raising the level of awareness and basic cyber security knowledge among citizens by cooperating with all relevant stakeholders.	2.3.1	Developing and distributing educational materials according for specific target groups.	P2, 2.1.1	medium	OBCS*	MISA, MKD-CIRT, NBRM, AEC, MoI, Universitites and all other relevant stakeholders	Budget of RM	2019	continuous
		2.3.2	Creating an e-learning platform.	P2	high	OBCS*	MISA, MKD-CIRT, CSDFI	Budget of RM	2020	continuous
		2.3.3	Supporting initiatives, campaigns, conferences, workshops and seminars in the field of cyber security intended for the general public.	P2, 2.1.1	medium	OBCS*, CSDFI	MISA, MKD-CIRT, Universities	Budget of RM	2019	continuous
		2.3.4	Raising awareness and basic knowledge in the field of cyber security for students in primary and secondary schools.		medium	Ministry of education and science	MISA, MKD-CIRT, Universities	Budget of RM	2019	continuous
2.4	Providing education and training and raising the level of awareness of cyber security in the public and private sector	2.4.1	Providing an adequate education and training in the field of cyber security for public administration staff.	P2, 1.6, 2.1	high	OBCS*	CSDFI, MISA, Universities	Budget of RM	2019	continuous
		2.4.2	Providing an adequate education and training in the field of cyber security for management staff in public and private sectors.	P2, 1.6, 2.1	medium	OBCS*	CSDFI, MISA, Private sector, Universities	Budget of RM / donor help / organizational budget	2019	continuous
		2.4.3	Strengthening the cyber security capacities in small and medium-sized enterprises.	P2	medium	OBCS*	CSDFI, Universities, MF, ME, MISA MKD-CIRT SSO	Budget of RM, donor help Budget of MKD-CIRT	2019	continuous

Number of activities	Activity	Code	Manner of implementation (Tasks)	Precondition	Priority	Leading institution	Collaborators	Financial source	Start date	End date
2.5	Advancing the cyber security capacities at national level	2.5.1	Provision of professional-expert education and training for individuals working in the field of cyber security.		medium	all relevant stakeholders			2020	2022 continuous
		2.5.2	Establishing retention mechanisms for ICT staff and cyber security work force.		medium	MISA, MF	all relevant stakeholders	Budget of RM		continuous
		2.5.3	Supporting the research capacities and business innovations through the establishment of Centre of excellence in the field of cyber security.	P1, 2.1	medium	FITD	NCSC, CSDFI, Universities	Budget of RM	2019	continuous
		2.5.4	Conducting research and establishing national priorities as a baseline for activities and investments for cyber security development.	P2	medium	OBCS*	FITD, CSDFI, all relevant stakeholders	Budget of RM	2021	2022
		2.5.5	Increasing cybersecurity capabilities in CII and IIS operators and the public sector	P2, P3, 1.3.4, 1.3.5	medium	OBCS* MKD-CIRT	CSDFI, MF, ME, MISA, Chambers of Commerce	Budget of RM, Budget of MKD-CIRT	2019	continuous
2.6	Providing response directions and guidelines in case of cyber incidents, cyber crisis at all levels in society, including guidelines for daily operations.	2.6.1	National guidelines for Disaster Recovery Plan Development	1.3.1	high	MKD-CIRT	CMC, OBCS*	Budget of MKD-CIRT	2019	2020
		2.6.2	Development of a Strategy for dealing with network and application layer attacks, as well as cloud attacks.		high	MKD-CIRT	CMC, OBCS*	Budget of MKD-CIRT	2020	2021
2.7	Provision and utilization of state-of-the-art hardware and software solutions for prevention, identification and management of cyber incidents.	2.7.1	Defining criteria, standards and guidelines in order to increase hardware and software security.	P2	medium	OBCS*	all relevant stakeholders	Budget of RM	2019	2022
		2.7.2	Provision of state-of-the-art hardware and software solutions for prevention, identification and management of cyber threats.	P2, 2.7.1	medium	OBCS*	all relevant stakeholders	Budget of RM		continuous
		2.7.3	Utilization control	P2		OBCS*	all relevant stakeholders	Budget of RM		continuous
2.8	Establishing a Centre for Internet Safety	2.8.1	Developing services in the line of improving the Internet safety		medium	civil organizations	MoI, line ministries, media and private sector	Donor help	2019	continuous

Number of activities	Activity	Code	Manner of implementation (Tasks)	Precondition	Priority	Leading institution	Collaborators	Financial source	Start date	End date
GOAL 3: COMBATING CYBER CRIME										
3.1	Advancing the cyber security capacities for combating cyber crime.	3.1.1	Analysis of the current capacities for combating cyber crime in RM.	P2	high	MoI, OBCS*	MKD-CIRT, all relevant institutions	Budget of RM / EU project funding	2018	2022
		3.1.2	Identification of all relevant institutions in the RM with competences and capacities for combating cyber crime.							
		3.1.3	Development of procedures and recommendations for cooperation between all institutions with competences for combating cyber crime.							
		3.1.4	Drafting a study on the need for training in combating cyber crime and digital forensics for all relevant institutions.							
		3.1.5	Developing training programs and curricula at national level for combating cyber crime and digital forensics.							
		3.1.6	Establishing a framework for cooperation with the private sector, Internet service providers and the academia.							
3.2	Harmonization of the national and international cyber crime policies.	3.2.1	Analysis of the current methodology, procedures and cooperation for combating cyber crime at national level.	P2, 3.1.1	high	MoI, OBCS*	MKD-CIRT, all relevant institutions	Budget of RM / EU project funding	2018	2022
		3.2.2	Comparison of the existing methodologies and procedures with international policies for combating cyber crime and electronic evidence.	P2, 3.2.1						
		3.2.3	Developing new or amending the existing methodologies and procedures for combating cyber crime and electronic evidence.	P2, 3.2.2						
3.3	Creating a single and comprehensive cyber crime legal framework, taking into account the legislation in the Republic of Macedonia and the EU.	3.3.1	Analysis of the current legal framework for cyber crime.	P2	high	MoI, OBCS*	all relevant institutions	Budget of RM / EU project funding	2018	2022
		3.3.2	Drafting a proposal for amendments to the legal framework for cyber crime and creating a special part that shall refer to cyber crime and electronic evidence, in compliance with EU legislation.	P2, 3.3.1						
3.4	Modernization of relevant institutions for effective combat against cybercrime.	3.4.1	Analysis of the current state and identification of the real necessary equipment of the competent institutions for effective combat against cyber crime and digital forensics.	P2	high	MoI, OBCS*	all relevant institutions	Budget of RM / EU project funding	2018	2022
		3.4.2	Preparation of a procurement plan for the necessary equipment and resources of the institutions in charge of combating cyber crime and digital forensics.	P2, 3.4.1						
		3.4.3	Developing digital forensic capacities and capabilities in other institutions and entities with cyber security responsibility.	P2, 3.4.2						
3.5	Establishing effective procedures for reporting and investigating cybercrime.	3.5.1	Establishing a system/platform for reporting cyber crime and information related to crimes in the area of cyber crime	P2	high	MoI, OBCS*	MKD-CIRT, all relevant institutions	Budget of RM / EU project funding	2018	2022
		3.5.2	Establishing procedures for including the private sector and academia in the information provision process related to crimes in the field of cyber crime	P2						

Number of activities	Activity	Code	Manner of implementation (Tasks)	Precondition	Priority	Leading institution	Collaborators	Financial source	Start date	End date
		3.5.3	Establishing procedures for data exchange obtained from the system with all institutions that have authorizations in combating cyber crime	P2						
3.6	Establishing formal mechanisms and procedures for cooperation and exchange of information in the area of cybercrime between relevant national entities and other security services.	3.6.1	Drafting a study required for cooperation within the cooperation framework between institutions		high	MoI, OBCS*	MKD-CIRT, all relevant institutions	Budget of RM / EU project funding	2018	2022
		3.6.2	Drafting cooperation and data exchange procedures between the relevant national entities and other security services							
		3.6.3	Establishing precise procedures for cooperation between the Computer crime and digital forensics center (MoI) and MKD-CIRT.							
3.7	Cooperation improvement with regional and international organizations combating cyber crime.	3.7.1	Analysis of the current state concerning cooperation with regional and international organizations for combating cyber crime.		high	MoI, OBCS*	MKD-CIRT, all relevant institutions	Budget of RM / EU project funding	2018	2022
		3.7.2	Establishing new mechanisms and developing procedures for cooperation with regional and international organizations for combating cybercrime.							
		3.7.3	Developing procedures at the national level for cooperation with international Internet service providers							
		3.7.4	Establishing procedures for participation of other institutions in charge of combating cyber crime in cooperation on regional and international level.							
3.8	Advancing the existing and establishing new mechanisms for cooperation and exchange of information with the private and civil sector and all other relevant entitites.	3.8.1	Analysis of the effectiveness of the existing cooperation mechanisms with MKD-CIRT, the private and civil sector and all other relevant enetities.		high	MoI, OBCS*	MKD-CIRT, all relevant institutions	Budget of RM / EU project funding	2018	2022
		3.8.2	Study and identification of the necessary cooperation with the public, private and civil sector and defining a cooperation framework							
3.9	Provision of professional and advanced, expert-level education and training for staff engaged with cyber crime identification and research.	3.9.1	Identification of the existing and relevant professional-expert t education and training at national and international level.		high	MoI, OBCS*	all relevant institutions	Budget of RM / EU project funding	2018	2022
		3.9.2	Drafting a plan and procedures for participation of representatives from all institutions in charge of combating cyber crime in professional-expert raining's at national and international level.							
3.10	Creating a multidisciplinary academic environment for promotion of the national investigation capacities for cyber crime.	3.10.1	Analysis of the current resources and capacities for academic research related to cyber crime and digital forensics		high	MoI, OBCS*	MKD-CIRT, all relevant institutions	Budget of RM / EU project funding	2018	2022
		3.10.2	Establishing a Center for Computer Security Excellence							
		3.10.3	Establishing procedures for participation in research activities in the Centre for Excellence in view of combating cyber crime and digital forensics							
	Active participation in the creation of international	3.11.1	Active monitoring of all new Regulations, standards, directives and recommendations on an international level for combating cyber crime and digital forensics.							

Number of activities	Activity	Code	Manner of implementation (Tasks)	Precondition	Priority	Leading institution	Collaborators	Financial source	Start date	End date
3.11	Active participation in the creation of international regulations and standards for cybercrime and their implementation at national level.	3.11.2	Drafting a plan for the implementation of all Regulations, standards, directives and recommendations on an international level for combating cyber crime and digital forensics, including all institutions in charge of combating cybercrime.		medium	MoI, OBCS*	all relevant institutions	Budget of RM / EU project funding	2018	2022
3.12	Continuous assessment of the adequacy and effectiveness of the national cybercrime regulation.	3.12.1	Analysis and assessment of the adequacy and efficiency of the existing legislation for combating cybercrime		medium	MoI, OBCS*	Remaining institutions	Budget of RM / EU project funding	2018	2022
		3.12.2	Drafting proposals to supplement and amend the national legislation in the field of cyber crime identification and investigation							
3.13	Continuous education of judicial authorities in the field of cyber security, cybercrime and electronic evidence.	3.13.1	Analysis of the necessary education and training of judicial authorities in the field of cyber crime research and electronic evidence		high	MoI, AJPP	MJ, PP	Budget of RM / EU project funding	2018	2022
		3.13.2	Drafting a Curriculum for Judicial Authorities							
		3.13.3	Drafting a Plan for conducting education and training of judicial authorities for cybercrime and electronic evidence investigation.							

Number of activities	Activity	Code	Manner of implementation (Tasks)	Precondition	Priority	Leading institution	Collaborators	Financial source	Start date	End date
GOAL 4: CYBER DEFENCE										
4.1	Defining the national capacities for cyber defence.	4.1.1	Securing an efficient system for the protection of classified information in the cyber space through continuous advancement of the level of cyber attack protection and cyber espionage of the national systems and networks processing classified information.	Law for classified information	high	DSCI	all stakeholders in national defence	Budget of RM	continuous	continuous
		4.1.2	Developing a cyber defence strategy	National Cyber Security Strategy	high	MoD	ARM, MoI, DSCI, CMC, MISA, MKD-CIRT, SSO	Budget of RM	Nov 2018	Mar 2019
		4.1.3	Developing national policies, procedures and instructions in the field of cyber defence	A4.1.2	high	MoD	ARM, MoI, DSCI, CMC, MISA, MKD-CIRT, SSO	Budget of RM	May 2019	Dec 2020
		4.1.4	Development of cyber defence abilities and capacities for all stakeholders in national defence	National Cyber Security Strategy	high	MoD	MKD-CIRT, OBCS*	Budget of RM / NATO programs	continuous	continuous
		4.1.5	Defining/overview of resources of the state, the private and public sector for active defence from cyber attacks	P2	high	MKD-CIRT, OBCS*	All public institutions, CII, IIS, IT operators, IT companies	Budget of RM	6 months after establishing the OBCS*	1 year
		4.1.6	Defining evaluation criteria for cyber defence capacities	Establish a Law for Information Security or amendments of the Law of Classified Information	high	OBCS*	All constituents in the national defence	Budget of RM	3 months after adoption of regulation	1 year
		4.1.7	Analysis of existing infrastructure, technical and organizational institutional capacities, in order to determine the state cyber defence capacities. To outline weaknesses and reduce the risks in order to mitigate them and advance the existing capacities.	4.1.6, P3	high	OBCS*	MoD, MKD-CIRT, all constituents in the national defence	Budget of RM	3 months after 4.1.6	1 year
4.2	Defining the military capacities within the Ministry of Defence (MoD) and the Army (ARM) for handling cyber threats.	4.2.1	Establishing and developing a military CERT	4.1.2	high	MoD, ARM	MoD, ARM	Budget of RM / NATO programs	6 months after 4.1.2	1 year
		4.2.2	Developing capacities and capabilities for cyber defence in the MoD and ARM.	4.1.2	high	MoD, ARM	MoD, ARM	Budget of RM / NATO programs	continuous	continuous
		4.2.3	Developing cyber capacities for alarming, prevention, protection, detection, forensics and defending the military CI systems (stationary and mobile)	4.1.2	high	MoD, ARM	MoD, ARM	Budget of RM / NATO programs	continuous	continuous
		4.2.4	Establishing a military cyber defence authority	4.1.2	high	MoD, ARM	MoD, ARM	Budget of RM	6 months after 4.1.2	1 year
		4.2.5	Utilizing the NATO partnership/membership for the development of resources, training and capacities.	NATO membership	high	MoD, ARM	MoD, ARM	Budget of RM	continuous	continuous
		4.3.1	Developing a CSIRC (Computer Security Incident Response Capability) for CIS at MoD and ARM	4.1.2	high	MoD, ARM	MoD, ARM	Budget of RM / NATO programs	1 year after 4.1.2	2 years

Number of activities	Activity	Code	Manner of implementation (Tasks)	Precondition	Priority	Leading institution	Collaborators	Financial source	Start date	End date
4.3	Establishing/developing, and maintenance of the defined cyber security capacities and capabilities.	4.3.2	Developing mobile cyber defence capacities (CD-deploy), compatible with NATO CII, at the level of battalion command.	4.3.1	high	MoD, ARM	MoD, ARM	Budget of RM / NATO programs	3 months after 4.3.1	2 years
		4.3.3.	Developing operational plans for all service providers in the cyber space according to national scenarios.	4.1.7	medium	OBCS*, MKD-CIRT	all service providers in the cyber space	Budget of RM	6 months after 4.1.7	2 years
4.4	Establishing a comprehensive cyber defence legal framework, taking into consideration the legal framework in Macedonia as well as NATO and EU directives.	4.4.1	Aligning cyber defence regulations, according to the national legal framework, as well as NATO and EU directives.	4.1.2	high	MoD, ARM	MJ, SL	Budget of RM	continuous	continuous
		4.4.2	Defining and implementation of measures for strategic management of cyber defence.	National Cyber Security Strategy, P2	high	OBCS*	all constituents of the national defence	Budget of RM	continuous	continuous
4.5	Defending (mitigating) and decreasing the cyber risks.	4.5.1	Developing a cyber threat risk assessment methodology for MoD and ARM.	4.1.2	high	MoD, ARM	MSSI	Budget of RM	6 months after 4.1.2	2 years
		4.5.2	Continuous protection of confidentiality, integrity and data and information authentication of military networks (CII).	continuous	high	MoD, ARM	DSCI	Budget of RM	continuous	continuous
4.6	Establishing and maintenance of international cooperation for deterring shared cyber threats and increasing the national and international security and stability.	4.6.1	Establishing a national contact point for NATO cyber operations and cooperation.	NATO membership	high	MoD, ARM	MoD, ARM	Budget of RM	NATO membership	6 months
		4.6.2	Establishing a contact point for secure communication, for the needs of national authorities with NATO, by securing interoperability and alignment with NATO cryptographic system (special documents for cryptographic system) for the protection of confidentiality, integrity and authentication of such data and information.	Reform programed	high	MoD	ARM, DSCI	Budget of RM	Dec 2018	Apr 20120
		4.6.3	Inclusion of the Republic of Macedonia in the collective NATO cyber defence and resource utilization	NATO membership	high	MoD	ARM	Budget of RM	NATO membership	continuous
4.7	Defining and coordinating the military planning of the way and use of military cyber capacities with the national cyber defence in different circumstances.	4.7.1	Defining regulation for the way and use of military cyber capacities in the process of national cyber defence in diverse situations.	4.1.2	high	MoD, ARM	MoD, ARM	Budget of RM	3 months after 4.1.2	2 years
		4.7.2	Including MoD and ARM experts in the national bodies for cyber threat management and handling.	establishing national bodies	high	OBCS*	MoD, ARM	Budget of RM	continuous	continuous
4.8	Inclusion and contribution in the collective cyber defence through international cooperation.	4.8.1	Establishing an interoperability system and aligning the national cryptographic system (specialized documents for cryptographic system) with the NATO cryptographic system for the protection of confidentiality, integrity and availability of the confidential information.	NATO membership	high	MoD	ARM	Budget of RM	NATO membership	continuous
		4.8.2	Implementation and monitoring of NATO cyber security/cyber defence standards and directives.	NATO membership	high	MoD	ARM	Budget of RM	continuous	continuous
		4.9.1	Training and awareness raising activities for cyber defence through education and training of the whole MoD and ARM staff.	4.1.2	high	MoD, ARM	Military academy	Budget of RM	continuous	continuous
		4.9.2	Defining and continuous training education of the necessary experts for operational and tactical cyber defence and CII cyber threats management.	4.1.2	high	MoD, ARM	Military academy	Budget of RM	continuous	continuous

Number of activities	Activity	Code	Manner of implementation (Tasks)	Precondition	Priority	Leading institution	Collaborators	Financial source	Start date	End date
4.9	Continuous education in order to secure highest level of awareness and personal responsibility with regards to cyber defence and the national defence and security.	4.9.3	Organizing national cyber defence exercises in cooperation with all stakeholders relevant to cyber security.	National Cyber Security Strategy	high	MKD-CIRT	MoD, OBCS*, all constituents in the national defence	Budget of RM, Budget of MKD-CIRT, donor help	continuous	continuous
		4.9.4	Raising the awareness of cyber threats and risks in order to sustain the cyber defence.	National Cyber Security Strategy, P2, 4.1.2	high	OBCS*	all constituents in the national defence	Budget of RM	continuous	continuous
		4.9.5	Integration of cyber defence in all operational exercises at a national level.	National Cyber Security Strategy	high	MoD, OBCS*, MKD-CIRT	all constituents in the national defence	Budget of RM	continuous	continuous
4.10	Developing and implementation of a system and programs for information exchange and sharing data, knowledge and experiences among the public, private and defence-security sector in the field of cyber security, in order to protect CII and IIS.	4.10.1	Active participation at military exercises and seminars for cyber defence.	National Cyber Security Strategy	medium	MoD, ARM	MoD, ARM	Budget of RM	continuous	continuous
		4.10.2	Developing a civil-military cooperation for the needs of cyber defence of the public and private sector.	National Cyber Security Strategy, P2	high	OBCS*	public and private sector, MoD, ARM	Budget of RM	continuous	continuous
		4.10.3	Developing systems and procedures for information exchange regarding risks and threats in the national and international cyber defence.	4.2.1	high	MKD-CIRT	MoD, ARM, MISA	Budget of RM	continuous	continuous
		4.10.4	Establishing cooperation and exchange of information in the national systems for collective defence in the field of cyber defence.	4.1.7	high	OBCS*	all constituents in the national defence	Budget of RM	4.1.7 end date	continuous
		4.10.5	Establishing a system for knowledge sharing and information exchange in the field of cyber defence.	2.1.1	medium	CSDFI	all relevant stakeholders	Budget of RM	continuous	continuous

Number of activities	Activity	Code	Manner of implementation (Tasks)	Precondition	Priority	Leading institution	Collaborators	Financial source	Start date	End date
GOAL 5: COOPERATION AND EXCHANGE OF INFORMATION										
5.1	Promoting collaboration in the field of cyber security on a national level.	5.1.1	Developing an effective model for cooperation at national level among institutions in charge of cyber security and advancing their existing structure and processes.	P2, P3	medium	OBCS*	all rekevant stakeholders	Budget of RM/ donor help	2019	2021
		5.1.2	Establishing a Register of Cyber Security National Experts (individuals from the public, private, academic and civil sector) with relevant expertise.	P2	high	MKD-CIRT	OBCS*	Budget of RM/ donor help	2019	2019
		5.1.3	Obliging all government and public institutions to become constituents of MKD-CIRT.	P1, P2	high	MISA	MKD-CIRT	Budget of RM/ donor help	2019	2019
		5.1.4	Building a network of CIRTs in the country, interconnected and connected with the national CERT.		medium	MKD-CIRT	all relevant stakeholders	Budget of RM/ donor help	2019	continuous
		5.1.5	Efficient data exchange between state and entities that manage CII and IIS.	P2, 1.3.1	medium	OBCS*	MKD-CIRT, CII owners, all relevant stakeholders	Budget of RM/ donor help	2019	continuous
		5.1.6	Promoting and advancing the norms, rules and principals of behavior of the state, pursuant to the stipulated principles on an international level.		medium	MISA	'all relevant stakeholders	Budget of RM/ donor help	2019	continuous
		5.1.7	Cooperation of stakeholders on research projects on a national and international level.	P1	medium	NCSC	Academic community, all relevant stakeholders	Budget of RM/ donor help	2019	continuous
		5.1.8	Cooperation of all relevant stakeholders in the process of developing and unifying security norms, standardizing cooperation, as well as defining and setting mandatory level of protection of entities that manage CII and IIS.	P2, 1.3.1	medium	OBCS*	all relevant stakeholders	Budget of RM/ donor help	2019	continuous
		5.1.9	Cooperation with the private sector, in order to facilitate a cyber space that provides a safe environment for the exchange of information, research and development, as well as to provide secure information security infrastructure that would stimulate entrepreneurship, thereby supporting competitiveness of all domestic companies and protecting their investments.	P1	high	NCSC	MASIT, MKD-CIRT, MISA ME, CDPMEA	Budget of RM/ donor help	2019	continuous
		5.1.10	Building trust among all relevant stakeholders, including the development of a national platform/system for the exchange of information regarding laws, incidents and imminent threats.	P1, 1.3.4, 1.3.5, 1.4.1, 1.4.2	medium	NCSC	MKD-CIRT	Budget of RM/ donor help	2019	continuous
		5.1.11	Cooperation of all relevant stakeholders in order to develop and implement technology that provides maximum security and transparency, as well as testing and asessment of the level of technology being utilized at present.	P2, 1.3.8, 1.3.9, 1.4, 2.5.5, 2.6.1, 2.6.2, 2.7.1, 4.1	medium	OBCS*	MISA, CSDFI, Universitites	Budget of RM/ donor help	2019	continuous

Number of activities	Activity	Code	Manner of implementation (Tasks)	Precondition	Priority	Leading institution	Collaborators	Financial source	Start date	End date
5.2	Promoting a collaboration in the field of cyber security on an international level	5.2.1	Establishing and strengthening cooperation and building trust with other public and private international CERT and CSIRT teams, academic communities and other international organizations.		high	MKD-CIRT	all relevant stakeholders	Budget of RM/ donor help	2018	continuous
		5.2.2	Active participation and contribution towards building international abilities for cyber security and trust building activities.	P2	medium	OBCS*	all relevant stakeholders	Budget of RM/ donor help	2019	continuous
		5.2.3	Developing efficient mechanisms and procedures for international cooperation on a diplomatic level in case of cyber incidents, attacks and crisis, according to internationally established principles.		medium	MFA	all relevant stakeholders	Budget of RM/ donor help	2019	continuous
5.3	Utilizing a coordinated approach in order to address the challenge of Interntet governance and norms of behaviour.	5.3.1	Cooperation of all relevant stakeholders in the development of national legislatives, and contributing in the process of defining international legislatives related to the cyber space behaviour, freedom of speech, personal data protection, privacy as well as basic human rights and liberties.		medium	MISA	MJ, DPDP, Ombudsman OF Macedonia, civil organizations	Budget of RM/ donor help	2019	continuous