Republic of North Macedonia

Ministry of Defence

Minister

Radmila Sekerinska Jankovska

CYBER DEFENCE

STRATEGY

Content

Introduction

Security of citizens, protection of sovereignty and territorial integrity, principles of democracy and rule of law are some of the concepts and basic principles of modern democratic society of the Republic of North Macedonia. To maintain these values, the state must build and maintain a complex system of national defence based on long-term visions and strategies. Social and technological advances in society have led to a need for changes in conventional forms and methods used in the defence area. Cyber attacks are becoming more sophisticated and damaging. Furthermore, the new hybrid method of warfare is based on asymmetric military methods and many activities are taking place in the cyberspace, which is why cyberspace is more often being defined as the fifth dimension of warfare.

NATO recognizes cyberspace as planning and operational domain, and the cyber attack as a potential trigger of Article 5 of the North Atlantic Treaty. Therefore, in accordance with the requirements of Article 3 of the North Atlantic Treaty, countries should maintain and develop individual and collective capabilities, in order to cope with challenges and threats in cyberspace. Republic of North Macedonia is committed to increasing the national capacities, but also to building collective capacities through participation in joint activities and intensifying the cooperation in the field of cyber defence at regional and international levels.

In this regard the Republic of North Macedonia adopted the National Cyber Security Strategy in July 2018, and in December 2018 the Action Plan for implementation of the strategy and started the implementation of the defined activities. The National Cyber Security Strategy recognizes cyber defence as an autonomous and specific branch of the broader concept of cyber security. Also, pursuant to the Defence Law, the cyber defence is perceived as part of the defence of the country. The law defines the defence of the state as a system for defence of the independence and territorial integrity, as well as protection of the lives of citizens and their property from external attack. This includes construction of an effective system of national defence, training and deployment of relevant force and assets, and participation in NATO collective defence system.

Cyber defence differes from cyber security mainly in the nature and severity of cyber attacks, with no opportunity to define precise criteria. Therefore, the readiness to defend against cyber attacks must be comprehensive and must not focus only in the security area. The state must develop its own capacities and capabilities to resist even such cyber attacks that could trigger the defence of the country. A specific feature of cyber defence will be that it will be active not only in emergencyand crisis situations, but will act consistently even in everyday situations.

The cornerstone for the development of an effective cyber defence in the Republic of North Macedonia is Government's commitment to capacity building and cyber defence reinforcement, outlined in the Action Plan for Cyber Security of the Republic of North Macedonia 2018-2022.The concept is based on a conscious understanding of the differences between cyber security and cyber defence. In this Cyber Defence Strategy are defined the conceptual conditions for a proper defence of the Ministry of Defence of the Republic of North Macedonia and the Army of the Republic of North Macedonia (Army) in cyberspace and are presented the basic vision, mission and objectives, describing the planned end state of separate problem areas. Activities arise from the defence commitment of the Republic of North Macedonia, reflecting current trends of modern defence doctrines and are in full compliance with the basic rules of a democratic state. With preparation and implementation of these activities the fundamental rights and freedoms of individuals are preserved and protected, as well as the aforementioned principles and values, because the security and freedom are not contradictory to each other. There is no freedom without security, or security without freedom.

The Cyber defence strategy has been developed in accordance with the National Cyber Security Strategy, European Union Cyber Security Strategy and Policy, and NATOs'commitment to cyber security for providing safe, reliable and resilient digital environment.

Key challenges for cyber defence of the Republic of North Macedonia

There are a number of potential attackers, state or non-state actors that can commit cyber attack with an intensity that can activate the cyber defence system of the Republic of North Macedonia. Cyber attacks are ideal tools for damaging the political, business or other targets, as well as a powerful tool for the attackers to enforce their intentions. At the same time, often it is very difficult to identify the attacker, thus reducing the possibility of potential appropriate response to the attack. These facts, together with the absence of geographical and similar restrictions, which reduce the ability to detect the location and identify the attackers, are basis for increase utilization of cyberspace for malicious activities of different reasons and for different purposes.

Primary targets of cyber attacks can be users and systems that closely interconnect the computer environment with the real infrastructure. Attacks can even directly target the components of the defence infrastructure.

One of the key challenges facing the cyber defence is the progress of offensive cyber capabilities of potential rogue states. Other challenges include the increasing use of cyberspace by terrorists and terrorist organizations, the growing trend of abuse of cyberspace by criminals and criminal organizations, and the correlation between state and non-state attackers.

The growing dependence of the functionality of the security and defence forces of the state of information and communication technologies increases the need for establishment of a functional cyber defence system.Lack of security policies, procedures and guidelines, low digital literacy and lack of awareness of individual users of security rules to be respected in cyberspace can be distinguished as more dominant weaknesses and challenges perceived.

The most important challenges, trends and potential threats to the Macedonian society, as well as the defence system of the Republic of North Macedonia are defined in the National Cyber Security Strategy.[1]

[1] National Cyber Security Strategy 2018-2022, http://www.mio.gov.mk/sites/default/files/pbl_files/documents/strategies/ns_sajber_bezbednost_2018-2022.pdf

Vision and Mission

Vision

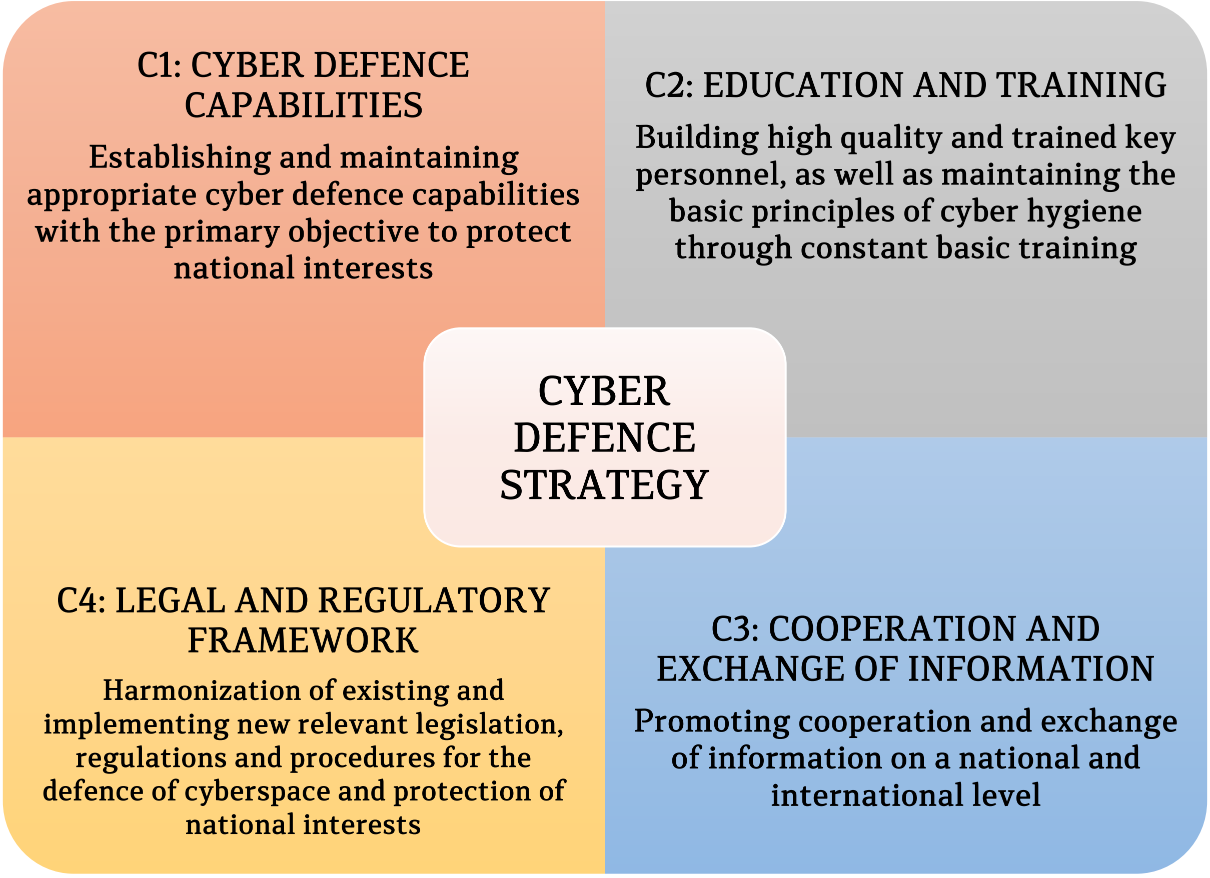
The vision of the Cyber DefenceStrategy, according to the National Cyber Security Strategy, is to create and maintain a safe, secure, reliable and resiliant digital environment, supported by quality built capabilities and capacities, highly qualified experts, a level of trust built and national and international cooperation in the field of cyber defence.

Mission

The mission of the Cyber Defence Strategy is to develop and strengthen capacities and capabilities for active monitoring of cyberspace threats and attacks, and reduction of the effects of these threats in order to protect the national interests.

Strategic goals

Cyber Defence Strategy is based on achieving four strategic objectives whose main objective is to strengthen the capabilities for monitoring and defence against cyber threats and attacks, and to increase security in cyberspace in all sectors and at all levels.



C1: CYBER DEFENCE CAPABILITIES

Establishing and maintaining appropriate cyber defence capabilities with the primary objective to protect national interests

C2: EDUCATION AND TRAINING

Building high quality and trained key personnel, as well as maintaining the basic principles of cyber hygiene through constant basic training

CYBER DEFENCE STRATEGY

C4: LEGAL AND REGULATORY FRAMEWORK

Harmonization of existing and implementing new relevant legislation, regulations and procedures for the defence of cyberspace and protection of national interests

C3: COOPERATION AND EXCHANGE OF INFORMATION

Promoting cooperation and exchange of information on a national and international level

Figure 1: Cyber Defence Strategy Objectives

1. CYBER DEFENCE CAPABILITIES

Establishing and maintaining appropriate cyber defence capabilities with the primary objective to protect national interests

In order to protect cyberspace, it is crucial to develop adequate cyber defence capabilities. These capabilities should provide the basis for successful cyber operations related to the defence of cyberspace, as in the Ministry of Defence of the Republic of North Macedonia and the Army, as well as at national and international level. Ministry of Defence of the Republic of North Macedonia and the Army will develop capacities and capabilities that will actively contribute to cyber defence in the country and will support the international organizations (UN, NATO, EU,etc.) to deal with the threats globally. Capabilities that will be developed will be able to proactively anticipate the dangers from potential attacks, locate active cyber attacks, as well as to analyze and practice possible responses for their prevention, by building capabilities for cyber resilience and cyber deterrence. Also skills for active and successful management of crises that would be faced with in the event of potential successful cyber attacks are to be developed. To meet this goal, one of the key challenges is facing a shortage of qualified and well-trained personnel for cyber defence. Hence, one of the major priorities will be more effective recruiting of suitable staff and retaining and motivating the existing one.

1.1. National capabilities for cyber defence

1.1.1 Developing appropriate skills and effective cyber defence capabilities for all constituents that are part of the national defence.

1.1.2 Defining the criteria for evaluation of cyber defence capabilities and capacities.

1.1.3 Analysis, recording and evaluation of existing infrastructure and institutional capacities available to the state, public and private sector, which can be used for the needs of cyber defence.

1.1.4 Development and implementation of measures for strategic management of national capacities for cyber defence in accordance with the Defence Law and other related national regulations.

1.2. Military capabilities in the Ministry of Defence of the Republic of North Macedonia and the Army to deal with threats in cyberspace

1.2.1 Establishment and development of a military team for monitoring, coordination and handling computer incidents (MIL-CIRT).

1.2.2 Development of capabilities and capacities for cyber defence in the Ministry of Defence and the Army of North Macedonia.

1.2.3 Establishment and development of Military Authority for cyber defence.

1.2.4 Continuously provide confidentiality, integrity and availability of data and information on military networks and systems.

1.2.5 Providing an effective system for classified information protection in cyberspace through continuous improvement of the level of protection from cyber attacks and cyber espionage systems and networks of the Ministry of Defence and the Army of North Macedonia through which classified information are processed.

1.2.6 Development of deployable cyber defence capabilities at battalion command level compatible with NATO.

1.2.7 Identification of needs for cyber professionals and defining the pool of potential human resources.

1.2.8 Developing motivating system of rewards and promotions of expert personnel in the field of cyber security and defence, based on quality and personnel presented results by determination of a salary supplement for the expert personnel in cyber defence and security area, depending on the tasks, expertise and irreplaceability.

1.2.9 Forming the active reserve for the needs of cyber defence and defining appropriate policies for recruitment and engagement of experts in this field.

1.2.10 Establishing programs for exchange of experience with experts from civil companies in order to improve the training of personnel for cyber defence.

2. EDUCATION AND TRAINING

Building high quality and trained key personnel, as well as maintaining the basic principles of cyber hygiene through constant basic training

This strategic objective focuses on building skills that will enable stakeholders to gain the appropriate level of knowledge in the field of cyber defence. Promoting cyber hygiene and raising awareness of cyber security means encouraging responsibility and understanding of cyber risks in all spheres of society, while providing clear message that personal data protection is usually responsibility of each individual, and then of the different service providers . Achieving this goal means creating skills, knowledge and experience for protection, while providing greater resistance to malicious cyber activities.

In the process of acquiring skills, knowledge and experience in the field of cyber security at the national level an important role will be given to the establishment of the Institute for cyber security and digital forensics within the Military Academy "General Mihajlo Apostolski" - Skopje, establishment of an ad-hoc inter-sector research teams composed of experts from public sector, private sector and academic community, as well as active participation in various research and training activities organized by partner countries and international organization.

2.1. Continuous education for ensuring a high level of awareness and personal responsibility in terms of cyber defence in the context of national defence and security

2.1.1 Raising awareness on cyber defence through education and training of the entire staff at the Ministry of Defence of North Macedonia and the Army.

2.1.2 Defining and continuously education of the required number of experts for strategic, operational and tactical cyber defence and cyber threat management at the Ministry of Defence of North Macedonia and the Army.

2.1.3 Forming and establishing an Institute for cyber security and digital forensics within the Military Academy "General Mihajlo Apostolski" - Skopje, with the main goal of research, education and training in the area of cyber defence.

2.1.4 Active participation in NATO Cooperative Cyber Defence Center of Excellence (CCDCOE) by sending national experts and participation in research activities of the Center.

2.1.5 Creating and developing simulations and programmes for cyber security incidents to be used in national cyber defence exercises.

2.1.6 Organization of national cyber defence exercises in cooperation with all stakeholders as part of the national defence system.

2.1.7 Integration of the cyber defence segment in all operation exercises at the national level, in the area of national defence.

2.1.8 Active participation in international military exercises and training on cyber defence.

2.1.9 Joint sharing of capacities and experience with NATO, EU and partner countries.

3. COOPERATION AND EXCHANGE OF INFORMATION

Promoting cooperation and exchange of information on national and international level

Isolation of a state in dealing with cyber threats is doomed to failure. Effective cyber defence can only be achieved in cooperation with state and non-state entities, both nationally and internationally. For this purpose it is necessary to define appropriate processes, procedures and protocols for cooperation and exchange of information between the stakeholders. Cyberspace is a complex dimension where it is difficult to define the boundaries. So, besides the need for effective cooperation at national level, there is a need for establishing strong regional and international alliances, mainly within the UN, NATO, EU. Within the efforts for active cooperation, preparation and participation in various training activities organized by international organizations would be essential, because they are an important source of information and exchange of experiences related to technical and legal dimensions of cyber defence. Fulfillment of this strategic goal will bring significant improvement to the cyber defence, not only of the Republic of North Macedonia, but also to the allied countries and organizations.

3.1 Establishment and maintenance of mutual international cooperation and exchange of information on shared deterring cyber threats and increasing national, regional and international security and stability

3.1.1 Development and implementation of a system and a programme for exchange and sharing of information, knowledge and experiences between the public, private and defence- security sector in the field of cyber defence, to protect the CII and III.

3.1.2 Development of civil-military cooperation for the cyber defence and promotion of the cooperation between the public and private sectors.

3.1.3 Establishing cooperation and information exchange in the area of cyber defence among all constituents of the national defence system.

3.1.4 Defining the national point of contact with NATO in terms of cyber operations and cooperation.

3.1.5 Establishing point for secure communication with NATO.

3.1.6 Participation of the Republic of North Macedonia in NATO collective cyber defence and setting a system for cooperation and exchange of information.

3.1.7 Establishing and maintaining cooperation with other partner countries in the field of cyber defence

4. LEGAL AND REGULATORY FRAMEWORK

Harmonization of existing and implementing new relevant legislation, regulations and procedures for the defence of cyberspace and protection of national interests

Republic of North Macedonia has adopted the National Cyber Security Strategy at the end of 2018, making regulation of cyber defence and strengthening of all other capacities associated with cyber defence at the outset. For this reason, regulations, acts and procedures related to cyber defence, and also with all other segments of cyber security, not defined in full. At this stage, it is necessary to use existing legislation and to define core competencies and responsibilities of the stakeholders, as well as the rights and obligations of the authorized personnel in the area of cyber security and defence. A very important segment is the definition and establishment of an efficient system to control the activities related to regulation of cyber defence. Additional legal acts will be defined and passed in order to create a legal framework in accordance with the national needs, in accordance with the guidelines of the international organizations. The fulfillment of this strategic goal will define basic legal aspects of cyber defence. An important step will be our participation in the legal regulation of cyber defence at international level.

4.1. Creating unique and comprehensive legal framework for cyber defence, by taking into account the legislation of the Republic of North Macedonia and the EU and NATO directives

- 4.1.1 Development and implementation of a system and a programme for exchange and sharing of information, knowledge and experience between the public, private and defence- security sector in the area of cyber defence, in order to protect and CII and the III.
- 4.1.2 Development of new and harmonization of existing regulations on cyber security and defence, in accordance with the legislation of the Republic of North Macedonia and the EU and NATO directives.

4.1.3 Definition and implementation of measures for strategic management of cyber defence in the Ministry of Defenceof North Macedonia and the Army

4.1.4 Development of methodology for risk assessment of cyber threats at the level of the Ministry of Defence of North Macedonia and the Army

4.1.5 Development of operational plans for all cyber service providers in accordance with the defence plan.

4.1.6 Development of system and procedures for information exchange about threats and risks in the field of cyber defence at international level.

4.1.7 Defining the roles and responsibilities of the armed forces in the protection of military CII and III and the development of adequate capabilities.

4.1.8 Defining and coordinating military planning regarding the method and the use of military cyber capabilities with the national cyber defence in various situations.

Implementation

The implementation of the Strategy will be done in accordance with the Action Plan and will be subject to continuous annual analysis and evaluation, with specific proposals for improvement. Taking into account that modern technologies are in constant development and it is almost impossible to predict the new trends of development, it is necessary for the Strategy to be subject to constant updating in accordance with the analysis and the identified needs.

Conclusion

The implementation of the strategic objectives and activities defined in the Strategy and the Action Plan must provide establishment of an efficient cyber defence system. Continuous investment in building capabilities and capacities for effective cyber defence will provide quality and technologically developed institutions that can effectively and efficiently deal with the challenges in cyberspace.

ANNEX

Acronyms

Army - Army of the Republic of North Macedonia

III - Important information systems

EU - European Union

CII - Critical Information Infrastructure

CIS - Communication Information Systems

NATO - North Atlantic Treaty Organization

UN - United Nations Organization

CIRT -Computer IncidentsResponse Team

CCDCOE - NATO Cooperative Cyber Defence Centre of Excellence

Introduction

The goal of this document is to define the steps of Republic of North Macedonia Defence Cyber Strategy implementation. A Working Group has been established in the Ministry of Defence and the Army that is responsible for development of strategic documents in the cyber defence area. The Working Group considered the already endorsed National cyber defence strategy, the SDR, LTPDC, the NATO memebrship Action Plan and the Plan for integration in NATO, as well as the NATO Policy on cyber defence and the Cyber Defence Action Plan, based on which the Cyber defence Strategy has been developed.

This Action Plan includes the main activities needed for strengthening the cyber defence capacities, in compliance with the proposed and adopted Strategy.

Activity no.	Activity	Code	Implementation manner (tasks)	Stakeholder	Associates	Timeline
OBJECTIVE 1. CYBER DEFENCE CAPABILITIES						
1.1	1.1. National cyber defence capabilities	1.1.1	Developing appropriate skills and effective cyber defence capabilities for all constituents that are part of the national defence	Ministry of Defence of the Republic of North Macedonia/Army	all constituents part of the national cyber defence system	2019-2023
		1.1.2	Defining the criteria for evaluation of cyber defence capabilities and capacities	Ministry of Defence of the Republic of North Macedonia/Army	all constituents part of the national cyber defence system	6 months after adopting the national criteria for III evaluation
		1.1.3	Analysis, recording and evaluation of existing infrastructure and institutional capacities available to the state, public and private sector, which can be used for the needs of cyber defence	Ministry of Defence of the Republic of North Macedonia/Army	all constituents part of the national cyber defence system	2019-2023
		1.1.4	Development and implementation of measures for strategic management of national capacities for cyber defence in accordance with the Defence Law and other related national regulations	Ministry of Defence of the Republic of North Macedonia/Army	all constituents part of the national cyber defence system	1 year according 1.1.3
1.2	Military capabilities in the Ministry of Defence of the Republic of North Macedonia and the Army to deal with threats in cyberspace	1.2.1	Establishment and development of a military team for monitoring, coordination and handling computer incidents (MIL-CIRT).	Army	Ministry of Defence of the Republic of North Macedonia	2019 basic capacity 2020-2023 final capacity
		1.2.2	Development of capabilities and capacities for cyber defence in the Ministry of Defence and the Army of North Macedonia	Ministry of Defence of the Republic of North Macedonia/Army		2019-2023
		1.2.3	Establishment and development of Military Authority for cyber defence	Army	Ministry of Defence of the Republic of North Macedonia	2020-2021
		1.2.4	Continuously provide confidentiality, integrity and availability of data and information on military networks and systems	Army	Ministry of Defence of the Republic of North Macedonia	2019/in continuation
		1.2.5	Providing an effective system for classified information protection in cyberspace through continuous improvement of the level of protection from cyber attacks and cyber espionage systems and networks of the Ministry of Defence and the Army of North Macedonia through which classified information are processed	Ministry of Defence of the Republic of North Macedonia/Army	all constituents part of the national cyber defence system	2019-2020
		1.2.6	Development of deployable cyber defence capabilities at battalion command level compatible with NATO	Army	Ministry of Defence of the Republic of North Macedonia	2020-2024
		1.2.7	Identification of needs for cyber professionals and defining the pool of potential human resources	Ministry of Defence of the Republic of North Macedonia/Army		2020

Activity no.	Activity	Code	Implementation manner (tasks)	Stakeholder	Associates	Timeline
		1.2.8	Developing motivating system of rewards and promotions of expert personnel in the field of cyber security and defence, based on quality and personnel presented results by determination of a salary supplement for the expert personnel in cyber defence and security area, depending on the tasks, expertise and irreplaceability	Ministry of Defence of the Republic of North Macedonia/Army		2020
		1.2.9	Forming the active reserve for the needs of cyber defence and defining appropriate policies for recruitment and engagement of experts in this field.	Army	Ministry of Defence of the Republic of North Macedonia	2020
		1.2.10	Establishing programs for exchange of experience with experts from civil companies in order to improve the training of personnel for cyber defence.	Ministry of Defence of the Republic of North Macedonia/Military Academy	academic community/organizations	2020-2022

Activity no.	Activity	Code	Implementation manner (tasks)	Stakeholder	Associates	Timeline
OBJECTIVE 2: EDUCATION AND TRAINING						
2.1	Continuous education for ensuring a high level of awareness and personal responsibility in terms of cyber defence in the context of national defence and security	2.1.1	Raising awareness on cyber defence through education and training of the entire staff at the Ministry of Defence of North Macedonia and the Army	Military Academy/ Ministry of Defence of North Macedonia/ Army		2019 /continuous in complaince with the adopted training plan 2018
		2.1.2	Defining and continuously educating the required number of experts for strategic, operational and tactical cyber defence and cyber threat management at the Ministry of Defence of North Macedonia and the Army.	Military Academy/ Ministry of Defence of North Macedonia/ Army		2019 - continuous in compliance with the annual education and training plan
		2.1.3	Forming and establishing an Institute for cyber security and digital forensics within the Military Academy "General Mihajlo Apostolski" - Skopje, with the main goal of research, education and training in the area of cyber defence.	Military Academy		2020-2023
		2.1.4	Active participation in NATO Cooperative Cyber Defence Center of Excellence (CCDCOE) by sending national experts and participation in research activities of the Center	Military Academy/ Ministry of Defence of North Macedonia/ Army		2020/in continuation
		2.1.5	Creating and developing simulations and programmes for cyber security incidents to be used in national cyber defence exercises	Military Academy/ Ministry of Defence of North Macedonia/ Army		in continuation when needed according 2.1.6
		2.1.6	Organization of national cyber defence exercises in cooperation with all stakeholders as part of the national defence system	Military Academy/ Ministry of Defence of North Macedonia/ Army	all constituents part of the national cyber defence system	in continuation /minimum one exercise annually
		2.1.7	Integration of the cyber defence segment in all operation exercises at the national level, in the area of national defence	Ministry of Defence of the Republic of North Macedonia/Army	all constituents part of the national cyber defence system	2019/in continuation according to the oeprational exercises plan
		2.1.8	Active participation in international military exercises and training on cyber defence.	Ministry of Defence of the Republic of North Macedonia/Army		in continuation according to the training and exercise annual plan
		2.1.9	Joint sharing of facilities and experience with NATO, EU and partner countries	Military Academy/ Ministry of Defence of North Macedonia/ Army		in continuation according to the bilateral, multilateral memorandums for cooperation and activities from annual plans
OBJECTIVE 3: COOPERATION AND EXCHANGE OF INFORMATION						

Activity no.	Activity	Code	Implementation manner (tasks)	Stakeholder	Associates	Timeline
3.1	Establishment and maintenance of mutual international cooperation and exchange of information on shared deterring cyber threats and increasing national, regional and international security and stability	3.1.1	Development and implementation of a system and a programme for exchange and sharing of information, knowledge and experiences between the public, private and defence - security sector in the field of cyber defence, to protect the CII and III	Military Academy/ Ministry of Defence of North Macedonia/ Army	all constituents part of the national cyber defence system	2020-2023
		3.1.2	Development of civil-military cooperation for the cyber defence and promotion of the cooperation between the public and private sectors	Military Academy/ Ministry of Defence of North Macedonia/ Army	all constituents part of the national cyber defence system	2019-2020
		3.1.3	Establishing cooperation and information exchange in the area of cyber defence among all constituents of the national defence system.	Military Academy/ Ministry of Defence of North Macedonia/ Army	all constituents part of the national cyber defence system	2019-2022
		3.1.4	Defining the national point of contact with NATO in terms of cyber operations and cooperation.	Ministry of Defence of the Republic of North Macedonia/Army	all constituents part of the national cyber defence system	2020-2021
		3.1.5	Establishing point for secure communication with NATO	Ministry of Defence of the Republic of North Macedonia/Army	DSCI/MoFA	2020
		3.1.6	Participation of the Republic of North Macedonia in NATO collective cyber defence and setting a system for cooperation and exchange of information	Ministry of Defence of the Republic of North Macedonia/Army	all constituents part of the national cyber defence system	2020-2023
		3.1.7	Establishing and maintaining cooperation with other partner countries in the field of cyber defence	Military Academy/ Ministry of Defence of North Macedonia/ Army	partner countries	2019/in continuation
OBJECTIVE 4: LEGAL AND REGULATORY FRAMEWORK						
4.1.	Creating unique and comprehensive legal framework for cyber defence, by taking into account the legislation of the Republic of North Macedonia and the EU and NATO directives	4.1.1	Development and implementation of a system and a programme for exchange and sharing of information, knowledge and experience between the public, private and defence - security sector in the area of cyber defence, in order to protect and CII and the III	Ministry fo Defence of the Republic of North Macedonia	Military Academy/ Army	2020-2021
		4.1.2	Development of new and harmonization of existing regulations on cyber security and defence, in accordance with the legislation of the Republic of North Macedonia and the EU and NATO directives	Operation body for cyber security (national)	Military Academy/ Ministry of Defence of North Macedonia/ Army	in accordance wit operation body activities

Activity no.	Activity	Code	Implementation manner (tasks)	Stakeholder	Associates	Timeline
		4.1.3	Definition and implementation of measures for strategic management of cyber defence in the Ministry of Defence of North Macedonia and the Army	Ministry fo Defence of the Republic of North Macedonia	Army	2019-2020
		4.1.4	Development of methodology for risk assessment of cyber threats at the level of the Ministry of Defence of North Macedonia and the Army	Ministry fo Defence of the Republic of North Macedonia	Military Academy/ Army	1 year after the end of Cyber Risk Assessment of the national IIIs
		4.1.5	Development of operational plans for all cyber service providers in accordance with the defence plan	Ministry fo Defence of the Republic of North Macedonia	all constituents part of the national cyber defence system	2020 - in compliance with the aproved defence plan
		4.1.6	Development of system and procedures for information exchange about threats and risks in the field of cyber defence at international level.	Ministry fo Defence of the Republic of North Macedonia	Army	2020-2023
		4.1.7	Defining the roles and responsibilities of the armed forces in the protection of military CII and III and the development of adequate capabilities.	Army	Ministry of Defence of the Republic of North Macedonia	2 years according 1.1.4
		4.1.8	Defining and coordinating military planning regarding the method and the use of military cyber capabilities with the national cyber defence in various situations	Army	Ministry of Defence of the Republic of North Macedonia	2021