REPUBLIC OF MACEDONIA

NATIONAL CYBER SECURITY STRATEGY

2018 - 2022

Version 1.2
July 2018

Contents

Document administration

Version	Date	Notes
1.0	11.06.2018	First draft
1.1	03.07.2018	Mature draft version, with implemented comments and suggestions from all stakeholders
1.2	17 July 2018	Final version, adopted by the Government of the Republic of Macedonia

Participants in document preparation:

Dimitar Mancev	Ministry of Information Society and Administration
Solza Kovachevska	Ministry of Information Society and Administration
Ana Malceva	Ministry of Information Society and Administration
Marjan Stoilkovski	Ministry of Interior
Natalija Veljanoska	Ministry of Interior
Jane Stojanov	Ministry of Interior
Alenka Gorgieva	Ministry of Defence
Mitko Bogdanoski	Ministry of Defence
Filip Stojkovski	Ministry of Defence
Orhan Ismaili	Ministry of Defence
Jovana Gjorgjioska	Ministry of Information Society and Administration
Elena Manceva	Ministry of Information Society and Administration

Executive summary

Strengthening the national capacities for cyber threat management and improving the cyber security have become a priority for the Republic of Macedonia.

The National Cyber Security Strategy of the Republic of Macedonia is a strategic document that fosters the development of safe, secure, reliable and resilient digital environment, supported by high-quality capacities, based on cooperation and trust in the field of cyber security. This document is organized in seven parts.

The **first section** introduces the topic, focusing on the increased dependency on cyber space services, the increased use of Information and Communication Technologies (ICT) and the negative influence of severe cyber threats on the functioning of the public and private sectors. This section emphasises the need for the existence of strategic documents in order to strengthen the national cyber security capacities.

In the **second section,** the Strategy examines the major cyber trends, challenges and threats that are key in relation to the cyber space of the Republic of Macedonia.

Section three lays down the cyber security principles that support the Strategy:

- Effective and efficient cyber security capacities
- Protection and prevention
- Security for economic development
- Trust and availability
- Legal security

Section four defines the stakeholders in the field of cyber security in the country: public sector, private sector, academic community, citizens and civil society organizations.

The **fifth section** states the vision and mission of the national Strategy.

Section six goes on to set up the "5C" Goals of the National Cyber Security Strategy. The objectives of the five goals are focused on:

1. Building a cyber resilient ICT infrastructure, identifying and implementing adequate solutions in order to protect the national interests
2. Promoting a cyber security culture, in order to raise the public awareness and understanding of cyber threats, as well as building and advancing the necessary capacities for protection.
3. Strengthening the national capacities for prevention, research and adequate response to cyber crime.
4. Strengthening the capacities for defence of national interests and reducing current and potential cyber space risks.

5. Cooperation and exchange of information on national and international level.

Section seven is devoted to the generalization of an Action Plan for the implementation of the National Cyber Security Strategy, along with the challenges for successful implementation. It highlights the responsibilities of authorities defined in the Strategy regarding the support of the goals and activities outlined in this document. In addition, this section establishes the organisational structure for coordination of the development and implementation of the course of actions defined in the Strategy and the Action Plan. In this manner, a *National Cyber Security Council* and a *Body with operational cyber security capacities* are described below, along with their jurisdiction and activities.

The measures and activities for the implementation of the goals set in this Strategy will be outlined in the Action Plan, developed within three months after the adoption of the Strategy by the Government of the Republic of Macedonia.

The National Cyber Security Strategy is based on the principles of the Cybersecurity Strategy of the European Union and the NATO Cyber Defence Pledge.

Introduction

The past years marked a growing and consistent use of Information and Communication Technologies (ICT), which represents a core driver of globalization, thus providing substantial contribution in the process of improving the economic development, standard of life and societal well-being.

Fast progress of ICT provides significant contribution for improvement and development of the Macedonian civil society. Stakeholders from the political, social and economic life in the Republic of Macedonia consistently utilize the opportunities offered by the great expansion of ICT. According to global indexes indicating the level of development of Information Society (such as IDI, NRI, e-GDI, GCI), the Republic of Macedonia is in the first statistical quarter. In this manner, the Ministry of Information Society and Administration and other governing institutions consistently introduce new electronic services with the purpose of simplifying the daily lives of the citizens.

Nevertheless, increased dependency on cyber space services demonstrates how dysfunctional ICT systems and severe cyber threats may have significant negative influence on the day-to-day operations of the public and private sector, as well as the society as a whole. Dependency on new technologies and the need for greater availability of services in the cyber space is a major driver for users and institutions to raise awareness of the importance of integrity, authenticity and confidentiality of the data. Macedonian communication networks are part of the global communication networks, which implies that cyber security incidents on other locations may often influence the Macedonian cyber space and services, and vice versa.

Analysis made by the most relevant institutions worldwide in the field of security and defence show that over the past years, cyber threats indisputably represent some of the most significant security risks for societies nowadays. Hence, cyber threats should be treated as an integral part of the national and international security.

Due to the reasons stated above, strengthening the national capacities for managing cyber threats and increasing the cyber security has become one of the key challenges for the Republic of Macedonia.

In the efforts to strengthen the national cyber security capacities, the existence of strategic documents related to this challenge is of crucial importance. In this manner, the National Cyber Security Strategy will primarily provide the basis for improvement of the framework conditions in this area. The need for developing and implementing a National Cyber Security Strategy is predominantly related to:

1. Activities, social interactions, economy, as well as basic human rights and freedom at large depend on ICT usage; hence, it is necessary to ensure the existence of an open, safe and secure cyberspace;
2. The use of ICT systems increases the risk of cyber incidents and abuse, which categorizes them as some of the major threats for the national security;
3. Definition and development of a cyber defence policy;
4. Establishing an integrated, multidisciplinary approach to secure closer cooperation and coordination between the defence and security sector, the institutions involved in the fight against cyber-crime, the private sector, civil society organizations and other relevant stakeholders;
5. Strengthening the operational capacity, as well as coordination and cooperation between relevant institutions included in the fight against cyber crime;
6. Establishing common standards, training and education of all institutions included in the development of cyber security;
7. Strengthening the cyber security institutional and legal framework;
8. Strengthening the national capacities for prevention and protection of cyber attacks, as well as conducting activities in order to raise the national awareness of cyber security.

The National Cyber Security Strategy is developed in accordance with the Cybersecurity Strategy of the European Union and the NATO Cyber Defence Pledge for safe, secure,

reliable and resilient digital environment to the benefit of citizens, business community and public administration.

Cyber trends, challenges and threats

Increased number of Internet and ICT users and increased dependency on ICT availability

Increased number of Internet users (in the first quarter of 2017, 73.6% households had access to the Internet at home) and ICT users, along with increased use of Internet by the companies (starting from January 2017, 91.2% of businesses with 10 or more employees had broadband Internet connection) brings an ever growing dependency on the performance of the Internet and ICT. Obstacles in the availability of ICT dependent specific services dependent may pose a great risk for the unimpeded functioning of the Macedonian society, especially in relation to the Critical Information Infrastructure (CII) and other Important Information Systems (IIS).

Implementation of e-services

Implementation of electronic services in the Republic of Macedonia will significantly improve the existing processes and overall functioning of the society. Nevertheless, the increasing number of e-services and applications bears new challenges and cyber risks.

Low level of cyber security in small and medium enterprises (SMEs)

A growing need to raise the awareness of the use of best practices for ICT and Information Systems (IS) protection in SMEs is evident. Such organizations often find it difficult to identify and define their needs in relation to cyber security, whereas many SMEs do not have the necessary resources and knowledge needed to surpass the challenges in this area. On the other hand, certain SMEs data and systems may be of critical significance for the country, especially if they are sub-contractors for large companies and institutions.

Increased dependency of the defence and security sector on ICT

The defence and security sector is ever more dependent and based on the functionality of ICT systems. Vulnerability of such technologies, as well as disruption or destruction

threats increases the risks of negative implications on the basic defence and security capabilities and fulfillment of criteria for full-fledged EU and NATO membership.

Cyber crime

The global connectedness, which if used appropriately may secure full anonymity, increases malicious users' opportunities to conduct theft and abuse of sensitive information. A large proportion of malicious actors and criminal organizations recognize cyber space as a domain where fast profit is feasible, as well as an environment which enables lower risk of detection. Globalization and anonymity not only enables malicious users to easily target specific victims, but also to execute operations of larger scale and scope.

Threats and risks related to the use of social media

The growing number of social media and the ever-increasing number of users of these networks, as well as the recent development of the face recognition algorithms, carry an inherent risk for personal data theft and digital identity theft. The targets of such attacks may be individuals, but also legal entities.

Low level of cyber security awareness by end users

A large number of Internet users, including users in the public and private sector, have low level of awareness of the most common cyber threats (such as phishing, fake e-stores, etc.), and subsequently fall victims of attacks that may easily be prevented by simple defence mechanisms.

A growing need for cyber security professionals

Existing educational programs at all levels of formal education (primary, secondary and tertiary educational sectors) in the Republic of Macedonia do not satisfy in full the needs for educating and training specialists able to respond to the latest challenges and trends in the cyber space. On the other hand, the demand for such experts on a global scale is growing exponentially.

Inadequate cyber hygiene

One of the main reasons for the widespread successful rate of cyber attacks is the improper practicing of the so called “cyber hygiene” by the users and business community. In this manner, establishing active control over employee cyber hygiene and thereby effectively mitigating cyber security risks represents a major challenge for organizations nowadays. Furthermore, one of the many challenges in this regard is the increased complexity in the effort to maintain basic cyber hygiene, such as asset identification, software updates, patching, standards management, as well as education and training of users in large organizations. Taking into consideration that the largest share of all cyber threats may be prevented by implementing proper cyber hygiene, this matter is of key importance for cyber security.

Internet of Things (IoT)

Although the number of devices connected to the Internet has increased substantially, cyber hygiene is ignored by most users with regards to their actions and device protection. The IoT concept only intensifies this challenge. While anti-virus software, firewalls, and other related technologies are automatically activated on traditional electronic devices, such as personal computers and laptops, this is not the case for smart devices such as TVs, fridges, video surveillance, etc. Along these lines, the last period noted a drastic increase in the malicious usage of these devices, and threats to and from these devices are expected to increase in the future.

Artificial Intelligence (AI)

The field of artificial intelligence - and particularly machine learning - already plays an important role in today’s global society. The continuous advancement of these fields already yield positive impacts, and is extensively being applied in the process of improving and perfecting security mechanisms for protection of cyber threats. On the other hand, AI is evolving into one of the major security challenges, since malicious users are increasingly utilizing this technology in the process of enhancing malicious software capabilities.

Increase of the number and level of sophistication of malicious software

An increase in the number and the level of sophistication of malicious software is evident in the last years. New malicious software variants are developed on a daily basis, whereas malicious actors significantly limit the attack source tracking, i.e. reverse engineering and forensic analysis, by using different mechanisms.

Recent developments have given rise to an increase in the number of registered malicious software for mobile device attacks, due to the enhanced vulnerability of mobile applications. This leads to an increasing number of users which do not employ basic security measures to protect their mobile devices (such as installing anti-virus software).

Compromised hardware and software

An increased number of users and ICT vendors are adding to the risk of supply-chain attacks where commercial of-the-shelf (COTS) hardware and software have been compromised with security weaknesses, malicious code or backdoors. Insufficient assurance in the validation of the COTS supply-chain may lead to personal data theft, acts of cyber espionage or involuntary participation in other malicious activities (e.g. botnet-based attacks).

Big data and Cloud services

Data security and protection, especially for those of public interest (data relevant for CII and IIS) are crucial for the Republic of Macedonia. The amount of data being processed both in the public and in the private sector increases on a daily basis, resulting in the rise of storage demand; hence, cloud storage has been introduced as a new form of data storage. Nevertheless, the use of on-line and cloud services often leads to inadequate security solutions with suspicions credibility.

Threats against industrial control systems and national critical infrastructures

A tangible prospect for the public and private sector to face increased number of cyber attacks, including industrial cyber espionage, cyber vandalism and vulnerability identification of the energy sector, financial sector, health sector, transport systems and other parts of CII and IIS emerges from the global trends. Thereby, a different attack approach is foreseeable, ranging from direct interruptions in the functionality of certain parts of the critical infrastructure, to total system block.

Dysfunctionality of the aforementioned systems may bear fatal consequences. Moreover, due to the high level of heterogeneity of the technical solutions, technical analysis in later stages may be considerably aggravated.

Botnets and DDoS/DoS attacks

Botnets are mostly used for DDoS/DoS attacks, and are becoming more robust, resilient, hard to discover and track. Recent developments in the field of IoT, which often involve weak security mechanisms, considerably contribute towards increasing the scope and capacities for attack used by malicious users.

Ransomware

The number of new ransomware malicious activities has increased exponentially, thereby posing a risk for all aspects of society, including CII and IIS. This malicious software, although simple in nature, may cause large damage by encrypting files or preventing access to applications or operating systems. With the purpose of getting access to their own data, i.e. to be able to decrypt the data, victims are often willing to pay a large financial sums to the attackers that developed and distributed the malicious software. Often, these activities are conducted by criminal organizations, in order to achieve financial gain. However, in certain cases ransomware is intended to cause damage or destroy certain targets and data, without the possibility to retrieve the data or reverse the action (e.g. NotPetya). Although individuals are most commonly targeted

by ransomware, an increasing number of cases are directed towards enterprises and institutions.

Mining cryptocurrencies

Even though a large part of registered malicious cases related to cryptocurrencies have been focused on scamming or robbing cryptocurrency owners, computer processing power theft with the intention to acquire greater capacity for data mining is gaining momentum. The attack is not only intended for regular users, but also targets more powerful computer systems which may be essential, therefore causing significant damage.

Cyber espionage

The increased percentage of digitization of the society and industry brought to life new channels and methods for certain entities to acquire unauthorized access to sensitive or confidential information. These activities may damage the national interests, businesses and their reputation, as well as citizens' well-being.

Cyber security principles

Effective and efficient cyber security capacities

The noteworthy technological development and the ever-growing accomplishments in ICT are increasingly enabling malicious users to invent new mechanisms for cyber security disruption. Therefore, it is vital for the information-communication infrastructure in the country to be able to respond to cyberspace challenges.

With the purpose of efficiently responding to the new risks and threats, the Republic of Macedonia will support research and development in the area of cyber security, as well as education and training at all levels in society, including training for end users.

Having in mind that an effective outcome from the research and development in the area of cybersecurity may be achieved only by close collaboration among all relevant entities, the Republic of Macedonia fully supports the multi-stakeholder approach in building efficient cyber security capacities.

In order to achieve effective management and in-time response to contemporary cyber threats, the Republic of Macedonia will facilitate the process of strengthening existing capacities and cooperation procedures between all relevant entities or individuals in the area of cyber security.

Protection and prevention

Severe cyber attacks on the security of the country, among which cyber operations and espionage sponsored by other states (including theft of intellectual property from critical state institutions, CII and IIS) and the use of cyber space in order to support terrorist activities are considered to be risks for the national security. Hence, one of the main principles of this Strategy is to support the national security system of the Republic of Macedonia.

Security for economic development

Developing a secure society and applying all security practices and processes through collaboration among all relevant stakeholders will enable businesses to remain

trustworthy and reliable for the clients, while simultaneously sustaining their profitability. Increasing the citizens' trust in the digital services and electronic commerce will directly contribute towards the development of the digital economy and global recognition of the Republic of Macedonia as a safe investment and corporate environment.

In this manner, the implementation of new ICT solutions and practices, as well as the global connectedness will support the economic growth, and also minimize negative externalities as a consequence of security incidents in the cyber space.

Trust and availability

Response to cyber space challenges is successful only when well-established procedures for cooperation among all stakeholders with capacity to contribute to cyber security are applied. Due to this fact, close cooperation between the public, private and civil sector is of utmost importance.

CII and IIS protection is vital for the Republic of Macedonia. Taking into consideration the fact that the largest part of this infrastructure and services are owned by the private sector, inclusion of this sector in the processes related to cyber security protection is vital.

Utilizing state-of-the-art prevention, security and protection measures does not completely rule out the occurrence of incidents, posing risks for the CII. When CII is involved, coordinated activities and well-prepared incident recovery plans should be adequately regulated, and their effectiveness regularly tested through joint cyber exercises and simulations.

In order to improve the cooperation in the field of cyber security among relevant stakeholders, the Republic of Macedonia will establish a Centre of Excellence. This Centre would be established with the purpose of facilitating exchange of experience among the public, private sector (above all companies managing CII and IIS), civil organizations, academia and other institutions.

Legal assurance

In the process of implementing cyber security measures, compliance with the legal acts, the principles of basic human rights and liberties, democracy and adherence to core values is essential. One of the main characteristics of the Internet is the transparency and accessibility for everyone at any time, with a guaranteed free information flow. The users of services in the cyber space require reliability of the cyber space, information integrity, freedom of expression, personal data protection, as well as privacy rights. Moreover, users expect to have unrestricted access to the Internet without interference, damage or illegal interception of communications. In this manner, the Macedonian legislation as well as the international legal acts related to human rights, freedom of expression and privacy protection are universal and also applicable in the cyber space.

Stakeholders

Defining the affected groups of actors in the area of cyber security is an important segment that enables further definition of the scope of the Strategy.

In this manner, the Strategy incorporates the following stakeholders:

1. **Public sector**, in terms of this Strategy, includes authorities and other subjects, which in different ways represent the users of the cyber space and subjects that are obliged to apply measures that arise from the Strategy;
2. **Private sector**, which is in close correlation with authorities and regulatory bodies as affected parties by this Strategy, especially legal entities which are subject to special regulations for critical infrastructure and the security and defence system; other legal and business subjects which in different manners represent the users of cyber space; and subjects which are obliged to apply the measures that arise from the Strategy, with all peculiarities of those legal and business entities, with regards to their scope of work, number of employees and markets which they cover;
3. **Academic community**, educational institutions from the public and private sector which in diverse ways represent users of cyber space and subjects which are obliged to apply the measures arising from the Strategy; Through the development and implementation of educational programs and trainings, and provision of cyber security expertise, the academic community plays a crucial role in developing a strong body of knowledge in the field of cyber security.
4. **Citizens and civil society organizations**, encompassing users of ICT and services. The state of security in the cyber space is reflected upon citizens in many different ways. In this manner, the subject matter of cyber threats are not only citizens who are active users, but also those who have their personal data present in the cyber space;

Vision and mission

Vision

The Republic of Macedonia to have a safe, secure, reliable and resilient digital environment, supported by high-quality capacities, high-quality experts, built on trust, national and international cooperation in the field of cyber security.

Mission

The Republic of Macedonia to have clearly defined and sustainable policies, which will be coordinated in the manner of advancing the national cyber security.

Goals

The *5C Goals* of the National Cyber Security Strategy are comprised of five key areas and are aimed to facilitate the strengthen the existing and build new capacities for defence from cyber attacks and increase the level of security in the cyber space across all sectors at all levels.

Figure 1: 5C Goals of the National Cyber Security Strategy

GOAL 1: Cyber Resilience

The Republic of Macedonia to have cyber resilient ICT infrastructure, and to identify and implement adequate solutions in order to protect the national interests.

Cyber resilience provides confidentiality, integrity and availability through identification, protection and establishment of pre-incident state of the cyber space. The public and private sector need to employ timely and accurate information and suggestions for cyber security and also to be able to cooperate in case of cyber incidents. In this manner, it is necessary to identify all relevant capacities for cyber security across all relevant stakeholders, and to define specific jurisdiction and activities in function of improving the cyber safety and managing cyber incidents. The end goal is to secure protection of an integral part of the infrastructure in the country, and for relevant institutions to use adequate solutions in the process of defending the state interests, thereby demonstrating readiness for severe, complex cyber threats.

Activities:

1. Advancing the capacities and capabilities of the National Centre for Computer Incident Response MKD-CIRT.
2. Identification and protection of CII and IIS.
3. Utilization of the best solutions for cyber incident response with the purpose of protecting the national security interests.
4. Taking measures and activities to handle cyber incidents of larger scale and scope.
5. Development of national procedures in time of piece, crisis, a state of emergency and state of war, in order to manage incidents which will enable efficient intra-institutional cooperation, where every institution have a pre-defined role, will employ appropriate protocols and procedures, as well as information exchange, communication and coordination channels.
6. Development of methodology for national level cyber threat risk evaluation.

7. Establishing a single and comprehensive legal framework for cyber resilience, taking into account the legal regulatory framework in the Republic of Macedonia and EU.
8. Continuous monitoring, adoption and implementation of internationally recognized standards and procedures in the field of cyber security.
9. Continuous update on the national strategic documents taking into account contemporary cyber security standards and technologies, as well as cyber threats.
10. Continuous monitoring and analysis, in order to assess the current state and to define the measures and recommendations for institutions in charge of CII and IIS in order to raise the level of cyber security
11. Continuous improvement of the resilience, integrity and reliability of CII and IIS.
12. Continuous analysis and monitoring of cyber threats and risks in the Republic of Macedonia through regular collection of information from the relevant parties.
13. Defining precise procedures for safekeeping and protection of data processed in the CII and IIS systems, as well as conducting continuous analysis and auditing the efficiency of the defined procedures.
14. Conducting regular audits in order to detect mistakes and vulnerabilities of the information systems and networks which are part of the CII and IIS.
15. Continuous advancement of the technological and organizational needs for efficient management of cyber threats.
16. Building and strengthening the national capacities for active cyber defence and taking appropriate countermeasures to handle and respond to cyber threats.

GOAL 2: Cyber capacities and cyber security culture

The public, private sector and the Macedonian society to have a comprehensive understanding of cyber threats and to have the necessary capacitates to protect themselves.

Rather than solely focusing on raising the awareness of cyber threats, this goal also refers to the commitment towards building the necessary cyber security capacities by all affected stakeholders with relevant activities in this field. Promoting cyber security culture induces responsibility and understanding of cyber-related risks by all actors, developing a learned level of trust in e-services, and users' understanding of how to protect personal information online. Accomplishing this goal implies that security solutions are developed at all levels of society, assuring greater resilience with regards to malicious cyber activities.

In addition, this goal will enable efficient dissemination of cyber security measures and activities undertaken at various levels, including all relevant stakeholders, in order to achieve the necessary level of understanding and skills for staff, users and other parties involved in the processes. The exchange of skills, knowledge and experience in the field of cyber security on a national level will be achieved through ad hoc inter-organizational research teams comprised of experts in the public sector, private sector and the academic community.

In the context of building and strengthening the necessary cyber security capacities, in order businesses and organizations to be able to handle the most sophisticated and complex attacks in the cyber space, expertise in this field will be secured through investment in cyber security, which is key to achieve competitive commercial performances.

Activities:

1. Increasing the cybersecurity capacities in SMEs.
2. Advancing the cyber security capacities in the private sector, including the national infrastructure, CII and the public sector.

3. Development and promotion of study programs and training in the area of cyber security at all levels.
4. Supporting the research capacities and business innovations through the establishment of scientific research center in the field of cyber security.
5. Participation in the national and international research projects and activities related to cyber security.
6. Providing education and training, as well as efforts to increase the awareness of cyber security in the private sector.
7. Providing response directions and guidelines in case of cyber incidents andcyber crisis at all levels in society, including daily operations.
8. Conducting research and fortifying national priorities as a baseline to predict activities and investments for cyber security development.
9. Acquiring and utilizing state-of-the-art hardware and software solutions for prevention, identification and management of cyber incidents.
10. Raising the level of awareness and basic cyber security knowledge among young student population.
11. Adapting and refining the existing study programs in primary and secondary schools in order to include cyber security elements in novel study programs with the purpose of producing high quality work force in the field of cyber security.
12. Increasing the awareness and basic understanding of cyber security for citizens and civil organizations.
13. Enabling high-quality education and training in the field of cyber security for public administration employees.
14. Providing adequate education and training in the field of cyber security for managerial staff in the public and private sector.
15. Continuous training of experts specializing in different aspects of cyber security.
16. Establishing retention mechanisms for ICT and cyber security work force.

GOAL 3: Combating cyber crime

Republic of Macedonia to strengthen its capacities for prevention, research and adequate response to cyber crime.

The development and utilization of information and operational technologies leads to the occurrence of different forms of abuse characterized as cyber crime. Cyber crime may appear in the form of Internet abuse and scams, but emerge as an attack on more sophisticated and complex systems. In this manner, cyber-crime may be motivated by different causes and carried out by diverse agents. Given the widespread range of cyber crime and scope of institutions and organizations in charge of cyber crime management and handling, this goal requires the establishment of a specialized, detailed national plan for cyber crime management, including the cyber space enabled crime. This plan should define the problem of cyber crime and the challenges generated by it. It requires defining the prevention activities and securing the functions vital for the society. The most efficient way for prevention is to provide effective directions and solutions so that cyber hygiene can become an integral part of the culture and mindset of the Macedonian society. Inter-institutional and multi-disciplinary approaches are key in order to efficiently tackle cyber-crime.

Activities:

1. Advancing the cyber crime handling and management capacities.
2. Harmonizing the national with international policies related to cyber-crime.
3. Development of a single, comprehensive legal framework for cyber crime, taking into consideration the applicable legal framework in the Republic of Macedonia and EU.
4. Modernizing authorities in charge of cyber crime in order to efficiently combat cyber crime.
5. Establishing efficient procedures to report and research cyber crime.
6. Establishing formal procedures for cooperation and exchange of information in the field of cyber crime among relevant national entities and other security services.

7. Advancing cooperation with regional and international organizations in the fight against cyber crime.
8. Advancing the existing and establishing new mechanisms for cooperation and exchange of information with the private and civil sectors.
9. Securing expert-specialist education and training for individuals working in the field of identification and research of cyber crime.
10. Developing a multidisciplinary academic environment for the advancement of national capacities for cyber crime investigations.
11. Active participation in the creation of international cyber crime regulations and standards, as well as their implementation on national level.
12. Continuous assessment of the adequacy and efficiency of the national cyber crime regulation.
13. Providing continuous education and training for law enforcement entities in the field of cyber security, cyber crime and electronic evidence.

GOAL 4: Cyber defence

Republic of Macedonia to strengthen its capacities in order to be able to protect national interests and reduce current and future cyber space risks.

In order to be able to tackle cyber space risks, the Republic of Macedonia defines its cyber defence capacities according to highest international standards, as part of the national cyber security framework. Developing cyber defence capabilities in the Army of the Republic of Macedonia is part of a comprehensive national defence approach. Establishing a cyber component in the national security is ensured by the inclusion of experts from the defence and security sector in all working groups and bodies focused on cyber crime.

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

The civil-military cooperation on international level is based on state-owned resources, which are also in operation in the cyber space; regarding warning, prevention, protection, distraction, detection and active defence.

Republic of Macedonia, as a country partner and candidate for membership in NATO, the European Union and other international military and civil organizations, in order to be included in collective defence, is required to fully comply with the standards and directions provided by these organizations and to use the resources and opportunities that these organizations offer. Compliance with international cross-border organizations refers to the development and implementation of common cyber security capacities, standards and trainings. Within the collective defence systems, the Republic of Macedonia will cooperate and exchange information with these organizations in the field of cyber defence.

Activities:

1. Defining the national cyber defence capacities.

2. Defining the military capacities in the Ministry of Defence and the Army for handling threats in the cyber space.
3. Establishing, developing and sustaining the defined capacities and capabilities for cyber defence.
4. Establishing a cyber defence system for the national critical infrastructure.
5. Creating a single and comprehensive cyber defence legal framework, taking into consideration the regulatory framework in the Republic of Macedonia, as well as NATO and EU directives.
6. Addressing and reducing the risks in the cyber space.
7. Establishing and sustaining a mutual international cooperation in order to join efforts in combating shared cyber threats and increasing the national and international security and stability.
8. Defining and coordinating military planning regarding the use of military cyber capacities and the national cyber defence in different situations.
9. Inclusion and contribution in the collective cyber defence through international cooperation.
10. Providing continuous education and training in order to secure a high level of awareness and individual responsibility with regards to cyber defence and national defence and security.
11. Development and implementation of a system and programs for the exchange and sharing of information, knowledge and experience between the public, private and defence and security sector in the field of cyber defence, in order to protect the CII and IIS.

GOAL 5: Cooperation and exchange of information

Republic of Macedonia to protect its cyber space through cooperation and exchange of information at national and international level, in order to facilitate an open, free, stable and secure cyber space.

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

International cooperation represents one of the key segments in the efforts to increase the capacities to handle cyber threats. In some cases, the Republic of Macedonia may confront cyber attacks which are partly or wholly organized and implemented by malicious users outside of the physical borders of the country. In this case, success of the counter measures undertaken to reduce the effects of registered cyber incidents and undertaking appropriate measures against the crime perpetrators largely depends on the established cooperation on bilateral, regional and international level. In order to ensure full and operational ability of state institutions in charge of cyber risk and incident management, international partnerships of those institutions with other nations and organizations are much needed. The Republic of Macedonia undertakes all necessary actions in order to be recognized as a country committed to the security of its own cyber space; a country which is actively involved in the global fight against mass malicious use of cyber space. In this manner, active international participation in tackling the global challenge of cyber threats would contribute to increase of state capacities for handling cyber risks.

Activities:

1. Promoting and advancing the Internet and norms of behavior of the state which reflects the interests of the Republic of Macedonia.

2. Developing an effective model for cooperation on a national level among institutions in charge of cyber security and advancing their existing structure and processes.
3. Establishing new and strengthening existing networks of operational national, bilateral, regional and international cooperation.
4. Active participation and contribution towards building international abilities for cyber security and trust building activities.
5. Efficient exchange of information between the state and the entities which manage the CII and IIS.
6. Support in the process of utilizing the cyber space economic opportunities for the benefits of the population in the Republic of Macedonia.
7. Cooperation among stakeholders in the manner of developing and implementing technologies which will secure maximum protection and transparency, as well as testing and assessment of the level of security of utilized technologies.
8. Cooperation with different stakeholders on a national and international level for various research projects in the field of cyber security.
9. Organizing and participating on various international activities and initiatives in the field of cyber security.
10. 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.
11. Promoting and advancing norms, rules and principles of responsible behavior by the state, according to internationally established principles.
12. Establishing and strengthening cooperation and building trust with other public and private international CERT and CSIRT teams, academic communities and other international organizations.
13. 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 behavior, freedom of speech, personal data protection, privacy, as well as basic human rights and liberties.

14. 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.
15. In cooperation with the private sector, to facilitate a cyber space that offers 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.
16. 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.

Implementation

Within three months of the adoption of the National Cyber Security Strategy, an Action Plan for implementation of the goals and activities defined in the Strategy will be developed. Relevant authorities defined in the Strategy and the Action Plan will be responsible for the implementation of the foreseen goals and activities. The implementation of measures defined in this Strategy will be coordinated by the National Cyber Security Council. Based on the Strategy, relevant authorities, ministries and other institutions will conduct analysis of their current legislation and update regulations and procedures accordingly. Relevant ministries will deliver periodic reports for the implementation status to the National Cyber Security Council. Depending on the current developments and needs, the National Cyber Security Strategy may be revised and updated.

For this purpose, the Republic of Macedonia will establish a **National Cyber Security Council** and a **Body with operational cyber security capacities**.

National Cyber Security Council

In order to be able to perform coordination and monitoring of the activities defined in the National Cyber Security Strategy and the Action Plan, as well as to be able to define new strategic directions and recommendations related to the cyber security segment, the Government of the Republic of Macedonia will establish a National Cyber Security Council, responsible for the execution of the following activities:

- Systematic monitoring and coordination of the implementation of the National Cyber Security Strategy considering all existing and upcoming potential challenges in the field of cyber security.
- Suggesting precise measures for improving the implementation of the National Cyber Security Strategy and Action Plan.
- Suggesting additions and updates for the Strategy and the Action Plan in order to establish advanced management and to incorporate new challenges in the field of cyber security.

- Identifying the challenges for managing cyber crisis and suggesting adequate measures for greater efficiency.
- Participation, coordination and alignment with the activities of the Security Council of the Republic of Macedonia.
- Analysis of the current level of security based on reports delivered by the Body with operational cyber security capacities.
- Authorize the plan of measures and activities for cyber crisis suggested by the Body with operational cyber security capacities.
- Developing programs and action plans for activities in the field of cyber security that need to be implemented by the Body with operational cyber security capacities.

Body with operational cyber security capacities

The Body with operational cyber security capacities may be established either as a separate, newly established entity (agency, directorate) or as a newly formed organizational unit within an existing state organ.

The Body with operational cyber security capacities will be in charge of operationalization of identified activities defined in the Strategy and Action Plan for cyber security, as well as directions and recommendations received by the National Cyber Security Council. The principal obligations of this Body include:

- Developing and issuing recommendations, opinions, reports, research and directions related to the implementation of the Cyber Security Strategy, the Action Plan, as well as other related strategic documents.
- Monitoring trends in cyber space security with the goal of detecting threats that may result in cyber crisis.
- Creating and sharing periodic evaluations for the state of cyber security.
- Continuous cooperation and exchange of information regarding cyber threats, vulnerabilities, incidents, risks and statistics with all relevant stakeholders.

- Proposing a plan of measures and responsive activities in case of cyber crisis.
- Proposing and implementing national and international exercises in the field of cyber security.
- Developing capacities for operational assistance of entities for handling attacks of larger scope and scale.
- Monitoring the current state of ICT of every relevant stakeholder (users of the capacities and services provisioned by this Body) and delivering regular reports for any changes or incidents registered by the entities with the goal of preventive alert for possible system misuse.
- Monitoring the implementation of activities incorporated in the National Cyber Security Strategy and other strategic documents and international standards, by all entities (users) of the services provided by the Body with operational cyber security capacities.
- Coordinative and consultancy activities during the implementation of new ICT solutions and developing software solutions for all stakeholders (users) of this Body.

Implementation risks

- One of the major risks related to the implementation of the Cyber Security Strategy is the lack of awareness for the importance of the need for safe cyber space. This risk is related to the lack of cyber hygiene and political will, as well as consensus for a systematic approach tackling the challenges related to cyber security. In this manner, unsystematic approach may cause harmful consequences affecting the country, especially in the case when the state is faced with advanced, large-scale cyber threats.
- Establishing effective cooperation among all relevant stakeholders is also one of the major risks associated with the implementation of the Strategy. For some stakeholders, cooperation in the field of cyber security is relatively novel, requiring organizations to implement certain changes. The main

challenge is the widespread range of interests and responsibilities of different stakeholders.

- In addition, trust between public and private sector may also pose one of the main obstacles in the effective implementation of the Cyber Security Strategy. Establishing trust is a process that requires dialogue, as well as extensive time and effort. Due to mistrust, certain institutions are not willing to report security incidents, mostly because of potential reputation loses. The lack of exchange of information and absence of obligatory reporting of incidents leads to insufficient awareness of the current state of cyber threats, which in turn may result in difficulties in the process of combating known challenges in the cyber space.
- A great implementation risk may also be the lack of financial and human resources and qualified work force to manage challenges in the cyber space.

The successful implementation of the Cyber Security Strategy will have positive influence on increased cyber security, thereby contributing towards the national security. In addition, ensuring a secure cyber space will increase the trust of users in the cyber space, which may significantly improve the development of new Internet-based services and thereby stimulate the economic growth of the Republic of Macedonia.

APPENDIX 1

Definitions

Botnet – a network of private computers infected with malicious software which is being controlled while owners are not aware of it.

Civil organizations – every association, foundation, foreign organizations, as well as other forms of organizations, registered according to provisions of the Law for associations and foundations, but also non formal civil movements or group of citizens dealing with initiatives in the field of protection of human rights and liberties.

Backdoor – a method in which the security mechanism of the system is bypassed, with the purpose of securing access to the information system or its data.

Malware - a software which is specifically designed to disrupt, damage, or to get unauthorized access to an information system.

Industrial control system – Information system in SCADA (Supervisory control and data acquisition) and distribution control system groups, used for industrial operations, such as manufacturing, production and distribution control through programming logistics controllers which are different from conventional information technologies.

Internet – global computer network which facilitates connection of information and communication devices and interconnected systems by using standardized communication protocols.

Information security – state of confidentiality, integrity and availability of information, achieved by the use of adequate security measures.

Information systems – systems included in the process of enabling any service, transaction or information/data transmitted over ICT.

Classified information – information protected from unauthorized access or use, defined by the level of classification.

Critical Information Infrastructure – refers to any information-communication system whose maintenance, security and safety are critical for the national security, economy, public health and country security. The national critical information infrastructure is part of the critical infrastructure (CI).

Cryptocurrency – decentralized virtual currencies, based on mathematical principles and protected by cryptography, where the principles of cryptography are used for the implementation of a distributed, decentralized, secure information economy.

Personal data – any information which refers to physically identifying an individual or an individual that may be identified, whereas an identifiable individual is a person whose identity may be determined directly or indirectly, especially on the basis of a Unique Master Citizen Number or on the basis of one or more physical characteristics, physiological, mental, economic, cultural or social identity.

Authorities – state administration bodies, other state organs, organs within ministries, governing organizations and independent bodies, judicial authorities and courts, municipality bodies, City of Skopje and municipalities of the City of Skopje, as well as other legal entities and individuals which by law are entitled to perform public authorizations. In this context, the term other subjects refer to: legal subjects that provide and secure services of public interest, e.g. entities in the field of education, health, finance, banking, insurance, energy, water supply, electronic communications and communal services.

National security – a system for contemporary form of organization and functioning of the society which implements specific activities and measures for prevention and repression in order to protect fundamental societal values from security challenges, threats and risks at all levels.

Ransomware – type of malicious software designed to block access to the information system or data stored in that system, often by encrypting, by which certain amount of ransom is required for the victim to pay for the attacker to enabling description of the information system or to allow access to data.

Awareness – refers to the security awareness of all legal subjects that share responsibility for information security.

Cyber security – activities and measures for protection of information systems that constitute the cyber space of attacks, discovery of attacks and cyber security incidents, as well as activation of a mechanism for counter-action and systems renewal to a state prior to the cyber attack.

Cyber war – an act of war in and around the virtual space with means predominantly related to information technology.

Cyber threat – potential cause for incident in the cyber space that may cause damage of any institution or system.

Cyber incident – one or more events related to cyber security that are harmful with respect to confidentiality, integrity or availability of information and disrupt the security of the information system.

Cyber crisis – an event or events in the cyber space that may cause or already have caused significant disruption or damage in the social, political and economic life of the Republic of Macedonia. Such situation may ultimately influence the security of the citizens, the system of democracy, political stability, the economy, living environment and other national values, i.e. the overall national security and defence.

Cyber crime – acts against the law conducted in the cyber space, e.g. crime that may only be conducted through the use of ICT devices and systems, where the systems and devices are either used as tools for the criminal act, or they are the primary target; crime enabled by the cyber space, such as traditional criminal acts and materials for child abuse, which increases with the growing use of computers, computer networks or other forms of ICT.

Cyber space - space where communication between information systems takes place. In context of this Strategy, the definition encompasses the Internet and all information systems related to it, as well as independent information systems.

Cyber attack – operations which individuals and/or information systems deliberately conduct in any place in the cyber space with the purpose of endangering the confidentiality, integrity or availability of information systems in the national cyber space.

Cyber defence – all cyber space defence measures with military and other capacities in order to achieve strategic military purposes.

Cyber resilience – the ability for preparation, adjusting, sustaining and fast recovery from disruptions stemming from intentional attacks, accidents or natural threats or incidents in the cyber space.

Cyber risk – potential risk from causing damage by using weaknesses in one or more information subjects.

Cyber sabotage – cyber attack directed against the integrity and availability of the ICT systems.

Cyber hygiene – reference for practices and steps that users of information devices and systems should take in order to maintain the system health and improve the Internet security.

Cyber espionage – cyber attacks directed against the confidentiality of ICT systems.

CERT – refers to an emergency team which will prevent threats and renew ICT systems in case of security incidents. In general, CERT/CSIRT/CIRT provides services for responding to emergencies, prevention services and managing the safety quality. CERT network includes the same people who work on cyber security.

APPENDIX 2

Acronyms

ИКТ – Information Communication Technologies

EGDI – e-Government Development Index

GCI – Global Cybersecurity Index

IDI – ICT development index

NRI - Networked Readiness Index

CII – Critical Information Infrastructure

IIS – Important Information Systems

DoS – Denial of Service

DDoS – Distributed Denial of Service

CERT – Computer Emergency Readiness Team

CIRT – Computer Incident Response Team

CSIRT - Computer Security Incident Response Team

SCADA - Supervisory control and data acquisition

EU – European Union

NATO – The North Atlantic Treaty Organization

MKD-CIRT – National Centre for Computer Incident Response