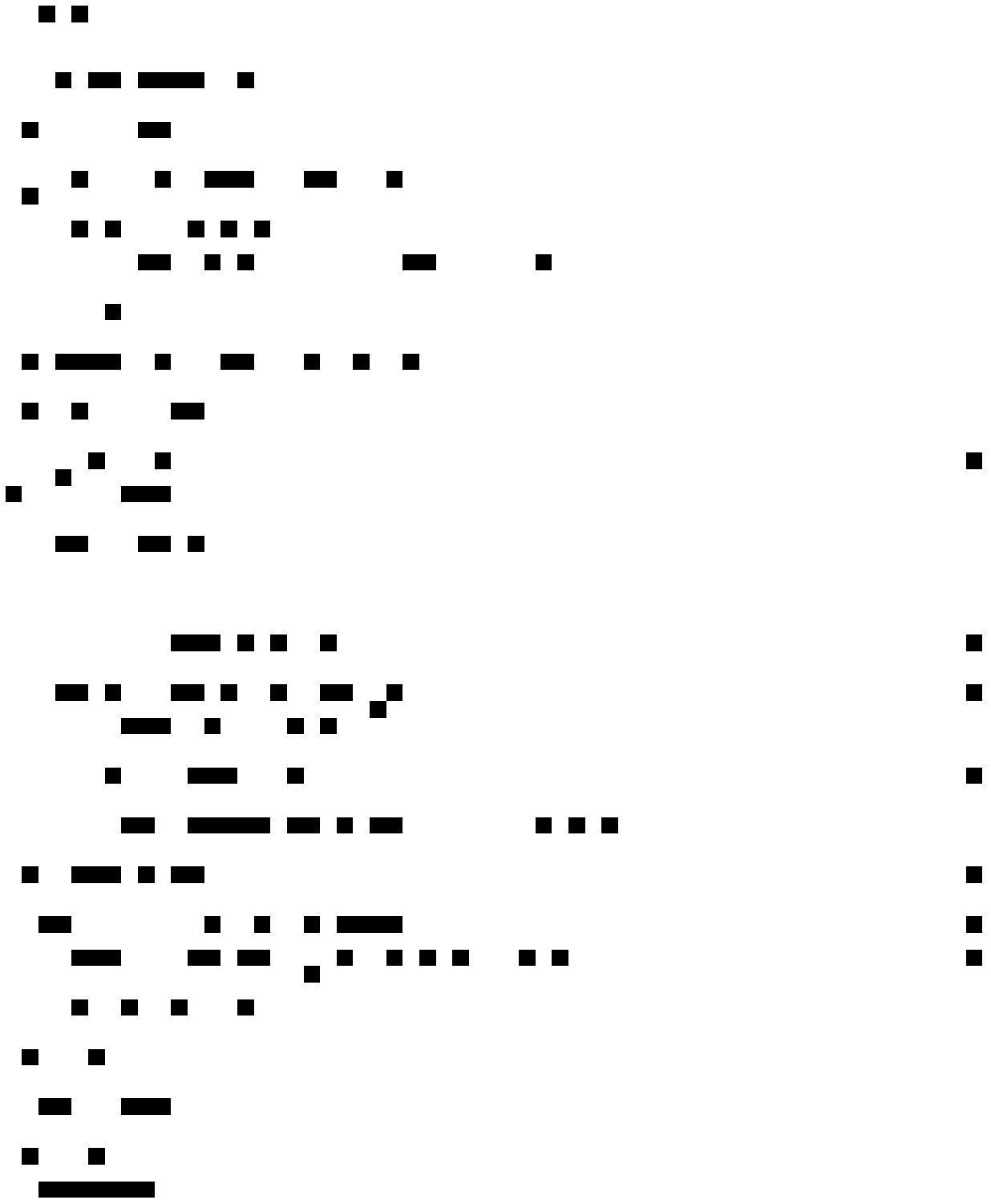


Document administration

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

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]

[illegible]

[illegible]

[illegible]

1. [illegible]
2. [illegible]
3. [illegible]
4. [illegible]

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.

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.

Stakeholders

[illegible]

[illegible]

- [illegible]
- [illegible]
- [illegible]
- [illegible]

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



[illegible] Principles

[illegible] [illegible] [illegible] [

[illegible]

[illegible]

[illegible]

1. [illegible]
2. [illegible]
3. [illegible]
4. [illegible]
5. [illegible]
6. [illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

Implementation

- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]

[illegible]

[illegible]

[illegible]

- [illegible]
- [illegible]
- [illegible]
- [illegible]

■

- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]

[illegible]

- [illegible]
- [illegible]

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.

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]