**International Journal of Publication and Social Studies**
*ISSN(e): 2520-4491*
*ISSN(p): 2520-4483*
*DOI: 10.18488/journal.135.2020.51.69.78*
*Vol. 5, No. 1, 69-78.*

*URL: www.aessweb.com*

# THE IMPORTANCE OF NATIONAL CYBER SECURITY STRATEGY OF THE REPUBLIC OF MACEDONIA

**Risto Rechkoski**

*University St.Kliment Ohridski, Bitola, Republic of Macedonia Faculty of Tourism and Hospitality, Ohrid, Republic of Macedonia.*
*Email: reckoice@t-home.mk*

**Article History**
Received: 25 March 2020
Revised: 27 April 2020
Accepted: 4 June 2020
Published: 29 June 2020

**Keywords**
Cyber -space
Cyber-security
Cyber-crime
Macedonian national cyber security strategy
Cyber security in public Administration
Implementation.

## *ABSTRACT*

Significance of the Cyber security in every society and every state in this time, at the beginning of third decade of XXI century is more than essential. Every society that has public aware of this should persist different measures and instrument in order to supply its citizens, legal entities, and also public and local institutions of authorities with possibility of secure cyber space. Strengthening the national capacities for cyber threat management and improving the cyber security have become a priority for the Republic of Macedonia. Government of Republic of Macedonia passes the National Cyber Security Strategy 2018-2022, in July 2018. The aim of the paper is to examine and pointed out the most important provisions of the Strategy. 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 has several parts, which are related to: Cyber trends, Challenges and threats, Cyber security principles, different Stakeholders that are involved in the Strategy, Vision and mission of the Strategy, Goals of the National Cyber Security Strategy, and its Implementation.

**Contribution/ Originality:** The aim of the paper is to examine and pointed out the most important provisions of the Strategy.

## 1. 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. Government of Macedonia (2018) according to global indexes indicating the level of development of Information Society (such as ICT development index-IDI, Networked Readiness Index-NRI, e-Government Development Index-EGDI, Global Cyber security Index-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.

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. Ministry of Information Society and Administration (2018)

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-defense policy.
4. Establishing an integrated, multidisciplinary approach to secure closer cooperation and coordination between the defense 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 cybercrime.
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 Cyber security Strategy of the European Union and the NATO Cyber Defense Pledge for safe, secure, reliable and resilient digital environment to the benefit of citizens, business community and public administration.

## 2. THE NATIONAL CYBER SECURITY STRATEGY IN MACEDONIA 2018-2022

The strategy is adopted by Government of Macedonia (2018). The strategy has seven integral parts. (http://vlada.mk, http://mioa.gov.mk).

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

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

The third part is about the cyber security principles that support the Strategy. These principles are:

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

Fourth part defines the Stakeholders in the field of cyber security in the country: public sector, public administration, private sector, academic community, citizens and civil society organizations.

The vision and mission of the national Strategy is pointed out in the fifth part.

Sixth part tries on to set up the "Cyber Security Goals and Instruments" of the National Cyber Security Strategy. The objectives of the five goals are focused:

- Building a cyber-resilient ICT infrastructure, identifying and implementing adequate solutions in order to protect the national interests.
- 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.
- Strengthening the national capacities for prevention, research and adequate response to cyber-crime.
- Strengthening the capacities for defense of national interests and reducing current and potential cyber space risks.
- Cooperation and exchange of information on national and international level.

Seventh part is devoted to the implementation of the National Cyber Security Strategy, along with the challenges for success. 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 organizational structure for coordination of the development and implementation of the course of actions defined in the Strategy and the Action Plan.

## 3. CYBER TRENDS, CHALLENGES AND THREATS IN MACEDONIA

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 (Ministry of Information Society and Administration, 2018).

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

A growing need to raise the awareness of the use of best practices for ICT and Information Systems (IS) protection in Small and Medium Enterprises- 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.

The defense 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 defense and security capabilities and fulfillment of criteria for full-fledged EU and NATO membership.

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.

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.

A large number of Internet users, including users in the public and private sector (Rechkoski, 2012) 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 defense mechanisms.

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

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 Internet of Things – 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 is expected to increase in the future.

The field of artificial intelligence-AI, 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.

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

Data security and protection, especially for those of public interest (data relevant for Critical Information Infrastructure-CII and Important Information Systems-IIS) are crucial. 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.

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. 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.

## 4. CYBER SECURITY PRINCIPLES

According to the Strategy, there are five security principles:

1. Effective and efficient cyber security capacities.
2. Protection and prevention.
3. Security for economic development.
4. Trust and availability.
5. Legal security.

About Effective and efficient cyber security capacities, it can be said that With the purpose of efficiently responding to the new risks and threats, 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. The technological development and the ever-growing ICT are increasingly enabling 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. Having in mind that an effective outcome from the research and development in the area of cyber security may be achieved only by close collaboration among all relevant entities, fully support of the multi-stakeholder approach in building efficient cyber security capacities must be done. (https:/aek.mk)

Regarding Protection and prevention, in these heavy times, when all the humanity is faced by different dangers, of different kinds, many severe cyber-attacks on the security of the country, among which cyber operations and espionage sponsored by other states unfortunately, 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, and with that to support security system of NATO, and EU.

Security is essential for economic development. 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. For trust and availability, close cooperation between the public, private and civil sector is of utmost importance. 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. 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.

In order to improve the cooperation in the field of cyber security among relevant stakeholders, the Republic of Macedonia should establish a Centre of Excellence. This Centre's purpose will be facilitating exchange of experience among the public, private sector, civil organizations, academia and other institutions.For the Legal security assurance very important are different instruments of Law and Politics, domestic, and especially international legal acts and conventions. With all these instruments protection of human rights, liberties, democracy and mutual values of the developed world must be performed. Transparency, accessibility for everyone is main characteristics of Internet, with guarantying free informational flow. Freedom of expression, personal data protection, information integrity, and of course right of privacy as a top of all, must be accomplished as high as it is possible. Regarding these things, Macedonian legislation is fully in accordance with world standards in respecting of human rights, freedom of expression and privacy protection (Constitution of the Republic of Macedonia, 1991; Law for Data in Electronic form and Electronic Signature, 2015; Law on E-Documents E-Identification and Confidential Services, 2019; Law on Electronic Communications, 2019; Law on Organization and Work of State Administration Bodies, 2011; Law on Prevention of Corruption, 2015; Law on the Government of the Republic of Macedonia, 2016).

## 5. STAKEHOLDERS

In this manner, the Strategy incorporates different stakeholders, acting mutually, in achieving objectives of the Strategy. These stakeholders are:

- Public sector.
- Private sector.
- Academic community.
- Citizens and civil society.

Public sector 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.

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 defense system; other legal and business subjects which in different manners represent the users of cyber space.

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. Macedonia can proudly say that more or less, in the four State Universities- in Skopje, Ohrid, Bitola and Stip, particular academic programs are in relation with cyber security. There are big cooperation between Macedonian academic community and American, European, Chinese and Russian academic communities, which gives a holistic approach to this issue on global level, and this approach is very needful and important.

The state of security in the cyber space is reflected upon citizens and civil society organizations in many different ways. In this manner, the subject matter of cyber threats is not only citizens who are active users, but also those who have their personal data present in the cyber space.

## 6. VISION AND MISSION OF THE STRATEGY

Vision of the Strategy is 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. This will related to the mission- Macedonia to have clearly defined and sustainable policies, which will be coordinated in the manner of advancing the national cyber security.

## 7. GOALS OF THE STRATEGY

The National Cyber Security Strategy is comprised of five key goals, that are aimed to facilitate the strengthen the existing and build new capacities for defense from cyber-attacks and increase the level of security in the cyber space across all sectors at all levels. All these five goals are related and connected one to another, and all of that systematically related, and it is shown on the Figure 1 below. These goals are so called 5C goals, logically why.

These goals are:

1. Cyber Resilience.
2. Cyber capacities and cyber security culture.
3. Combating cyber-crime.
4. Cyber defense.
5. Cooperation and exchange of information.

1. Cyber Resilience, means, the Republic of Macedonia to have cyber resilient ICT infrastructure, and to identify and implement adequate solutions in order to protect the national interests. It 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. This includes many activities, among them more important are:

- Utilization of the best solutions for cyber incident response with the purpose of protecting the national security interests.
- 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.
- Development of methodology for national level cyber threat risk evaluation.
- Establishing a single and comprehensive legal framework for cyber resilience, taking into account the legal regulatory framework in the Republic of Macedonia and EU.
- Continuous monitoring, adoption and implementation of internationally recognized standards and procedures in the field of cyber security.
- Continuous update on the national strategic documents taking into account contemporary cyber security standards and technologies, as well as cyber threats.
- Building and strengthening the national capacities for active cyber defense and taking appropriate countermeasures to handle and respond to cyber threats.

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. 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.

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.

This consists of:

- Development and creation of study programs in this field, on all levels of education, depending primary, secondary schools, and student and academic programs.
- Education to wider population.
- Different Trainings and promotion.
- Researches in all levels about this, and in different aspects.
- Mutual projects and cooperation between different stakeholders.

3. Republic of Macedonia must 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 hey in order to efficiently tackle cyber-crime. For this goal many activities can be taken, such as:

- Harmonizing the national with international policies related to cyber-crime.
- Development of a single, comprehensive legal framework for cyber-crime, taking into consideration the applicable legal framework in the Republic of Macedonia and EU.
- Modernizing authorities in charge of cyber-crime in order to efficiently combat cyber-crime.
- Establishing efficient procedures to report and research cyber-crime, and also formal procedures for cooperation and exchange of information in the field of cyber-crime among relevant national entities and other security services.
- Cooperation with regional and international organizations for fighting cyber-crime.
- Developing multidisciplinary academic environment and capacities for cyber-crime investigations and resolving.

4. About Cyber defense, Republic of Macedonia should 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, Macedonia defines its cyber defense capacities according to highest international standards, as part of the national cyber security framework. Developing cyber defense capabilities in the Army of Macedonia is part of a comprehensive national defense approach.

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 defense.

Republic of Macedonia, as a country-member of NATO, and EU candidate, and other international military and civil organizations, in order to be included in collective defense, 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. Different activities can be taken within the collective defense systems, and surely Macedonia will cooperate and exchange information with all relevant organizations in the field of cyber defense.

5. Cooperation and exchange of information

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.

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. 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.


**Figure-1.** 5C goals of the national cyber security strategy.
**Source:** Ministry of Information Society and Administration (2018).

## 8. IMPLEMENTATION OF THE STRATEGY

The implementation of measures defined in this Strategy should 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, which may be established either as a separate, newly established entity (agency, directorate) or as a newly formed organizational unit within an existing state organ.

## 9. CONCLUSIONS

According to all mentioned above it can be concluded that:

1. The past years marked a growing and consistent use of ICT, which is a substantial pillar of globalization, and with that essential contribution is provided in the process of improving the social-economic growth, standard of life. Fast progress of ICT provides significant contribution for improvement and development of the whole society. Different stakeholders, from the political, social and economic life consistently utilize the opportunities offered by the great expansion of ICT.

2. The awareness of the Macedonian society for cyber security is on very high level, many measures and instruments are undertaken for this purpose. On legal level, and in accordance with that approach, Government of the Republic of Macedonia adopted National Cyber Security Strategy 2018-2022, in July 2018. This is Strategy that refers for the period of five years.

3. 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. It is consisted of seven parts, each to another related and connected. Beginning with Introduction; than Cyber trends, challenges and threats; Cyber security principles as third part; different Stakeholders; Vision and mission; Goals as a sixth part and Implementation as a final part.

4. The main goals of the Strategy, also known as a 5C Goals, and they are: Achieving of Cyber resilience;

Building of Cyber capacities and appropriate cyber culture; Combating a Cyber-crime; Cyber defense as a main pillar of cyber stability; and Cooperation and exchange of information on all levels, between different stakeholders, in national, regional and international level.

5. The stability of cyber space will result with bigger trust of different stakeholders, different users, in Internet utilization for services in different processes, and that will lead to economic growth, not only in Macedonian society, but also on wider level. Nowadays, the whole world is one Global Village, and it faced the same threats, not only in cyber security, but also on existential issues, and common actions, and mutual cooperation and understanding must be undertaken.

**Funding:** This study received no specific financial support.
**Competing Interests:** The author declares that there are no conflicts of interests regarding the publication of this paper.

## REFERENCES

Constitution of the Republic of Macedonia. (1991). *Official Gazette of macedonia Number 52/91*. Skopje: Parlianment of Macedonia.

Government of Macedonia. (2018). *Strategy for public administration reform in Macedonia 2018-2022*. Skopje: Governent od Macedonia.

Law for Data in Electronic form and Electronic Signature. (2015). Official gazette of Macedonia, Number. 34/2001, 6/2002, 98/2008, 33/2015.

Law on E-Documents E-Identification and Confidential Services. (2019). Official gazette of Macedonia, Number.101/.

Law on Electronic Communications. (2019). Official gazzete of macedonia, Number. 39/14, 188/14, 44/15, 193/15, 21/2018, 98/2019.

Law on Organization and Work of State Administration Bodies. (2011). Official gazette of Macedonia, Number. 58/2000, 44/2002, 82/2008, 167/2010, 51/.

Law on Prevention of Corruption. (2015). Official gazette of Macedonia, Number 28/2002, 46/2004, 126/2006, 10/2008, 161/2008, 145/2010, 97/2015, 148/2015.

Law on the Government of the Republic of Macedonia. (2016). Official gazette of Macedonia, Number 59/2000, 12/2003, 55/2005, 37/2006, 115/2007, 19/2008, 10/2010, 51/2011, 15/2013, 139/2014, 196/2015, 142/2016.

Ministry of Information Society and Administration. (2018). *National strategy for cyber security of the Republic of Macedonia*. Skopje: Government of Macedonia.

Rechkoski, R. (2012). Priciples of public administration (pp. 216). Ohrid: Faculty of Tourism and Hospitality.