EK-A2

University	**:**	**Istanbul Technical University**
Institute	**:**	**Informatics Institute**
Science Programme	**:**	**Applied Informatics Department**
Programme	**:**	**Cybersecurity Engineering and Cryptography**
Supervisor	**:**	**Prof. Dr. Ertuğrul KARAÇUHA**
Degree Awarded and Date	**:**	**PhD – June 2020**

SUMMARY

DETERENCE WHITIN THE FRAMEWORK OF CREATING TURKEY'S NATIONAL CYBER SECURITY STRATEGIES AND POLICIES

Mustafa ŞENOL

With the rapid development of technology, especially computers and communication systems, with the discovery and widespread of the Internet, conveniences and achievements provided by the information and communication systems, that is, the informatics systems and infrastructures have made informatics systems and services indispensable in people's lives all around the world. The effectiveness and efficiency attained in the processing, transmission, sharing, using, storage, and protection of information, which is the most important asset for humanity since the beginning of history, has increased and continues to increase day by day.

Parallel to these developments, the improvements of government's powers, particularly in the economic, political, and military fields that have taken place in shortest time, have made the cyber space, which is a combination of physically and virtually valuable assets, more important. The cyber space has become to be referred to as the 5th operational domain after land, sea, air, and space operation domain. As the importance of cyberspace increases, malicious movements and attacks that have come with the development of information and informatics systems continue to increase rapidly today.

While the facilities and conveniences provided by the cyberspace with the developments in information and communication technologies make life more dependent on such facilities and conveniences every day, significant damages that individuals, societies, and countries have suffered as a result of the use of cyber space for threats, attacks, to harm life and property, and similar malicious purposes, have caused great changes in the understanding of the notion of security. In this context, it has started to be accepted that cyber security is a national security issue and an integral part thereof.

Measures are considered and strategies and policies are being developed to preventing cyber attacks initiated by using means of cyber power, informatics systems and infrastructures that are required for the initiation and maintenance of cyber war and are attained in cyberspace and the ability to use them effectively, and wars caused by cyber attacks, and to dissuade those who think about cyber attacks or war to pursue such thoughts and actions.

Governments are trying to carry out various works in the fields of cyber security, cyber warfare, and cyber deterrence, to evaluate the situation within the framework of technological developments, take measures by identifying risks and threats, make targets in line with their

needs by making predictions for the future, develop strategies and policies and implement them effectively.

With the increase in the use of computers, and the widespread of the Internet, which is a constantly growing communication and information communication network around the world, significant progresses have been attained in Turkey compared to the past with the works initiated to prevent and eliminate the risks, threats, dangers, etc. that occur in parallel with the developments in the world. In this context, besides increasing the efficiency by eliminating the deficiencies and inadequacies related to cyber security strategies and policies against cyber attacks and incidents, it is thought that it would be appropriate to address the issue of cyber deterrence, which is recently a hot topic of conversation and study, with a holistic approach along with cyber security strategies and policies.

Significant progresses have been made from the past to present with studies initiated to prevent and eliminate the negativity emerging in parallel with the developments in the world, and with the increasing use of computers and the Internet becoming more widespread in Turkey as well.

In addition to increasing the effectiveness by eliminating the deficiencies and inadequacies related to the national cyber security strategies and policies created within this scope, it was evaluated that it would be appropriate to address the issue of cyber deterrence with an integrated approach together with cyber security strategies and policies.

Based on the thoughts put forward, in this study it is aimed to answer what ways should be followed to develop a needed strategy and how this strategy should be developed in order to ensure effectiveness of the cyber security of assets, information and communication systems and infrastructures owned in a country in cyberspace, to become an effective power for cyber war and deterrence and to create a summary resource for the studies to be carried out.

As a method, to facilitate an understanding of the subject and to provide term unity, first, basic concepts related to the subject have been discussed, certain studies in Turkey and abroad are reviewed and brief samples are provided and discussed. Later, an approach regarding the guidelines, principles, and procedures for the establishment of a national cyber security strategy and the development and implementation of the existing one is presented and opinions are evaluated.

In this context, the information, computer and communication systems and developments in these issues are examined from a historical perspective; primarily peer-reviewed academic publications and journals, publications and documents of relevant institutions and organizations, books, magazines, library and internet environments were scanned about cyber space, cyber attacks, cyber crime, cyber terrorism, cyber security, cyber defence, cyber warfare, cyber intelligence, cyber power, etc. concepts, cyber security strategies and policies, and cyber deterrence with technical concepts related to information systems and security, for following of developments, various conferences and workshops were participated, and meetings were held with the relevant institutions and organizations.

In this context; on Strategy and Security, more than 20 books, documents and studies; on Cyber Security and Strategy over 30 books, documents and studies; on Cyber Security Strategy Documents and Action Plans documents of nearly 20 countries, primarily USA, China, Russia, France, England, Israel, India, North Korea, Germany, Canada, Netherlands, Finland, Japan, Australia and Iran; on Turkey's National Cyber Security Strategies and Action Plans, from beginning to present, preparing the implementation 17 strategy documents and action plans; on Deterrence and Cyber Deterrence, over 30 books, documents and studies

have been examined; Seminars, symposiums, panels, workshops and conferences related to developments on the subject, more than 20 events were participated.

After researching, analysing and editing studies have been made and the content of this thesis consists of 7 Main Sections stated below, which has been prepared in accordance with the principles of Istanbul Technical University Postgraduate Thesis Writing Guide and Postgraduate Thesis Template.

In the Introduction section, the importance and need to develop strategies and policies to provide national cyber security against malicious acts and attacks experienced with the developments in information and communication systems have been explained.

In Terms and Concepts Related to Cyber Security, the most used terms and concepts that are closely intertwined with the subject are defined and briefly explained in order to correctly understand the cyber security issue with a holistic approach providing a term and concept unity.

In Cyber War, information is provided on cyber attacks and wars that started in the past that continue today and will continue increasingly in the future, which support the view that cyber security is an integral part of national security, and national security as a result of cyber attacks and attacks in cyber environment.

In Cyber Deterrence, it is discussed that a common approach in terms of deterrence is very new in cyber security applications in the world, but adequate attention and priority was not given in Turkey; examples from wars from the past to present are given, explaining the idea that deterrence might be better rather than winning in wars

In National Cyber Security Strategy and Policies, strategy and policy concepts are explained, information is provided about current cyber security strategies and policies of leading countries in this regard and Turkey with intuitional and national cyber security strategies

In Creating Cyber Security Strategies and Policies to Provide Deterrence, an approach style has been put forward for the preparation and implementation of the national cyber security strategy and policies that will also provide deterrence for Turkey, considering existing strategies and action plans, based on the information obtained from the studies of some international institutions with national cyber security strategy documents of countries leading in national cyber security.

In Conclusions and Suggestions, results of the conducted study within the scope of the thesis topic, the evaluation, and opinions and suggestions were presented.

The approach presented and proposed with this thesis is, an 8-stage cycle; “Creating and Implementing the National Cyber Security Strategy Life Cycle”, beginning with the assessment of the current situation, followed by the achievement of the specified goal, organization, scope, planning and implementation stages including control and audit activities and development activities in the process, within the framework of scientific tactics and techniques.

Additionally in this life cycle, the structuring of “The National Cyber Security Presidency” is recommended, as the main body responsible for this cycle, 'for managing the National Cyber Security Strategy and the Cyber Power', and to meet the needs of “a strong central public authority to ensure coordination in the field of cyber security” emphasized in the 2016-2019 National Cyber Security Strategy and still seen to be deficient in Turkey