Cyber Security and Defense: Proactive Defense and Deterrence

Mustafa Şenol
Faculty of Engineering and Architecture
Istanbul Gelisim University
Istanbul, Turkey
msenol@gelisim.edu.tr

2022 3rd International Informatics and Software Engineering Conference (IISEC) | 978-1-6654-5995-2/22/$31.00 ©2022 IEEE | DOI: 10.1109/IISEC56263.2022.9998314

***Abstract*— With the development of technology, the invention of computers, the use of cyberspace created by information communication systems and networks, increasing the effectiveness of knowledge in all aspects and the gains it provides have increased further the importance of cyber security day by day. In parallel with the developments in cyber space, the need for cyber defense has emerged with active and passive defense approaches for cyber security against internal and external cyber-attacks of increasing type, severity and complexity. In this framework, proactive cyber defense and deterrence strategies have started to be implemented with new techniques and methods.**

Keywords*— *Cyber security, cyber defense, proactive cyber defense, cyber deterrence

I. INTRODUCTION

"Security", which is defined in dictionaries as "the legal order in social life is carried out without interruption and people can live without fear" [1], is a concept that takes place in the whole life of a person, starting from his birth. People need security in order to protect their life, property and valuable assets. In human life, when it comes to the goals and objectives that are desired to be achieved as personal, family, society, institution or nation, insecurity and security emerge according to the dangers, threats and the presence and proximity of risks and their level of realization [2].

Security has been provided in various ways with strategies and policies developed by individuals, societies, institutions and organizations and countries in the historical process. National security means the protection of a nation's country, its land, sea, air and space areas and all its homeland, people, institutions, values and interests against internal and external threats by using all military, political, diplomatic, economic and geographical opportunities. The term "defense" is used as a part of security in the sense of people encountering with wars and resisting attacks with military applications [1].

In defense, military units try to destroy the offensive power and determination of the enemy by deploying on suitable terrain, shooting, taking advantage of obstacles, limited counter-attacks, maneuvering and close combat, in short, using active and passive defense techniques. States use their power primarily have the other party give up, that is to say deter from their wishes or actions. When deterrence is not provided, offensive or defensive conflicts and wars are experienced in which the parties may be harmed.

In the development of humanity, their transition from the hunting society to the agriculture, industry and information society was made possible by their ability to perceive, think, reason and speak, by comprehending their environment and the universe and changing them with their findings. In this process of change and development, it has been understood that the most valuable and empowering asset is knowledge. The need to ensure the protection of information due to the power it provides has revealed the concept of "information security".

The development of technology, the invention of computers, the use of cyber space created by information communication systems and networks, and the increase in the effectiveness of information in all respects have added indispensable gains to the lives of nations and states. The fact that life has become easier with these gains and that information systems are indispensable for human life has brought dangers. As the futurologist Toffler says, our technological strength is increasing day by day, but the side effects and potential dangers grow much faster than that. [3]

After the developments in technology and information systems and networks, it has become more difficult to ensure the security of the information, almost all of which is transferred to the digital environment, for its production, storage, transmission, distribution, sharing and use. Cyber space has been accepted as the fifth battleground after land, sea, air and space, with cyber incidents, crimes and attacks in the cyber environment. The need to ensure the security of personal, institutional and national cyberspace, including the security of information, which has become more difficult to protect, has emerged, namely the concept of "cyber security".

Although cyber security is necessary and important for individuals in terms of ensuring the security of personal data and information, when it is insufficient or not provided at all, the extent of damages and harms at institutional and national dimensions is very large. Similar to military terms, "national defense" constitutes the most important dimension of national security, while "cyber defense" constitutes one of the most important dimensions of cyber security. Institutions, organizations and states use their cyber power primarily to discourage the aggressor from their wishes and actions in the cyber environment, that is, to provide cyber deterrence. When cyber deterrence is not provided, are faced with cyber incidents and wars, mainly cyber defense or offensive, where all parties can be harmed.

In this study, the importance of cyber security has been emphasized and the concepts of cyber security and cyber defense have been examined and definitions have been made to eliminate the complexity in terms and concepts. The cyber defense approach, active and passive cyber defense approaches, which are inspired by military operations and strategies, are examined, and proactive cyber defense techniques and methods are emphasized within the active cyber defense approach. It has been pointed out that the effective implementation of the proactive cyber defense approach will also provide cyber deterrence.

II. CYBER SECURITY AND CYBER DEFENSE

Parallel to the development of technology, with the development of computers, information and communication systems and networks, data and information are now in

978-1-6654-5995-2/22/$31.00 ©2022 IEEE

digital environment in the current information age. Along with cyberspace, which is distinguished by the use of electronic and electromagnetic spectrum from computer screens to rays coming from the sun [4], many terms and concepts that started with "cyber" have entered the life of humanity. One of the most common of these is indisputably "cyber security", due to its importance and priority, including the security of data and information.

Although cyber security is personally important, it is necessary to develop strategies and policies, create laws and implement them effectively by considering them at institutional, national and international levels. The concept of "cyber defense" is also widely used, especially within the scope of preventing incidents and attacks on the cyber environment. In order to ensure the security and defense of information, information systems and networks effectively, and to achieve the goals determined by strategy and policies, first of all, it is necessary to use terms and concepts correctly and to ensure a consensus.

A. Cyber Security

There have been many studies on information security and related cyber security, so there are many definitions in the literature. When it comes to personal cyber security, the security of one's accounts, credit cards, computers, smart devices and objects comes to mind. When it is approached institutionally, much broader meanings and needs emerge, and the national cyber security dimension becomes unlimited, including all citizens and institutions of the country, and even extending to the international dimension.

With this broad and unlimited perspective, the definition of cyber security should also be broad and inclusive. The definition of cyber security in Turkey 2020-2023 National Cyber Security Strategy and Action Plan is defined as “All activities that involves protecting the information technologies which constitutes the cyberspace from attacks, ensuring the confidentiality, integrity and availability of those systems, detecting attacks and cyber incidents, activating response mechanisms against those, and restoring the systems back to pre-cyber incident conditions.” [5].

When the definition is examined, it is seen that not only the definition of cyber security is made, but also the precautions to be taken and the studies to be done to ensure cyber security are briefly summarized as seen in Table 1.

TABLE I. MEASURES TO BE TAKEN AND WORKS TO BE DONE TO ENSURE CYBER SECURITY

R. Nu.	Precautions and Studies for Cyber Security
1.	To protect the information systems which constitutes the cyber space from attacks,
2.	To ensure the confidentiality, integrity and accessibility of data and information processed in the cyber environment,
3.	To detect cyber-attacks and cyber incidents,
4.	To activate response mechanisms against cyber incident and attack detections,
5.	To return the systems to their pre-existing cyber security situation after the cyber incident and attack.

- Protecting the information technologies which constitutes the cyberspace from attacks,

Cyberspace has a physical and virtual structure that includes users and consists of hardware and software. Structures incorporating information systems constitute critical infrastructures that may cause loss of life, economic harm of large-scale, national security gaps and public disorder when the confidentiality, integrity and availability of data / information is disrupted [5]. For cyber security at corporate and national level, necessary measures are taken to prevent valuable assets in cyberspace from being adversely affected and damaged by cyber-attacks and events, especially in critical infrastructure sectors such as electronic communications, energy, finance, transportation, water management and critical public services.

- Ensuring the confidentiality, integrity and availability of data and information processed in the cyber environment

Three basic principles in ensuring the security of data and information, "confidentiality, integrity and availability", form the basis of cyber security. Plans, systematic and in accordance with international standards are carried out to prevent unauthorized use, access and disclosure, deletion, modification and damage of data and information by unauthorized persons, and to ensure that they can be accessed where, when and in quality. The use of advanced, improved technology and quantum crypto and encryption systems (AES, RSA, etc.) in the protection of data and information provides significant assurance and gains.

- Detecting cyber-attacks and cyber incidents

All kinds of cyber incidents, especially intentional cyber-attacks that will cause damage to the security of information systems or the data and information processed by these systems, must be detected first. While the types, severity and complexity of cyber-attacks have increased from past to present, detection has also become more difficult. Even cyber attackers, whose technical knowledge, education and training levels have decreased considerably, have begun to cause serious damage to information and information systems. [6] For the detection of cyber-attacks and incidents, threats are correctly evaluated, an effective risk management operation is carried out, necessary software and hardware measures (intrusion detection & prevention systems - IDPS, security information and event management systems - SIEM) are taken on time and in place, and tried to be implemented the determined strategies and policies effectively

- Activating response mechanisms against cyber incident and attack detections

In the cyber environment, whether at the personal, corporate or national level, adequate measures and solutions should be implemented in accordance with pre-determined policies, without delay after detection, as well as detecting a cyber-incident or attack. Measures are tried to be implemented systematically and automatically in line with the warnings and directions of IDPS / SIEMs, or quickly after a very short analysis and evaluation. All kinds of detections are taken into account and the necessary reaction is shown.

- After the cyber incident and attack, returning the systems to their pre-existing cyber security situation.

After a cyber-incident and attack, it is of great importance for the systems to be operated smoothly and to replace the losses experienced by taking the process to its pre-event state, especially in terms of reputation as well as financial aspects. Necessary lessons are learned by conducting rapid and detailed post-incident investigations, and all kinds of new measures and practices are put into practice in a short time to prevent similar incidents and attacks. Detection of cyber security events and attacks in the cyber environment, showing the necessary reactions and returning the environment to the pre-event state, Cyber Incident Response Teams / Center (CIRT / CIRC), Cyber Security Operations Center (CSOC), etc. These are the works that require continuity and smooth application within the scope of the duties and responsibilities of the formations.

As can be seen and understood in its detailed definition, cyber security is a process that requires continuity. In parallel with the development of technology and information systems, techniques, methods and strategies covering pre-, during and post-incident processes are developed and implemented in order to ensure cyber security, with the lessons learned and the experiences gained from the dangers encountered, the type, severity and complexity of the incidents and attacks.

Active and passive cyber security measures are implemented with policies determined in accordance with national and international standards at personal, institutional, national and international dimensions and levels. Passive cyber security approaches are based on the monitoring, tracking, examination and evaluation of dangers, threats, attacks and events in software and hardware integrity. Active cyber security approaches, on the other hand, include studies aimed at identifying risks and preventing their realization by using data, information and determinations obtained through passive cyber security measures, by dealing with dangers, threats and events before they happen. Active and passive cyber security measures are more prominent in cyber defense processes and studies in all stages from cyber security to war (Figure 1 and Table 2), especially in order to prevent cyber-attacks and to minimize possible damages and harms if they cannot be prevented.

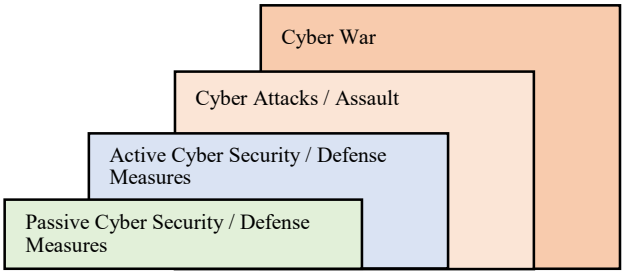

Fig. 1. Cyber security, defense, offensive and war phases

B. Cyber Defense

The military definition of the concept of defense, which is explained in the dictionaries as "resisting and protecting against attacks" [1, 7], is defined as "Combat which is based on destroying the offensive power and determination of the enemy with fire, obstacles, maneuvers and close combat by deploying on a suitable terrain section. form" [8].

Although it is seen that it is used synonymously with security in daily life, as it can be understood from the definitions, the term defense is generally used for the measures taken and the work done in the case of an attack within the concept of security. Referring to the understanding that sports such as karate, taekwondo and judo are used to protect oneself in case of an attack, it is the result of this correct approach that they are called "defensive sports".

According to the tactics, strategies and methods applied with active and passive measures taken in the field of military operations, defensive operations are called by various names such as active / passive defense, position defense, volatile defense. [8, 9] Of these, passive defense; is carried out by passive measures, including the use of reconnaissance, surveillance, concealment, dispersal, deception and protection facilities to minimize the effects of the enemy's weapons and fire. Active defense; is carried out in the form of defense based on the destruction of the enemy piecemeal by means of limited counterattacks against the open sides and back, with active measures based on fire and maneuver, in order to prevent, frustrate or reduce any kind of attack of the enemy.

Position / Area defense; In the absence of sufficient number of agile units, passive defense is based on the principle of holding a certain land in order to meet and destroy the attacking enemy with increasing fires. It is a form of active defense based on the principle of destroying the enemy with counter-attacks in order to meet the expected enemy attacks, channel them to unsuitable terrain, prevent the advance, harass and disrupt its arrangement, if there is sufficient mobile forces in hand.

Based on the definitions and explanations of security and defense terms and concepts, the definition of cyber defense can be made as "precautions and studies to prevent and counter attacks on information and information systems in the cyber environment". In Turkey's National Cyber Security Strategy, it is appearing to be highlighted that important to consider cyber security as a part of national security with a holistic approach within the strategy objective of "Integration of Cyber Security into National Security", and to take the place of cyber defense as well as land, air, sea and space security in high-level national security policies. [5]

Similar to the active and passive defense methods used during military defense operations, active cyber defense in which active measures are predominantly included in the cyber environment is carried out by adopting passive cyber defense approaches in which passive measures are predominantly included (Table 2).

TABLE II. ACTIVE AND PASSIVE DEFENSE MEASURES AND STUDIES

Forms	Passive Cyber Defense	Active Cyber Defense
Precautions / Studies	• Password and secret codes, • Keeping logs, • Cyber intelligence, • Periodic maintenance, updates and patches, • Virus protection systems, Firewalls, • IDPSs, • Backup systems, Staff training and awareness	• Cyber intelligence and information gathering, • SIEMs, • Threat monitoring and response, • Deception / Honeypot systems, • Back attack (hacking) studies, • Counterattacks, Staff training and awareness

Passive or inactive cyber defense is a form of cyber defense in which passive cyber security and defense measures

are taken to protect information, information systems and networks against cyber-attacks in the cyber environment, and software and hardware systems with less human interaction are used intensively. It includes the techniques and methods in which the attackers have the priority and superiority in decision-making, the attacks are monitored, the necessary records are kept, analysis and examinations are made, but generally unresponsive to the attackers who have the priority and superiority (initiative) to make the decision. It is also called the "reactive cyber defense" approach because it is aimed to react to cyber attackers after their actions and to remove or reduce the negative effects of the actions.

Active cyber defense, on the other hand, is a form of cyber defense that is implemented by taking active cyber security and defense measures to prevent attacks on information, information systems and networks and to neutralize attackers with the data and information obtained from the application of passive cyber defense measures. In active, that is, effective cyber defense, in case of detections about attacks and attackers, legal solutions are produced in line with the predetermined strategies and policies, and a reaction is shown.

The main and primary goal in active cyber defense is to prevent attacks, discourage attackers from attacks or, if necessary, to neutralize the attacker by attacking. Along with the development of technology over time, the diversification and development of threats have also led to changes and developments in active defense techniques and methods, and many new terms and concepts have emerged and been used. As Berninato emphasized, with the fact that active defense tactics were known by everyone, the definitions and principles related to the concept also became chaotic [10], and a confusion of terms and concepts began to be experienced in this regard.

With the strategies and policies of institutions / organizations and states, active cyber defense measures in studies on the subject are reactive, proactive, preventive, pre-emptive cyber defense, etc. are explained with terms and concepts.

The term “reactive” is explained in dictionaries as “Reacting to events or situations rather than taking action to change or prevent something” [11]. Reactive cyber defense, in addition to being used in the sense of inactive cyber defense, is applied in the form of acting according to the examinations and evaluations to be made after any cyber incident and attack while applying passive defense measures. It is considered as a passive defense approach due to the monitoring of cyber incidents and attacks at the beginning, and as an active defense approach because it reacts in line with the evaluations to be made afterwards.

The term “proactive” is defined in the dictionaries as “Not only reacting when change occurs, but taking action by causing change” [11]. Proactive cyber defense is a cyber-defense approach that aims to prevent threats, attacks and events in the cyber environment before they occur and without causing any negative effects, and includes effective actions, including neutralizing the attacker with counter-attacks if necessary.

Based on this widely accepted definition, it is thought that it would be more inclusive and explanatory to use the term "pre-emptive (“ön alıcı” or “önleyici” in Turkish language) cyber defense" instead of "proactive cyber defense", since it is a proactive cyber defense approach primarily aimed at prevention.

III. PROACTIVE CYBER DEFENSE

The North Atlantic Treaty Organization (NATO) defines active cyber defense as "proactive measures that include the timely detection and prevention of cyber intrusions, attacks and actions or responding to cyber threats and attacks to protect critical infrastructures, networks, valuable assets and information in the cyber environment" [12]. This definition is a broad definition that includes passive cyber defense. In Turkey's National Cyber Security Strategy, it is emphasized that the continuation of the development of proactive cyber defense understanding and the reinforcement of proactive cyber defense with the studies to be carried out are among the priority targets. [5]

The application of active cyber defense, which is similar to active / volatile defense among defense techniques and methods in military operations, as proactive cyber defense is explained in detail in Denning and Strawser's study titled "Adapting Air Defense to Cyber Space". Air and missile defense operations is defined as "Detecting and recognition enemy air and missile attacks from the earliest and most advanced line as much as possible, starting from peace, passive air defense measures to reduce the effects of enemy air and missile attacks with active activities that ensure their effective prevention and destruction” [8]. In Denning's study, based on the definition of air defense operations, active cyber defense is defined as "A direct defensive action consisting of all measures other than passive cyber defense measures taken to destroy, frustrate or reduce the effectiveness of cyber threats against friendly forces and entities". [13]

Although it is very similar to air and missile defense operations, there are indecisions and concerns in the implementation of proactive cyber defense due to deficiencies and inadequacies in cyber security and war law, which do not yet have rules like the law of war and internationally accepted laws. Attacks and wars are prohibited in accordance with the United Nations (UN) treaties, but they are only possible if certain conditions, especially self-defense, are fulfilled. In addition, according to the laws of most countries, cyber-attacks, cyber fraud, etc. crimes are defined and prohibited. Due to the limitations and prohibitions in this context, it is appropriate to be careful in applying a proactive cyber defense approach at the personal and corporate level, and to act in coordination and together with the relevant state units, security and judicial forces. In the practices to be carried out by state units within the scope of national cyber security, it is necessary to act in accordance with UN law and international agreements, international ethics and customary rules in order not to become an aggressor state.

Within the scope of active cyber defense, the scope of proactive defense techniques, methods and strategies are listed in Table 2. The primary step in preventing attacks starts with recognizing the attacker. Cyber intelligence and information gathering activities about current and potential attackers are planned and continued. It is operated on a 24/7 basis by establishing security information and event management systems.

Although there are many techniques and methods for proactive cyber defense applications, the most common ones in terms of effective results can be grouped into 4 groups as

threat monitoring, honeypot systems, back-hacking attacks and counter-attacks.

- Threat monitoring and response

While information systems and networks are protected by passive cyber security and defense measures, they are constantly scanned with IDPS and SIEMs, and evaluated by taking into account all kinds of records and warnings. It is necessary to act proactively during the process, to detect and remove threats from the system before any adverse event occurs and without damaging the systems and valuable assets.

In this context, the pre-receptive studies are also called threat hunting and it is defined as “the process of searching, detecting, removing and separating the threats escaping from the security solutions in the information network or data set, pre-receiving and repetitively” [14].

- Deception / Honeypot systems

War deceptions constitute techniques and methods that have been used for centuries in the historical process and have achieved successful results. In the cyber environment, various deception techniques and methods are used by the attackers against information systems and users for various purposes.

Today, many deception techniques and methods are used by cybersecurity professionals within the scope of proactive defense to detect, stall, slow down and keep the attackers who take action against the cyber environment, as if confirming the proverb "who goes hunting, hunts".

- Back hacking studies

In dictionaries, hacking is defined as breaking into someone else's computer system to gain information or do something illegal [11]. Hackers are computer programmers, usually knowledgeable and skilled in computer and network security, who can detect and exploit vulnerabilities to gain access to their targeted information systems and data. Today, there are malicious hackers, as well as bona fide hackers working to protect the information systems of institutions and organizations.

Malicious hackers work for illegal purposes like that usually enter the target information system without authorization and permission, stealing or corrupting personal / corporate data and information, revealing confidentiality, gaining financial gain or espionage, etc. One of the proactive cyber defense methods in the fight against hackers who take illegal action is the back hacking method, which also has a retaliatory feature against the attacker hacker or the source of the attack.

A back-hacking attack method is defined as "a measure that involves gaining access to the attacker's computer and regaining access to his own network by a cyber-defender for the purposes of gathering information to prove the attacker's guilt, examining his behavior to prevent future actions, etc."[15]

- Counterattacks

It covers applications that are prepared and run for malicious software and programs that have been infiltrated into friendly information systems and networks, unlike hacking attacks against the source of the attack and the attacker in the cyber environment. Within the scope of proactive cyber defense, although there are various techniques and methods for different purposes, one of the most widely used is the "white worm" application. A white worm application consists of software and programs designed by some informatics experts to find and destroy malicious software, and contain viruses that are deliberately placed on a system or network [17].

The effectiveness and success of proactive defense depends on the coordination and execution of passive defense measures and the high level of cyber security training and awareness of user personnel, especially basic cyber security measures. One of the most important results of the effective implementation of proactive cyber defense measures is that it provides cyber deterrence on the attacker.

IV. CYBER DETERRENCE

The concept of deterrence, which is described in dictionaries as "the act of taking measures to prevent and imped an aggression" [1], was used in the BC. It was explained by the Chinese war strategist Sun Tzu in the 500s as "The best is to subdue without fighting" [17]. Explaining deterrence as “intimidating the other party not to commit hostile acts”, Libicki describes cyber deterrence as “to discourage the attacker from attack by nullifying or punishing the action of the attacker in the cyber environment” [18].

The cyber deterrence strategy is based on two basic methods (Figure 2). In the first of these, intelligence, detection and determination, attribution, prevention, preemtion and assurance etc. cyber security and defense capabilities are further increased with these studies, and it is aimed to prevent and frustrate cyber attacks and actions. In the second, the connection announcement, threats and competencies are announced to the attacker, and the determination to punish and retaliate with various sanctions is demonstrated.[19]

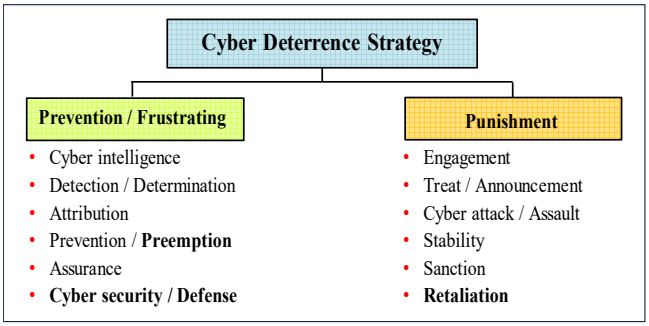

Fig. 2. Cyber Deterrence Strategy Technigues and Methods [19]

Within the scope of active cyber defense, with passive defense measures and pre-emptive cyber defense approach, it is possible to detect and attribute the attacker and his actions with cyber intelligence, and with a strong cyber security, it is possible to frustrate the actions of the attacker. For a resilient and strong cyber security, the use of advanced and improved crypto and encryption systems provide great benefits in the protection of data and information, as well as intrusion detection and prevention systems,

In addition, with proactive defense techniques and methods, threat monitoring and reaction, deception and honeypot systems, retaliation with counter cyber-attacks and initiation and punishment of legal actions, a resultant cyber

deterrence against the cyber attacker is provided. It has never been seen in history that a decisive victory was won by defense in classical wars. To have a decisive cyber-attack power and stability against the attacker in the cyber space battlefield, and by applying this power with pre-emptive techniques and methods, it can always be a deterrent.

V. Conclusion And Evaluation

Developments in technology and information and communication systems do not stop, and sometimes there are advances at the speed of light that also challenge the imagination of people. Parallel to these developments and advances, dangers, threats and attacks on valuable assets, especially critical infrastructures in the cyber environment, are changing, diversifying and increasing in severity every day.

The importance of cyber security and cyber defense against cyber events, especially cyber-attacks, which will continue to increase in the future in cyber space, is increasing day by day, and the need to develop strategies and policies consisting of the tactics, techniques and methods used in the precautions taken in this context arises.

It is seen that a wide variety of terms and concepts have emerged and used within the active and passive cyber security and defense strategies, which have been developed and used by being inspired by the knowledge and experience gained in the field of military operations in the process.

In cyber security and defense, the application of active and passive defense measures together, completely and decisively, constitutes the basis of effectiveness and success. However, it is obvious that the correct understanding of terms and concepts, and the fact that practitioners and users speak the same language within the unity of terms and concepts, achieve the targeted results.

In cyber security and defense, holistic strategies and policies covering active and passive security and defense measures should be developed and implemented in order to be successful against cyber attackers at the personal, institutional or national levels.

Especially within the scope of active cyber defense, national studies should be carried out to eliminate deficiencies and inadequacies in the effective implementation of proactive cyber defense measures and international cooperation should be made in this regard. A proactive and preventive cyber defense strategy provides high gains and success in cyberspace, however, it should be acted carefully and in accordance with international law and agreements and should not become an aggressor state.

With the studies to be carried out within the scope of cyber security and defense, national cyber power will increase even more and great contributions will be made to the whole national power by strengthening proactive defense, ensuring cyber deterrence, detecting cyber-attacks and incidents before they occur and taking precautions.

References

[1] TDK Dictionary, https://sozluk.gov.tr/ (Accessed: 15 September 2022).

[2] Dedoglu, B., “International Security and Strategy”, Yeniyüzyıl Publications, Istanbul, 2014.

[3] Goodman, M., “Future Crimes The Dark Side of the Digital World”, TIMAS Publications, Istanbul, 2016.

[4] Singer, P. W. and Friedman, A., “Cyber Security and Cyber War”, Buzdagi Publications, Ankara, 2015.

[5] T.R. Ministry of Transport and Infrastructure, “National Cyber Security Strategy and Action Plan (2020-2023)”, Ankara, 2020.

[6] ITU, Global Cybersecurity Agenda High-Level Experts Group Global Strategic Report. ITU Press, Cenevre, 2008.

[7] Oxford Learner’s Dictionary, https://www.oxfordlearners dictionaries.com/ definition/english/defence?q=defence, (Accessed: 17 September 2022).

[8] MS 76-3 TAF Joint Glossary of Military Terms, General Staff Printing House, Ankara, 2010.

[9] USA JCoS, “JP 3-53 Doctrine for Joint Psychological Operations”, ABD, 2003.

[10] Berninato, S., Active Defense and Back Hacking, (Digital - Transformation Cyber Security, Harward Business Review Press), Optimist Publications, Istanbul, 2020.

[11] Camridge Dictionary, https://dictionary.cambridge.org/us/ dictionary/english/ (Accessed: 17 September 2022).

[12] Štrucl, D., Comparative study on the cyber defence of NATO Member States, https://ccdcoe.org/uploads/2022/04/Comparative-study-on-the-cyber-defence-of-NATO-Member-States.pdf (Accessed: 5 October 2022).

[13] Denning, D. E. and Strawser, B. J., Active Cyber Defense: Applying Air Defense to the Cyber Domain, (Understanding Cyber Conflict: Fourteen Analogies, Ed.: Perkovich, G. ve Levite, A. E.) Georgetown University Press, ABD, 2017.

[14] Sazak, S. and Köroğlu, U, Threat Hunting for Effective Cyber Defense BGA Publications, Istanbul, 2017.

[15] Herpig, S. et al, Active Cyber Defense - A comparative study on US, Israeli and German approaches, https://www.kas.de/documents/ 263458/263507/Active+Cyber+Defense+-+A+comparative+study+on +US,+Israeli+and+German+approaches.pdf, (Accessed: 5 October 2022).

[16] Dewar, R., Active Cyber Defence, ETH Zurich, Switzerland, 2017.

[17] ITzu, S. (2016). Art of War. (Transl. P. Otkan ve G. Fidan), T. Is Bankasi Kultur Publications, Istanbul.

[18] Libicki, M.C., Cyberdeterrence and Cyberwar. RAND Corp., ABD, 2009.

[19] Senol, M. and Karacuha, E., Creating and Implementing an Effective and Deterrent National Cyber Security Strategy, Journal of Engineering, Hindawi Publishing Corp, https://doi.org/ 10.1155/2020/5267564, 2020.