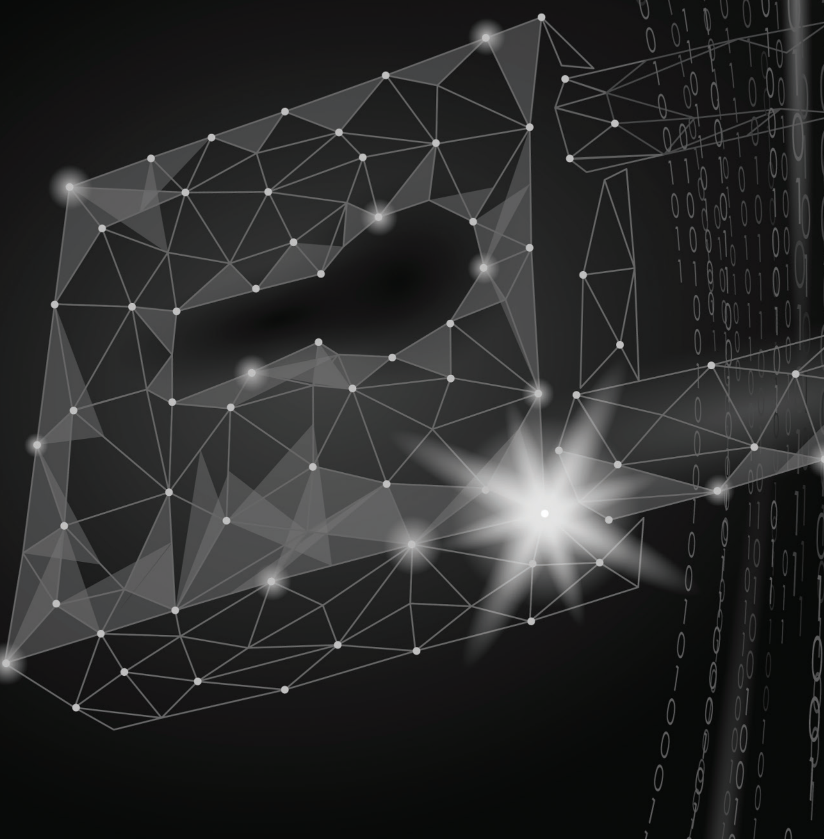
SETA Emerging Military Technologies Series .2.

Cyber Security:

Global Trends & Türkiye's Capabilities

Ahmet Naci Ünal



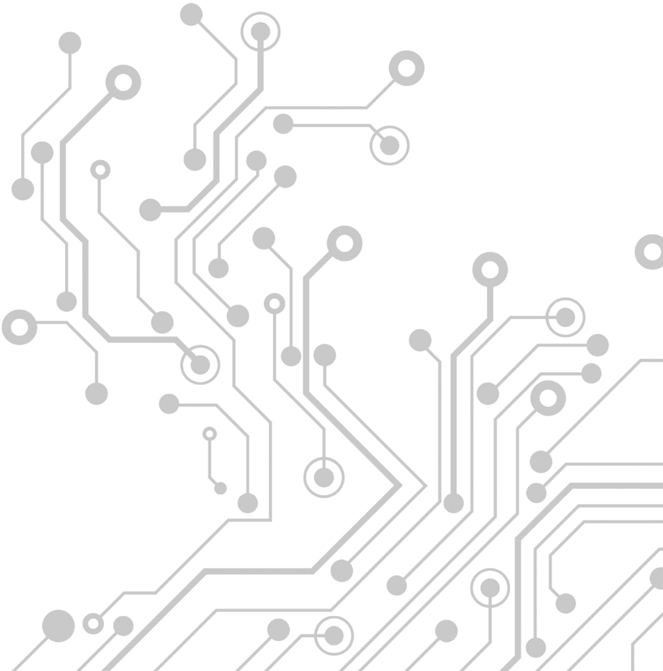
SETA

SETA Emerging Military Technologies Series .2.

Cyber Security:

Global Trends & Türkiye's Capabilities

Ahmet Naci Ünal



SETA

AHMET NACİ ÜNAL

Dr. Ahmet Naci Ünal is a faculty member at Bahçeşehir University's School of Engineering and Natural Sciences. In addition to conducting academic research on electronic-based defense technologies, cybersecurity concepts and decision-making support systems, he serves as Director of the BAU Cybersecurity Application and Research Center and Coordinator of the Cybersecurity and Information Law master's programs at the BAU Institute of Graduate Education. Dr. Ünal is the author of multiple books and articles focusing on his areas of expertise.

Emerging Military Technologies Series is a SETA Project aims to shed light on the key aspects of new and developing key military technologies by elaborating on global trends and Türkiye's capabilities. A part of the Project is sponsored by STM Savunma Teknolojileri, Mühendislik ve Ticaret A.Ş.

SETA Publications 204
First Published in 2022 by SETA
ISBN: 978-625-8322-16-3

The conclusions and recommendations of any SETA Foundation publication are solely those of its author(s), and do not reflect the views of the Institution, its management, or its other scholars.

Layout: Sema Türk Bayazit
Printed in Türkiye, Turkuvaz Haberleşme ve Yayıncılık A.Ş., İstanbul

SETA | FOUNDATION FOR POLITICAL, ECONOMIC AND SOCIAL RESEARCH
Nenehatun Cd. No: 66 GOP Çankaya 06700 Ankara TÜRKİYE
Tel: +90 312.551 21 00 | Fax :+90 312.551 21 90
www.setav.org | info@setav.org | @setavakfi

SETA | İstanbul
Defterdar Mh. Savaklar Cd. Ayvansaray Kavşağı No: 41-43
Eyüp İstanbul TÜRKİYE
Tel: +90 212 395 11 00 | Fax: +90 212 395 11 11

SETA | Washington D.C. Office
1025 Connecticut Avenue, N.W., Suite 1106
Washington, D.C., 20036 USA
Tel: 202-223-9885 | Fax: 202-223-6099
www.setadc.org | info@setadc.org | @setadc

SETA | Berlin
Kronenstraße 1, 10117 Berlin GERMANY
berlin@setav.org

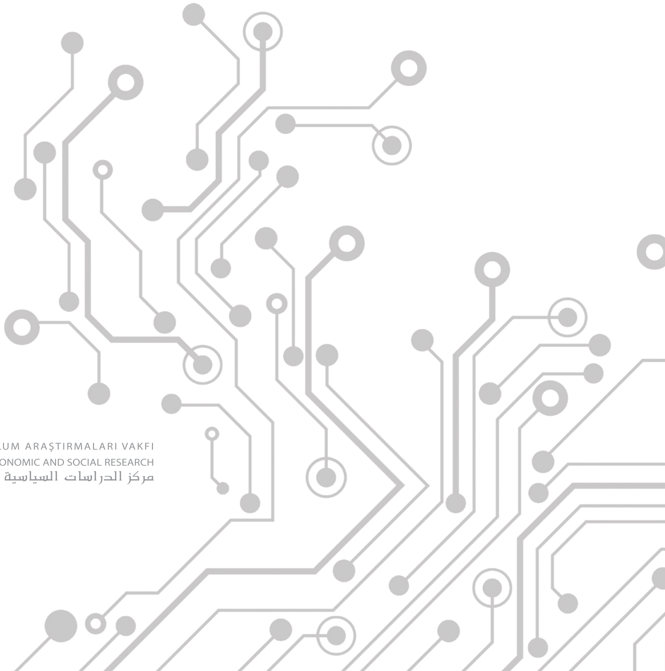
SETA | Bruxelles
Avenue des Arts 6, 1000 Bruxelles BELGIUM
Tel: +32 2 313 39 41

SETA Emerging Military Technologies Series .2.

Cyber Security:

Global Trends & Türkiye’s Capabilities

Ahmet Naci Ünal



SETA
SİYASET, EKONOMİ VE TOPLUM ARAŞTIRMALARI VAKFI
FOUNDATION FOR POLITICAL, ECONOMIC AND SOCIAL RESEARCH
مركز الدراسات السياسية والاقتصادية والاجتماعية

Contents

Introduction

"Data", which is defined as "the representation of facts, concepts or commands in a form conducive to communication, interpretation and processing[1]", constitutes one of the most important building blocks in today's digitized world and is also considered an important asset covering all areas of life. All living things, including humans, and technology-based systems on Earth all operate as data sources. This data is processed by information systems and converted into information for use in private, general, or interdisciplinary areas, and is used in the form of a continuous data flow to increase the quality of life of people and to use the available resources efficiently. In the effective realization of this data flow, network structures consisting of smart sensors, communication technologies that will provide fast and uninterrupted communication, and decision support systems for swift decision-making are used. In the creation of all the information produced or used by these intelligent networks, effective interface software, machine learning techniques, mesh network structures, and cloud computing technologies are needed to establish standards in the communication of the systems with each other. Thanks to these interdisciplinary technologies, instant data changes can be effectively tracked, and swift decision-making processes can be carried out. Cyberspace, which is a highly dynamic environment, is used to achieve this agility. Cyberspace is defined as "a networked global environment in which information technology infrastructures, including the internet, communication networks, computer systems, embedded processors, and controllers, are interconnected."[2]

When this definition is taken into consideration, cyberspace represents an unlimited integrated physical/virtual environment not only based on the internet,

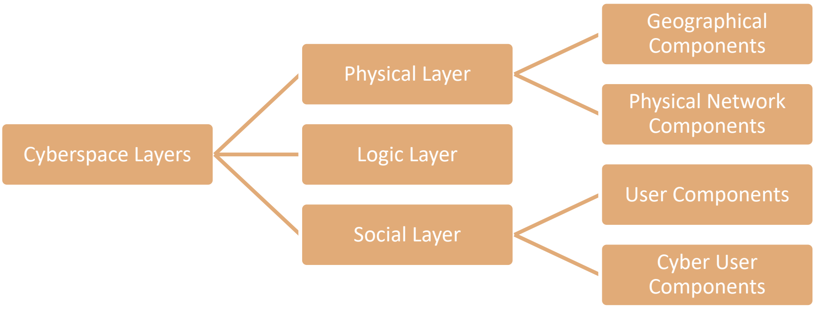
[1] Translated from Turkish entry for "Data" (veri), Turkish Language Association Current Turkish Dictionary, https://sozluk.gov.tr/, (Accessed on December 20, 2021).

[2] Department of Defense Dictionary of Military and Associated Terms, https://irp.fas.org/doddir/dod/jp1_02.pdf p. 58 (Accessed on December 20, 2021).

but also with systems that can communicate with each other through different network structures. In other words, cyberspace is an environment in which the processes of obtaining, using, and storing data/information take place. In addition, although it is a virtual environment, its effects are physical.

Approaches to the concept of cyberspace are not limited to defining the concept, but also determining its situational position. In this context, cyberspace is positioned as the fifth dimension in addition to the four dimensions consisting of land, sea, air, and space. It is also stated that while each of these five dimensions is considered to be independent of each other and intersection areas are limited, cyberspace nodes (connection points) are connected to each dimension. Cyberspace, as shown in Figure 1, is examined in three main sections: the physical layer, the logic layer, and the social layer. Of these three layers, the physical layer and the social layer are also divided into two sub-components:[3]

Figure 1: Layers of Cyberspace



A summary of these layers and their subcomponents is presented below:

- **The physical layer** consists of geographical and network components. Geographical components are environments where information systems that work depending on existing networks are located. Physical network components are wired/wireless/optical infrastructures and all kinds of technical components that provide access to these infrastructures.

- **The logic layer specifies the** nodes to which existing networks are connected. These communication nodes encompass all kinds of information systems including computers, smartphones, and sensors.

[3] "Cyberspace Operations Concept Capability Plan 2016-2028", February 22, 2010, https://irp.fas.org/doddir/army/pam525-7-8.pdf, p. 8- 9, (Accessed on Dec. 20, 2021).

- **The social layer** consists of both real and cyber (virtual) users. While the user components only refer to users who physically exist, the cyber user components can be much more numerous than the physical user components.

When we think about the technologies we use, we can see that cyberspace layers are effectively a part of our lives. These environments include education, communication, all energy production resources, health, finance, security, banking, chemistry, defense, law, transportation, supply chain, aviation, and space.

Under these conditions, it is as important to ensure the security of systems that communicate with cyberspace as it is to operate in cyberspace. This protection covers different processes of data, including production, storage, and transmission. The data to be protected includes not only numerical but also physical values.

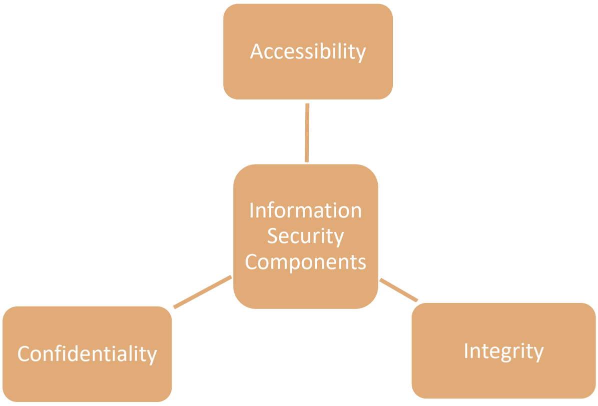
Physical environments can be summarized as handwritten papers, printouts and files where these papers are kept, official or private letters/reports, fax printouts, and meeting rooms. Digital environments can be summarized as various files, emails, social media data in data banks, cloud computing systems, information systems, or external memories. Perhaps the most important source of information among them is the human being. Since all these components operate in a space, it is also important to ensure the physical security of the environments. At this stage, the concept of information security, which is defined as "*the attempt to prevent the acquisition of information assets by unwanted persons in all kinds of environments by using the right technology for the right purpose and in the right way in order to protect the information from threats or dangers as an asset,"* comes to the forefront.[4]

As shown in Figure 2, it is possible to examine the information security components under three main headings: accessibility, integrity, and confidentiality.[5]

[4] Şeref Sağıroğlu, "Siber Güvenlik ve Savunma: Önem, Tanımlar, Unsurlar ve Önlemleri", *Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık*, ed. Şeref Sağıroğlu, Mustafa Alkan, (Grafiker Yayınları, Ankara: 2018), p.26.

[5] Computing Services Information Security Office, "Security 101", Carnegie Mellon University, https://www.cmu.edu/iso/aware/presentation/security101-v2.pdf, (Accessed on June 20, 2021).

Figure 2: Information Security Components



Here:[6]

Accessibility is the protection of information and information systems against corruption by unauthorized access. Timely and reliable access to information and information systems.

Integrity is the prevention of unauthorized editing or deletion of information to ensure that information and information systems are accurate, complete, and intact.

Confidentiality means the protection of information from unauthorized access or disclosure. It allows those who have the right to access information to do so while preventing unauthorized persons from doing so.

When we examine these brief definitions and information security components, we can say that the concept of information security is wide enough to cover all people and devices that share the environment, starting from the entrance door of the institution, campus, home, or workplace. However, almost all of the technologies associated with these elements today continue their activities in connection with cyberspace. Online activities, especially during the COVID-19 outbreak, have turned our daily living spaces into an official working environment or classroom. Therefore, the concept of security is realized by ensuring the security of the cyberspace dimension where all these factors are shared, not only the physical environment, outputs, or produced data. This understanding of security brings the concept of "cyber security" to the forefront beyond information security.

[6] Sağıroğlu and Alkan, *Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık*, pp. 3-5.

Cyber Security

The International Telecommunication Union[7] defines cyber security[8] as “the totality of tools, policies, security concepts, security measures, guidelines, risk management approaches, actions, training, best practices, assurances and technologies that can be used to protect the cyber environment, organization and user assets”. It contains all the information produced and/or stored by individuals or institutions through user assets and information processing devices, personnel, infrastructure, applications, services, communication systems, and cyberspace facilities connected to the system.

When we examine this definition, we can see that the concept of cyber security covers all virtual and physical environments. Of course, these environments include not only the hardware and software of information systems but also the communication technologies that provide communication of these systems with all systems using cyberspace.

For this reason, to protect any object, living thing, or data, we need to know what kind of threats we will encounter, in other words, we need to be able to define the threat. When it comes to cybersecurity, it is useful to examine these threat sources and the methods that the threats actively use.

Cyber Threats

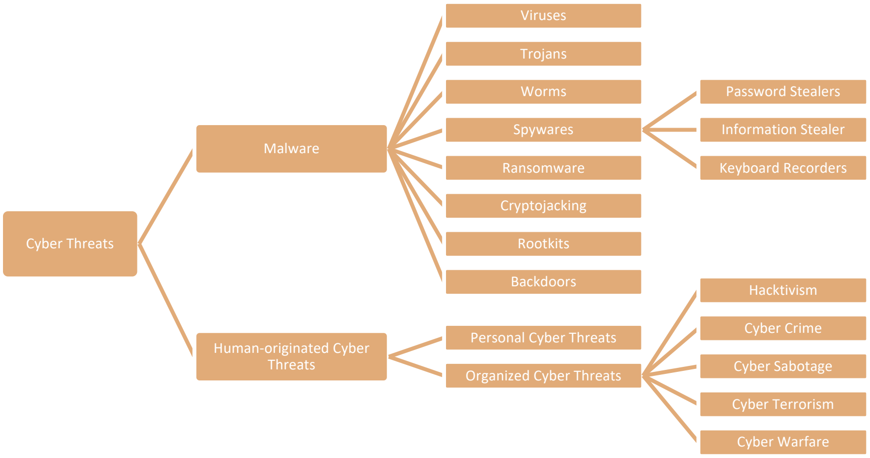
Cyber threats can be defined as elements that damage the activities of stakeholders such as hardware, software, physical environment, etc. using the cyberspace environment, and weaken the certainty of the systems. For all sys-

[7] International Telecommunication Union-ITU

[8] ITU, “*Definition of cybersecurity*” https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx, (Accessed on Dec. 20, 2021).

tems operating in cyberspace, cyber threats pose the most important security challenge. Therefore, the effective realization of cyberspace activities depends on effective cyber threat identification, detection, analysis, and reduction of the threat level/risk of damage. In this context, Figure 3 can be used for the basic identification activity to be done. [9]

Figure 3: Cyber Threats



According to Figure 3, first, it is important to determine whether the cyber threat is human-induced or software-based. With this classification, the aim is to determine what harmful software was used and with which strategies malicious people have developed the software.

Malware

Malware is the common name for any software designed to compromise any system operating in cyberspace or exploiting cyberspace activities. The most basic malware sources are viruses, trojans, worms, spyware, ransomware, cryptojacking and rootkits. The following are brief descriptions of these malware sources:

- **Viruses:** The oldest type of malware. They can be stored in any type of file that is transmitted. They can modify existing programs and copy

[9] While creating this figure, we benefited from the following: Özkaya, E. et al., *Cybersecurity: Attack and Defense Strategies*, (Buzdağı Publishing House, 2020) and Samet, R. and Aslan, Ö. (2018) "Cyber Security and Defense: Importance, Definitions, Elements and Measures". *Siber Security and Defence Awareness and Deterrence*, ed. Şeref Sağıroğlu, Mustafa Alkan, (Grafiker Yayınları, Ankara: 2018), pp. 228-232.

themselves to other information systems when the appropriate environment is created.

- **Trojans**: Malware that masquerades as a harmless program but infects without the user's knowledge and can cause your files to be shared, modified, tracked, and deleted when activated by the person or people who made this malware. Trojans cannot infect another system on their own and become active.

- **Worms:** Just like viruses, they can multiply and infect information systems. This proliferation occurs in very large volumes both in the system where it is located and in which it infects. For this reason, they cause large congestion of network traffic of information systems and slow down network connection access.

- **Spyware:** They collect the information of the system users with the data contained in the information system and share it with the person or persons who infect the spyware. The shared data can be all kinds of financial information such as e-commerce, banking, and credit card passwords, as well as all data and files in information systems.

- **Ransomware:** A type of malware that is made unusable by encrypting user-created files or the entire information system in the information system they infect. A certain amount of ransom is demanded from the user to make the information system accessible again.

- **Cryptojacking:** Settles in the user's information system without the user's knowledge. It then uses the processing power of the information system it infects to mine cryptocurrency.

- **Rootkits:** A type of malware that allows malicious people to access and control the target information system. Your information system becomes a complete zombie information system after a rootkit infection.

- **Backdoors:** These are software that can disable traditional security installations and open the information system to remote access without the user's knowledge. Trojan horses are often used to create backdoors. Mostly, they are loaded into the information system before complex attacks and wait for the day of the attack to become active.

User-Caused Cyber Threats

Users play an important role within the scope of cyber security vulnerabilities. Some can undermine the security of information systems with various habits they consciously/unconsciously or intentionally/unintentionally have and may even cause cyber security breaches. The majority of the activities related to being unaware or unconsciously causing harm are most often related to a lack of technical knowledge. In these cases, the damage done during such activities may not involve a systematic process because it is not intentional and organized. However, some cybersecurity incidents can be carried out directly by people with malicious intentions.[10]

These human-caused cyber threats, whether individual or organized, generally involve four types of activities:[11]

- **Fraudulent Purpose**: The use of the data belonging to institutions for personal gain.
- **Sabotaging Information Technologies:** A large and unpredictable action against the institution aimed at preventing the availability of the overall infrastructure.
- **Intellectual Property Theft:** The unauthorized leakage of copyrights, patents, trademarks, and trade secrets belonging to the corporation.
- **Espionage**: The illegal acquisition of all kinds of data from industrial or government organizations.

In addition, when this process is examined from a holistic perspective, it should not be forgotten that the factors specified within the scope of malware and human-induced factors can be used together. This situation is also a harbinger that both malicious software and human-caused threats will rapidly transform with the developing technology. In the face of these evolving threats, the concept of the "cyber attack lifecycle," which is developed and effectively used by cyber security researchers, has gained importance.

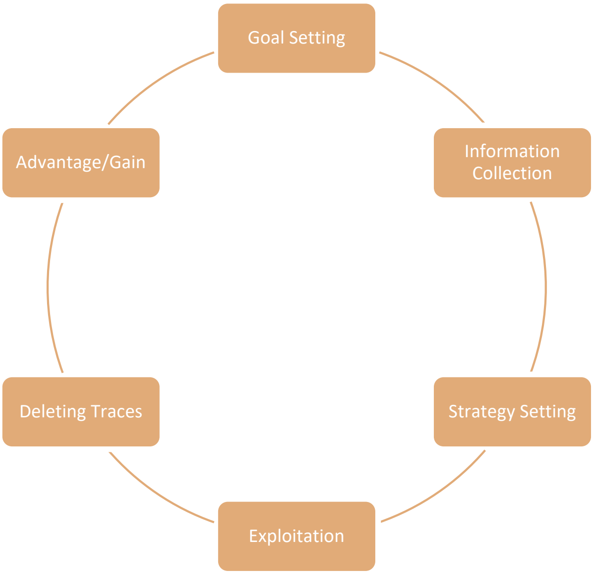
[10] The Department of Homeland Security, "Insider Threat", https://www.dhs.gov/science-and-technology/cybersecurity-insider-threat, (Accessed on Dec. 21, 2021).

[11] Mazzarolo and et al., "Insider Threats in Cyber Security: The Enemy within the Gates." ArXiv, (2019), https://search.ebscohost.com/login.aspx?direct=true&db=edsarx&AN=edsarx.1911.09575&lang=en&site=eds-live, (Accessed on Dec. 21, 2021).

Cyber Attack Lifecycle

It is not possible to discuss a 100% secure environment in all systems operating in cyberspace or benefiting from cyberspace facilities. This is because the continuous development in information technologies also transforms the sources of cyber threats. The way to minimize the effects of cyber threats is to carry out detailed and up-to-date risk analyses. Reliable data is needed to make this analysis accurate. Therefore, it is necessary to identify the threat by analyzing the detected threat data and to determine the type of threat and the attack stage. In other words, answers to the questions "what is it?", "where is it?", "what does it do?" are sought with regards to the threat. However, when the threat comes from cyberspace, it becomes difficult to find answers to these questions and the time it takes to identify threats is extensive. What can be done in this context is to develop "cyber threat source-centered thinking". The most important factor that helped develop this idea is the process described as the "cyber attack lifecycle," shown in Figure 4.[12]

Figure 4: The Cyber Attack Lifecycle



The cyber attack lifecycle shows the activity of cyber attackers and attack processes. In this process, first of all, the target of the cyberattack is determined.

[12] Salih Erdem Erol and Şevket Sağıroğlu, "Siber Güvenlik Farkındalığı, Farkındalık Ölçüm Yöntem ve Modelleri". *Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık*, ed. Şeref Sağıroğlu, Mustafa Alkan, (Grafiker Yayınları, Ankara: 2018). Can be accessed from https://bilgiguvenligi.org.tr/bilgi-merkezi/.

During the determination of the target or after the target is determined, information is collected about the target system by using methods such as port scanning, social engineering, network infiltration, and traffic monitoring. After the identification of areas of weakness, the strategy for how to capture the target system begins to be analyzed.

At this stage, how to attack the target information system, which attack technique will be used, and which cyberattack tools to use, such as the type of malware, are decided. Following these decisions, the target system is attacked, and the system is infiltrated. After this infiltration, targeted objectives such as stealing information, changing information, encryption of data or information system, or data deletion are carried out. After the intended attack activity in the information system is concluded, the existing traces begin to be deleted. Here, the stronger the information and technology infrastructure of the attacker, the more successful the trace deletion activity will be. Because leaving a trace means facilitating or accelerating the detection of the anomaly created in the information system. For this reason, cyber traces are eliminated as effectively as possible. The final stage is to evaluate the benefit/gain obtained as a result of this attack. After the completion of the cycle, the search for a new target begins. In other words, the process continues with other goals or with different components of the same goal.

A proper evaluation of this cycle by the attacked units will be useful in obtaining important clues in the stages of detecting, identifying, and tracing the cyber attacker. Perhaps the most important issue to be considered here is the effect of the threat source used in the cyberattack, which is briefly described with the expression benefit/gain, on the attacked system. Accurately determining and identifying this impact can be an opportunity to deter cyber attackers from achieving their goals.

Cyber Threat Impact Assessment and Deterrence

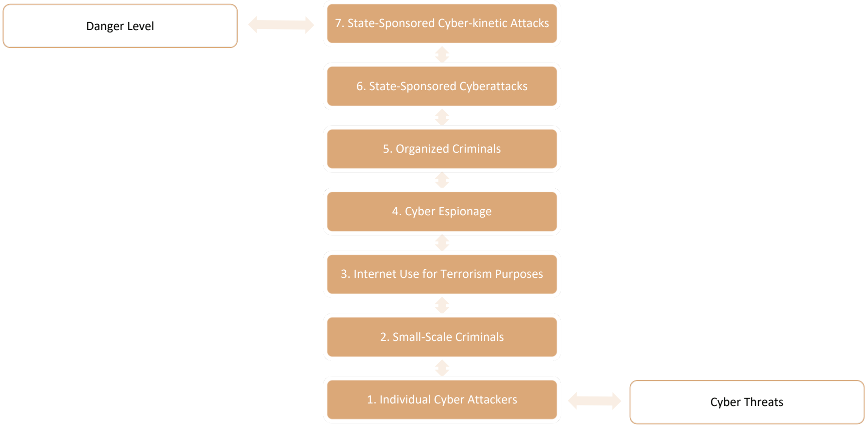
The first step in solving any problem or issue is to correctly define the problem or issue from a holistic point of view and to uncover its relevance. In this context, to be able to analyze the issue or problem, one must find the root causes of that problem and proceed with scientific analysis methods from part to whole. In other words, the process between the root cause and the problem must be modeled or classified correctly. Thanks to this classification, since the area that needs to be concentrated on will be separated from other areas, attention will be focused on the event and energy will be used efficiently and effectively.

Cyber Threat Impact Assessment

To reach a conclusion within the scope of a cyber threat impact assessment, we need to compare threat sources with hazard levels. The most important point that should not be ignored in studies that use the phrases "cyber threat spectrum[13]" or "cyber threat levels"[14][15] in academic sources is that each of these classified/assessed threats can target individuals, institutions, or states.

A graphic representation of the study of the "cyber threat spectrum", which is expressed as a comparison of cyber threats and the danger levels of these cyber threats, is found in Figure 5. In fact, this structure, which is carried out for classification purposes, will be examined from the cyber threat impact assessment approach in our study.

Figure 5: The Cyber Threat Spectrum


Danger Level
7. State-Sponsored Cyber-kinetic Attacks
6. State-Sponsored Cyberattacks
5. Organized Criminals
4. Cyber Espionage
3. Internet Use for Terrorism Purposes
2. Small-Scale Criminals
1. Individual Cyber Attackers
Cyber Threats

According to Figure 5, there are seven types of cyber threats: individual cyber attackers, small-scale criminals, internet use for terrorism purposes, cyber espionage, organized criminals, state-sponsored cyberattacks, and state-sponsored cyber-kinetic attacks. These types are compared in a two-dimensional universe consisting of "cyber threats" and "danger levels" and scaled according to the

[13] Steven Bucci, "The Confluence of Cyber Crime and Terrorism", The Heritage Foundation, June 12, 2009, https://www.heritage.org/defense/report/theconfluence-cyber-crime-and-terrorism (Accessed on Sept. 18, 2019).

[14] Deb Bodeau et al., "Improving Cyber Security and Mission Assurance Via Cyber Preparedness (Cyber Prep) Levels", 2010 IEEE Second International Conference on Social Computing, pp. 1147-1152, doi: 10.1109/SocialCom.2010.170, (Accessed on Jan. 4, 2022).

[15] Jenna Ahokas and Tuomas Kiiski, "Cybersecurity in Ports", *Publications of The Hazard Project*, Vol. 3, (2017) pp. 14-15.

classification of the danger levels of the cyber threats, from low to high. In this context, "individual cyber attackers" pose the least threat in terms of both threat and danger level, while "state-sponsored cyber-kinetic attacks" have the highest threat impact value. Here, an example of a "state-sponsored cyber-kinetic attack" would be rendering power generation facilities inoperable as a result of a cyberattack without any physical contact/attack.

In the first approach of the studies, called "Cyber Threat Levels" [16], the levels are divided into five categories: "cyber vandalism", "cyber fraud", "cyber surveillance", "cyber espionage" and "cyber warfare," as shown in Table 1.

Table 1: Cyber Threat Levels

Levels	Types of Cyber Attackers	Aims and Objectives of Attackers
Level 1 (Cyber Vandalism)	Small groups of attackers	Disrupting the organizational structure
Level 2 (Cyber Fraud)	Individual or small groups of attacks	• Political-ideological goals • Indirect espionage
Level 3 (Cyber Surveillance)	• Large attack groups • Terrorist organizations • Organized crime groups	• To have general infrastructure knowledge • Obtaining basic data for large-scale attacks
Level 4 (Cyber Espionage)	Professional intelligence agencies	Special tasks and programs of countries
Level 5 (Cyber Warfare)	Military units	Destroy the target's information infrastructure

These five threat levels are examined via two main sections: "types of cyber attackers" and "aims and objectives of cyber attackers". In this cyber threat classification, the level with the least impact value is defined as "cyber vandalism" and is represented by small groups of attackers, while "cyber warfare," listed with the highest impact potential, is represented by military units.

In the other study conducted within the scope of cyber threat levels[17], cyber threats are examined through five categories: hacktivism, cyber-crime, cyber espionage, cyber terrorism, and cyber warfare, as shown in Figure 6. These categories are compared in relation to three impact values: motivation, actors, and goals.

[16] Deb Bodeau et al., *Improving Cyber Security and Mission Assurance Via Cyber Preparedness (Cyber Prep) Levels*, pp. 1147-1152.

[17] Jenna Ahokas and Tuomas Kiiski, *Cybersecurity in Ports*, pp. 14-15.

Figure 6: Cyber Threat Levels

Severity of Impact

Cyber Threats	Motivations	Actors	Targets
Cyber Warfare	Political or social changes	States, individual cyber pirates, terrorist groups,	Critical infrastructures, states, armed forces, critical targets
Cyber Terrorism	Political change, fear, political, religious, or ideological goals	Terrorists or states	Infrastructures, public targets, organizations and individuals
Cyber Espionage	Stealing Information	States or organizations	States, organizations, and individuals
Cybercrime	Economic, financial or information advantage, human trafficking, Smuggling	Criminals	Organizations, individuals, and various entities
Hacktivism	Political change, egoism	Activists, hacktivists, or individuals	Governments, organizations, and individuals

Here, while the cyber threat impact value (severity) increases from "hacktivism" to "cyber war", the issues contained in each cyber threat are examined in terms of their motivations, actors involved in the activities, and their goals.

The three studies examined in this context are shown collectively in Table 2 with the names of their authors:

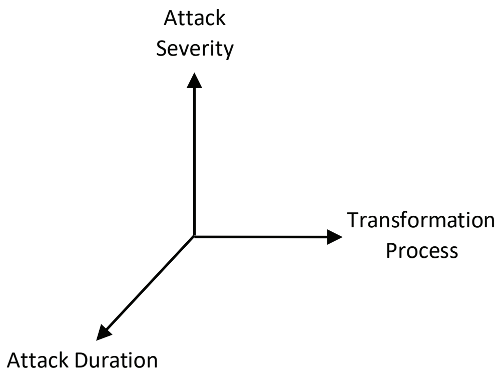
Table 2: The Cyber Threat Assessment in Total

Bucci (2009)	Bodreu et al. (2010)	Ahokas and Kiiski (2017)
Individual Cyber Attackers	Level 1 (Cyber Vandalism)	Hacktivism
Small-Scale Criminals	Level 2 (Cyber Fraud)	Cybercrime
Internet Users with Terrorist Purposes	Level 3 (Cyber Surveillance)	Cyber Espionage
Cyber Espionage	Level 4 (Cyber Espionage)	Cyber Terrorism
Organized Criminals	Level 5 (Cyber Warfare)	Cyber Warfare
State-Sponsored Cyberattacks	-	-
Government-Sponsored Cyber-kinetic Attacks	-	-

In these three studies – all different in terms of both content and publication dates – the lowest threat level is considered to be human-based threats, while the highest-level threat assessment is listed as “cyber warfare”. However, cyber threat assessment is not a conclusion but the beginning of a process that will form the basis for determining the effectiveness of cyberattacks. In this context, the functional structure of the human brain can be used as a model for the analytical process.

The human brain evaluates the phenomena in its environment and shapes a set of solutions on a three-dimensional scale while analyzing any problems. In addition to the three studies described in this section, another study designs a three-dimensional cyberattack space, as shown in Figure 7, and focuses on the cyberattack’s level of impact: [18]

Figure 7: Cyber Attack Effectiveness in a Three-Dimensional Environment Model

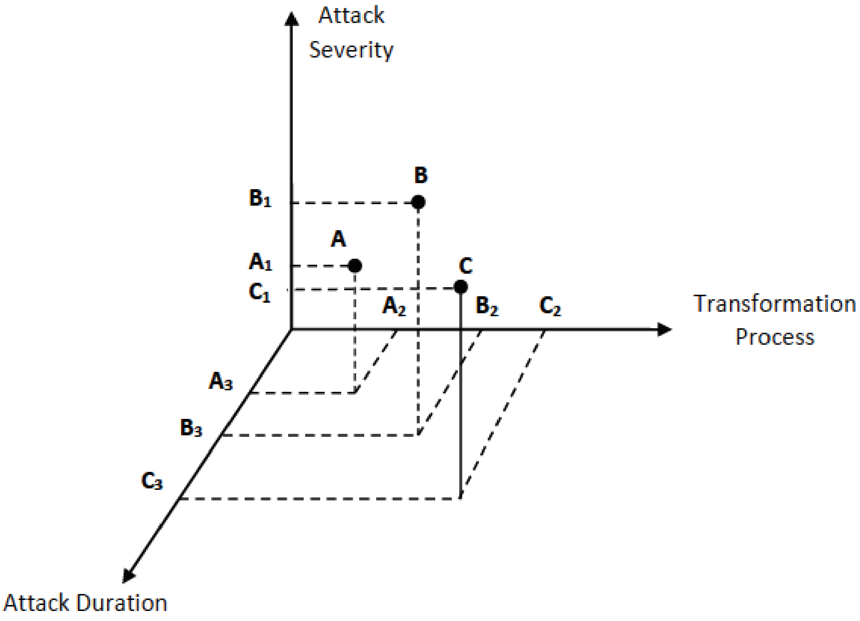


Cyberattacks consist of three dimensions: “attack severity”, “transformation process” and “attack duration”. Therefore, the effectiveness of the attacks to be carried out is evaluated on three axes, different from each other and integrated, as shown in Figure 7.

For example, let’s say the letters A, B, and C shown in Figure 8 represent three different cyberattacks.

[18] Martin C. Libicki, “Cyberdeterrence and Cyberwar”. Rand Corp.., 2009, https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf, (Accessed on April 18, 2019).

Figure 8: An Example Illustration of Three Dimensions of the Effectiveness of Cyberattacks



Here, when we look at the projections of A, B, and C cyber threats in all three dimensions, we see that the impact values are different from each other. For example, it is seen that B1 > A1 > C1 is in the axis of "attack severity", C2 > B2 > A2 is in the axis of "transformation process" and C3 > B3 > A3 in the "attack duration" dimension. In other words, while the B cyberattack source has the most important effect on the axis of "attack severity", the C cyberattack source has the greatest impact on the "transformation process" and "attack duration" axes. Therefore, it is of great importance to classify the differences in the threat assessment phase. The faster we assess this threat and the time needed to respond, the more successful the level of deterrence will be.

Cyber Deterrence

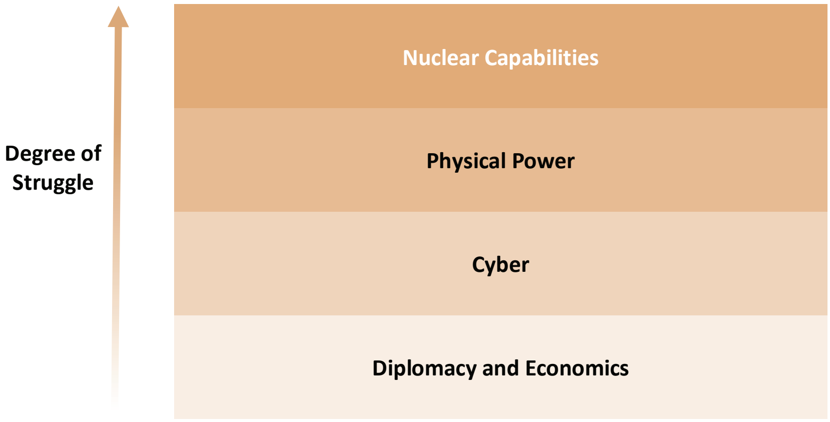
The word "deterrence" is defined as "the work of taking measures to prevent and block an aggression"[19]. In other words, "it is the ability to neutralize the other

[19] Definition translated from the entry for "Deterrence" (caydırıcılık), Turkish Language Association Current Turkish Dictionary https://sozluk.gov.tr/, (Accessed on Dec. 21, 2021).

side without making any attack with the existing means". Although it is mostly used in military literature, the concept of cyber deterrence has taken its place in academic literature, especially since the 2010s, with the perception of cyberspace as a threat source and considering cyber threats as effective elements in cyber-physical environments.

In particular, in the studies aimed at developing the concept of cyber warfare, cyber deterrence is emphasized and can be expressed graphically, as shown in Figure 9.[20]

Figure 9: Cyber Deterrence



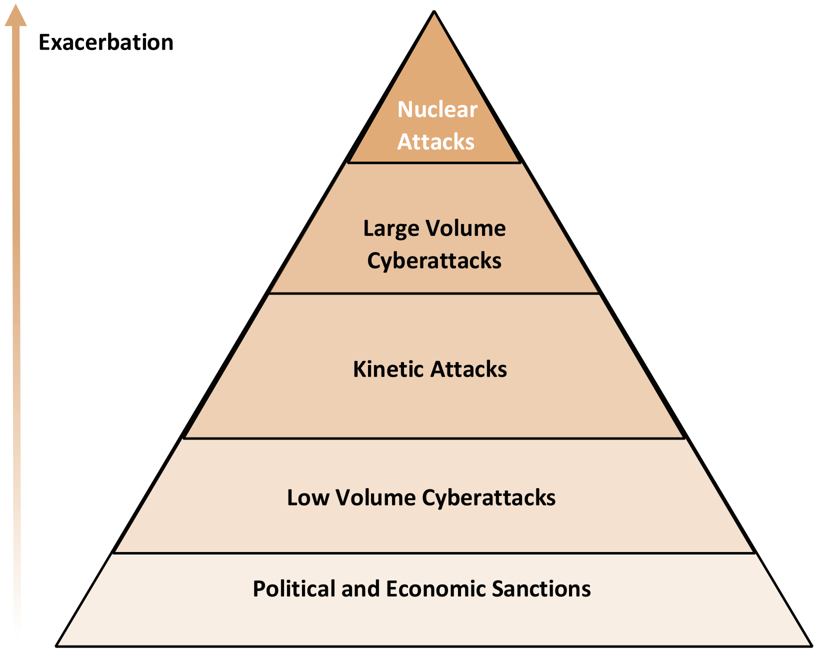
In this classification, deterrence indicators related to countries' fighting capabilities and effects are graded according to diplomacy and economic conditions (although all conditions are important), cyber capabilities, physical strength levels, and nuclear capabilities. In the ranking made in this context, while diplomacy and economic conditions are evaluated as having the least level of deterrence, nuclear capacity is considered the most important power multiplier, that is, the component with the highest deterrence factor. Therefore, according to this rating, just having nuclear capabilities can provide the highest level of deterrence.

In a different study conducted six years after the study conducted in 2009, the conditions specified in Figure 10 attracted attention. [21]

[20] Martin C. Libicki, *Cyberdeterrence and Cyberwar*, p. 29.

[21] Annegret Bendiek and Tobias Metzger, "Deterrence Theory in the Cybercentury. Lessons from a State-of-the-art Literature Review", SWP-Berlin, May 2, 2015, https://www.swp-berlin.org/fileadmin/contents/products/arbeitspapiere/Bendiek-Metzger_WP-Cyberdeterrence.pdf, (Accessed on Dec. 21, 2021).

Figure 10: A Possible Tension Pattern



According to the graph in Figure 10, nuclear capabilities naturally maintain their position at the top, while cyberattacks are located below and above the kinetic attacks according to their size/volumetric conditions. This shows that a large-scale cyberattack has become almost equivalent to nuclear power in today's world. In fact, while nuclear weapons only continue to serve as a deterrent due to the long-term health (radioactive) threat created if they are used, a large-scale cyberattack can be effective in many areas. In addition, since nuclear weapons are under the control of states, they may be easier to control. However, cyberattacks can be easily carried out by cyber attackers at different levels, as shown in the graphs in Figures 5 and 6 and Tables 1 and 2.

The fact that cyberattacks are so effective and that they have almost reached the level of nuclear weapon effectiveness raises the question of whether strategies are the only determinants of effectiveness. Although the strategies determined have an important place in the effectiveness of these attacks, the most important factor in the realization of these strategies is the types of malware, which we can call cyber weapons, used in the attacks.

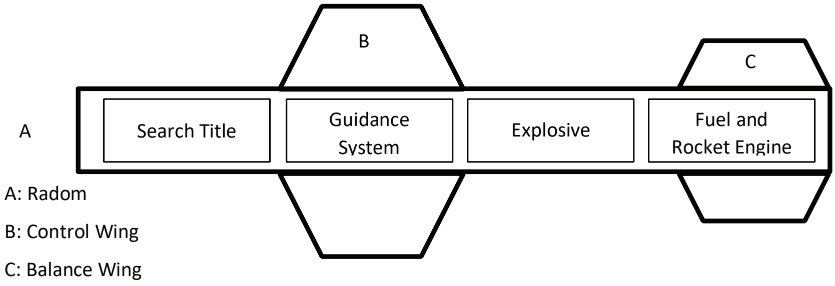
Cyber Weapons

In the recent past and present, while normal weapon systems have been referred to as “classical (conventional) weapons”, “weapons of mass destruction” are listed as such according to their impact factor and are also referred to by the names of the technologies they, use such as “biological weapons”, “chemical weapons”, “nuclear weapons” and “cyber weapons”.

All weapons, except for cyber weapons, are physically sent to their targets by various platforms. The degree of physical destruction they cause is determined and the results can be evaluated physically. Cyber weapons, on the other hand, are not carried by any external platform, are not guided by any system, and their degree of destruction is not detected by classical reconnaissance tools. However, they cause at least as much physical impact as other weapon systems.

Guided missiles can be studied as the most advanced weapon system available for all warheads except cyber weapons. Guided missiles consist of four basic parts: a propulsion system, a search coil, a guidance system, and a warhead (ammunition), as shown in Figure 11.[22]

Figure 11: The Basic Sections of Guided Missiles[23]



[22] Filippo Neri, *Introduction to Electronic Defense Systems*, (Artech House, London: 1991), p. 231.
[23] It was created by the author using footnote 24.

These components are:

- A guidance system that consists of a search coil designed with active, passive, or semi-active guidance methods, equipped with infrared (infrared-IR), radio frequency (RF), or various detectors according to the environment in which it will be used, and a maneuvering system much superior to a manned aerial platform[24],
- The rocket engine is the propulsion system that will determine the speed and range of the missile,
- The explosive prepared according to the degree of impact and destruction.

In cyber weapons, the guidance system that will target the cyber targets, the engine system that will provide the thrust, and the warhead that will affect the degree of destruction are all gathered in malicious software. Therefore, all the activities of developing, using, and determining the effect of cyber weapons are carried out under cyberspace conditions. However, the consequences of a cyber weapon attack can often manifest themselves as physical destruction after a certain period of time. If you don't have a strong cyber defense system, you may not even realize that an attack has been carried out for a long time.

Cyber Weapons and Design Stages

The identification or regulation of cyber weapons is considered an unresolved issue not only among international law researchers but also among specialists in information technology and international politics as well as security researchers. In other words, given the various technical, legal, security, and political aspects of the term cyber weapons, it is unlikely that a universally accepted definition will be determined. This ambiguity is similar to the lack of an internationally recognized definition of terrorism. [25]

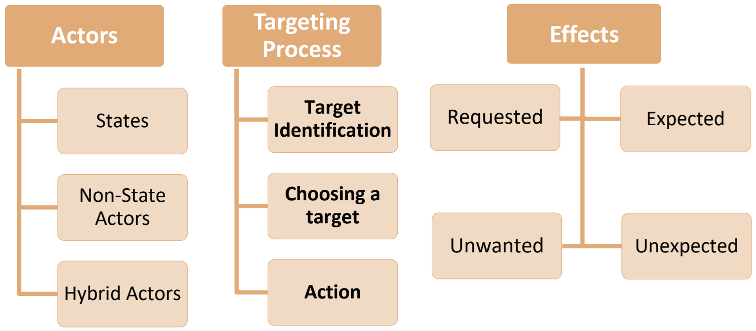
However, while this uncertainty manifests itself only in the definition, studies on cyber weapons continue. The conceptual representation created with some additions made in terms of demonstration by taking advantage of another study focusing on

[24] For manned systems, the maximum amount of G that a human can withstand is 9, as the maneuverability is limited, while this amount is much higher for guided missiles.

[25] Ivana Kudlácková et al., "Cyber Weapons Review in Situations Below the Threshold of Armed Conflict," 2020 12th International Conference on Cyber Conflict (CyCon), 2020, pp. 97-112, doi: 10.23919/CyCon49761.2020.9131728. https://ieeexplore.ieee.org/document/9131728, (Accessed on Dec. 21, 2021).

different dimensions of cyber weapons is presented in Figure 12 and the evaluations related to this process are summarized within the scope of the same source. [26]

Figure 12: A Conceptual Representation of the Concept of Cyber Weapon Use



Here, actors indicate states, non-state entities, and hybrid areas where these two factors are used in common. "States" refer to political structures, the governments that govern, and the official institutions belonging to these states. This high-level formation has economic, political, technical, and military facilities and creates strategies within a certain process, designs/has designed in accordance with these strategies, tests/has tested and can be used as soon as it evaluates the necessity. However, it is often not possible for a large structure such as state organs to act and act swiftly within the scope of this process.

Non-state actors, on the other hand, can act according to individual, ideological, economic, or ethical values without contacting the state components. Most of these structures, which we can label as hackers, cyber professionals, security researchers, private organizations, or institutions, can be more flexible and faster and conclude the cyber weapon development process more quickly. While states are more experienced and productive in conventional weapons, especially considering their economic means, non-state actors have more motivation to focus on developing cyber weapons due to limited economic resources.

The issues expressed by hybrid actors represent situations in which states and non-state actors, or non-state actors and malicious individuals or organizations act jointly. These cyber weapons can be used by states with economic or social concerns and can be used by malicious formations for activities such as cyber terrorism, cybercrime, and cyber warfare attacks.

[26] Clara Maathuis et al., "Cyber weapons: A Profiling Framework," 2016 International Conference on Cyber Conflict (CyCon U.S.), 2016, pp. 1-8, doi: 10.1109/CYCONUS.2016.7836621, (Accessed on Jan. 4, 2022).

The second step is the process of defining the targets in line with the purpose/objectives determined by the actor(s) in or out of cyberspace and selecting the appropriate one(s) among the defined targets. This process, in which goals are selected and prioritized, can be called the "targeting process" for short.

Although it is not mentioned in the study examined, it is necessary to design or provide a cyber weapon to be used against the target within the scope of this process.

Within the scope of taking action, the attack with the designated cyber weapon on the target is determined according to the purpose of the actor.

After all these processes are carried out, the effect of the cyber weapon used on the target is examined. Just like in physical attacks, the desired effects may be encountered as well as unwanted effects. Under both conditions, these effects are evaluated on the basis of expected or unexpected results.

In a study investigating the possibility of cyber weapon controls, cyber weapons are evaluated in three parts: [27]

- Assault weapons used solely for the purpose of attacking or causing harm;[28]
- Cyberattack weapons used only for the purpose of attack or harm,
- Cyber defense weapons used to protect against attacks with cyberattack weapon(s).

Cyber Weapon Development Process

As mentioned earlier, despite the uncertainties in the concept of cyber weapons, perhaps the most detailed study on this subject was done by Maathuis et al.

In this study, the cyber weapon development process is determined as identification, reconnaissance, design, development, testing, verification, intrusion and control, attack, maintenance, and infiltration. [29]

[27] Dorothy Denning, "Reflections on Cyberweapons Controls", https://faculty.nps.edu/dedennin/publications/Reflections_on_Cyberweapons_Controls.pdf, (Accessed December 21, 2021).

[28] In this study a damaging weapon has been considered an offensive weapon even if its presence is used for deterrent purposes or against an aggressor.

[29] Clara Maathuis et al., *Cyber weapons: A Profiling Framework*, pp.1-8.

Effects Of Cyber Weapons On Physical Weapon Systems And Platforms

The digitization of the fronts has come to the agenda with concepts such as "electronic war order", "electronic warfare", "information war", and "network-centered operations", which started to be developed toward the end of the 20th century. Currently, we see that almost all components of modern armed forces are equipped with software and hardware-supported systems. Although most military systems operate in isolation from the cyberspace environment, they are developing projects to create the internet of battlefield things[30] infrastructures in the near future. Although there are no developments to give concrete examples today, it is possible to get an idea about the areas in which the developments have taken place through the papers presented in various scientific branches in the academic world. The environment planned or envisaged to be within this scope consists of military (friendly and threat) and civilian sensor nodes, including three-dimensional radars and laser image detection and ranging[31] sensors in addition to existing smart sensors. These network structures are planned in a volume that will cover a wide range of cyber geography, from small on-board computing devices to powerful edge clouds. This hardware-driven environment must also be supported by time, performance/functionality, security, and reliability. In this context, it needs algorithms for the discovery of civilian and threat nodes using side-channel propagation, algorithms for rapid top-down synthesis of internet functions of mission-specific military objects, and risk assessments. It is also stated that there will be a need to support sensor observations with algorithms to take advantage of the

[30] Internet of Battlefield Things (IoBT)

[31] Laser Imaging Detection and Ranging (LiDar)

physical dynamics of sensor observations to ensure safe and flexible situation prediction and control in the face of data pollution.[32]

Principles of Cyber Warfare: 33

Principles of cyber warfare are examined under eight subheadings: “absence of physical boundaries”, “physical (kinetic) effects”, “confidentiality”, “variability and inconsistency”, “identity and privileges”, “double use”, “infrastructure control” and “information as operational environment”. These subsections are summarized below: [34]

Absence of Physical Boundaries

In the physical world, each platform operates in its defined geography and within the specified time frame. The physical limitations of distance and space do not apply in cyberspace. Physical distancing in cyberspace is neither an obstacle nor a facilitator for the execution of attacks. A cyberattack can be carried out with equal effectiveness from the other side of the world or from the next room. While there are physical limitations to achieving the target in the kinetic world, there are no similar limitations in the detection and capture of the target in cyberspace. Cyber attackers can even create and make multiple copies of a cyber weapon without consuming a lot of time and/or materials.

Physical (Kinetic) Effects

The purpose of cyber warfare is to create physical effects. This involves physical damage or simply influencing the decision-making process of the targeted actor. One of the most topical questions is which cyber incidents should be considered cyber warfare. The concept we call physical warfare is generally realized in the form of the use of the armed forces of countries. This is clearly stated in the legislation of the United Nations.

However, there is no clear international definition of cyber warfare. The most important study on this subject is the *Tallinn Handbook*, published by the

[32] T. Abdelzaher et al., “Will Distributed Computing Revolutionize Peace? The Emergence of Battlefield IoT,” 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS), 2018, pp. 1129-1138, doi: 10.1109/ICDCS.2018.00112. (Accessed on April 5, 2022).

[33] Raymond C. Parks and David P. Duggan, “Principles of Cyberwarfare,”, *IEEE Security & Privacy*, Vol. 9, Issue 5, (Sept.-Oct. 2011), pp. 30-35, doi: 10.1109/MSP.2011.138.

[34] Ibid.

University of Cambridge, of which the first and second versions were published digitally.[35]

Another approach to the concept of cyber warfare includes cyberattacks targeting critical infrastructures. "Critical infrastructures; infrastructures that house information systems that, if the confidentiality, integrity or accessibility of the information they process are impaired, which can lead to loss of life, large-scale economic damage, national security deficits or disruption of public order".[36]

In this context, the cyberattack on Iran's Natanz nuclear facilities is considered to be the first cyber warfare incident. In summary, instead of a physical attack that could cause nuclear pollution, a cyberattack aimed to disable the reactor in the center of this facility. In order to do this, the attack aimed to accelerate, slow down and destabilize the centrifuge systems, which are an important component of the reactor. To achieve this goal, cyberattacks on SCADA[37] systems that control the aforementioned systems have been on the agenda. The malware created in this context was sent to Iran, transferred to the facility information systems, loaded on the microcontrollers used at the production stage (without the knowledge of the manufacturer), and activated on the day of the attack. The emergence of this attack was carried out by investigating the root causes of this damage, as it was activated in the facilities of different countries that received other microcontrollers loaded with malware and similar damage occurred.[38] This attack started the history of cyber warfare under the name "stuxnet".

Privacy

People can take active steps to hide in cyberspace, but everything we do in cyberspace is visible. There is no such thing as being completely hidden. There are only less detectable traces, i.e., trying to hide outliers in existing data streams. Therefore, steps similar to reflecting radar energy in the physical world by hiding

[35] Michael N. Schmitt, "Introduction. In Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations", (Cambridge University Press, Cambridge: 2017).

[36] "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı", T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, January 2013, https://www.btk.gov.tr/uploads/pages/2-1-strateji-eylem-plani-2013-2014-5a3412cf8f45a.pdf, (Accessed on April 8, 2022).

[37] The Supervisory Control and Data Acquisition (SCADA) can be defined as a Central Control and Data Acquisition system. These systems are an electronic microcontroller where systems consisting of many control units spread over a wide area are controlled and monitored by information systems from a single center.

[38] Daniel P. Hughes, "Archer's Stakes in Cyber Space: Methods to Analyze Force Advantage'', *Cyber Weaponry Issues and Implications of Digital Arms* ed. Henry Prunckun, pp. 71-85. (Springer, 2018).

infrared signals by cooling them cannot be taken in cyberspace. Instead, it attempts to store evidence from existing data streams.

Variability and Inconsistency

In cyber warfare, discrepancies can translate into attacks that don't always behave the same way, environments that change the attack, and fluctuations in attack performance. The unchanging side of cyberspace is what requires change in the physical world. For example, unless a person in the physical world uses a faster processor, software performance will not exceed a computer's processing power capacity. The communication bandwidth will be limited to the communication infrastructure.

One effect of this principle is that you can never be sure that a particular step in an attack will work. Attacks are planned using data paths that indicate a change in the state of a system from the initial threat access to the point of reaching the target. Each path in this process contains a set of attack scenarios or a set of attack scenarios that a particular attacker can reach.

Identity and Privileges

Some individuals in cyberspace may have the authority, access, or ability to perform any action that an attacker wants to perform. The attacker's goal is to try to capture that person's identity in order to hide their identity.

Dual Use

Cyber warfare vehicles are dual-use, just like physical combat vehicles. Warplanes using up-to-date technology (e.g., F-16s) can be used both for an attack on ground targets and for defense against enemy aircraft from the air. The most important element that determines this type of use is the ammunition used. In cyber warfare, the same tools are used in attack and defense, both as hardware and software. For example, while vulnerability scanners are used when attacking, similar browsers are used to find and repair weaknesses in their systems. Similarly, the equipment that network administrators use to diagnose network problems is also used by attackers for reconnaissance.

Infrastructure Control

Both defenders and attackers control a very small part of the cyberspace they use. Whoever can control a part of the cyberspace used by the opponent can control his opponent. For this reason, methods such as penetration tests are based on determining the degree of vulnerability to threats by simulating attacks on their networks in advance.

Information as an Operational Environment

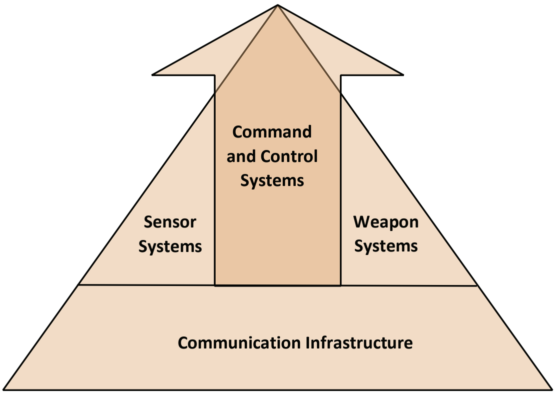
While elements such as terrain conditions, weather, and the position of threatening troops in physical warfare all affect the operational environment, in the cyberspace environment, this process consists of information systems, wired/wireless/optical infrastructures that work depending on the existing networks and all kinds of technical components that provide access to these infrastructures. Therefore, in both physical and cyber warfare environments, information is considered the most important power multiplier.

A Holistic View of the Cyber Operation Landscape

The components that should be most important in the establishment of physical armed forces are personnel, intelligence, logistics, and operations. All of these areas constitute an important military force element with a strong command-control-communication-computer-intelligence-surveillance-reconnaissance structure. [39]

In the case of cyber warfare, when using the cyberspace environment of similar structures, the structure summarized in Figure 13 is of particular importance: [40]

Figure 13: A Holistic Approach to the Cyber Operation Landscape



[39] Command and Control, Computing, Communications, Intelligence, Reconnaissance, Surveillance – C4ISR

[40] Nuri Mutlu, "Komuta Kontrole Bütüncül Bakış", *Aselsan Dergi,* Issue 109, (June 2021), p. 21. https://www.aselsan.com.tr/22021_4611.pdf, (Accessed on Dec. 13, 2021).

While sensor systems as well as kinetic and cyber weapon systems come to the fore, an uninterrupted and secure communication network comes into play. In this context, a summary of these systems is available under the following subheadings.

Cyber Command and Control Systems

Cyber command and control systems are responsible for the success of the given task with the person/people who plan activities such as routing, coordinating, and controlling, and the process of regularly checking personnel, equipment, network infrastructures, and security software with various methods and technologies.

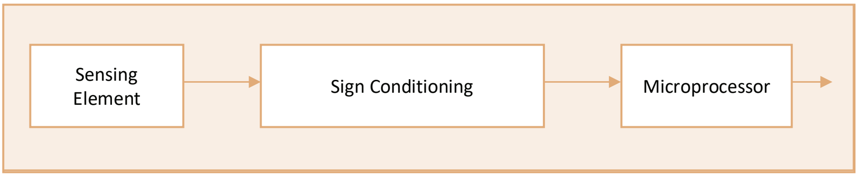
In order to manage this process effectively, it is necessary to determine whether the detected data is harmful or not and to perform threat analysis. If there is certainty or intense suspicion that there is a threat, it is necessary to determine the measures to be applied according to the threat rating.

In this context, the elements that are or may be a threat can be listed as human-induced threats, web pages/applications containing malicious software, use of web pages for harmful propaganda purposes, compromise/dysfunction of information systems/turning them into zombie (botnet) information systems, the transmission of fake data created by seizing sensors in smart network structures to secure systems, as well as attacks on critical infrastructure facilities and simultaneously on different targets.

Sensor Systems

Signals such as sound, light, pressure, electromagnetic scattering, frequency, etc. produced by various sources are defined by special devices and converted into electric signals by these devices. They are then transferred to an information system or other intelligent network systems. The devices that perform this identification and transformation process are called smart sensors.

Figure 14: Smart Sensors



Intelligent sensors, modeled on the working principle in Figure 14[41], detect the signs in their environment that they can identify by the sensing element and convert them into electrical signs. Then the signal converted to the format to be processed at the "signal conditioning layer" is transferred directly to the microprocessor. The signal made ready for use by the microprocessor is transmitted either to the evaluation center or to other intelligent network nodes. The most important features of smart sensors are that they are small, their energy needs are low, their sensitivity is high, they can process data quickly and they are used effectively. The effective creation of this process depends on the effective management of data from a wide variety of sources and the uninterrupted transfer of data to the central server.

Cyber-physical environments created based on the internet of things are used in operational environments as well as in civilian environments and are called the Internet of Battlefield Things. However, since the beginning of the 21st century, this area is known in the military literature as network-centered operation or network-centered warfare.[42]

Weapon Systems

When we examine the weapon systems, we can see that many weapon systems and platforms, regardless of the force command, are software-supported and are based on embedded systems. In this context, the weapon system/platform that will have the most advanced technology – the development of which continues in great secrecy – is the 6th generation fighter aircraft. In the light of the projects described, an insight study (STMThinktech) [43] has prepared an infographic about the possible technologies that can be used. The technologies in this image are summarized below:

- Artificial intelligence: Coordination with Unmanned Aerial Vehicle (UAV) fleets

[41] B. F. Spencer et al., "Smart sensing technology: opportunities and challenges", *Structural Control and Health Monitoring*, Vol. 11, Issue: 4, pp. 349–368.

[42] Cyber-physical systems established by the United States National Science Foundation (NSF) are systems created by the seamless interaction of computation and physical components and designed accordingly.

[43] "The Projected Characteristics Sixth-Generation of Warplanes", STM Thinktech, Nov. 10, 2020, https://thinktech.stm.com.tr/tr/altinci-nesil-savas-ucaklarinin-ongorulen-ozEllicities, (Accessed on Jan. 4, 2022).

- Powerful sensor connectivity with allied powers on ground, air, sea, and space platforms
- Larger airframe and more efficient engines
- Pilot helmets that combine sensor information and images to use
- Truly network-centric operation
- Cyber warfare and cybersecurity capabilities
- Ability to use directed energy weapons,
- Increased invisibility with electronic jamming, electronic warfare systems, and infrared dimming
- Optionally as piloted aerial platforms

It is thought that the sixth-generation fighter planes will gain operational functionality through software placed on fixed hardware, just like the fifth-generation fighter planes. In this context, all systems are becoming a component of cyber warfare. However, thanks to smart sensors, the almost unlimited area of operation can cause these platforms to operate like a command-and-control center. For this reason, especially network-centric operations/network-centric warfare play a key role in this process.

Network-Centric Operations/Warfare

The concept of network-centric warfare broadly describes "the combination of emerging tactics, techniques, and procedures that a networked power can use to create a decisive war advantage."[44] It models the operational environment with land, sea, air, and space dimensions and uses platforms that use these dimensions (together with the equipment they use) together. Prior to this concept, it develops the concept of the electronic operation area, which is shown as three-dimensional and develops instant imaging and operation facilities.[45]

[44] John J. Garstka, "Network-Centric Warfare Offers Warfighting Advantage" Signal, May 2003. https://www.afcea.org/content/network-centric-warfare-offers-warfighting-advantage/#:~:text=Datalinks%20are%20the%20new%20weapon,create%20a%20decisive%20warfighting%20advantage, (Accessed on Dec. 16, 2021).

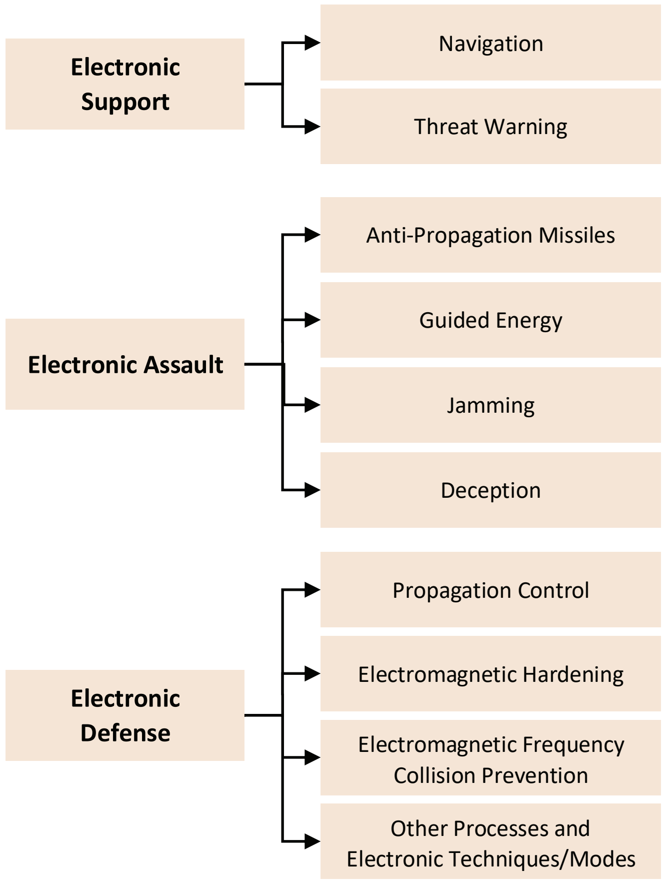
[45] Electronic Order of Battle (EOB)

Electronic Warfare

Electromagnetic systems and directed energy for military purposes are used to monitor the electromagnetic spectrum[46], gather information, control or attack the enemy, and prevent the use of the electromagnetic spectrum when necessary. [47][48]

Electronic warfare consists of three main parts: electronic support, electronic attack, and electronic protection. The basic subcomponents of these sections are shown in Figure 15:[49]

Figure 15: Electronic Warfare Divisions


Electronic Support
Navigation
Threat Warning
Electronic Assault
Anti-Propagation Missiles
Guided Energy
Jamming
Deception
Electronic Defense
Propagation Control
Electromagnetic Hardening
Electromagnetic Frequency Collision Prevention
Other Processes and Electronic Techniques/Modes

[46] Spectrum: It is the classification of electromagnetic waves according to their frequency and wavelength.

[47] D. Curtis Schleher, *Electronic Warfare in the Information Age*, (Artech House, London: 1999), p. 2.

[48] D.B. Hoisington, *Electronic Warfare Volume I*, (Lynx Publishing, 1994), pp. 1a-1, 1a-16, 1a-17.

[49] Ibid.

Electronic Support:

It is the electronic warfare department for emergency threat detection and includes the activities of searching, detecting, and identifying conscious/unconscious electromagnetic energy emission sources. It consists of the subcomponents of navigation and threat warning.

Electronic Assault:

It is the branch of electronic warfare that involves the attack of electromagnetic systems with electromagnetic systems or directed energy weapons in order to reduce, neutralize or eliminate electromagnetic threats' combat capabilities. It consists of anti-propagation missiles, directed energy, jamming, and deception.

Electronic Protection:

It is the electronic warfare department that covers the protection of personnel, facilities, and equipment from the effects of friendly or enemy electronic warfare activities that reduce, neutralize, or destroy friendly combat capabilities. This section consists of the subcomponents of propagation control, electromagnetic hardening, electromagnetic frequency collision prevention, and other processes/measures.

Creation Of The Cyber Defense System

A person needs information and various means of accessing or producing information to defend himself as an individual, understand and detect attacks, and make decisions about the method of defense. To put it briefly, defense is the act of protecting the system against attacks. Therefore, cyber defense refers to an active process that secures the critical processes being carried out against attacks.

Work on the Creation of Cyber Defense:

Although the concept of cyber defense is meant to protect our cyber infrastructure, it also plays an active role in the development of strategies to counter cyberattacks when necessary. In this context, first of all, the individual awareness of the people who use and manage our cyber assets as well as the knowledge of the experts regarding their duties and other activities should constantly undergo a transformation that will aid in supporting decisions based on the threat data. Of course, the use of sensors is of great importance in collecting the data to be used for this process. Through these sensors, elements such as the capacity and strategy of the attack can be predicted. Based on the data generated by the situation analysis, the defense system may need to be activated. This process can be briefly described as cyber command and control. In this context, while the command researches the options and evaluates them quickly depending on the situation within the scope of the decision-making process, the control aspect is an established system to communicate the decisions and implement them reliably throughout the system.[50]

[50] O. Sami Saydjari, “Cyber defense: Art to science”, *Communication of the Acm*, Vol. 47, Issue 3, (March 2004), pp. 52–57.

The points mentioned so far are a comprehensive review of cyber defense, and it has also been pointed out that "cyber intelligence" should be added as an additional factor to these layers.[51] Through these methods, cyber defense activities can be strengthened by incorporating lessons learned from past attacks into specified processes.

[51] Michael Robinson et al., "Cyber warfare: Issues and challenges", *Computers & Security*, Issue 49, (2015), pp. 70-94.

Cyber Security Activities In Türkiye And The World

When the current levels of cyber security activities are evaluated, it is seen that they have developed both in terms of the security of individuals and concerning the national security of countries. However, simple mistakes in individual factors can directly affect the security of a country. For this reason, high-level measures need to be developed.

In this context, “The task of preparing and coordinating the policy, strategy and management plans related to the provision of national cyber security with the ‘Decision of the Council of Ministers on the Conduct, Management and Coordination of Works on National Cyber Security (BKK)’ and the Electronic Communications Law No. 5809 in the Official Gazette dated 20/10/2012 and numbered 28447 was given to the responsibility of the Ministry of Transport, Maritime Affairs and Communications[52],” and with the same law, a “Cyber Security Board” was established in Türkiye.

The Turkish Cyber Security Cluster was established under the leadership of the Presidency of Defense Industries of the Republic of Turkey and with the contributions of all relevant public institutions/organizations, the private sector, and academics as a platform to develop the cyber security ecosystem in our country in line with the main goal of a Türkiye that produces technology in the field of cyber security and competes with the world. Platform activities are carried out with the support and coordination of the Presidency Digital Transformation Office. [53]

The national cyber security targets determined within the framework of Türkiye’s 2023 vision are as follows: [54]

[52] Ministry of Transport and Infrastructure

[53] Turkish Cyber Security Cluster, https://www.siberkume.org.tr/Index, (Accessed on April 11, 2022).

[54] Arife Yıldız Ünal, “Ulusal Siber Güvenlik Stratejisi ve Eylem Planı siber güvenlikte 2023 vizyonunu gerçeğe dönüştürecek”, Anadolu Agency, Dec. 29, 2020. (Accessed on April 11, 2022).

- 24/7 protection of cyber security of critical infrastructures. To have the latest technological facilities in the field of cyber security at the national level. Development of domestic and national technological opportunities within the framework of operational needs.
- Continuing to develop a proactive cyber defense approach based on the fact that the response to cyber incidents is a whole that covers before, during, and after the incident. Measurement and monitoring of the competence levels of cyber incident response teams. Increasing the competencies of cyber incident response teams.
- Increasing the level of preparedness for cyber incidents on a corporate, sectoral, and national basis with risk-based analyses and approaches based on planning. Ensuring secure data sharing between institutions and organizations.
- Ensuring that the source and destination of the data traffic remain within the country. Development of a regulatory and supervisory cybersecurity approach in critical infrastructure sectors.
- Preventing producer dependence on information technology products in critical infrastructure sectors. Identification of requirements for securing next-generation technologies. Supporting innovative ideas and R&D activities and ensuring the realization of their transformation into domestic and national products and services.
- Safe use of cyberspace by all segments of society. Maintaining activities to keep cyber security awareness at a high level in the whole society.
- Establishment of corporate information security culture in institutions and organizations. Ensuring that children are protected in cyberspace. Strengthening human resources with projects for individuals who are interested in cyber security or who want to specialize in this field.
- Dissemination of cyber security training in formal and non-formal education and enrichment of training contents. Development of mechanisms to ensure information sharing and cooperation with national and international stakeholders.
- Minimizing cybercrime and increasing deterrence. Development of mechanisms to ensure accurate and up-to-date information sharing on the internet and social media.

Cyber security strategies are being developed in other countries that use technology effectively as well as in our country. In this context, the policies and strategies determined by the United States, Russia, China, the United Kingdom, Israel, and Iran are presented below: [55]

United States

Joint action of the U.S. public and private sectors to protect critical infrastructure,

To act together between the public and private sectors against attacks that may come from cyberspace space, as well as to put forward tactics and plans for the development of this joint mobility, to encourage and support the private sector to fulfill its duties in the field of cyberspace and to develop a federal system within the scope of all these objectives,

Increasing the awareness of the U.S. business and employer sector and the whole society against cyberattacks, and giving importance to training and orientation activities on this issue at the federal level,

Since Russia's increasing cyber power and cyber challenges pose serious threats to the security of the United States, developing plans to eliminate these threats,

Since China poses a threat to the United States, especially in the field of cyber espionage activities, the United States should take the necessary measures to protect its technological innovations and the commercial interests of its private sector,

Protecting all official computer, software, and network technologies in agriculture and food sectors, drinking water and public health and emergency response systems, social security, information and telecommunication infrastructures, energy, transportation, banking and finance and chemical sectors, postal and shipping systems as national critical infrastructures and protecting these areas against cyberattacks,

Realization that cyberspace is a common use area at the global level, and that these areas should be safe and free to ensure the free movement of goods and

[55] Dr. Ali Burak Darıcılı, "Devletlerin güncel siber güvenlik stratejileri", *Anadolu Agency*, Dec. 2, 2020, (Accessed on April 11, 2022).

services, ideas, entrepreneurs, and capital. In this context, the United States should take all kinds of measures to ensure these freedom opportunities, and in this context, the technical and administrative measures of Russia and China for the fragmentation of the internet should be combated at the global level,

The United States should give full support to the countries concerned against cyberattacks aimed at destabilizing allied countries.

Russia

Within the principles set forth by the Gerasimov doctrine, Russia aimed to direct and manage the processes of hot conflict with less conventional power, and therefore with less human loss and cost, by incorporating methods that did not have a military character into its military capacity. In this context, before a military intervention, it aims to gain an advantage with cyber-attacks against the target region, country, community, or state, to wear down the target, suppress it with psychological warfare methods, demoralize it, break the defense resistance, damage its critical infrastructure and damage its economy.

China

Provision of new generation technologies that have a significant impact on achieving economic growth and stability within the scope of cyber espionage operations,

Controlling the internet to maintain the influence of the Chinese Communist Party (CCP) in the country's governance and thus controlling local opposition movements, separatist groups, and possible social upheavals,

Developing measures against network technology-centered adversary information warfare plans, countering activities aimed at interfering in the internal affairs of the country,

Establishment of an effective counter-contraction structure against cyber espionage activities planned by foreign intelligence services against China,

Supporting military capacity within the possibilities provided by new generation technologies originating from the field of cyberspace, as well as preparing plans against the critical infrastructures of potential adversary military forces, Organizing information warfare strategies and cyberattack activities centered on network technologies against target regions and administrations.

England

Defense: British governments must ensure that the defense of the national IT infrastructure is strengthened and that it is protected against cyber threats that target the U.K.'s critical data and systems. In order to achieve this goal, the public and private sectors should act together.

Deterrence: The U.K. should strengthen existing active and passive resilience to cyber threats and create a perception of effective deterrence.

Development: British governments must improve the U.K.'s cyber capacity to counter cyber threats. In this context, the development of the U.K.'s growing cyber security industry should be supported.

Israel

With its strategic plans, Israel is an exemplary model in the global cyber security economy. The public authority in Israel encourages the private sector in the field of cyber security with concrete economic programs in line with the security and commercial interests of the country, and in line with this incentive, Israel's various universities and research centers focus on R&D studies in the field of cyber security and constantly create new developments and revealing products in this field.

In this context, according to the data of the Organisation for Economic Cooperation and Development (OECD), Israel has become one of the leading states in the world by allocating a share of around 4% of its GNP (10 billion euros) to scientific R&D expenditures. Moreover, Israel's information, communications, and technology sector is growing rapidly. In 2014, Israel's share in the global cyber security industry grew by 8 percent, reaching $6 billion. On the other hand, in 2016, it is known that more than 350 large and small companies were operating in the cyber security industry in Israel. This number increased rapidly in 2017 and reached 420 active companies. Twenty-six of these cyber security companies were among the top 500 most active and rapidly growing cyber security companies in the world for 2017.

Iran

In the aftermath of the Stuxnet attack targeting nuclear facilities, Iran accelerated its cybersecurity efforts with a retaliatory reflex. However, Iran's efforts to improve its cyberattack capacity, which accelerated with a motivation for retaliation in the first place, have turned into a goal to make Iran an effective actor in cyberspace with the measures taken in the following periods. In this context, Iran has made it its national goal to have a strong cyberattack capacity. The background of this goal is basically that Iran, which is not a global power, wants to take advantage of the asymmetrical advantages provided by cyberspace in its power struggle against the U.S., Saudi Arabia, and Israel in the Middle East.

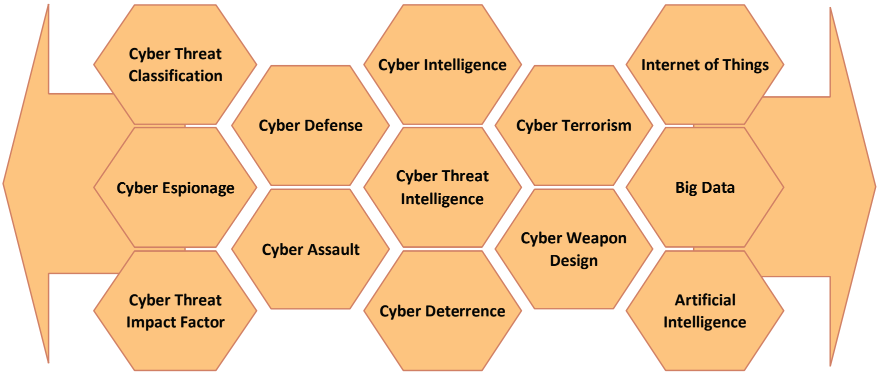
In Iran's cyberattack capacity, the Supreme Council of Cyber Security, the Revolutionary Guard Corps, the Iranian Ministry of Intelligence, the Cyber Command, and the Iranian Cyber Army, which is a proxy structure connected to these institutions, have an important role in determining cyber policies.

Iran's cyberattack targets appear to be aligned with Iran's traditional domestic and foreign defense priorities.

Assessment

The concept of cyber security – considering the dimension of today's technology – is now a field that cannot be abandoned. This concept is considered a field that closely concerns not only individuals, but also sectors, organizations, institutions, and of course, states. Although it consists of just two words – cyber and security, this is just the tip of the iceberg. What are the components that make up cyber security? When we ask, we may not at first realize how deep the subject is. We can express some of the components that make up this field as shown in Figure 16.[56]

Figure 16: A Selection of Cybersecurity Components



When we examine the selection of cybersecurity components in Figure 16, it is possible to see that these components are both civil and military-related. Therefore, many of the phenomena within the scope of cyber security have dual uses (just as cyber weapons can be used for both cyber defense and cyber offensive

[56] In this illustration, it is tried to express that the area consists of wider components with the arrows in the horizontal direction and that the figure is limited only to the subjects covered in this report.

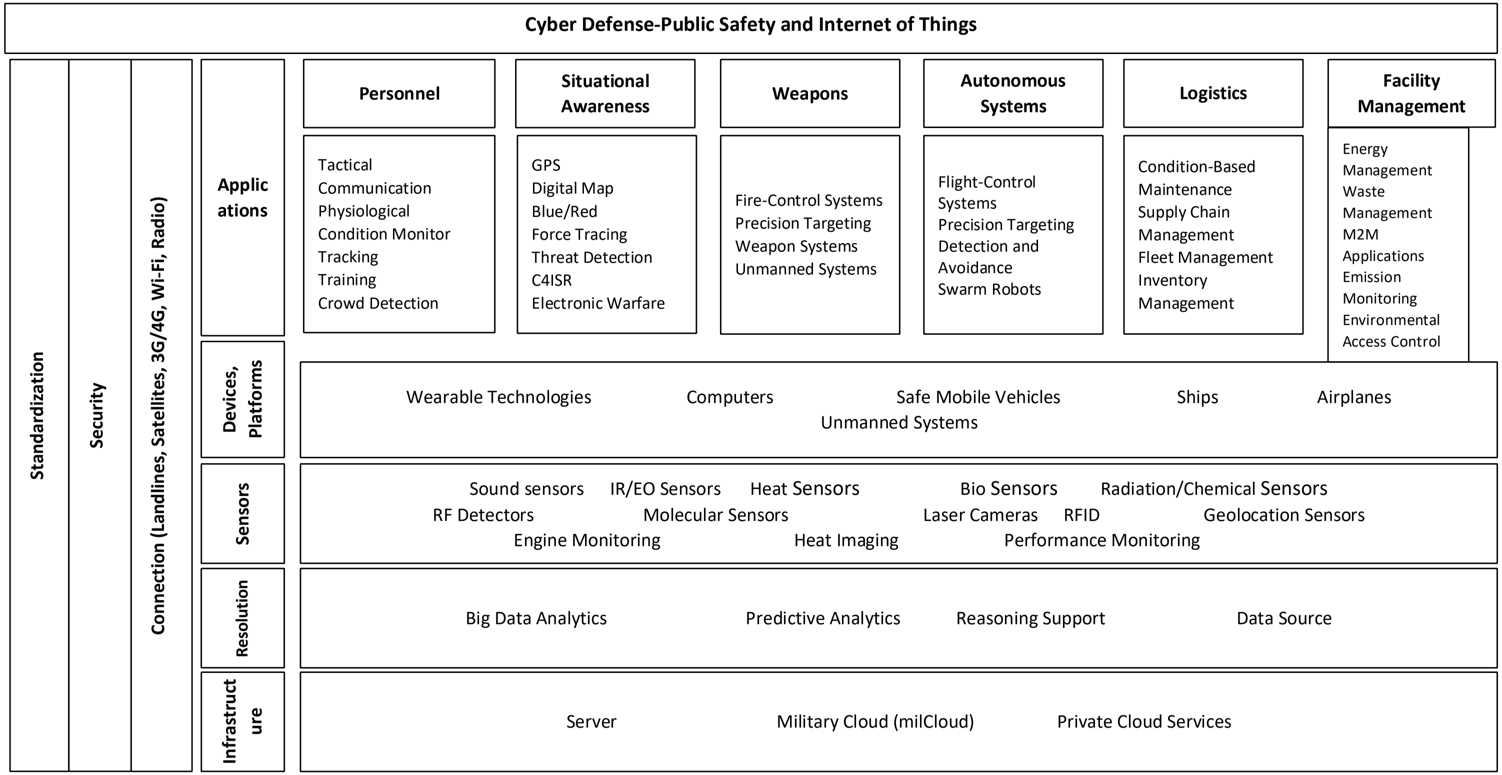
purposes). Therefore, when we consider the highest layer of cyber security as cyber warfare, this concept will not be limited to the armed forces but will also cover the areas of responsibility of all layers that make up the elements of national power. In particular, the components of artificial intelligence, big data, and the Internet of Things shown in the rightmost column in Figure 16 should also be seen as technologies that can further complicate this process and agile the types of threats.

When we focus especially on the environments created by military systems, it is seen that the dimension created by all weapon systems and platforms used in physical battlefields has become cyber-physical environments within the scope of data collected, produced, shared, and used. For this reason, it is possible to talk about a military big data environment. In this context, even if the operational data is encrypted or anonymized in certain environments, the fact that almost petabytes of data are produced, shared, and stored shows that this area is open to cyber activities (cyber espionage, terrorism, attack, etc.). In the context of all these developments, it would be appropriate to use the concept of the "Internet of Military Things"[57] instead of the concepts of network-centered operation or network-centered war. We can summarize the importance of the Internet of Military Things structure within the scope of cyber defense-public security with the help of Figure 18[58]. This structure can also be evaluated as an indicator of how complex the system to be installed and used is. The military operating environment, in particular, should have a cyber security shield.

[57] Internet of Military Things - IoMT

[58] Fraga-Lamas et al., "A Review on Internet of Things for Defense and Public Safety", *Sensors*, Vol. 16, Issue 10, (2016).

*Figure 18: Cyber Defense-Public Security and the Military Internet of Things**



Cyber Defense-Public Safety and Internet of Things

Standardization

Security

Connection (Landlines, Satellites, 3G/4G, Wi-Fi, Radio)

Applic ations

Personnel: Tactical Communication, Physiological Condition Monitor, Tracking, Training, Crowd Detection

Situational Awareness: GPS, Digital Map, Blue/Red Force Tracing, Threat Detection, C4ISR, Electronic Warfare

Weapons: Fire-Control Systems, Precision Targeting, Weapon Systems, Unmanned Systems

Autonomous Systems: Flight-Control Systems, Precision Targeting, Detection and Avoidance, Swarm Robots

Logistics: Condition-Based Maintenance, Supply Chain Management, Fleet Management, Inventory Management

Facility Management: Energy Management, Waste Management, M2M Applications, Emission Monitoring, Environmental, Access Control

Devices, Platforms: Wearable Technologies, Computers, Safe Mobile Vehicles, Ships, Airplanes, Unmanned Systems

Sensors: Sound sensors, IR/EO Sensors, Heat Sensors, Bio Sensors, Radiation/Chemical Sensors, RF Detectors, Molecular Sensors, Laser Cameras, RFID, Geolocation Sensors, Engine Monitoring, Heat Imaging, Performance Monitoring

Resolution: Big Data Analytics, Predictive Analytics, Reasoning Support, Data Source

Infrastruct ure: Server, Military Cloud (milCloud), Private Cloud Services

* Ibid

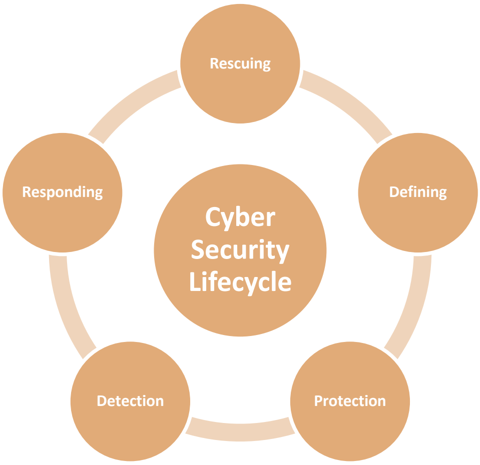
In addition, considering that both adversary forces and friendly forces act together with an effective artificial intelligence platform, it will be equally difficult to detect, identify and intervene in the anomalies caused by the malicious software on the system.

In this context, if we evaluate big data, the Military Internet of Things, and artificial intelligence technologies together and in an integrated structure under the umbrella of cyber security, we can say that the process acts bidirectionally, with dilemmas such as defense/attack, friend/adversary, etc.

Considering that these components can affect all civilian/official security layers, it is of great importance to protect "critical infrastructures"[59], which are defined as "infrastructures containing information systems that may lead to loss of life, large-scale economic damage, national security vulnerabilities or disruption of public order when the confidentiality, integrity or accessibility of the information they process is disrupted". Damage to the components that make up critical infrastructures can lead to national security vulnerabilities.

For this reason, ensuring effective cyber security on all layers – civilians and military – should be considered the top priority. In determining the effective cybersecurity process, the "cyber security lifecycle" shown in Figure 19 can be used as an important guide. [60]

Figure 19: The Cyber Security Lifecycle



[59] Definition of Critical Infrastructure is included in the "National Cyber Security Strategy and 2013-2014 Action Plan" published and effectuated in the Official Gazette dated June 20, 2013 and numbered 28683.

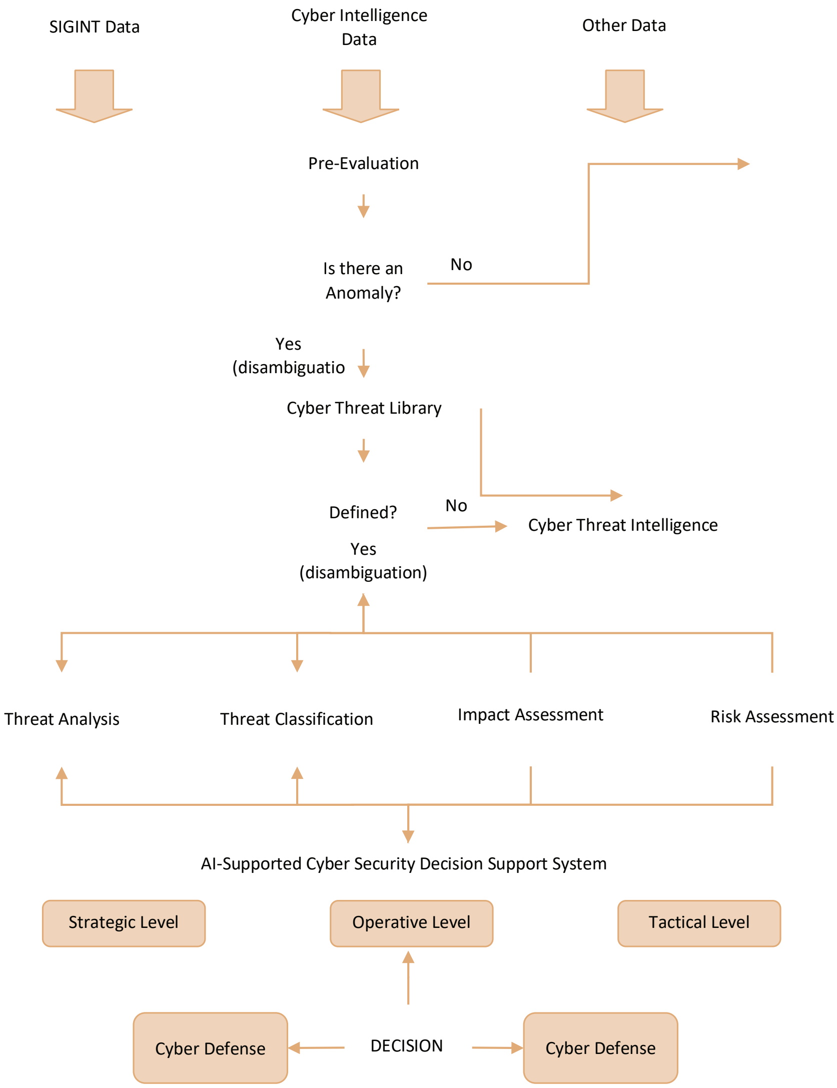
[60] "Framework for Improving Critical Infrastructure Cybersecurity", NIST, 2018, https://www.nist.gov/cyberframework, (Accessed on May 20, 2019).

In order to increase cyber security lifecycle effectiveness, an "Artificial Intelligence-Supported Cyber Security Decision Support System" can be designed as shown in Figure 20. [61]

In this design, data from all kinds of sources are subjected to preliminary evaluation and it is investigated whether there are anomalies in the data. If there is no anomaly, normal activities are continued, while if there is an anomaly, this data is sent to the cyber threat library and compared with the existing threat data. If it cannot be identified, it is investigated in terms of cyber threat intelligence, and threat identification is determined. It is then processed into the cyber threat library. Data defined as an anomaly is transferred to the "Artificial Intelligence Supported Decision Support System" after it undergoes threat analysis, threat classification, impact assessment, and risk assessment. Here, the cyber threat layer (strategic, operational, or tactical) of the cyber threat is determined and the appropriate options (in accordance with the level) are presented to the relevant decision maker. An effective decision is made by the decision maker with the help of these options and within the scope of the current legislation.

[61] Considering the issues mentioned in this report, the design was made in the form of a simple algorithm process.

Figure 20: The AI-Supported Cyber Security Decision Support System



One of the main reasons why the effects of the concept of cyber security are multifaceted is that it covers all layers of society. Today, the age of being introduced to cyberspace has dropped to as young as preschool, especially because of the smartphones parents use to distract their children. Therefore, from preschool age to death, humanity operates in cyberspace. Therefore, the weakest link in cyber security processes, which have an integrated structure, is individuals who do not have cyber security awareness. For this reason,

- Planning training to include all layers of society, including the planned and current threats that will strengthen the awareness of cyber security and cyber security measures, considering the education level of the individuals and the age difference,

- To create cyber security strategies and cyber security implementation policies to include all institutions, organizations, and sectors, starting from the smallest unit of society, the family, to keep these policies up to date and to support realistic practices,

- Encouraging national source coding in the production of all software required for sensitive technology, especially critical infrastructure systems, on an institutional basis and creating it in accordance with secure software creation standards,

- And it is evaluated that it would be appropriate to encourage the realization of unique projects on interdisciplinary topics of all related disciplines (psychology, sociology, management organization, behavioral sciences, strategic management, engineering fields, etc.) in areas such as cyber threat detection, cyber threat analysis, cyber threat classification, cyber threat impact assessment, cyber deterrence, and determination of cyber attacker profiles.

Bibliography

https://www.resmigazete.gov.tr/eskiler/2013/06/20130620-1-1.pdf “National Cyber Security Strategy and 2013-2014 Action Plan” published in the Official Gazette dated June 20, 2013 and numbered 28683. [03.01.2022]

Akram, V. Dağdeviren, O. (2020). Nesnelerin İnterneti için Gerçek Zamanlı Tasarsız Veri Toplama Platformu. Bilişim Teknolojileri Dergisi, 13 (4), 451-462. DOI: 10.17671/gazibtd.745598 [04.01.2022] Bendiek, A. and Metzger, T. (2015). Deterrence Theory in the Cybercentury.Lessons from a State-of-the-art Literature Review. Working Paper RD EU/Europe, 2015/02, May 2015 SWP Berlin. https://www.swp-berlin.org/fileadmin/contents/products/arbeitspapiere/Bendiek-Metzger_WP-Cyberdeterrence.pdf. [21.12.2021]

Bodeau, D.J., Graubart, R. and Fabius-Greene, J. (2010). Improving Cyber Security and Mission Assurance Via Cyber Preparedness (Cyber Prep) Levels. 2010 IEEE Second International Conference on Social Computing, Minneapolis, MN, 2010, pp. 1147-1152, doi: 10.1109/SocialCom.2010.170. [04.01.2022]

Bucci, S. P. (2009). “The Confluence of Cyber Crime and Terrorism”. Heritage Lectures, Pg.2 https://www.heritage.org/defense/report/theconfluence-cyber-crime-and-terrorism [18.09.2019].

C. Maathuis, W. Pieters and J. Van Den Berg, “Cyber weapons: A Profiling Framework,” 2016 International Conference on Cyber Conflict (CyCon U.S.), 2016, pp. 1-8, doi: 10.1109/CYCONUS.2016.7836621. [04.01.2022]

D. Fernández Vázquez, O. Pastor Acosta, C. Spirito, S. Brown and E. Reid, “Conceptual framework for cyber defense information sharing within trust relationships,” 2012 4th International Conference on Cyber Conflict (CYCON 2012), 2012, pp. 1-17. [04.01.2022]

Darıcılı, A.B. (2020): https://www.aa.com.tr/tr/analiz/devletlerin-guncel-siber-guvenlik-stratejileri/2062810 [11.04.2022]

Denning, D. https://faculty.nps.edu/dedennin/publications/Reflections_on_Cyberweapons_Controls.pdf [21.12.2021]

Erol, S.E. ve Sağıroğlu, Ş. (2018). "Siber Güvenlik Farkındalığı, Farkındalık Ölçüm Yöntem ve Modelleri". Sağıroğlu, Ş., Alkan, M. (Ed.), Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık, (115). Ankara: Grafiker Yayınları. Can be accessed on https://bilgiguvenligi.org.tr/bilgi-merkezi/. [03.01.2022]

Fraga-Lamas P, Fernández-Caramés TM, Suárez-Albela M, Castedo L, González-López M. A Review on Internet of Things for Defense and Public Safety. Sensors (14248220). 2016;16(10):1644. doi:10.3390/s16101644 [04.01.2022]

Garstka, J.J., "Network-Centric Warfare Offers Warfighting Advantage" Signal, May 2003. https://www.afcea.org/content/network-centric-warfare-offers-warfighting-advantage/#:~:text=Datalinks%20are%20the%20new%20weapon,create%20a%20decisive%20warfighting%20advantage [16.12.2021].

Gündüz, M. and Daş, R. (2018). Nesnelerin interneti: Gelişimi, bileşenleri ve uygulama alanları. Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi, 24 (2), 327-335. Retrieved from https://dergipark.org.tr/tr/pub/pajes/issue/36922/419740 [04.01.2022]

https://apps.dtic.mil/sti/pdfs/ADA446831.pdf pp. 8 - 10 [16.12.2021]

https://irp.fas.org/doddir/army/pam525-7-8.pdf pp. 8- 9 [20.12.2021]

https://irp.fas.org/doddir/dod/jp1_02.pdf p. 58 [20.12.2021]

https://thinktech.stm.com.tr/tr/altinci-nesil-savas-ucaklarinin-ongorulen-ozellikleri [04.01.2022]

https://www.cmu.edu/iso/aware/presentation/security101-v2.pdf p. 2 [20.12.2021]

https://www.dhs.gov/science-and-technology/cybersecurity-insider-threat [21.12.2021]

https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx [20.12.2021]

Hughes, D.P. (2018). Cyber Weaponry Issues and Implications of Digital Arms. Henry Prunckun (Edt.), Archer's Stakes in Cyber Space: Methods to Analyze Force Advantage (pp. 71-85). Springer. https://doi.org/10.1007/978-3-319-74107-9

I. Kudlácková, D. Wallace and J. Harašta, "Cyber Weapons Review in Situations Below the Threshold of Armed Conflict," 2020 12th International Conference on Cyber Conflict (CyCon), 2020, pp. 97-112, doi: 10.23919/CyCon49761.2020.9131728. https://ieeexplore.ieee.org/document/9131728 [21.12.2021]

Jenna Ahokas, Tuomas Kiiski, Cybersecurity in Ports, Publications of The Hazard Project, Vol 3., 2017 pp. 14-15 ISBN 978-951-29-7071-1

Lee, G.M. and Crespi, N. (2010). Shaping Future Service Environments with the Cloud and Internet of Things: Networking Challenges and Service Evolution. 4th International Symposium on Leveraging Applications, ISoLA 2010, Heraklion, Crete, Greece, 2010, pp. 399-410. [04.01.2022]

LIBICKI, M. C. (2009). "Cyberdeterrence and Cyberwar". Rand Corp. https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf p. 29 [18.04.2019].

Mazzarolo, Guerrino, and Anca Delia Jurcut. 2019. "Insider Threats in Cyber Security: The Enemy within the Gates." https://search.ebscohost.com/login.aspx?direct=true&db=edsarx&AN=edsarx.1911.09575&lang=tr&site=eds-live [21.12.2021]

Michael Robinson, Kevin Jones, Helge Janicke, Cyber warfare: Issues and challenges, Computers & Security, Volume 49, 2015, pp. 70-94, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2014.11.007 [04.01.2022]

Mutlu, N. "Komuta Kontrole Bütüncül Bakış", Aselsan Dergisi, Issue 109, June 2021, p 21. https://www.aselsan.com.tr/22021_4611.pdf (Accessed on 13.12.2021)

Network Centric Warfare Department of Defense Report to Congress, 27 July 2001 http://www.dodccrp.org/files/ncw_report/report/ncw_main.pdf pp. 4-1 [16.12.2021]

NIST. (2018). "Framework for Improving Critical Infrastructure Cybersecurity" https://www.nist.gov/cyberframework [20.05.2019].

Özkaya, E. et al.., "Siber Güvenlik: Saldırı ve Savunma Stratejileri", Buzdağı Yayınevi, 2020.

R. C. Parks and D. P. Duggan, "Principles of Cyberwarfare," in IEEE Security & Privacy, vol. 9, no. 5, pp. 30-35, Sept.-Oct. 2011, doi: 10.1109/MSP.2011.138. [04.01.2022]

R. N. Akram et al., “Security, privacy and safety evaluation of dynamic and static fleets of drones,” 2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC), 2017, pp. 1-12, doi: 10.1109/DASC.2017.8101984. [04.01.2022]

Sağıroğlu, Ş. (2018). “Siber Güvenlik ve Savunma: Önem, Tanımlar, Unsurlar ve Önlemleri”. Sağıroğlu, Ş., Alkan, M. (Ed.), Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık, Syf. 26. Ankara: Grafiker Yayınları. Can be accessed on https://bilgiguvenligi.org.tr/bilgi-merkezi/ [03.01.2022]

Samet, R. ve Aslan, Ö. (2018) “Siber Güvenlik ve Savunma: Önem, Tanımlar, Unsurlar ve Önlemleri”. Sağıroğlu, Ş. ve Alkan, M. (Ed.), Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık, Syf. 228 – 232. Ankara: Grafiker Yayınları. Can be accessed on https://bilgiguvenligi.org.tr/bilgi-merkezi/. [03.01.2022]

Schmitt, M. (2017). Introduction. In Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press. doi:10.1017/9781316822524.006

Siber Kümelenme: https://www.siberkume.org.tr/Index [11.04.2022]

Spencer, B.F., Ruiz-Sandoval, M.E., Kurata, N. (2004). Smart sensing technology: opportunities and challenges. 2004 Structural Control and Health Monitoring, 11: 349–368 (DOI: 10.1002/stc.48), https://onlinelibrary.wiley.com/doi/epdf/10.1002/stc.48 [03.01.2022]

T. Abdelzaher et al., “Will Distributed Computing Revolutionize Peace? The Emergence of Battlefield IoT,” 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS), 2018, pp. 1129-1138, doi: 10.1109/ICDCS.2018.00112. [05.04.2022]

Türk Dil Kurumu Güncel Türkçe Sözlüğü https://sozluk.gov.tr/ [20.12.2021]

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı https://www.btk.gov.tr/uploads/pages/2-1-strateji-eylem-plani-2013-2014-5a3412cf8f45a.pdf [08.04.2022]

Ünal A.Y. (2020). https://www.aa.com.tr/tr/ekonomi/ulusal-siber-guvenlik-stratejisi-ve-eylem-plani-siber-guvenlikte-2023-vizyonunu-gercege-donusturecek/2091907 [11.04.2022]

SETA Emerging Military
Technologies Series .2.

Cyber Security:

Global Trends & Türkiye's Capabilities

The quantification of fronts began to attract interest in the late twentieth century with the development of new concepts like the electronic order of battle, electronic warfare, information warfare and network-centered operations. Today, almost all components of the modern armed forces have already been equipped with software- and hardware-backed systems. Whereas most military systems are operated by being isolated from cyberspace, there are projects under development to create an military Internet of Things (IoT) in the near future.

Cyber threats represent the most significant security issue for all systems operating in the cyberspace. That is why the effective conduct of cyber space activities depends on the active definition, identification, analysis and mitigation of cyber threats. At the same time, most of the concepts that fall within the scope of cyber security can be used in two ways — just as cyber weapons can be used for cyber defense and cyber attacks. That is why the components, which make up critical infrastructure, being damaged could directly lead to national security vulnerabilities. Therefore, ensuring effective cyber security in all civilian and military layers must be treated as a priority.

SETA

9 786258 322163