T.C.
ANKARA YILDIRIM BEYAZIT UNIVERSITY
INSTITUTE FOR INTERNATIONAL RELATIONS AND STRATEGIC RESEARCH

CYBERSECURITY COMMUNICATION POLICIES: EFFECTIVE METHODS FOR COMMUNICATING CYBER THREATS TO THE PUBLIC

MASTER'S THESIS

UBEYD TALHA SARI

DEPARTMENT SECURITY STUDIES

ANKARA, 2024

T.C.
ANKARA YILDIRIM BEYAZIT UNIVERSITY
INSTITUTE FOR INTERNATIONAL RELATIONS AND STRATEGIC RESEARCH

CYBERSECURITY COMMUNICATION POLICIES: EFFECTIVE METHODS FOR COMMUNICATING CYBER THREATS TO THE PUBLIC

MASTER'S THESIS

UBEYD TALHA SARI

DEPARTMENT OF SECURITY STUDIES

PROF. DR. FATİH CEMİL ÖZBUĞDAY
Thesis Advisor

ANKARA, 2024

ONAY SAYFASI

The thesis study Cybersecurity Communication Policies: Effective Methods For Communicating Cyber Threats To The Public prepared by Ubeyd Talha SARI is approved ~~anonymously~~/by majority votes by the jury as Master's thesis in Ankara Yıldırım Beyazıt University International Relations and Strategic Research Institute.

JURY MEMBER		Institution	Signature
Prof. Dr. Fatih Cemil ÖZBUĞDAY		Ankara Yıldırım Beyazıt University Faculty of Political Sciences	
Approved	~~Denied~~		
Assoc. Prof. Dr. İbrahim Demir		Ankara Yıldırım Beyazıt University Institute for International Relations and Strategic Research	
~~Approved~~	Denied		
Assoc. Prof. Dr. Göktuğ ŞAHİN		Ankara Hacı Bayram Veli University Faculty of Economics and Administrative Sciences	
Approved	~~Denied~~		

The Date of Thesis Defence: 08 May 2024

I certify that the conditions for a master's thesis in Ankara Yıldırım Beyazıt University Department of Security Studies have been met.

The Head of The Social Science
The Title, Name, Surname: Assoc. Prof. Dr. İbrahim DEMİR

Institute: International Relations and Strategic Research Institute

DECLERATION

I declare that this thesis is my own work, that I have not had any unethical behaviour infringing patent rights and copyright at any stage from the planning to writing of the thesis, that I have obtained all the information in this thesis within academic and ethical rules, and that I have cited all the information and comments used in this thesis.

Name, Last Name : Ubeyd Talha SARI

Signature :

ACKNOWLEDGEMENT

I extend my heartfelt gratitude to Prof. Dr. Fatih Cemil ÖZBUĞDAY for his unwavering guidance, patience, and profound wisdom throughout the journey of this research. His invaluable insights, unwavering support, and readiness to assist have been indispensable in shaping this work. I am deeply grateful for his mentorship, which has enriched my academic journey immeasurably. Additionally, I am grateful to my institution for providing a conducive academic environment and offering insightful classes that have contributed significantly to the development of my scholarly pursuits.

ABSTRACT

Cybersecurity Communication Policies: Effective Methods for Communicating Cyber Threats to the Public

Cybersecurity communication policies allow a state or a company to effectively communicate about cybersecurity issues. This research aims to explore the field of cybersecurity communication and answer how to inform the public about cyber threats. Given the limited body of research and data available on cybersecurity communication policies, particularly within the context of raising awareness of cyber threats, this research seeks to establish a baseline understanding. Using exploratory research approaches by utilizing secondary data, previous incidents of cyber attacks serve as illustrative examples to highlight the importance of effective cybersecurity communication policies. Through this approach, this research seeks to contribute to academic discourse and provide practical insights for stakeholders in enhancing cybersecurity readiness and resilience. Raising awareness through campaigns and informational materials aimed at both internal and external stakeholders is essential for a successful communication policy, with simplicity and understandability being the cornerstone of effective communication. Media relations in cases of cyber attacks provide the opportunity to provide information to the public directly and effectively. It is important to make statements about cybersecurity measures, threats, and measures taken by a reliable spokesperson. Social media and other online platforms, where people spend most of their time today, are one of the ways to communicate effectively against cyber threats. Considering the managerial aspect of the situation, governments and large organizations need to be able to immediately announce cyber threats to the public also by using emergency notification systems. In conclusion, this research aims to advance understanding of cybersecurity communication policies and their role in addressing cyber threats. By synthesizing existing knowledge and analysing real-world incidents under an exploratory research approach, it seeks to provide actionable insights for enhancing cybersecurity readiness and fostering a culture of security awareness.

Keywords: Cybersecurity Communication, Cybersecurity Communication Policies, Communicating Cyber Threats

ÖZET

Siber Güvenlik İletişim Politikaları: Siber Tehditlerin Kamuya Aktarılması İçin Etkili Yöntemler

Siber güvenlik iletişim politikaları, bir devlet veya bir şirketin siber güvenlik konuları hakkında etkili bir şekilde iletişim kurmasına olanak sağlar. Bu araştırma, siber güvenlik iletişim alanını keşfetmeyi ve halkın siber tehditler hakkında nasıl bilgilendirileceği sorusunu yanıtlamayı amaçlamaktadır. Siber güvenlik iletişim politikaları üzerine mevcut araştırma ve veri kısıtlılığı göz önüne alındığında, özellikle siber tehditlere karşı farkındalığı arttırma bağlamında, bu araştırma temel bir anlayış oluşturmayı hedeflemektedir. Önceki siber saldırı olayları, kullandığı ikincil veriler ile keşifsel araştırma yöntemlerinden yararlanarak, etkili siber güvenlik iletişim politikalarının önemini vurgulamak için örnek olaylar olarak hizmet etmektedir. Bu yaklaşım aracılığı ile bu araştırma, akademik söylemlere katkıda bulunmayı ve paydaşlara siber güvenlik hazırlığı ve dayanıklılığını artırmak için pratik öngörüler sağlamayı amaçlamaktadır. Kampanyalar ve bilgilendirme materyalleri aracılığıyla hem iç hem de dış paydaşlara farkındalık yaratmak, başarılı bir iletişim politikası için esastır; basitlik ve anlaşılırlık etkili iletişimin temel taşıdır. Siber saldırı durumlarında medya ilişkileri, halka doğrudan ve etkili bir şekilde bilgi sağlama fırsatı sunar. Güvenilir bir sözcü tarafından siber güvenlik tedbirleri, tehditler ve alınan önlemler hakkında açıklamalar yapmak önemlidir. Günümüzde insanların zamanlarının çoğunu geçirdiği sosyal medya ve diğer çevrimiçi platformlar, siber tehditlere karşı etkili iletişim kurmanın yollarından biridir. Durumun yönetimsel boyutu da göz önüne alındığında, hükümetler ve büyük kuruluşlar siber tehditleri halka anında bildirebilmelidirler; bunu acil durum bildirim sistemlerini kullanarak yapabilirler. Sonuç olarak bu araştırma, siber güvenlik iletişim politikalarının derinlemesine anlaşılmasının, siber tehditlerle başa çıkmada rolünü ele almayı amaçlamaktadır. Varolan bilgiyi sentezleyerek ve gerçek dünya olaylarını keşifsel bir araştırma yaklaşımı altında analiz ederek, siber güvenlik hazırlığını artırmak ve güvenlik farkındalığı kültürünü teşvik etmek için uygulanabilir içgörüler sağlamayı hedeflemektedir.

Anahtar Kelimeler: Siber Güvenlik İletişimi, Siber Güvenlik İletişim Politikaları, Siber Tehditlerin Aktarımı

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

CCD-Coe	Cyber Defense Center of Excellence
DDoS	Distributed Denial of Service Attacks
DL	Defense League
DNC	Democratic National Congress
DoS	Denial of Service Attacks
ICS	Industrial Control Systems
ICT	Information and Communication Technologies
NATO	North Atlantic Organization
NSA	National Security Agency
SCA	Cybersecurity Alliance
SCADA	Supervisory Control and Data Acquisition
SQL	Structured Query Language
USOM	National Cyber Incident Response Center

LIST OF TABLES

TABLES

LIST OF FIGURES

FIGURES

1. INTRODUCTION

Globalization, which manifests itself as changes in relationships and social and cultural change, has a variety of effects on society and the individual. It is well known that effects can be seen in connection with various everyday phenomena. At this point, mass media appears to be a component that enhances the benefits of globalization. Through mass media, societies that began with globalization continue to focus on a common denominator, and all societies and individuals are evaluated from a single perspective. As a result, globalization can achieve its objectives thanks to the flow of information that constitutes mass media content (Tekke and Lale, 2021). It is now possible to say that social media continues to play the role of mass media. By collaborating in the processes of information production, transmission, and distribution, mass media and social media increase their influence. Over time, the content produced by the media, which is accelerated by social media, transcends reality. In such a case, the digital ethical principles that must be followed are ignored (Sayedi and Büyüksaraçoğlu, 2020).

Individual and social privacy and anonymity are not possible in social media, where the boundaries between individuals and societies dissolve, and individuals meet based on similarity, togetherness, and being the same. The content is false, inaccurate, deceptive, and manipulative when the source is not based on true facts and events. Cyberspace, which includes the transmission of true or false information via online platforms, as well as the sharing, transmission, and storage of information via these platforms, is a concept that influences people's lives (Kostyuk and Wayne, 2019). Threats and risks associated with this design concept require different actions at both global and local levels. Cybersecurity policies include different measures. The focus of cybersecurity policies prepared by taking digital principles into consideration is the processes of producing, protecting, storing, and distributing information and data. Cybersecurity policies are very important to protect people from the disinformation and disinformation processes they encounter when publishing their digital information (Zhang and Borden, 2020).

Cybersecurity is the safeguarding, creation, storage, and transmission of all types of data and information in cyberspace. Cybersecurity, as defined by the International Telecommunication Union (ITU), is the combination of policies, security measures, guidelines, practices, operations, and technologies used to protect the information of users

and cyber organizations that comprise cyberspace. Cybersecurity has three main goals, known as the CIA triad in the literature: confidentiality, integrity, and availability (Gürkaynak et al., 2014). Confidentiality entails concealing information. Individuals' personal data, secrets, and information are confidential matters that must be kept confidential, and access must be controlled. The term "integrity" refers to the fact that the system and the data it contains cannot be changed or manipulated without permission. Availability refers to the expected use of the system. There are various perspectives on information security in cyberspace, both social and political, including technological, legal, user-friendly, and managerial. As can be seen, the three main goals of cybersecurity overlap with the four ethical principles (confidentiality, accuracy, accessibility, and intellectual property rights) mentioned by Mason (1986). In this context, the technology-human relationship and the ethical dimension of the digital world appear in the context of "human," the most fundamental actor of cybersecurity. Therefore, in addition to its technical importance, it can create social disharmony, trigger violence, increase polarization, etc. Manipulation of information for social or political reasons reveals the human dimension of cybersecurity. In terms of target, this human dimension of cyber-attacks differs from traditional cybersecurity threats. Cyber-attacks on computer infrastructure are common; misinformation takes advantage of cognitive biases and misconceptions. Cybersecurity communication strategies are planned and coordinated approaches that allow a company or institution to communicate about cybersecurity issues effectively (Tabansky, 2011).

The aim of the thesis is to examine cybersecurity communication policies in depth and syntesize effective methods used in communicating cyber threats to the public. For this purpose, the study is divided into seven sections. Following this Introduction part, the reader will find the Methodology in the second; and in the third part, Cybersecurity. The third part will provide broad aspects, with definitions and examples of cyber incidents. The findings in the fourth part include which policies can be implemented and offer initial insights into the complexities and details of effective cybersecurity communication, laying a strong foundation for future studies. In the fifth part, the reader will find the ways outlining how to implement the policies discussed in the fourth part, ensuring effective execution and adherence to cybersecurity policies. In addition, the communication model presented in the sixth part offers a comprehensive framework that can be adapted and implemented within Türkiye's policy landscape (Figure 6.1). In the last part, the Conclusion, a summary of the study's findings and recommendations, which addresses the benefits, challenges, and

recommendations for effective cybersecurity communication policies, can be found. When the literature review on the subject was conducted, it was seen that cybersecurity communication policies were examined, but the emphasis on cyber threats-public communication was not examined. For this reason, it is thought that the study will fill the gap in the literature and provide a theoretical framework for future research.

2. METHODOLOGY

In this study, exploratory research was chosen over qualitative research methods. Inductive research was preferred for exploratory research. Exploratory qualitative studies using an inductive approach do not attempt to theorize a priori and instead build on existing bodies of knowledge (Waters, 2007). This method uses conceptual frameworks derived from extensive literature reviews and a priori theorizing, which provides a higher level of structure for both experienced and novice qualitative researchers alike. Because conceptual frameworks provide the foundation for hypotheses and sensitizing concepts. Sensitizing concepts define the exploratory research process and direct the researcher's data collection and reporting efforts. Inductive thematic analysis and pattern matching are extremely useful tools, particularly for guiding sector-specific research (Swedberg, 2020).

Given these justifications for using the inductive method in exploratory research, the overarching goal of this study is to add to the growing body of knowledge on inductive qualitative research. This study aims to provide novice researchers and academics with answers to study questions as a useful a priori framing tool. The use of study questions as a tool to provide greater structure during the design and implementation phases of exploratory research is discussed in depth. In the research, studies on cyber security communication policies and various published reports were examined, and a novel policy was developed on the subject. Sources cited in the thesis: Scientific journals, books, published theses, reports from international organizations, and sectoral publications are all potential sources. These sources were used to answer the following research questions, which are summarized in the thesis:

- What are cyber security communication policies?
- What are cyber threats?
- What are the policies used to communicate cyber threats to the public?

To ensure the scientific validity and reliability of this thesis, a variety of sources, including research and compilation, were carefully chosen based on the subject.

3. CYBERSECURITY

Cybersecurity is a concept that has gained importance with the widespread use of information technologies and the internet. Cybersecurity is a discipline that aims to protect computer systems, networks, software, and data from malicious attacks. The main goal in this area is to ensure information security and protection against cyber threats (Karaarslan and Akbaş, 2017).

Cybersecurity involves taking precautions against various threats. These include various types of attacks and threats, such as computer viruses, malware, ransomware, data leaks, phishing, and DDoS attacks. Several techniques, strategies, and policies have been developed to combat these threats and protect systems. With cybersecurity, which is of great importance in many sectors and organizations, businesses, governments, financial institutions, the healthcare sector, and individuals try to protect their information assets by taking various precautions (Aslay, 2017). In this context, security is ensured by using technological tools such as firewalls, antivirus programs, security software, strong encryption methods, and network monitoring systems. In addition, raising cybersecurity awareness, educating users, and creating security policies are also important. Because, in addition to technological measures, it is also critical for users to be conscious and careful in terms of cybersecurity. In this context, it is important to follow basic security rules such as using strong passwords, downloading software from reliable sources, and not opening unknown e-mail attachments (Sağıroğlu and Alkan, 2018).

As a result, cybersecurity is a serious problem faced by individuals, institutions, and states today. With rapidly developing technology, cyber threats also increase, and therefore, security measures need to be constantly updated and improved (Özdemirci and Torunlar, 2018).

3.1. Cybersecurity Concepts

Cybersecurity is a concept that has emerged with the rapid development of information and communication technologies in today's digital world. The main goal in this field is to protect computer systems, networks, software, and other digital assets from malicious attacks. Cybersecurity includes several concepts and methods (Alazab et al., 2021).

The first of these is the firewall. A firewall is a security feature that protects computer networks. Firewalls monitor network traffic, preventing unwanted access and limiting unauthorized access to systems. The second is malware. Malware, including viruses, trojans, and ransomware, is software that has the potential to damage computer systems. Cybersecurity uses a variety of methods to detect and remove such software. Another example is authentication and authorization. These are security measures used to verify user identities and restrict access to only authorized individuals. This context considers methods such as encryption and two-factor authentication (Wilson and Kiy, 2014). Security policies are one of these methods, and they consist of rules and policies developed by institutions or organizations to determine and implement cybersecurity policies. These policies aim to ensure the safety of employees and systems by setting security standards. Another method is encryption. Encryption is a method for improving the security of data, communication channels, or storage areas. Encryption renders data unintelligible, allowing only authorized users to access it. Intrusion detection and prevention systems (IDS/IPS) monitor network activity to detect and prevent malicious attempts. These systems aim to detect potential attacks and respond quickly. Awareness and education are important aspects of all cybersecurity research. These are activities carried out to increase cyber security awareness, educate users, and ensure that they comply with security policies. User attention and awareness play a critical role in preventing many cyber attacks. Finally, security vulnerability scanning and assessment are the processes carried out to detect and close security vulnerabilities in systems. This aims to make systems more robust by detecting and fixing vulnerabilities (Wilson and Kiy, 2014; Alazab et al., 2021).

Cybersecurity is a constantly evolving field and should be updated in parallel with the changes in technology and threats. These concepts constitute the basic elements in determining and implementing strategies to protect the digital assets of cybersecurity experts, organizations, and individuals (Çelik, 2018).

3.2. Layers of Cyberspace

Cyberspace layers are a concept used in the field of cybersecurity to evaluate and protect systems and networks at different levels. These layers include different levels of security measures and technologies so a holistic cybersecurity policy can be created.

Generally, three basic layers are mentioned: the network layer, the system layer, and the application layer (Arda, 2020).

The network layer consists of three layers. As previously stated, firewalls monitor network traffic, prevent unauthorized access, and control unwanted data flow. IDS/IPS systems (Intrusion Detection and Prevention Systems) monitor abnormal activity and detect attack attempts. They can prevent attacks by intervening in appropriate situations. Virtual private networks (VPNs) are the final layer of the network. VPNs play an important role in the network layer, ensuring data security and establishing an encrypted tunnel across the internet (Medeiros and Goldoni, 2020). The system layer consists of three major components. Antivirus software detects and removes malware. They defend against virus and malware attacks on user computers or servers at the system level. Identity and access management is also used to control system login and access; this management verifies user identities and restricts access to private information to authorized individuals. Security updates (Patch Management) at the system level are also critical. It ensures that the operating system and software are regularly updated to address security vulnerabilities. This updates computer systems against potential attacks (Altıner and Çakır, 2018). Security tests and audits of software and applications are performed at the application layer. This assesses the resilience of software and applications to cyber-attacks. Web security also includes security measures for preventing attacks on web applications. Web application security protects against a wide range of attacks. Security awareness training aims to raise users' awareness of cyber security and teach them safe behaviors. This accounts for the human factor at the application layer (Korhan, 2017).

The layers of cyberspace listed above combine to ensure the integrity of an organization or individual's cybersecurity policy. Each layer provides a certain level of security and works together to provide broad protection. These layers are integrated to create a more effective defense mechanism against cyber-attacks (Altıner and Çakır, 2018).

3.3. Cyber Incident

A cyber incident refers to any activity that occurs against a computer system or network, usually with a malicious purpose. These events are often referred to as cyber-attacks, cyber-crimes, or cyber threats. Cyber incidents include various threats and risks to the digital assets of individuals, institutions, or governments (Romanosky, 2016).

The ways in which cyber incidents occur are very different. One of these examples is malware. Malware refers to cyber events in which malicious software such as viruses, trojans, and ransomware infects target systems. Such software has the potential to damage systems, steal data, or lock them. Another example is a ransomware attack. This type of attack involves cybercriminals locking institutions' computer systems and demanding a ransom. Victims are frequently forced to pay a ransom to gain access to their computers or files. Phishing is another popular form of cyber-attack (Sertçelik, 2015). Attackers use fake e-mails or websites to trick users into disclosing sensitive information. DDoS attacks, also known as denial of service attacks, overwhelm the target's services, causing them to crash. These types of attacks frequently consume network resources, disrupting normal operations. Data leaks are incidents in which malicious individuals steal and disclose sensitive information from an organization. Such cyber incidents result in the disclosure of sensitive information, such as customer data, trade secrets, or financial information. The final type of cyber-attack is advanced persistent threats (APT), which are defined as long-term, targeted, and often sophisticated attacks. APTs are frequently carried out by state-sponsored actors and involve data theft, monitoring systems, or long-term espionage activities (Van Niekerk, 2017).

Cyber incidents pose a serious threat in almost every sector and level today. Therefore, it is important for individuals, institutions, and governments to take cybersecurity measures, increase security awareness, and constantly update security measures. This creates a more effective defense mechanism against cyber incidents (Hemsley and Fisher, 2018).

3.4. Cybercrime

Cybercrime is a general reference to crimes committed with computer systems, networks, and digital technologies. These crimes, unlike traditional crimes, occur in the digital environment and generally include activities such as hacking, data theft, phishing, use of malware, and cyberbullying. Cybercrime has become more sophisticated and widespread with the rapid development of technology. These crimes can often cross-national borders because they can be carried out worldwide via the Internet. Cybercrimes seriously affect individuals, institutions, and states (Hekim and Başıbüyük, 2013).

Cybercrimes can threaten the security of individuals, institutions, and states. Therefore, it is important to take cybersecurity measures and create effective legal

frameworks to combat cybercrime. International cooperation and information sharing also play a critical role in combating cybercrime (Cengiz, 2021).

3.5. Cyber Attacks

Cyber-attack is a term that refers to malicious activities carried out on computer systems, networks, or digital devices. These types of attacks generally aim to steal information, damage computer systems, or disrupt services. Today, cyber-attacks have become more frequent and complex with the widespread use of digital technologies and the internet. Cyber-attacks can be of different types. Malware (viruses, trojans, worms), phishing, DDoS attacks (Denial of Service Attacks), malware infection, and many other methods can be used for cyber-attacks (Öztürk, 2018). These attacks can often result in information theft, financial harm, reputational damage, service disruptions, or more sophisticated espionage purposes. Cyber-attacks can affect individuals, companies, government agencies, and even national security. For example, the theft of personal data can lead to identity theft, while a company being hacked can lead to financial losses and loss of customer trust. Additionally, attacks on government institutions can threaten national security. It is important to take strong security measures to protect against cyber-attacks. These measures include using strong passwords, using security software and up-to-date anti-virus programs, regularly updating software and systems, and providing cybersecurity training to employees. It is also important to adopt security policies that are monitored and updated by cybersecurity experts. In this way, an effective defense can be provided against cyber-attacks (Li and Liu, 2021).

Cyber-attacks target individuals, companies, government institutions, or any digital asset. Large companies and government agencies often attract more attention and are subject to more sophisticated attacks. Many cyber-attacks aim to steal valuable information. This information includes personal data, financial information, trade secrets, and strategic information. Denial of service attacks (DDoS) are attacks that attempt to disrupt the normal operation of a service or network. Attackers often send heavy traffic onto a system, consuming resources or causing the service to crash (Duo et al., 2022).

The importance of cyber-attacks is increasing day by day because addiction has increased with digitalization. Companies' reputations, financial health, and even national security are affected by cyber-attacks. Therefore, security measures and cybersecurity

awareness are of great importance. Protection and prevention: Individuals, companies, and states need to take security measures to protect against cyber-attacks. These measures include using strong passwords, using security software, performing software updates, and providing cybersecurity training to employees. To combat cyber-attacks, security measures should be constantly updated, and cybersecurity awareness should be increased. This is an important step to protect the digital assets of individuals and organizations (Yıldırım, 2018). Dozens of cyber security incidents have occurred in the past years in the United States, one of the countries with the most cyber security problems in the world. Some of the events that have a global impact are as follows (Luiijf et al., 2013; Aytekin, 2015; Karataş, 2020):

- In 2009, Walmart, a Fortune 500 company, experienced information theft from its cash registers due to a computer system breach. Target lost 148 million dollars after the personal information of 110 million customers was stolen in 2013.
- McAfee's research estimated that cyber-attacks cost the US economy approximately 154 billion dollars in 2013.
- In 2014, 60 million credit card numbers were stolen from Home Depot.
- In 2014, a breach of Apple's iCloud accounts resulted in the theft and public disclosure of personal information and photos, primarily of well-known celebrities. As a result of this incident, the company's release of the phone model was delayed by several weeks.
- 234 000 computers affected by the Cryptolocker virus suffered a loss of 27 million dollars in just the first two months.
- In 2014, 2.6 million paycard information from Michael's, 4.5 million patient information from Community Health Systems, 905,000 personal information from the US Postal Service, 76 million household information from JP Morgan Chase, and 7 million private sector financial information, 1.2 million credit card information was stolen from Staples.
- Ponemon Institute's 2013 research on 60 companies found that cyber-attacks resulted in an average of 11 million dollars in damage, with losses ranging from 1.3 million to 58 million dollars. This was a 26% increase from the previous year's research.

Cybersecurity incidents occurring in the UK can be listed as follows (Stoddart, 2016):

- According to the results of research commissioned by the Cabinet Office to Detica in 2011, the cost of cyber-attacks to the UK economy reaches 27 billion pounds annually.
- As a result of the research conducted by the Ponemon Institute on 36 representative companies in 2013, cyber-attacks caused an average of 3 million pounds of damage to companies. Each attack caused financial losses between 370,000 pounds and 17 million pounds, and this was a 36% increase compared to the research conducted the previous year.

3.5.1. Denial of Service Attacks (DOS, DDOS)

Denial of service attacks (DoS) and distributed denial of service attacks (DDoS) are types of attacks that constitute a special category of cyber-attacks and aim to prevent access to services or resources on the internet (Çatak, 2018).

Denial of service attacks (DoS): In this type of attack, attackers send excessive amounts of traffic to a target's computer system or network, consuming resources and therefore preventing normal operations from occurring. These attacks aim to make the target's internet services or network connection temporarily or permanently unavailable. For example, they can crash a website by sending an excessive number of requests (Kumar, 2016).

Distributed denial of service attacks (DDoS): DDoS attacks are similar to DoS attacks but are a more complex and effective version. In this type of attack, a larger and more effective attack is made on the target by using traffic from many different sources. Attackers often coordinate their attacks using botnets or zombie computers, making it difficult to track down and stop the attack. DDoS attacks cause the target to experience a traffic load that is too large to handle normal traffic, resulting in services crashing or degrading service quality. Important internet services such as financial institutions, e-commerce sites, government institutions, and large corporations are among the potential targets of DDoS attacks. To protect against such attacks, companies and institutions often take security measures such as traffic filtering, backup systems, intrusion detection, and guidance from cybersecurity experts. At the same time, service providers and companies are trying to develop various strategies and solutions to increase resilience against DDoS attacks (Elleithy et al., 2005).

3.5.2. Malware

Malware is malicious software designed to damage or gain unauthorized access to computer systems, networks, or digital devices. This type of software usually operates for malicious purposes without the user's knowledge or permission.

Viruses are one of the most common types of malware. They are self-replicating malware that infects computers and spreads to other files or programs. Viruses frequently spread through the system without the user's knowledge. Trojan horses (Trojans) are programs that appear to be harmless or useful but actually serve a malicious purpose. Trojan horses infiltrate computers, open backdoors, steal information, and gain unauthorized access (Duran and Bakır, 2023). Worms are another type of malware that spreads quickly and replicates itself across computer networks. Worms frequently consume system resources and clog network traffic, resulting in effects like denial-of-service attacks. Phishing software is intended to deceive users and collect personal information. They frequently send users malicious links via fake websites or email messages. Another important type is ransomware. They are malware that encrypts computer files or systems and demands a ransom from the user. Failure to pay the ransom may result in permanent loss of access to files or systems (Toğaçar, 2023).

The widespread use of malicious software has increased the importance of computer security and cybersecurity measures. Users should use strong passwords, use reliable antivirus software and firewalls, perform regular system updates, and be aware of information security. Additionally, being careful via email and the internet can reduce the risk of malware infection. Organizations should update their security policies and provide cybersecurity training to their employees (Aslan and Samet, 2020).

Malware is a malicious computer program that allows unscrupulous people who want to use computer systems for malicious purposes to capture system information or cause serious damage to those systems. Although this software is a broad term, it includes malware such as viruses, trojans, worms, spyware, keyloggers, adware, and ransomware. This software can be used to carry out cyber-attacks against society, companies, institutions, and countries. The basic and main purpose here is to obtain critical information by using systems without permission. Malware such as viruses and Trojan horses are usually delivered to victims as e-mail attachments, infect the computers of people who open the attachments, and

multiply and spread like an epidemic in the systems and networks that communicate with those computers. Malware is often spread through free or ad-supported programs, inappropriate websites, games, and chat groups. In general, all malware has the feature of repeating itself. These software programs can behave differently at different points in their life cycle, and the malicious actor can manually install them on the victim's computer system, resist and clean the programs used against him, and remove such programs using different tactics (Gandotra et al., 2014).

3.5.3. Rootkit

Rootkits are malicious programs that corrupt the system by installing themselves as kernel modules of the operating system. Since this type of software is a one-time malware only when the operating system is running, it loses its malicious properties when the system is rebooted. However, they also cause very long-term damage; it often takes days or even months to turn the system on and off. Once infected by a rootkit, it can serve as a springboard for many future attacks. For example, it is often used to hide sensitive user information such as passwords and credit card numbers, as well as to hide keyloggers that steal keystrokes by silently recording them. They can also install backend programs on the system, which will allow a remote attacker to break into the system in the future. Rootkits can also perform other covert actions, such as disabling firewall/antivirus tools or affecting the output quality of the system's pseudorandom number generator, which can result in the weakening of encryption keys (Atasever, 2019).

None of the rootkit activity is directly visible to the user because the rootkit software hides its presence and allows it to remain undetected for long periods of time. Therefore, it provides long-term control of infected systems. A root card is a very difficult-to-understand computer program that infects the computer, hides among running processes, and gives malicious parties full access to the system remotely. Its purpose is not to slow down the system or spread like a virus but to take control of the computer and hide its location. Although it was originally created and used to hide user access to system data in multi-user systems, it is also used maliciously (Canbek and Sağıroğlu, 2007). A file executed with elevated privileges, possibly from a secure location, could cause this malware to be installed on the system. However, another common infection method is to gain authority over the system by exploiting vulnerabilities such as the operating system kernel in a multi-user

system. It is very difficult to determine which documents this malware changed, which part it placed with the vulnerabilities it found, where the files were hidden, and which web services it monitored and ran with the relevant command. However, sometimes methods such as hiding the values of a rootkit's most appropriate commands and possible infection points and then taking them under control can be used (Gündoğdu, 2023).

3.5.4. Feeding

"Cyber baiting," or more commonly known as "phishing," is a tactic in which cybercriminals try to obtain sensitive information by misleading individuals or organizations, usually through methods such as email, SMS, or fake websites. This type of attack aims to deceive victims by pretending to be a reliable source, usually using social engineering (Kara, 2019).

Baiting attacks can happen in a variety of ways. The first of these is an email trap. Cybercriminals frequently request information from victims by sending bogus emails claiming to be from government agencies. These emails frequently employ tactics such as instilling urgency, posing account security risks, and promising rewards. SMS phishing can also be done through text messages (SMS). Fake messages are sent to users, often simulating an emergency and encouraging them to click on a link or call a phone number (Yilmaz, 2018). Cybercriminals can use fake websites to trick users into entering account information, passwords, or other sensitive data by making them appear to be legitimate websites. In phone harassment, attackers call users and pretend to be representatives of an official organization, attempting to persuade them to reveal personal information or click on malicious links. To avoid phishing attacks, users can employ various strategies (Doğan, 2021). Take a traditional approach to emails and messages and be wary of requests from unknown senders. First and foremost, before clicking on links, make sure the web address is correct, especially on sites containing financial information. Furthermore, use strong passwords and avoid using the same password on multiple accounts. Yılmaz (2018) recommends regular checks and updates for security software.

Acting consciously and developing security awareness can provide more effective protection against phishing attacks. This type of cyber-attack, one of the oldest and increasingly sophisticated cyber-attacks developed in the 1990s, is still widely used to commit all types of personal and corporate identity fraud. These attack methods are mostly

used to capture important and confidential information such as usernames, passwords, credit card information, and domain names. Cyber attackers impersonate government agencies via phone or email and trick users into stealing their information by asking them to click on a malicious link or additional links they send (Bowen et al., 2009). Here, it tricks the recipient of an email, for example, with a message from a bank of which he is a customer or an email from his workplace that contains something he wants or needs. Phishing scams can trick victims using social media systems such as phone calls and text messages, as well as emails. The word phishing, which is formed by combining the English words password and fishing, is translated into Turkish as "Yemleme." Password hunters often contact their victims via email and ask for information. The accounts, passwords, and private information of people who respond to these attackers fall into the hands of fraudsters. To prevent this cyber-attack, banks, private companies, and institutions are recommended to never ask their customers for private information via e-mail and then share the incoming e-mail or message with them (Ayap et al., 2022).

3.5.5. Zombie Computers

"Zombie computers" generally refers to computers that have been placed under the control of a malicious actor, often within a botnet. These computers have been compromised without the owners' knowledge or permission, often through viruses or malware. Zombie computers are often used in information theft, phishing, attacks, or other harmful activities by communicating with other computers on the network (Erhan et al., 2013).

Zombie computers are often organized into a botnet. A botnet is a network of large numbers of zombie computers, usually managed remotely by a command and control (C&C) server. Attackers can launch large-scale attacks using this botnet. Hijacking zombie computers is usually done using malware. This malware infiltrates the computer system and takes control without the computer user's knowledge or permission. Zombie computers usually infect by exploiting security vulnerabilities in operating systems and applications. Therefore, it is important to ensure that security software is up-to-date and provides strong protection. Zombie computers are used for cybercrimes, phishing, DDoS attacks, and other malicious activities. Computer users should regularly update their security software and follow security best practices to keep their computers safe (Marecki, 2019).

3.5.6. Social Engineering

Social engineering is an information security attack method often used to manipulate or deceive people's behavior. This method aims to reach targeted information by using human psychology rather than providing a technical vulnerability or direct access to the computer system. Social engineering attacks generally include methods such as fraud, phishing, malware infection, and bypassing security protocols (Yavanoğlu et al., 2012).

Social engineering aims to obtain information by gaining people's trust or misleading them, not by bypassing technical defenses on computer systems. These types of attacks are often based on social interactions we encounter in our daily lives. For example, an attacker can call and pose as a trusted person or organization and thus attempt to obtain the target's information. To protect against social engineering attacks, it is important to be aware and careful. Be wary of suspicious emails, unknown phone calls, or unexpected requests, and be wary of requests from unreliable sources. In addition, using strong passwords, regularly updating security software, and receiving training on information security are important steps to protect against social engineering attacks (Mutlu and Korkut-Owen, 2017).

Unlike other types of cyber-attacks, social engineering is a cyber-attack that is carried out by taking advantage of the users' communication, emotions, thoughts, trust, and, in short, human weaknesses. Attackers using this cyber-attack method leak information to the targeted people by telling all kinds of lies, creating fake scenarios, presenting themselves as a reliable source or an authorized person, or using easy forms of reward. In addition, attackers can deceive their victims and access the information they want by using fake e-mails, phone conversations, chat areas, and social media that they have prepared (Salahdine and Kaabouch, 2019). In short, because of the common use of printers, after taking the printouts of the work done in the workplace and making the necessary arrangements, these printouts are not destroyed, a large amount of information related to the organization and its work is stolen, and the usernames, secrets or things left by the staff on their work desks about the work they have completed. Methods such as obtaining information from notes are within the limits of social engineering. Using a female voice in social engineering is more effective than a male voice, and more successful results are obtained (Gupta et al., 2016).

3.6. Cybersecurity Incidents

There are many reasons for cyber-attacks that ignore security breaches. These reasons include political desires, seizing and changing data without permission, limiting and damaging the enemy's ability to win, putting pressure on the economy, making propaganda, and even showing off their talents and having fun. In addition to the numerous methods used to carry out attacks, the existence of security and employee vulnerabilities also makes the attackers' job easier (Sertçelik, 2015).

3.6.1. Estonia

The attack in Estonia is one of the most talked about cybersecurity breaches and is an example of the importance of the issue. Instead of chaos, which shows how effectively cyber threats can affect people's lives, the Estonian attacks have given the Estonian people a literal doomsday scenario. Although everything became clear from the outside with the removal of the bronze soldier statue of the Estonian government from Tallinn Square, to understand the background of the attacks, it is first necessary to know the demographic and socio-cultural situation of Estonia. Famous as "the most wireless country in Europe," only half of its citizens had access to basic phone lines when it gained independence in 1991. However, the new government saw this deficiency as an opportunity and encouraged research and development in the field of telecommunications and information technologies, allowing the country to enter many innovations because of these activities. For example, the software used in the Skype application comes from Estonia (Dilek et al., 2023).

In 2005, Estonians had the opportunity to vote electronically for the first time in the world, as approximately 60% of the population now required the Internet. Approximately 96% of banking transactions in the country were carried out over the Internet. However, while all these important advances were made, the information technology infrastructure seemed weak because the government did not do the necessary work on Internet security and cyber defense. This image increased the possibility of cyber-attacks on technological infrastructure. Finally, on the evening of April 26, 2007, shortly after the removal of the Red Army monument, a very effective cyber-attack of unknown origin took place. It was erected in memory of the Russian soldiers who saved the Estonian people from Nazi occupation in 1947. This attack could not be detected in the first 24 hours. The first target victim was the home page of the ruling Reform Party. In a short time, the websites of other political parties,

the government, and the Estonian Parliament were also attacked, and their servers had to be closed due to the attacks. These attacks expanded further a week later, and the attackers targeted the country's main media companies (Kişman and Güleç, 2021). It was then revealed that the IP addresses of the computers used in the attack came from abroad. In other words, the only way to prevent these attacks, even slightly, was to stop internet traffic coming from abroad. However, in such a situation, the media will have great difficulty in announcing the attacks against their country to the world. In the third week of attacks, the country faced the most serious cyber-attacks on 9-10. On the evening of May, attacks involving nearly 4 million data packets per second attacked the country's banking system and targeted the country's largest bank, Hansapanga, and due to these attacks, banking systems had to shut down their servers. Initially, for political purposes, the attackers limited citizens' access to information through the media and dealt a real blow to the banking system, that is, to the economy. Although the attacks were planned and intense, the government's decision to cut off international network connections was a very correct decision and ensured that the severity of the attacks remained at an appropriate level. Although the government openly blamed Russia for these attacks, the Russian government said it had nothing to do with the incident. Although the Russian state directs these cyber-attacks to some extent, it has been observed that the attackers generally act on their own (Erendor, 2016). As a result, the impact of these cyberattacks was not limited to Estonia; they also went beyond that border. Today, we are talking about the cyber-attacks experienced by this country, and the fact that Estonia is cited as an example in almost every cybersecurity meeting is proof of this. North Atlantic Organization (NATO) experts, who visited the country because of the events, played a very important role in Estonia's defense mechanisms against cyber-attacks, and the country also took an important step in the field of cybersecurity. Following the attacks, a competence center was established in the country in 2008 under the name of Cyber Defense Center of Excellence (CCD-Coe), which became operational in August of the same year. Additionally, the Defense League (DL) started activities to improve the country's cyber defense capability. The Cybersecurity Alliance (SCA), operating within DL, is responsible for work under three headings. These obligations were to protect the electronic life of the Estonian people, train IT experts, raise awareness, and inform citizens about cyber protection (Darıcılı, 2014).

In summary, the Estonia cyber-attack refers to a large-scale cyber-attack incident against Estonia in 2007. This attack was carried out against Estonia's government

institutions, financial institutions, media, and infrastructure systems. The attack is thought to have been launched by a pro-Russian group protesting the Estonian government's decision to move a Soviet military monument. The incident took place between April and May 2007. At the beginning of the attack, various websites in Estonia became inaccessible because of cyber-attacks (Herzog, 2011). The targeted sites included government agencies, banks, media organizations, and other important institutions. The methods of the attack included DDoS (Distributed Denial of Service) attacks, hacking, and using various cyber weapons. The attack attracted attention as one of the first large-scale attacks faced by a state in the cyber domain. The Estonian government requested assistance from NATO in response to the attack. NATO directed cyber defense capabilities to Estonia and provided support to establish a cyber defense center in the country. The incident became a topic of international attention regarding cybersecurity and set an important example of how the international community would respond to similar cyber-attacks. The Estonian cyber-attack encouraged other states to take their cybersecurity seriously and develop effective defense strategies against cyber-attacks. Additionally, this incident triggered greater cooperation and norm-setting efforts on cybersecurity at the international level (Haataja, 2017).

3.6.2. Stuxnet

In 2006, U.S. military and intelligence agencies prepared a secret cyberattack plan to stop Iran's uranium enrichment program. This malware, developed jointly by US and Israeli intelligence officials, targeted approximately 100,000 centrifuges in 2010, modifying their equipment. This malware, which specifically targets critical infrastructures such as SCADA (Supervisory Control and Data Acquisition) industrial systems, was developed to disrupt and monitor Iran's nuclear activities (Kenney, 2015).

In November 2010, it revealed its true intentions by infiltrating Iran's high-security nuclear bomb facilities and staging a coup against the country's uranium enrichment program. Malware slowly infiltrated these areas and began to wreak havoc. Stuxnet planned to control centrifuges used to enrich uranium by targeting their programmable logic controllers (PLCs). Centrifuges are machines that rotate very fast and are used to enrich uranium. When the control software began to malfunction, the speed of the high-speed spinning machines went out of control, and the machines began to break down. The scary thing about a virus that takes over a system and secretly causes damage is that it does not

malfunction the hosts, so internal damage goes unnoticed for a long time. Replacing broken machines with new ones and repairing machines damaged by the virus caused many business interruptions. The Stuxnet virus appears to have disrupted Iran's nuclear activities for two years. The fact that this virus affected approximately 60% of Iran in the world strengthened the perception that this malware was developed specifically to stop and destroy Iran's nuclear weapons (Buchanan, 2022).

As can be seen from the above information, Stuxnet is an example of a complex cyber-attack and malware that was discovered in 2010 and had wide repercussions around the world. Characteristics of Stuxnet generally suggest that it was a state-sponsored cyber-attack. The prominent feature of this attack is that it aims to affect the functioning of nuclear facilities by targeting industrial control systems (ICS) (Ermiş, 2018). Stuxnet was first discovered in June 2010 by VirusBlokAda, a Belarus-based security company. The attack specifically targeted Iran's nuclear program. The unique and sophisticated features of this malware are considered a turning point in the future evolution of cyber-attacks (Aydın et al., 2021).

The first thing to consider when analyzing Stuxnet's features and effects is its targeting of industrial control systems. Stuxnet targeted Siemens' industrial control systems. It hacked nuclear facility control systems, specifically Siemens' WinCC and Step7 software. Stuxnet is a highly sophisticated malware example that uses complex programming techniques to target zero-day vulnerabilities and self-propagation capabilities (Baezner and Robin, 2017). Additionally, Stuxnet targeted the control systems of Iran's Natanz nuclear facility, attempting to affect its centrifuges. This suggests that Stuxnet is a state-sponsored cyber-attack. Stuxnet's advanced design and specific targeting of industrial control systems suggested that the attack was carried out by a state or a state-sponsored actor. This has frequently led to speculation that the United States and Israel are behind such an attack (Collins and McCombie, 2012).

Stuxnet raised awareness of cyberattacks targeting industrial systems in the cybersecurity community. At the same time, state-sponsored cyberattacks have demonstrated that hackers have the capacity to interfere with physical systems rather than simply steal information (Kenney, 2015).

3.6.3. Duqu

In September 2011, a year after the release of Stuxnet, a new malware named Duqu emerged. Duqu comes from the generated file names, the prefix. Duqu's modus operandi is like Stuxnet, but instead of causing harm, it aims to conduct similar intelligence research by gathering information about industrial control methods. However, looking at its targets, Duqu has a much wider range of threats than Stuxnet. Similarities between Stuxnet and Duqu malware are that they target industrial control systems and use valid certificates, and both were detected in Iran. Although there are some similarities between the two viruses, there are also differences (Aslay, 2017). While the destructive Stuxnet aims to damage systems, Duqu was created to collect important information about SCADA techniques. Stuxnet attacks were designed to compromise systems and increase attack efficiency. Duqu points out that major dangers may arise in the future (Sertçelik, 2015).

Duqu is a sophisticated type of cyber-attack and often involves malware specifically designed for the target. First discovered in 2011, Duqu is a variant of the Stuxnet worm and uses similarly advanced attack techniques. Duqu is a type of espionage attack whose main goal is to hijack computer networks and steal confidential information. Duqu attacks are typically directed at large organizations in specific industries and are often associated with state-sponsored actors. Such attacks can be used to steal sensitive information, conduct espionage, or weaken target organizations. The attack usually has a complex and sophisticated nature. Duqu has features such as infiltration techniques, advanced encryption, and security bypass capabilities. Therefore, it can often be difficult for target organizations to be detected and blocked by information security experts (Çahmutoğlu, 2020).

Duqu attacks have been one of the notable events in the cybersecurity community and have contributed to the development of defense mechanisms against similar sophisticated attacks. It is important for organizations to constantly update and strengthen their security measures to prevent and detect attacks (Venkatachary et al., 2017).

3.6.4. Flame

Flame is a malware, a sophisticated cyber-attack discovered in 2012. Flame is like attacks such as Duqu and Stuxnet but is distinguished by its own unique features. Flame is often referred to as a "super spy" or "advanced persistent threat" and is generally believed

to be a state-sponsored attack. Flame is designed as an espionage tool with a wide range of targets. Targets may include strategically important organizations such as government agencies, the energy sector, financial institutions, and research centers. This attack attracts attention with its ability to infiltrate computer networks, collect data, and carry out espionage activities (Bencsáth et al., 2012).

Flame's complexity allows the attack to have a wide range of abilities. These capabilities may include features such as capturing screenshots, recording audio, recording keyboard inputs, playing documents, and even communicating with nearby devices via Bluetooth. Flame spreads by exploiting weaknesses in target systems and contains an advanced encryption and obfuscation mechanism that is difficult to discover. The Flame attack caused a huge shock to the cybersecurity community, and its complexity demonstrated how sophisticated state-sponsored attacks can be. Developing and strengthening defense mechanisms against such attacks is critical to increasing resistance against similar attacks (Bıçakçı, 2014).

A new one is added to the observed cyber incidents every year, making Flame the largest and most complex type of attack and the largest and most complex cyber espionage malware developed to carry out targeted attacks. Although this malware collects information in cyberspace, it has not been detected for years, and the reason why it has not been detected for a long time is that it constantly updates itself. What distinguishes this malware, discovered in 2012, from other malware is that it is very large and modular. When SyS Lab (Cryptology and System Security Lab) detected Flame Cry, it reported that it had been running for at least 5 years and that it had at least 5 encryption types, 3 compression types, at least 5 file formats, and proprietary code injection methods. This malware not only has advanced capabilities to obtain and produce data without permission but also infiltrates every computer function to obtain the information it needs. Compared to Stuxnet, Flame's architecture is 20 times more complex. According to research, more than 600 institutions and organizations, academic institutions, government methods, and more than 1,000 computers, including Iran and some Middle Eastern countries, have been affected (Holat, 2021). The famous Russian anti-virus company Kaspersky insists that the Flame malware was developed using stronger, more complex, and better technology than any cyber-attack that has ever existed. Flame viruses can infiltrate systems via the Internet and access computer interfaces without users' knowledge. This remote malware can record audio using

a microphone. It sends all the information it receives back to its source via the Internet, and it is not known how much information it receives (Çatal, 2015).

3.6.5. Conficker

Conficker is a malware attack discovered in 2008 and generally classified as a worm. This attack is known as a worm that spreads by targeting computers with the Microsoft Windows operating system and taking control of the infected systems.

Conficker is highly effective and complex in terms of its propagation methods and infection capabilities. It attracts attention with its ability to update itself after infecting the system. In this way, it can renew itself even when security measures are increased or security vulnerabilities are closed. The attack has the potential to have a large-scale impact, especially by spreading through computer networks. Conficker creates a large botnet by forcing infected computers to connect to a control point. This botnet can be used to carry out malicious activities, steal information, or perform other harmful actions. Conficker's speed of spread and its ability to control the systems it infects have caused this attack to pose a serious threat. Microsoft and other security companies have attempted to protect users by providing security patches and removal tools against Conficker. However, such attacks have been a reminder that computer users and security experts must constantly keep their security measures up to date (Schmidt, 2012).

Conficker, also known as Downup, Downadup, and Kido, was discovered in October 2008 and is a software worm targeting Microsoft Windows operating systems. This worm infected Windows users' computers through a buffer overflow vulnerability. Conficker cracks passwords using a specially designed remote procedure call (RPC) request to execute code on target computers and can exploit vulnerabilities to spread spam and malicious code. Once this virus takes over the computer, it blocks system services such as Windows Automatic Updates, Windows Security Center, Windows Defender, and Windows Error Reporting, as well as installs other malware and allows malicious parties to access private information (Goztepe et al., 2014). Conficker, an international task force created to clean up this virus, estimates that this worm has more than 600 thousand IP addresses. This virus, which targets not only companies but also many personal users, acts as a web server. This malware, which infiltrated systems with the Joint Photographic Experts Group (JPG) extension, has infected millions of computers worldwide and is known as one of the worms

that have infected the most computers to date. To combat the virus, Microsoft formed the Konficker Challenge and Technology Industry Collaborative in 2009 and offered a $250,000 reward to find the developer or developers of the.

3.6.6. Sony

The world-famous Sony Pictures comedy movie "The Interview," which tells the story of the assassination of North Korean leader Kim Jong-un, turned into a full-fledged case of cyber terrorism. Because of this killer comedy, Sony faced a major cyber-attack. First, skulls began appearing on the screens of Sony employees, and in the following days, Sony's internal networks were destroyed by a sophisticated attack. In the following days, a group calling itself pacifist claimed that they carried out the attack. This group claimed that more than 100 terabytes of confidential Sony data were compromised. Although North Korea was held responsible for the attacks, a North Korean representative denied the accusation but supported the attacks and congratulated the 4,444 attackers (Ünal, 2015). As a result of this attack, some Sony Pictures films were shared on the Internet before they were released and were illegally downloaded and watched millions of times. So, Sony suffered a loss of one million dollars. The salaries of more than 6 thousand employees worldwide, including 17 managers, have been published. Senior management discussions were leaked, and in addition to the financial loss, Sony's reputation was also damaged. Despite the worsening situation, the film's leads, Seth Rogan and James Franco, continued to mock the attackers (McCormack, 2015).

In summary, Sony was exposed to a large-scale cyber-attack in 2014. This attack targeted Sony Pictures Entertainment's networks. The attack had a far-reaching impact, targeting Sony's film production division, employees' personal information, and internal communications. The cyber-attack was claimed by a group called "Guardians of Peace." After carrying out the attack, this group stole Sony Pictures Entertainment's internal information and leaked many sensitive documents. Attackers exposed large amounts of data, including movie scripts, internal emails, financial information, and employees' personal information. This attack received widespread coverage in the cybersecurity community and media, with a particular focus on internal security measures, data protection policies, and cybersecurity strategies. Following the attack, Sony took steps to strengthen its security measures and sought to increase its resilience against similar incidents. The Sony Pictures

cyberattack has increased awareness of cybersecurity issues among the public and companies and highlighted how important cybersecurity policies are. Companies must constantly update and strengthen their defense mechanisms against similar attacks (Daugirdas and Mortenson, 2015).

3.6.7. Bangladesh Profiteer

Although the source of the cyber-attack on the central bank of Bangladesh in March 2016 is not clear, it is said that North Korea was behind it by entering the bank's accounts and transferring 81 million dollars from the bank's accounts to the USA in 2016. The authorities noticed this, and the escalation of the theft was prevented. It is still unclear who committed this theft, which has become one of the biggest cyber robberies in history. Dor, founder and president of the cybersecurity firm RDeye, said that the software used in the Sony attack was also used in the attack. Dor also claimed that the attack on the bank was carried out after two years of planning (Valeriano and Maness, 2014). An Israeli official claimed that this attack could only be carried out with national support. The bank's CEO, Atiur Rahman, resigned following the robbery. Viewing the cyber robbery as an "earthquake," Rahman said the bank quickly alerted domestic and foreign intelligence agencies and called in international experts to investigate the situation. According to the first data found in the Case, the attackers infiltrated the bank's servers and transferred $30 million of the money they seized to the account of a casino owner in the Philippines (Hatipoğlu, 2021).

The cyber-attack that Bangladesh Bank suffered in 2016 was recorded as one of the biggest cyber robberies in its history. The main target of the attack was the bank's foreign currency reserves obtained from the Federal Reserve account in America. The attack consisted of a series of complex and coordinated steps. The cyber-attack started through a trojan, which is malicious software that runs in a virtual environment. This trojan infiltrated the bank's computer networks and transferred foreign currency via the SWIFT (Society for Worldwide Interbank Financial Telecommunication) system. SWIFT is a secure communication platform used by financial institutions around the world to transfer money (Boztaş, 2012). Using this trojan, attackers successfully transferred large amounts of foreign currency and thus seized millions of dollars. The emergence and stopping of the incident depended on the Bangladesh Bank's cooperation with many international financial

institutions and authorities and its rapid awareness of this situation. The Bangladesh Bank cyber-attack once again emphasized how critical cybersecurity measures are in the financial sector. To prevent similar incidents and be resilient against such attacks, financial institutions must implement a variety of security measures, such as strong encryption, security software, network monitoring systems, and staff training. At the same time, international cooperation and information sharing are also important to strengthen cybersecurity (Zahra et al., 2022).

3.6.8. National Security Agency Leak

One of the most prominent and large-scale cyber-attacks to date is the incident carried out by Edward Snowden in 2013, which caused the leak of confidential documents of the National Security Agency (NSA) (Karaarslan, 2019).

Edward Snowden was a systems administrator working for the NSA, and his classified documents contained stunning information about the extensive surveillance and espionage programs the United States runs. By leaking this information to the press, Snowden revealed that the NSA was monitoring the personal contact data and internet activities of millions of people (Carroll and Windle, 2018). This was met with great shock and concern, especially by America's allies and the wider public around the world. The leaked documents sparked a wide-ranging debate about security and privacy issues around the world. Additionally, technology companies and non-governmental organizations have called for stronger security measures and transparency to protect the data privacy rights of individuals and users. This incident started a global conversation around cybersecurity, freedom of information, and privacy. The documents leaked by Snowden led to policy changes in the field of cybersecurity in many countries and triggered efforts to advocate stronger control mechanisms and user rights (Broadhurst and Chang, 2012).

In August 2016, the US National Security Agency (NSA) was subjected to a cyber-attack. Cyber materials developed by the country's cybersecurity experts and used in espionage activities were leaked to the internet. An agent working in NASA's Special Access Operations (TAO) department, which is responsible for hacking operations, said that these materials are extremely dangerous for the security of large institutions, organizations, and states because they are sold on the Internet. Although the question of who or what caused the leak remains unresolved, some experts suspect government hackers, while others say it

was the result of intentional or unintentional errors by NSA employees. The investigation into the case continued, but the main suspects were Russian hackers who leaked information about President Donald Trump to the world by launching cyber-attacks on the Democratic National Congress (DNC) (Karasoy and Gezici, 2023). He suspected that this information was spread on the Internet because of the mistake of an NSA official, a former TAO official told the media. This statement can be considered as an indication that the digital environment in which TAO employees work is not secure enough. Another claim that emerged from the leak is that every NSA employee obtained this information from outside. A group calling itself Shadow Brokers and claiming responsibility for the leak released some of the seized files and put them up for auction. They said that when these files reach 570 million dollars, they will reveal the remaining information to the world. However, this offer did not attract much attention from cyber weapons dealers, and only $981 was offered (Aslay, 2017).

3.6.9. Spyware Placed on Hard Drives

It has been reported that the US National Security Agency has installed spyware on hard drives produced by some companies to monitor the transactions on these devices. Security company Kaspersky, which disclosed the spyware that appeared on the computers of companies such as Western Digital, Seagate, Micron, Samsung, and Toshiba, reported that it affected many computers in 30 countries, that it was a Stuxnet-like spyware and that it was made by a group called “Equation Group.” He also said it was part of an operation that had been going on for 20 years. The company in question also stated that this spyware has the most advanced techniques of any spyware ever produced and has been developed very professionally in terms of obtaining and hiding information. This spyware can bypass steps such as virus scanning and disk formatting because hard drives can be overwritten by the software (Tek, 2022). Additionally, it can both spy/track and steal data as long as it is connected to the internet. The countries most affected by this software are Iran, Russia, Pakistan, Afghanistan, China, Mali, Syria, Yemen, and Algeria. It was determined that this spyware targeted banks, telecommunications companies, energy companies, nuclear research companies, media companies, and institutions affiliated with religious groups, as well as military and public institutions and organizations. Although there is no information on how the software was placed on the disks, it has been suggested that the placement may be physical and that the NSA may have requested the source code from the people who produced the software or that the software may have been leaked. The companies that

developed this software, Western Digital, Seagate, and Toshiba, said that they were not aware of such an incident, while other companies did not comment. There is a high probability that the NSA behind espionage on this scale will damage trust in the USA and leave American IT companies in a very difficult situation (Torun and Torun, 2022).

Spyware placed on hard drives describes a type of cyber-attack that targets computer systems and often focuses on stealthily stealing information. These types of attacks involve malware intended to capture, monitor, or manipulate sensitive data of users or organizations. This software often tries to operate for long periods of time without the victim noticing (Wazid et al., 2013). Spyware placed on hard drives can often infect computer systems through methods such as email attachments, malicious websites, or infectious USB devices. By placing this software on the victim's computer, attackers can hijack the system and perform various espionage activities. Such spyware can often have the following capabilities (Belous and Saladukha, 2020):

- Data stealing: It can steal users' personal information, financial data, or corporate information.
- Remote control: It allows attackers to control and manage the victim's computer remotely.
- Monitoring: It can monitor keyboard inputs, screenshots, or other user interactions.
- Privacy violation: It can violate the privacy of personal space by controlling cameras or microphones.
- Malicious activities: It may perform harmful actions on the system, encrypt files, or waste system resources.

Security software, up-to-date anti-virus programs, and security patches should be used to prevent such attacks. Additionally, it is important for users to be aware of computer security and avoid suspicious links, emails, and file attachments (Tek, 2022).

3.6.10. WannaCry

The "WannaCry" ransomware cyber-attack, which took effect on May 12, 2017, brought the global problem to the agenda again. The sudden shock of cyber-attacks showed the whole world how invisible they have become and how they have become a global problem. China, India, and Russia lead the way. This large-scale attack, which also affected

critical infrastructures from the USA to the UK, shocked many countries. Such large and powerful attacks, which can remain active for a long time and have a significantly prolonged effect, can endanger health and security systems. Similar attacks are also observed in cyberspace, where such critical infrastructures are interconnected, sending threat signals to countries at all levels. This ransomware, whose source or identity is unknown, first encrypts data and then demands a ransom of between $300 and $600 to decrypt this data (Ghafur et al., 2019). WannaCry was distributed via an infected file, often sent as a spam attachment. But what makes it different from other ransomware is that it can spread to all machines on the network by finding a weak spot in Windows security. As we mentioned above, Russia is one of the countries affected by this attack (Avcı, 2023). The country's public institutions, such as banks, the Ministry of Internal Affairs and Health, and the State Railways, were affected. Taiwan and Ukraine follow Russia in the number of attacks. England was most affected by the attack. The country's National Health Service (NHS) collapsed, and some car manufacturers were forced to halt production. This attack affected Türkiye less than other countries. Türkiye was the country most affected in the first two hours of the attack. Türkiye, which fell to 8th place on May 12, fell to 14th place at the beginning of the week. According to the statement of ESET Türkiye Deputy Director Alev Akkoyunlu, widespread use in Türkiye is among the target countries (Çelik and Çeliktaş, 2017).

In summary, WannaCry was a ransomware that caused a significant cyber-attack worldwide in 2017 and affected thousands of computers. This attack caused widespread damage across many industries and countries. The attack is known as ransomware because it infiltrates computer systems, encrypts files, and asks users to pay a certain amount of cryptocurrency (usually Bitcoin). The WannaCry attack targeted the Microsoft Windows operating system and exploited an NSA-discovered vulnerability called EternalBlue to infect computers (Mohurle and Patil, 2017). WannaCry specifically targeted critical infrastructures such as healthcare institutions, financial institutions, and telecommunications companies. It blocked access to users by locking computers and encrypting files. A ransom was then demanded to ensure that the files were opened or the computers were released unless the ransom was paid. The large-scale impact of the attack forced many countries and companies to take emergency measures. Microsoft quickly attempted to close the vulnerability by releasing a security patch. The WannaCry attack increased cybersecurity awareness, causing companies and individuals to review and strengthen their security measures. It has also led

to calls for more effective global cooperation against similar types of attacks (Ghafur et al., 2019).

3.6.11. SQL Injection

This type of attack, which attacks with Structured Query Language (SQL) query language constructs, targets the query operation executed by a database. Methods to bypass login pages, clone a database, and even execute commands on the Windows operating system are being explored using SQL injection (Halfond et al., 2006). In web applications, unauthorized persons can access system data by examining the query commands specified to execute database queries. A SQL injection vulnerability affects the SCADA history database due to improper or inadequate filtering of human input that does not ensure the integrity of special characters used in the SQL query language. For example, a malicious user can gain arbitrary read/write access to a database by adding a literal escape character to a database query. SQL statements are used for security checks such as authentication and to ensure communication between databases (Polat and Bülbül, 2023). SQL injection can abuse the database by sending SQL commands to the database. If a database-backed job can retrieve data from a server using a trusted network, it is a target for SQL injection. For example, a client application may use an isolated DMZ (Demilitarized Zone), which is a physical or logical subnet that contains services exposed to external networks and exposes those services to a larger, unprotected network, such as the Internet, as shown in Figure 2.5. If you connect to a database on a secure network using a web server, SQL injection attacks can be performed on the SQL server over the secure network. In the event of a serious cyber-attack, even if security measures cut off all other connections to the server, the attacker can still access and hijack SQL Server over a trusted network (Kara et al., 2023).

SQL injection is a type of cyber-attack that is considered one of the vulnerabilities of web applications and allows malicious actors to gain access to sensitive data. This attack occurs when the data entered by the user is not processed or checked correctly. In this type of attack, the attacker inadvertently gains access to the database by inserting malicious SQL codes into the web application's database queries. For example, let's consider a web application that processes data coming through a web form. If this application directly inserts the incoming data into an SQL query without adequately validating or cleaning it, the attacker can take advantage of this point and damage the database through the malicious

SQL codes he added. With SQL injection, an attacker can steal information from the database, add data to the database, modify existing data, or, in some cases, even perform malicious actions such as deleting the database (Katole et al., 2018).

To protect against such attacks, it is important for web applications to properly validate and sanitize input data, use parameterized queries, and take preventative measures such as firewalls. Additionally, detecting and closing possible SQL injection vulnerabilities by regularly performing security tests and code audits is a critical security measure (Tobin et al., 2015).

3.7. National Cybersecurity

National Cybersecurity is a concept that aims to protect a country's information and communication technologies, computer systems, and digital infrastructure. Threats occurring in this area generally include cyber-attacks, information leaks, malware attacks, and similar digital threats. National Cybersecurity includes a strategic and technical approach that aims to ensure the security of information systems used in various sectors of the state and society (Hekim and Başıbüyük, 2013).

Countries take various measures to strengthen their national security strategies and policies against cyber threats, increase resistance to cyber-attacks, and protect their digital infrastructures. In this context, cybersecurity teams are formed, cybersecurity standards and guidelines are developed, systems for the detection and prevention of cyber-attacks are established, and information-sharing mechanisms are established (Ünver, 2017). National Cybersecurity is also of great importance at the international level. Because cyber threats often have a character that transcends borders. A cyber-attack in one country can also affect other countries. Therefore, international cooperation and information sharing constitute an important part of national cybersecurity strategies (Aydın et al., 2021).

Cybersecurity is a shared responsibility between governments, private sector organizations, and individuals. A strong national cybersecurity infrastructure is critical to ensuring the digital security of both the state and its citizens. In this context, constantly updated cybersecurity policies, information sharing, training programs, and technological innovations are important elements to ensure national cybersecurity (Gündoğdu, 2023).

3.8. National Cybersecurity Strategy

National Cybersecurity Strategy refers to a comprehensive approach that a country adopts against cyber threats. This strategy includes objectives, policies, plans, and measures for using information and communication technologies and protecting digital infrastructures. Creating a country's national cybersecurity strategy aims to develop an effective combat strategy against cyber threats (Aslay, 2017).

The National Cyber Security Strategy consists of basic elements (Kurnaz and Önen, 2019). First and foremost, a thorough analysis and evaluation of a country's cyber risks is required. This process aims to identify potential threats and vulnerabilities by assessing the security of the country's digital infrastructure. The national cyber security strategy determines the country's cyber security goals as well as the policies that will be used to achieve them. These goals frequently include safeguarding digital infrastructures, increasing resilience to cyber-attacks, and effectively combating cyber threats. The legal framework and regulations establish the national cyber security strategy, as well as legal regulations and policy frameworks for cyberspace. This includes sanctions, liabilities, and penalties for cyberattacks. The national cybersecurity strategy promotes cooperation and coordination among government agencies, the private sector, academic institutions, and other stakeholders. This encourages information sharing and collaboration on cybersecurity issues. The strategy for education and awareness includes developing training programs and campaigns to raise cybersecurity awareness and educate the public. This initiative aims to raise cybersecurity awareness among individuals, institutions, and the public sector. Finally, in technological innovation, it strategically encourages technological developments in the field of cyber security and aims to create the necessary technological infrastructure to strengthen the country's defense capability (Aslay, 2017; Kurnaz and Önen, 2019).

The National Cybersecurity Strategy is a critical tool to ensure that the government, private sector, and other stakeholders work collaboratively to create a stronger defense mechanism against cyber threats. This strategy should be regularly reviewed and updated to adapt to updated threats and technological developments (Sağıroğlu and Alkan, 2018).

3.9. Türkiye Cybersecurity Strategy and Action Plans

Türkiye has developed a series of strategies and action plans to counter major threats to cybersecurity, strengthen digital infrastructures, and raise public awareness against cyber threats. These efforts were generally carried out within the scope of Information and Communication Technologies (ICT) Strategy and Action Plans (Kurnaz and Önen, 2019).

Such strategies and action plans contain a variety of elements. Türkiye conducts regular risk analysis and assessment studies to detect cyber threats and understand vulnerabilities in digital infrastructure. Furthermore, Türkiye implements the necessary legal regulations to support cyber security. This includes sanctions, responsibilities, and penalties for combating cybercrime. Regarding institutional cooperation, various mechanisms are being developed to strengthen collaboration between Türkiye's public and private sectors. This collaboration seeks to develop a more effective defense mechanism against cyber threats (Aldemir and Kaya, 2020). Türkiye organizes training programs and awareness campaigns to raise cybersecurity awareness and educate the public. In terms of technological innovation, Türkiye promotes technological developments in the field of cyber security and aims to build the technological infrastructure required to strengthen the country's defense capacity. Türkiye promotes international cooperation in cyber security and aims to meet international standards (Bıçakçı et al., 2015).

Türkiye's cybersecurity strategy and action plans aim to ensure that the government, private sector, and other stakeholders come together to create a stronger defense mechanism against cyber threats. However, security strategies and action plans may be updated over time, so it is important to consult official sources to obtain the most up-to-date information (Öcal, 2022).

The 2020-2023 National Cybersecurity Strategy and Action Plan was published in the Official Gazette on 29 December 2020 and numbered 31349. The action plan consists of 12 sections in total, and the service-specific part has not been disclosed to the public in the form of tables. In the executive summary, it is stated that the level of development in national cybersecurity is very high, national strategies must be strong to catch up with the developments, and the action plan covers the targets, actions, and policies for the next four years in line with Türkiye's vision and mission in the field of cybersecurity and is based on the results obtained from previous action plans. It was stated that the progress made should be carried out further. The actions that were implemented and should be carried out periodically within the scope of the action plan covering

the 2013-2014 and 2016-2019 periods were reviewed. Thus, within the scope of the current situation and the studies carried out, the new action plan aims to improve the old action plans and eliminate their deficiencies. A Preparatory Workshop was organized with the participation of national stakeholders to determine the actions to achieve the planned gains in line with the strategic objectives. 127 participants from 67 institutions attended the workshops in question. In the second part of the action plan, definitions regarding the concepts are included. The third section contains the introduction part of the action plan, and developments around the world are evaluated. In Türkiye, it is aimed to reduce risks with studies under the heading of cybersecurity, and legislation, critical infrastructures, response to cyber incidents, and awareness studies are carried out with the 2013-2014 Action Plan, the National Cyber Incident Response Center (USOM) was established in 2013, and the 2016-2019 National Cyber In addition to the old plan, the Security Strategy and Action Plan includes determinations and evaluations that aim to combat cybercrimes, develop human resources, establish a cybersecurity ecosystem, show progress in the International Telecommunication Union Global Cybersecurity Index, and have similar objectives in the action plan covering the 2020-2023 period. The vision of the action plan is given as: "To support the development of the country's economy, the protection of social life and the provision of national security; "To have a securely functioning cyber environment in our country and to become an international brand in cybersecurity." and its mission is "To carry out studies in coordination with all relevant stakeholders to protect our assets in cyberspace, especially our critical infrastructures, from threats and to reduce the possible effects of cyber incidents, with the awareness that cybersecurity is an integral part of our national security." The principles of the 2020-2023 Period Action Plan include the relationship between cybersecurity and national security, continuity of project execution, the importance of cybersecurity, cooperation between stakeholders, transparency, accountability and ethical values, critical infrastructures, cyber security-based designs, confidentiality, integrity-accessibility issues, Attention was drawn to the issues of legal infrastructure, R&D and the use of domestic products and services (Karasoy and Babaoğlu, 2021).

Cybersecurity is one of the most discussed and researched topics of the last twenty years. News can be found every day, and the scope and importance of this topic are likely to continue for a long time. This shows that countries intervene more strongly, try to improve their technologies, and constantly face cyber-attacks or threats. For this reason, countries prepare action plans, strategies, and guidance documents to act more systematically and get involved in the field of cybersecurity. Türkiye's 2013-2014, 2016-2019, and 2020-2023 action plans will be reviewed according to the 11 evaluation criteria explained in the previous

paragraph, and finally, recommendations will be made after all plans are discussed together. Although there is continuity in the National Cybersecurity Strategy and Action Plan 2020-2023, it violated the temporary continuity principle published at the end of 2020. The Action Plan defines critical infrastructures such as electronic communications, energy, finance, and transportation. The aim of this action plan, as in other action plans, is to become a leading country by supporting research and development as well as the development of domestic products. In the action plan, international cooperation was defined as one of the main goals, and special attention was given to cooperation and support mechanisms in technological development. The action plan for the years 2020-2023, as in other action plans, included activities to strengthen and train human resources. This action plan does not include targets for the development of the legal infrastructure. This action plan, for which no budget was allocated, aimed for the first time to reduce cybercrimes by increasing deterrence. So far, no document regarding the monitoring of the action plan has been published. Briefly, it is possible to state that the content of the criteria and action plans is presented in the table below (Table 1.1) (Çakır and Taşer, 2023; Karasoy and Babaoğlu, 2021).

Table 1.1. Content of Türkiye Action Plans (Çakır and Uzun, 2021)

Action Plan Period	Continuity	Protection of Critical Infrastructures	R&D Supports	Leadership in Cyberspace	National and International Cooperation
2013-2014 Period	It is the first plan.	Critical infrastructures are not defined and are intended to be protected.	It is targeted specifically for domestic technologies.	It is aimed to conduct an international exercise.	Cooperation with both local and international actors is targeted.
2016-2019 Period	There is a 1-year break in between.	Critical infrastructures are not defined and are intended to be protected.	Support and coordination of domestic product R&D studies and protection of R&D outputs are included.	There is no statement on this subject in the document.	Information sharing-based cooperation and international cyber incident management cooperation with all stakeholders are aimed.
2020-2023 Period	There is continuity. However, it was published at the end of 2020.	Critical infrastructures have been determined, and the main goal for its protection has been included.	It was stated that R&D and development of domestic products would be supported.	The goal of becoming a leading country is included in this action plan.	International cooperation has been set as a goal.

3.9.1. Mission

To determine effective and continuous policies and to implement them by ensuring coordination to ensure National Cybersecurity (DDO, 2023).

3.9.2. Vision

To contribute to the prosperity and security of citizens and the development and efficiency of the country's economy; in this case, in order to benefit from ICTs in the most effective way, it is necessary to cooperate with all stakeholders in terms of cybersecurity and create an ecosystem that is an international competitive power in the cybersecurity environment, where risks and threats in the cyber environment are competently managed (Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 2023).

3.9.3. Aim

The main goal of this National Cybersecurity Strategy and Action Plan is; it is the awareness that cybersecurity and national security are a single piece in all sectors and the full acquisition of competencies to take managerial and technological measures to ensure the security of stakeholders with the systems existing in the national cyber environment. To achieve this basic goal, determining, realizing, and controlling the objectives and sub-action plans are also among the objectives of this document (Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 2023).

3.9.4. Update

Developing technologies will be kept up to date with the coordination to be provided at the national level for the demands of the private sector and the public, considering the changing conditions and needs, and the actions that do not end in 2023 will be transferred to the next action plan (Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 2023).

4. CYBERSECURITY COMMUNICATION POLICIES

Cybersecurity has become an important issue for individuals, institutions, and states today. The rapid development of information technologies and the spread of digitalization have increased cyber threats and increased risks in this area (Kişman and Güleç, 2021).

Cybersecurity communication strategies seek to raise an institution's or individual's awareness of cybersecurity, strengthen defense against threats, and establish effective communication (Topçu, 2022). The goal of cyber security communication strategies in education and awareness is to make employees and users aware of cyber threats. Training programs aim to raise awareness about topics like safe internet use, password management, and phishing. In addition, an institution or organization must have a good communication plan in case of a cyber-attack. (Yıldırım, 2018) describes a plan that regulates internal and external communication, as well as strengthens communication with stakeholders during crisis situations. Cybersecurity strategies should incorporate current technology and infrastructure security solutions. Many precautions must be taken, including firewalls, security software, regular security scans, and up-to-date backup systems. Finally, organizations must assess cyber risks and develop an effective risk management policy to mitigate these risks. This includes identifying potential threats, assessing risks, and taking the necessary precautions. In this process, cyber security is more than just an internal concern for an organization. Collaboration should include clear communication with industry partners, government agencies, and other stakeholders. When an attack occurs, the organization must have a policy in place to recover quickly and resume normal operations. This phase focuses on learning from security incidents and strengthening resilience against future attacks (Topçu, 2022; Yıldırım, 2018).

Cybersecurity communication policies should be treated as a continuous process and updated against changing threats. An effective cybersecurity policy should include not only technological measures but also the human factor and continuous improvement. Cybersecurity communication policies are a concept of great importance for individuals, institutions, and states in today's digital age. The rapid development of information technologies and the spread of digitalization have increased cyber threats and revealed the need to fight effectively against these threats. In this context, the importance of cybersecurity communication policies stands out at several basic points. First, cybersecurity

communication policies aim to raise awareness. Unless users and employees are aware of cyber threats, it is difficult to effectively implement defense mechanisms (Topçu, 2022). Through education and awareness campaigns, individuals become more sensitive to cyber dangers, and security awareness increases. Secondly, cybersecurity communication policies aim to ensure effective communication in crisis situations. When cyber-attacks or security incidents occur, a rapid and coordinated communications policy is critical to limiting damage and accelerating recovery. These policies support transparent and reliable communication with internal and external stakeholders. Third, cybersecurity communication policies emphasize the ability to adapt to constantly evolving threats. As cyber threats are constantly evolving, it is important that security policies keep up with this change. Policies that act proactively against innovative threats strengthen defense mechanisms and create a security infrastructure that is more resistant to attacks (Köksoy, 2020).

As a result, cybersecurity communication policies not only increase the cybersecurity of an organization or individual but also contribute to the creation of a digital security culture in general. These strategies aim to effectively prepare for and cope with the security challenges faced by the information society, which plays a critical role in creating a secure environment in the digital world (Öcal, 2022).

4.1. Transparency and Accuracy

Cybersecurity communication plays a critical role in ensuring trust between institutions and individuals and in sharing information accurately and effectively. In this context, the principles of transparency and accuracy are some of the cornerstones of cybersecurity communication (Nurse et al., 2011).

Transparency refers to clear and understandable communication about cybersecurity-related events, risks, and security measures. Institutions should communicate their cybersecurity policies, risks, and measures taken through transparent communication with their users, customers, and other stakeholders. A transparent approach builds trust in society and industry regarding cybersecurity and enables more effective crisis communication in times of crisis. Transparency also plays an important role among employees within the organization. Employees are more motivated to understand and comply with security policies in a transparent corporate culture. Transparent information sharing and internal

communication increase internal security and improve security awareness (Pappas et al., 2019).

Integrity refers to the use of true and reliable information in cybersecurity-related communications. Correct information prevents misunderstandings and wrong decisions. Especially in situations where security incidents occur, accurate information flow plays a critical role in incident response and recovery processes (Ocak, 2021). The principle of accuracy is also important in creating defense strategies against cyber threats. An institution that acts with real and accurate information can evaluate threats more effectively and create a stronger defense mechanism against these threats. In addition, the principle of accuracy is of great importance in measuring the impact of security measures and managing improvement processes (Tate, 2022).

The principle of accuracy and transparency is fundamental to my proposed communication model since it supports public confidence in cybersecurity measures (Figure 6.1). Organizations can promote transparency and ensure accuracy in safeguarding against misinformation, enabling informed decision-making and risk mitigation, by offering transparent measurements of cyber threats and regularly updating the public.

4.2. Appropriate Language Use

The use of language in cybersecurity communication is of great importance in ensuring that information transfer is understandable, effective, and accurate.

It is critical to use appropriate language to ensure that users and stakeholders are aware of cybersecurity issues, understand risks, and comply with security policies (Ergan and Ergan, 2021). Cybersecurity terms and concepts are frequently technical in nature, making them difficult for general users to understand. The language used in communication must be understandable in order to simplify technical terms and appeal to a large audience. Reducing complexity in information sharing allows users to better understand security issues. On the other hand, information about cyber security is generally serious, allowing users to form an emotional bond with the subject. An emotional tone in language can encourage users to pay closer attention to security concerns and take the necessary precautions. However, it is critical that this emotional tone does not go overboard and cause unnecessary anxiety. Cybersecurity communication frequently includes education and awareness campaigns. To

ensure the success of these campaigns, the language used must be educational and informative. An interesting and informative language that is similar to everyday language makes users more vulnerable to security threats. Ambiguity and ambiguity about information security are not acceptable in cybersecurity communication. Clear, precise, and unambiguous language provides users with clear instructions on what precautions to take. This improves compliance with security policies. Providing cybersecurity practice tips directly to users ensures that general security information is useful and applicable in their daily lives. Associating language with daily experiences can help users better adopt cybersecurity principles (Ergan and Ergan, 2021; Ramirez and Choucri, 2016).

The use of language in cybersecurity communication is an important part of a clear and effective communication policy that can appeal to a wide audience, including non-technical users. This can increase awareness, strengthen the adoption of security policies, and contribute to an overall safer digital environment (Quigley et al., 2015). Proposed communication model highlights how important it is to communicate cyber threat information to a variety of groups using understandable language (Figure 6.1). It is a key element for having an effective communication policy. Organizations can only improve understanding and engagement by steering clear of technical jargon and embracing a user-centric approach. This will help to cultivate a proactive cybersecurity awareness and resilience culture.

4.3. Existence of Emergency Plans and Communication Protocols

Emergency Plans and Communication Protocols play an important role in the field of cybersecurity. These plans determine how an organization will respond to a cyber-attack or other emergency and regulate the methods to communicate during this process (Ocak, 2021). These plans are indispensable for organizational resilience and crisis management. The preparation of emergency plans is to guide cybersecurity teams and stakeholders through structured responses to threats. These plans, carefully outlining step-by-step procedures, ensure swift and coordinated action in the face of cyber-attacks. At the same time, communication protocols establish the framework for efficient dissemination of information, determining channels, tools, and stakeholders involved in the process.

Moreover, the delineation of team member roles within these protocols enhances coordination and clarity during crises. Centralized management of communications,

overseen by designated leaders, fosters efficient information flow and coordination among teams. Strong preparedness plans, in line with my proposed communication model, offer organizations the capacity to respond to cyber threats quickly and effectively (Figure 6.1). These plans support public confidence and minimize potential disruptions by providing preparedness and response plans.

4.4. Collaboration With Social Media Platforms

Cybersecurity is an issue that is becoming increasingly important in today's digital age. With the rapid development of information and communication technologies, cyber threats are also increasing. At this point, cybersecurity communication, combined with social media management, plays a critical role in protecting an institution or individual's digital existence (Khidzir et al., 2016).

Social media platforms provide the opportunity to reach a wide audience quickly. However, this also attracts the attention of malicious individuals and institutions. Cyber-attacks can be carried out via social media through methods such as social engineering and information stealing. Therefore, communication strategies regarding cybersecurity should be integrated with social media management (Mete, 2021).

Several elements are required to ensure effective cybersecurity communication via social media. The first goal is to raise awareness and educate people. Users, employees, and stakeholders must be aware of cybersecurity. A community that is aware of fake news and fraudulent attempts spread via social media will be more resistant to cyber threats. Another option is communication strategy (Köseoğlu and Aydın, 2022). Institutions must be able to effectively communicate security policies via social media. At the same time, a communication policy should be developed to ensure timely and accurate information flow in the event of a cyber-attack (Van der Walt et al., 2018). The third key component is reputation management. Social media is a powerful tool that can have an impact on an organization's reputation, both positively and negatively. Ensuring accurate and reliable information flow in the event of a cyber-attack or data breach is critical for protecting the institution's reputation. Finally, incident response and crisis management are critical. In the event of a cyber-attack, social media can spread rapidly. Developing an effective incident response and crisis management strategy is crucial for minimizing damage to both users and organizations (Köseoğlu and Aydın, 2022; Van der Walt et al., 2018).

As a result, cybersecurity communication and social media management should be considered as complementary elements. Correct communication strategies and effective social media management can create a digital environment that is more resilient and secure against cyber threats (Labuschagne et al., 2011).

4.5. The Development of Education and Awareness Programs

Cybersecurity has become increasingly important today, with the increasing threats faced by individuals, institutions, and states in the digital environment (Tuğal et al., 2021). Therefore, training and awareness programs regarding cybersecurity are of great importance.

There are numerous basic points that demonstrate the significance of these programs. First and foremost, cyber security training teaches individuals to be more aware and cautious in the digital world. These programs teach users how to protect themselves from email scams, malware, and other online threats. Cybersecurity training reduces internal cybersecurity risk by teaching employees how to use strong passwords, avoid opening unknown email attachments, and understand other security measures. Another important consideration is data security. The data that institutions and individuals store digitally is extremely valuable. Training programs assist security-conscious users in managing data more securely (Sabillon et al., 2021). This ensures that sensitive information is kept secure from unauthorized access. Recognizing and preventing attacks is critical in cyber security training programs. Cybersecurity training teaches users how to recognize potential attacks and take precautions against them. This allows for faster detection of attacks and the implementation of precautions. Furthermore, users must be prepared for current threats, as digital threats are constantly evolving. Training programs teach participants how to prepare for current threats. This helps to build a stronger community against emerging malware and other types of attacks. Finally, cybersecurity education raises general awareness of cyber threats in society at large. This allows individuals and organizations to better understand their cyber security responsibilities and take a more active role in this area (Ünal and Ergen, 2018).

As a result, cybersecurity education and awareness programs play a critical role in making individuals, organizations, and communities safer from threats in the digital world. These programs, supported by continuous training and updated information, contribute to ensuring cybersecurity in a sustainable manner (Sabillon et al., 2021). This is the reason it is

an important component of communication policies emphasized in my proposed communication model. People can improve their digital literacy and become better equipped to identify, avoid, and handle cybersecurity threats by using easily accessible and educational resources (Figure 6.1).

4.6. Developing a Crisis Communication Capacity

Crisis communication is a strategic approach that covers the process of effectively managing challenging situations faced by an organization or individual and organizing communication in the process. These situations can often include unexpected events, disasters, risk of reputational damage, cyber-attacks, or other similar issues. Accurate and fast communication in times of crisis is of vital importance in protecting the reputation of organizations, maintaining trust, and accelerating the problem-solving processes (Hekim and Başıbüyük, 2013).

The main purpose of the crisis communication policy is to gain the trust and understanding of stakeholders by providing transparent, consistent, and effective communication in the face of negative situations. Crisis communication in cybersecurity refers to the process of communicating effectively when an organization's or individual's digital assets are in danger. Such situations are often associated with data breaches, malware attacks, service outages, or other cyber threats.

The first important consideration in cyber security crisis communication is a quick and effective response. A quick response during a crisis can help control the spread of the attack and reduce damage. Determining an effective communication strategy is equally important. Another example is openness and trust. Transparent communication during a crisis can help to maintain trust among customers, employees, and other stakeholders (Zhang and Borden, 2020). Taking responsibility and being transparent, rather than hiding negative situations, can help to strengthen one's reputation after a crisis. Sharing accurate and up-to-date information is also essential. A lack of information or misinformation can exacerbate the crisis's effects. Sharing current, accurate, and clear information quickly alleviates anxiety and uncertainty. Managing social media is an important aspect of crisis communication. In times of crisis, social media provides a quick way to reach large audiences. However, it is critical to effectively manage and control these platforms (Wang and Park, 2017). Sharing accurate information and correcting misconceptions on social media is critical. Stakeholder

communication should also be considered, as it is critical to communicate with customers, employees, shareholders, and other stakeholders during a crisis. Making a communication plan and sticking to it will help you manage the situation. As previously stated, training employees in cyber security ensures that they are prepared for potential crisis situations. Furthermore, raising public awareness of cyber threats promotes a more informed response during times of crisis. When a crisis occurs, it is critical to learn from the experience and improve procedures. This enables necessary corrections to be made to avoid a similar situation from occurring again (Wang and Park, 2017; Zhang and Borden, 2020).

Cybersecurity crisis communication requires a holistic approach that includes not only technical measures but also an effective communication strategy. This increases the chances of maintaining the trust of your organization and stakeholders and emerging stronger from the crisis (Boeke, 2018).

4.7. Investing on Reliable Sources and Communication Channels

Cybersecurity is an important problem faced by individuals, companies, and states today. With the rapid development of information technologies, cyber threats are also increasing, and it becomes important to develop effective communication policies to protect against these threats. In this context, reliable sources and communication channels play a critical role in sharing cybersecurity-related information.

Reliable sources are a key factor in obtaining accurate and up-to-date information. Reliable sources specialized in cybersecurity-related news, threat analyses, and protection methods play an important role in raising awareness of individuals, companies, and institutions. These sources include official websites of organizations specializing in cybersecurity, reports of security companies, and information obtained from cybersecurity conferences. Communication channels are also vital in sharing cybersecurity information. Secure and encrypted communication channels play an important role in protecting sensitive information. Platforms that discuss sensitive issues related to cybersecurity encourage effective communication, especially between security experts, companies, and government institutions. In addition, it is possible to increase cybersecurity awareness and reach large segments of society through platforms that reach large audiences, such as social media (Tekke and Lale, 2021).

Effective communication using reliable sources and communication channels provides better preparedness against cyber threats. In this way, individuals, companies, and government institutions become more resistant to cyber-attacks by strengthening their security measures. Providing reliable information correctly contributes to increasing cybersecurity awareness and making the digital environment a safer place in general (Kiraz, 2021).

4.8. Designing Interactive Feedback Mechanisms

In cybersecurity communication, interactive feedback mechanisms are important elements that support users and organizations in defending more effectively against cyber threats. These mechanisms improve security awareness by increasing information sharing, strengthening users' security habits, and allowing cybersecurity measures to be implemented more effectively (Bozkanat and Çömlekçi, 2020).

One of the key advantages of interactive feedback mechanisms is that they provide users with information about cyber threats in real-time. In this way, potential risks can be reacted quickly, and security measures can be updated instantly. Interactive feedback mechanisms that allow users to report suspicious activities or potential threats offer the security team the chance to prevent cyber-attacks with early warnings. Additionally, these mechanisms are an effective tool for educating users on cybersecurity policies and best practices (Figure 6.1). Providing users with feedback through interactive training, simulations, or awareness campaigns allows them to be more aware and ready against cyber threats (Loftus and Narman, 2023). This helps organizations strengthen their defense mechanisms, considering how critical the human factor is in their cybersecurity policy. Additionally, interactive feedback mechanisms encourage community building on cybersecurity issues. By increasing information sharing among users, a collective awareness can be created against cyber threats. This contributes to faster detection of vulnerabilities and the creation of an overall defense strategy thanks to shared information (Zhang and Borden, 2020).

As a result, interactive feedback mechanisms stand out as an effective tool in cybersecurity communication. Proper implementation of these mechanisms to make users more aware, encourage them to react quickly through early warning systems, and

continuously improve security measures contribute to creating a stronger defense against cyber threats (Khader et al., 2021).

4.9. Continuous Improvement and Evaluation

Cybersecurity emerges as a constantly changing field due to the rapid development of technology and the ever-evolving threats in the digital world. In this dynamic environment, continuous improvement and evaluation processes in cybersecurity communication play a critical role in updating and improving the security status of organizations, individuals, and institutions (Yurttaş and Güzel, 2023).

Continuous improvement is the review and improvement of cybersecurity policies, procedures, and technological measures over time. This process provides the ability to quickly adapt if new threats emerge or existing threats evolve. It also enables organizations to effectively revise their security policies, close security gaps, and maintain compliance with the latest technology and best practices. Evaluation processes aim to objectively evaluate the security situation of organizations and optimize security strategies using these evaluations (Aydın et al., 2021). These assessments are an important tool in identifying security weaknesses, evaluating the effectiveness of existing measures, and understanding the cybersecurity maturity of the organization. Regular implementation of these processes provides the opportunity to continuously raise the organization's security level and increase its capacity to adapt to changing threats. Continuous improvement and evaluation of cybersecurity communications also increase transparency and trust among stakeholders. These processes, which aim to show how committed organizations are to the security of customers and other stakeholders, contribute to the creation of a transparent security culture. It also reinforces the trust of internal and external stakeholders by demonstrating that cybersecurity strategies are effective and constantly improved (Yohanandhan et al., 2020).

As a result, continuous improvement and evaluation processes in cybersecurity communications help organizations increase their security levels and become more resilient to changing threats. These processes are of critical importance in keeping cybersecurity strategies up to date, increasing security awareness, and constantly evaluating the security status of organizations (Baumeister, 2010).

5. THE MEANS OF COMMUNICATION OF CYBER THREATS TO THE PUBLIC

Cyber threats pose a serious risk to individuals, companies, and states today. These threats increase with the widespread use of information technologies and can affect various segments of society. Communicating cyber threats to the public is an important element for transparency, awareness-raising, and effective combat (Demir, 2021).

Cybersecurity communication policies allow a company or individual to effectively communicate about cybersecurity issues. Effective communication policies are critical in today's world, where awareness of cybersecurity is growing, and threats in this field are constantly evolving. Raising awareness is essential for a successful communication policy. Campaigns and informational materials to raise awareness of cyber threats among employees, customers, and other stakeholders may be included in training to raise awareness about cybersecurity both within and outside the organization. The most important rule of effective communication is undoubtedly to use simple and understandable language (Hathaway et al., 2012). Technical terms should be avoided, and cybersecurity issues should be expressed in as simple and understandable a language as possible. This will make it easier for users of different levels to understand the issue and take appropriate action. Additionally, highlighting problems and solutions helps attract public attention. The emphasis should include not only the possible risks but also the measures and security policies taken against these risks. Communication should focus on strengthening the cybersecurity culture. This includes encouraging employees to pay more attention to security issues and integrate cybersecurity into their daily work processes. In the event of a cyber-attack, public notification channels should be prepared. Transparency is important to maintain customer trust and the reputation of the organization. At the same time, it is critical to share the precautions and updates implemented following the cyber-attack. Organizations should develop comprehensive communication plans outlining how they will communicate in the event of a cybersecurity incident (Al-Mohannadi et al., 2016). These plans should include communication policies for both internal and external stakeholders. In the event of a cybersecurity incident, organizations must be able to respond quickly and effectively. Being prepared for potential scenarios should be part of crisis communication strategies. Organizations can use cybersecurity communication policies to strengthen their security culture, inform stakeholders, and prepare for potential threats. These policies are critical in

raising cybersecurity awareness and creating a secure digital environment (Denning and Denning, 2010).

Communicating cyber threats to the public is critical for raising awareness of cybersecurity issues in society and institutions, encouraging them to be prepared for potential risks, and ensuring effective communication in crisis situations. An open and transparent approach to communicating cyber threats to the public aids in gaining society's trust. Explanations accompanied by detailed and understandable information increase public awareness and trust. In addition, press conferences and media relations in cases of cyber-attacks provide the opportunity to provide information to the public directly and effectively. It is important to make statements about cybersecurity measures and threats and measures taken through a reliable spokesperson. Social media and other online platforms, where people spend most of their time today, are one of the ways to communicate effectively against cyber threats. It is possible to instantly inform the public and share security measures through official accounts (Raiyn, 2014). This is because interactive websites and online portals about cyber threats provide users with the opportunity to provide information with interactive content and access security-related resources. Considering the managerial aspect of the situation, governments and large organizations need to be able to immediately announce cyber threats to the public by using emergency notification systems. These systems can deliver data via text messages, emails, or app notifications. Publicly available reports and analyses provide detailed information on the scope and impact of cyber threats, as well as the countermeasures implemented. Feedback and recommendations from security experts may be included in such reports. Collaboration and partnerships between the public and private sectors promote effective cybersecurity communication. Collaboration among stakeholders on security issues can result in a more comprehensive and robust cybersecurity awareness (Pipyros et al., 2014).

First, communicating cyber threats to the public increases society's general security awareness. When the public has accurate and up-to-date information about current cyber threats, individuals and organizations can protect themselves more effectively. This awareness is critical in terms of taking cybersecurity measures, developing safe internet usage habits, and creating a society that is more ready against threats. Transparency is also an important factor in combating cyber threats. Public communication helps us better understand the effects of cyber-attacks and evaluate the measures taken against these attacks

(Yanarışık, 2022). In addition, transparent communication creates reliability and trust, enabling society to support the fight against cyber threats carried out by the state or the private sector. Communicating cyber threats to the public encourages collaboration between cybersecurity experts, security companies, and government agencies. Information sharing, threat intelligence, and dissemination of best practices contribute to the creation of a collective security strategy. Since cyber-attacks can often affect many organizations, such collaborations are critical to improving society's overall cybersecurity. However, a careful balance is required when communicating cyber threats to the public. When sharing information, extreme transparency about the details of cyber-attacks and defense strategies can provide an advantage against attackers. Therefore, protecting sensitive information and sharing in a controlled manner are the basic elements of an effective cybersecurity strategy (Terzi, 2018).

As a result, communicating cyber threats to the public is a critical element for improving the overall security of society, ensuring transparency, encouraging cooperation, and creating effective combat strategies. This process increases cybersecurity awareness, helping society to resist cyber threats more resiliently (Ünal, 2021).

5.1. Press Releases and Media Communications

Press releases and media communications are key to an effective information and awareness policy in communicating cyber threats to the public. Since the media has the capacity to reach a wide audience, it is used as a powerful tool to ensure that society is prepared against cyber threats and to equip it with accurate information (Boholm, 2021).

Press releases are a way to provide information quickly and clearly about cybersecurity incidents or threats. Government agencies, cybersecurity companies, or other relevant organizations can inform the public about current threats through press releases. In these statements, important information may be shared, such as a summary of the incident, affected systems or data, precautions taken, and steps the community should take. Media communication is an important tool to increase social awareness against cyber threats and strengthen security awareness (Berg et al., 2021). Interviews, expert opinions, and analysis through trusted media outlets inform the public about the complexity and severity of cyber threats. At the same time, media communication can contribute to creating a culture of defense against cyber threats by encouraging individuals and institutions to increase security

measures. The media has a responsibility to convey accurate information about cyber-attacks. Therefore, it is important to share accurate and reliable information in cybersecurity-related news. In addition, content explaining the precautions and defense strategies taken against cyber threats enables society to act more consciously. However, media communications should avoid creating panic about cybersecurity incidents. Using accurate and balanced language allows society to access information and helps prevent unnecessary anxiety and fear (Lawson et al., 2016).

As a result, press releases and media communication play an important role in raising public awareness, strengthening protection measures, and creating an effective cybersecurity culture in the fight against cyber threats. A reliable and effective communication policy increases society's resilience against cyber threats.

5.2. Social Media and Website Use

The use of social media and websites in communicating cyber threats to the public plays a critical role in quickly informing the public, announcing security measures, and generally increasing cybersecurity awareness.

There are several reasons why these critical tools are used. The first reason is the availability of timely information and updates. Social media and websites can quickly and directly share information about cyberattacks or threats. Instant updates are an effective way to notify the public as soon as possible and announce the actions taken. Another critical point is to reach a large audience. Because of their ability to reach a large number of people, social media platforms and websites are effective tools for raising cybersecurity awareness. Millions of people use these platforms every day to get information quickly. One important reason for its use is interactive communication. Social media offers an interactive communication environment. Users can ask questions about cyber threats, give feedback on security measures, and share information with the larger community. This increases society's awareness of the issue. As with all other processes, the most important thing for users is to be a reliable source. Corporate websites and official social media accounts are trusted sources. The accuracy and reliability of the information presented on these platforms make it more credible in the eyes of society. This facilitates the dissemination of accurate and reliable information (Zeebaree et al., 2020). During a cybersecurity incident, crisis management can effectively communicate through social media and websites. Accurate and

timely updates provide clarity on how the community should respond to the incident while avoiding panic. Education and awareness, like cyber security, are extremely important. Social media and websites serve as effective platforms for cybersecurity education, awareness campaigns, and information sharing. Information shared in video content, infographics, articles, and other formats teaches the public about safety issues. Finally, social media can help to create a community around cybersecurity issues. People can interact on topics of common interest, share their experiences, and support one another. This is a method for creating a safer digital community (Arat and Aslan, 2021; Tekke and Lale, 2021).

Social media and websites enable fast, effective, and wide-ranging information sharing in communicating cyber threats to the public. These platforms are important tools to make society more aware, prepared, and resilient against cyber threats (Zeebaree et al., 2020).

5.3. Cyber Emergency Messages

"The communication of cyber threats to the public is an issue of increasing importance today. Cybersecurity incidents can pose serious risks to public institutions and communities in a rapidly changing and evolving threat environment. Therefore, cyber emergency messages are important for the public and organizations to be aware of these threats." It has a critical role in terms of raising awareness against the disease and taking appropriate precautions (Ünver et al., 2009).

Cyber emergency messages should be created using effective communication policies. These messages should be organized clearly and understandable and should not cause panic. Messages should include basic information such as the severity of the incident, systems or services affected, actions taken, and how the public should respond. Additionally, cyber emergency messages must be disseminated quickly through reliable communication channels. Various platforms such as SMS, e-mail, social media, and official websites are used to inform the public. These communication channels offer the potential to reach a wide audience and convey emergency information effectively. Public agencies and private sector organizations should create advanced plans for cyber emergency messaging and update those plans regularly. In addition, educational campaigns should be organized to increase awareness of society against cyber threats, and awareness-raising activities should be carried out on how the public can be protected against such incidents (Eroğlu, 2014).

As a result, cyber emergency messages are an important tool to ensure that the public and institutions are prepared for cyber threats. Effective communication and planning will ensure that these messages spread quickly and increase the safety of society." (Sertçelik, 2015).

5.4. Public Service Announcements and Videos

Using public service announcements and videos to communicate cyber threats to the public is an effective way to increase public awareness and take appropriate precautions. These types of media tools are important for raising awareness and providing education on cybersecurity issues, as they have the potential to reach a wide audience (Singh et al., 2020).

Public service announcements serve the purpose of quickly informing the audience by containing short and concise messages. In these spots, basic information can be given about cyber threats that may be encountered in daily life. For example, basic security measures such as using strong passwords, using up-to-date software, and avoiding unknown connections are emphasized. Videos, on the other hand, can be effective in providing more detailed information and recreating real-life scenarios (Akgul et al., 2022). For example, topics such as how a phishing attack can occur and how to protect against malicious software can be demonstrated interactively. Additionally, videos featuring expert insights, real-life case studies, and success stories can provide viewers with more in-depth knowledge of dealing with cyber threats. Public service announcements and videos can reach a wide audience by being published on various media platforms and social media. Preparation and distribution of these materials in cooperation with official institutions, non-governmental organizations, and the private sector increases society's awareness of cybersecurity. Additionally, such communication tools can be combined with cybersecurity training and campaigns to create a more comprehensive awareness strategy. In this way, the public is enabled to act more prepared and consciously against cyber threats (Wood and Ravel, 2017).

5.5. Public Meetings and Seminars

Organizing public meetings and seminars is an effective method for communicating cyber threats to the public, raising awareness of individuals and institutions on cybersecurity issues, and educating them on protection measures. Such events are valuable in terms of

providing direct interaction and participation and supporting society to act more ready and consciously against cyber threats (Öztürk and Yıldız, 2019).

Community meetings allow local communities to come together and share information on cybersecurity issues. In these meetings, expert speakers provide information on basic topics such as cyber threats, safe internet use, strong password practices, and avoiding unknown connections. Additionally, interaction can be increased by giving participants the opportunity to ask questions and share their experiences. Seminars, on the other hand, offer a more structured educational environment. A wide range of topics are discussed, such as protection policies against cyber threats, the use of security software, and safe online shopping habits (Gedikli, 2019). Seminars can help participants strengthen their knowledge by supporting interactive learning materials and practical applications. Joint efforts are carried out in cooperation with local governments, non-governmental organizations, schools, and the private sector to organize such events. Additionally, various communication tools such as local media, social media, and posters are used to promote these events (Clark and Hakim, 2016).

Public meetings and seminars contribute to society's creation of a more resilient and secure digital environment by supporting awareness of cybersecurity issues. These events have the potential to increase information sharing as well as provide participants with skills to protect against cyber threats more effectively (Kim et al., 2017).

5.6. NGO's and NPO's as Reliable Sources

It is important to use reliable sources and effective communication channels when communicating cyber threats to the public. Equipping the public with accurate and up-to-date information promotes a safer digital environment by raising awareness about cyber security. In this case, official public organizations and cyber security institutions serve as primary sources for ensuring information reliability. These organizations provide reliable information on cyber threat mitigation measures, current threat status, and protection policies. Furthermore, cybersecurity experts and subject matter experts in security companies can be trusted sources due to their extensive knowledge of cyber threats. These experts help to raise public awareness by sharing research on security issues and updates. Furthermore, universities and educational institutions that provide cybersecurity training are valuable resources for keeping up with developments in this field and informing the general

public. They promote knowledge sharing through conferences, seminars, and publications. Moreover, official public institutions and reputable cybersecurity organizations can share current information through official websites and social media accounts (Karakaya et al., 2020). These platforms have the potential to reach a large number of users quickly. Non-governmental organizations and public collaborations are examples of credible sources and communication channels. Nongovernmental organizations (NGOs) can make significant contributions to cyber security awareness and training. Collaboration between the public and private sectors can increase the effectiveness of these organizations' cybersecurity efforts. Finally, education and awareness campaigns designed to provide accurate information to society are essential. Brochures, posters, videos, and other media tools are used to reach a large audience regarding cybersecurity issues.

Various tools can be used as communication channels, such as SMS, e-mail, social media platforms, press releases, radio, and television. Using multiple channels allows information to be disseminated quickly and effectively, but the reliability of these channels must be considered. Equipping society with accurate and reliable information helps create a society that is more resistant to cyber threats (Atıcı and Gümüş, 2003).

5.7. Interactive Feedback Mechanisms

Public communication of cyber threats and interactive feedback mechanisms are of great importance today due to the complexity and rapid change of the digital world. These mechanisms help the public and private sectors become more resilient to cyber threats by ensuring that cybersecurity-related information is effectively shared, collected, and managed. Interactive feedback mechanisms accelerate the flow of information in the processes of detecting, analyzing, and combating cyber threats (Guan et al., 2016).

Interactive feedback mechanisms enable the rapid detection of cyber threats and the immediate communication of this information to the public. Threat information is shared interactively by security experts, organizations, and public institutions using a sharing platform. Data standardization and compatibility are critical to the interactive feedback mechanism. Interactive feedback mechanisms ensure that cyber threat data is standardized and presented in a consistent manner. This enables information sharing between organizations and ensures interoperability. Additionally, real-time analysis and response is critical. The interactive sharing of threat information improves real-time analysis and

response processes (Ghiasi et al., 2023). This allows for faster detection and effective counterattacks. Again, at this point, public-private sector collaboration is required. Interactive feedback mechanisms encourage collaboration between the public and private sectors. Sharing threat information securely strengthens the cyber security ecosystem and helps to create a common understanding among the parties. Interactive feedback mechanisms enable users to provide feedback while also increasing their awareness of cyber threats. It also enables security professionals to combat cyber threats more effectively by providing ongoing training and knowledge updates (Ashibani and Mahmoud, 2017).

As a result, interactive feedback mechanisms offer several advantages in combating cyber threats. However, for these mechanisms to work effectively, they must be carefully designed regarding issues such as security, privacy, and compliance (Ghiasi et al., 2023).

6. DISCUSSION AND POLICY SUGGESTION

In light of this study, implementing its findings in today's Türkiye could involve several key policymakers responsible for cybersecurity and public communication. These include the Police Department, Ministry of Transportation and Infrastructure, and Directorate of Communications. The Police Department operates a dedicated counter against cybercrime, constituting an operational division within the institution. Meanwhile, the Ministry of Transportation and Infrastructure oversees cybersecurity policies and action plans. Effective communication of cyber threats requires collaboration among all responsible institutions, with the Directorate of Communications playing a central role as the main actor. While technical expertise is essential, this study's primary objective is to develop effective communication policies for public awareness. By empowering the Directorate of Communications as a policymaker and operator, this study can be readily implemented. It is critical to highlight the dynamic nature of cyber threats and the changing landscape of digital risks when utilizing the proposed communication model. In order to effectively address emerging challenges, policymakers must acknowledge that cybersecurity is not only a technical issue but also a socio-technical one that needs interdisciplinary collaboration and comprehensive approaches. In addition, cultivating a culture of cybersecurity resilience and awareness needs proactive interaction with several kinds of stakeholders, including the public, government agencies, businesses, NGO's and NPO's. In order to strengthen collective defense against cyber threats, policymakers should place a high priority on creating multi-stakeholder partnerships and encouraging information-sharing networks. In today's world, where cyber threats are pervasive, the proposed model below can serve as a valuable tool. The Directorate of Communications would formulate communication policies utilizing preparedness plans, educational materials, media collaborations, communication protocols, transparency, accuracy, and appropriate language. These policies would then be implemented to inform the public effectively. Public feedback mechanisms, including social media, would enable continuous improvement and evolution of the policy.

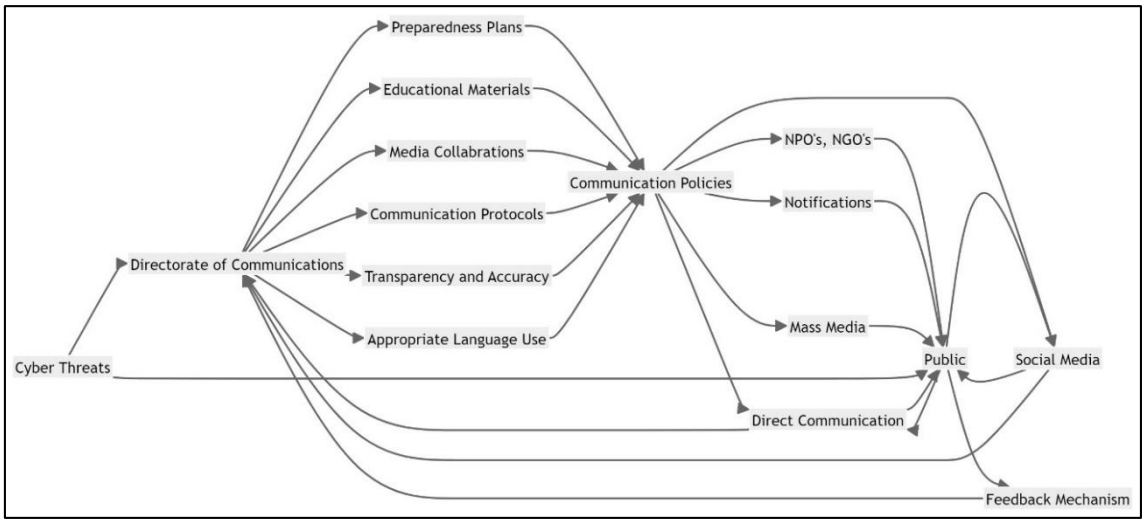

Figure 6.1. Communication model proposal

7. CONCLUSION

In this study, cybersecurity communication policies were thoroughly examined, focusing on communicating cyber threats to the public. Cybersecurity's critical importance lies in raising public awareness, promoting precautionary measures, and enhancing security consciousness. Effective communication ensures increased awareness and preparedness, facilitates rapid response and mitigation, and encourages cooperation for developing strong solutions. However, the risk of panic, sensitive information sharing, and potential unresponsiveness and distrust need to be addressed. Recommendations for effective communication policies include transparency, a multi-channel approach, continuous education and awareness, strategic planning, and evaluation and adaptation. Specific methods like public service announcements and videos, public meetings and seminars, reliable sources and communication channels, and interactive feedback mechanisms were analyzed, each presenting unique benefits and shortcomings. While public service announcements and videos facilitate broad awareness, they may lack technical details, while public meetings and seminars foster interaction but face accessibility challenges. Reliable sources offer trustworthy information but may lack diversity in perspective, while interactive feedback mechanisms encourage participation but require careful management. Overall, a balanced and adaptable communication policy is essential for effective cybersecurity communication, necessitating continuous improvement and adaptation to combat cyber threats.

8. REFERENCES

Akgul O, Roberts R, Namara M, Levin D, Mazurek ML. (2022). Investigating influencer VPN ads on YouTube. 2022 IEEE Symposium on Security and Privacy (SP), 876-892. https://www.cs.umd.edu/~akgul/papers/vpn-ads.pdf. 27 January 2024.

Alazab M, Rm SP, Parimala M, Maddikunta PKR, Gadekallu TR, Pham QV. (2021). Federated learning for cybersecurity: Concepts, challenges, and future directions. *IEEE Transactions on Industrial Informatics*, 18(5):3501-3509.

Aldemir C, Kaya M. (2020). Bilgi toplumu, siber güvenlik ve Türkiye uygulamalari. *Kamu Yönetimi ve Politikaları Dergisi*, 1(1):6-27.

Al-Mohannadi H, Mirza Q, Namanya A, Awan I, Cullen A, Disso J. (2016). Cyber-attack modeling analysis techniques: An overview. *4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, Vienna, 69-76.

Altıner M, Çakır F. (2018). Siber uzay ve uluslararasi ilişkiler/teorisi. *Cyberpolitik Journal*, 2(4):183-190.

Arat T, Aslan MM. (2021). Sosyal medyada veri güvenliği ve kişisel mahremiyet sorunu. *Akdeniz Üniversitesi İletişim Fakültesi Dergisi*, 35:387-401.

Arda E. (2020). *Siber Uzay Ortamında Saldırı Tehditlerinin Farkındalığı, Tespiti ve Önlenmesi Üzerine Bir Gerçek-Zaman Sistem Önerisi*. Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilimdalı, Yüksek Lisans Tezi, Ankara: Başkent Üniversitesi.

Ashibani Y, Mahmoud QH. (2017). Cyber physical systems security: Analysis, challenges and solutions. *Computers & Security*, 68:81-97.

Aslan ÖA, Samet R. (2020). A comprehensive review on malware detection approaches. *IEEE access*, 8:6249-6271.

Aslay F. (2017). Siber saldırı yöntemleri ve Türkiye'nin siber güvenlik mevcut durum analizi. *International Journal of Multidisciplinary Studies and Innovative Technologies*, 1(1):24-28.

Atasever KN. (2019). *Jaya Optimizasyon Algoritması Tabanlı Metamorfik Kötücül Kod Tespiti*. Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilimdalı, Yüksek Lisans Tezi, Denizli: Pamukkale Üniversitesi.

Atıcı B, Gümüş Ç. (2003). Sanal ortamda gerçek tehditler: siber terör. *Polis Dergisi*, 37:57-66.

Avcı İ. (2023). Akıllı ulaşım sistemlerinde siber saldırılar ve önlemler. *Akıllı Ulaşım Sistemleri ve Uygulamaları Dergisi*, 6(1):194-208.

Ayap NRD, Dabu ACY, Reyes AM, Ventura ABK, Trinidad GP, Blancaflor EB. (2022). Beat the bait: A case study on phishing attack. *3rd African International Conference on Industrial Engineering and Operations Management*, Nsukka, Nigeria.

Aydın H, Barışkan MA, Çetinkaya A. (2021). Siber güvenlik kapsaminda enerji sistemleri güvenliğinin değerlendirilmesi. *Güvenlik Bilimleri Dergisi*, 10(1):51-174.

Aytekin A. (2015). *Türkiyenin Siber Güvenlik Stratejisi ve Eylem Planının Değerlendirilmesi*. Bilişim Enstitüsü, Bilişim Sistemleri Anabilimdalı, Yüksek Lisans Tezi, Ankara: Gazi Üniversitesi.

Baezner M, Robin P. (2017). *Stuxnet (No. 4)*. ETH Zurich, Center for Security Studies (CSS).

Baumeister T. (2010). *Literature Review on Smart Grid Cybersecurity*. Department of Information and Computer Sciences, Tech Report, Honolulu: University of Hawaii.

Belous A, Saladukha V. (2020). Computer viruses, malicious logic, and spyware. In: A Belous and V Saladukha (eds.). *Viruses, Hardware and Software Trojans: Attacks and Countermeasures*. Champaign, Springer, 101-207.

Bencsáth B, Pék G, Buttyán L, Felegyhazi M. (2012). The cousins of stuxnet: Duqu, flame, and gauss. *Future Internet*, 4(4):971-1003.

Berg SH, O'Hara JK, Shortt MT, Thune H, Brønnick KK, Lungu DA, Røislien J, Wiig S. (2021). Health authorities' health risk communication with the public during pandemics: a rapid scoping review. *BMC Public Health*, 21(1):1-23.

Bıçakçı S, Ergun FD, Çelikpala M. (2015). Türkiye'de siber güvenlik. *Ekonomi ve Dış Politika Araştırma Merkezi (EDAM) Siber Politika Kağıtları Serisi*, 1:1-35.

Bıçakçı S. (2014). NATO'nun gelişen tehdit algısı: 21. yüzyılda siber güvenlik. *Uluslararası İlişkiler Dergisi*, 10(40):100-130.

Boeke S. (2018). National cyber crisis management: different European approaches. *Governance*, 31(3):449-464.

Boholm M. (2021). Twenty-five years of cyber threats in the news: a study of Swedish newspaper coverage (1995–2019). *Journal of Cybersecurity*, 7(1):tyab016.

Bowen BM, Hershkop S, Keromytis AD, Stolfo SJ. (2009). Baiting inside attackers using decoy documents. In: Y Chen, TD Dimitriou and J Zhou (eds.), *Security and Privacy in Communication Networks: 5th International ICST Conference, SecureComm 2009, Athens, Greece, September 14-18, 2009, Revised Selected Papers 5*, Berlin, Springer, 51-70.

Bozkanat E, Çömlekçi MF. (2020). Yeni medya çalışmalarının geleceği ve büyük veri kaynaklı riskler: bir delfi çalışması. *Connectist: Istanbul University Journal of Communication Sciences*, 58:37-64.

Boztaş A. (2012). *Üçüncü Dünya Güvenliği Yaklaşımları Kapsamında Afrika'nın Büyük Göller Bölgesi'ndeki Çatışmaların Analizi*. Sosyal Bilimler Enstitüsü, Uluslararası İlişkiler Anabilim Dalı, Doktora Tezi, Sakarya: Sakarya Üniversitesi.

Broadhurst R, Chang LY. (2012). Cybercrime in Asia: trends and challenges. In: B. Hebenton, SY Shou and J Liu (eds.), *Handbook of Asian Criminology*. Singapore, Springer, 49-64.

Buchanan SS. (2022). *Cyber-Attacks to Industrial Control Systems since Stuxnet: A Systematic Review*. Doctoral Dissertation, Laurel: Capitol Technology University.

Çahmutoğlu E. (2020). Siber uzayda güç ve siber silah teknolojilerinin küresel etkisi. *Analytical Politics*, 1(1):63-79.

Çakır H, Taşer M. (2023). Türkiye'de yapilan siber güvenlik faaliyetlerinin ve eğitim çalişmalarinin değerlendirilmesi. *Gazi University Journal of Science Part C: Design and Technology*, 11(2):347-366.

Çakır H, Uzun SA. (2021). Türkiye'nin siber güvenlik eylem planlarinin degerlendirilmesi. *Ekonomi İşletme Siyaset ve Uluslararası İlişkiler Dergisi*, 7(2):353-379.

Canbek G, Sağıroğlu Ş. (2007). Kötücül ve casus yazilimlar: kapsamli bir arastirma. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi*, 22(1):121-136.

Carroll P, Windle J. (2018). Cyber as an enabler of terrorism financing, now and in the future. *Journal of Policing, Intelligence and Counter Terrorism*, 13(3):285-300.

Çatak FÖ. (2018). Topluluk yöntemlerine dayalı dağıtık hizmet dışı bırakma saldırılarının algılanması. *Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, 22(1):283-289.

Çatal B. (2015). Diplomaside değişim ve dönüşüm: siber diplomasi. *Medeniyet Araştırmaları Dergisi*, 2(3):43-54.

Çelik S, Çeliktaş B. (2017). Güncel siber güvenlik tehditleri: fidye yazılımlar. *Cyberpolitik Journal*, 2(4):296-323.

Çelik S. (2018). Siber uzay ve siber güvenliğe multidisipliner bir yaklaşım. *Academic Review of Humanities and Social Sciences*, 1(2):110-119.

Cengiz G. (2021). Siber Suçlar, sosyal medya ve siber etik. *İletişim Çalışmaları Dergisi*, 7(3):407-424.

Clark RM, Hakim S. (Eds.). (2016). *Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level* (Vol. 3). Champaign, Springer.

Collins S, McCombie S. (2012). Stuxnet: the emergence of a new cyber weapon and its implications. *Journal of Policing, Intelligence and Counter Terrorism*, 7(1):80-91.

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi. (2023). *Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023)*. https://cbddo.gov.tr/siber-guvenlik-stratejisi/. 22 April 2024.

Darıcılı AB. (2014). Rusya Federasyonu kaynaklı olduğu iddia edilen siber saldırıların analizi. *International Journal of Social Inquiry*, 7(2):1-16.

Daugirdas K, Mortenson JD. (2015). United States responds to alleged North Korean cyber Attack on Sony Pictures Entertainment. *The American Journal of International Law*, 109(2):419-422.

Demir Ü. (2021). Uluslararası güvenlik açısından ülkemizdeki bilgi güvenliği ve siber güvenlik eğitimlerinin mevcut durumunun incelenmesi. *İstanbul Rumeli Üniversitesi Uluslararası Güvenlik Sempozyumu. İRÜİSTANBUL*, 2-7.

Denning PJ, Denning DE. (2010). Discussing cyber attack. *Communications of the ACM*, 53(9):29-31.

Dilek E, Talih Ö, Bensghir T. (2023). Estonya 2007 siber saldırılarının incelenmesi ve ülkelerin ulusal siber güvenlik politikalarına etkileri. *Bilgi Yönetimi*, 6(2):332-347.

Doğan D. (2021). *Siber Güvenlik Açısından Siber Saldırı Senaryolarının Incelenmesi*. Lisansüstü Eğitim Enstitüsü, Yüksek Lisans Tezi, İstanbul: Maltepe Üniversitesi.

Duo W, Zhou M, Abusorrah A. (2022). A survey of cyber attacks on cyber physical systems: Recent advances and challenges. *IEEE/CAA Journal of Automatica Sinica*, 9(5):784-800.

Duran A, Bakır H. (2023). Hiperparametreleri ayarlanmış makine öğrenimi algoritmalarını kullanarak Android sistemlerde kötü amaçlı yazılım tespiti. *International Journal of Sivas University of Science and Technology*, 2(1):1-19.

Elleithy KM, Blagovic D, Cheng WK, Sideleau P. (2005). Denial of service attack techniques: analysis, implementation and comparison. *Journal of Systemics Cybernetics and Informatics*, 3(1):66-71.

Erendor ME. (2016). Risk toplumu ve refleksîf modernleşme çerçevesinde siber terörizm: tanımlama ve tipoloji sorunu. *Cyberpolitik Journal*, 1(1):114-133.

Ergan SN, Ergan Ç. (2021). Sosyal medyanın eğitsel kullanımı üzerine bir örnek olay araştırması. *Nitel Sosyal Bilimler*, 3(1):72-106.

Erhan D, Anarım E, Kurt GK, Koşar R. (2013). Effect of DDoS attacks on traffic features. *21st Signal Processing and Communications Applications Conference (SIU)*, Kuzey Kıbrıs Türk Cumhuriyeti, 1-4.

Ermiş U. (2018). Bir güvenlik sorunu olarak siber uzay. Türk Asya Stratejik Araştırmalar Merkezi. https://tasam.org/Files/Icerik/File/Bir_G%C3%BCvenlik_Sorunu_Olarak_Siber_Uzay_pdf_092192a5-1b0d-4950-974d-68558aa8652f.pdf. 09 March 2024.

Eroğlu Y. (2014). *Ergenlerde Siber Zorbalık ve Mağduriyeti Yordayan Risk Etmenlerini Belirlemeye Yönelik Bütüncül Bir Model Önerisi*. Eğitim Bilimleri Enstitüsü, Eğitim Bilimleri Anabilim Dalı, Doktora Tezi, Bursa: Uludağ Üniversitesi.

Gandotra E, Bansal D, Sofat S. (2014). Malware analysis and classification: A survey. *Journal of Information Security*, 5(2):56-64.

Gedikli AT. (2019). *Kitle Iletişim Faaliyetlerinde Kişilik Haklarına Saldırı Hallerinde Başvuru Yolları*. Sosyal Bilimler Enstitüsü, Uluslararası Ticaret Hukuku Anabilim Dalı, Yüksek Lisans Tezi, İstanbul: Altınbaş Üniversitesi.

Ghafur S, Kristensen S, Honeyford K, Martin G, Darzi A, Aylin P. (2019). A retrospective impact analysis of the WannaCry cyberattack on the NHS. *NPJ Digital Medicine*, 2(1):98.

Ghiasi M, Niknam T, Wang Z, Mehrandezh M, Dehghani M, Ghadimi N. (2023). A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future. *Electric Power Systems Research*, 215:108975.

Goztepe K, Kilic R, Kayaalp A. (2014). Cyber defense in depth: Designing cybersecurity agency organization for Türkiye. *Journal of Naval Science and Engineering*, 10(1):1-24.

Guan X, Yang B, Chen C, Dai W, Wang Y. (2016). A comprehensive overview of cyber-physical systems: From perspective of feedback system. *IEEE/CAA Journal of Automatica Sinica*, 3(1):1-14.

Gündoğdu S. (2023). Uluslararası politikada bir etki aracı olarak siber güvenlik ve Türkiye'nin siber güvenlik politikası uygulaması: Ulusal Siber Olaylara Müdahale Merkezi (USOM). *Fırat Üniversitesi Sosyal Bilimler Dergisi*, 33(3):1325-1337.

Gündüz MZ, Daş R. (2021). Akıllı şebekeler: siber güvenlik unsurları ile veri iletimi. *Bingöl Üniversitesi Teknik Bilimler Dergisi*, 2(2):47-61.

Gupta S, Singhal A, Kapoor A. (2016). A literature survey on social engineering attacks: Phishing attack. *International Conference on Computing, Communication and Automation (ICCCA)*, Noida, India, 537-540.

Gürkaynak G, Yilmaz I, Taskiran NP. (2014). Protecting the communication: Data protection and security measures under telecommunications regulations in the digital age. *Computer Law & Security Review*, 30(2):179-189.

Haataja S. (2017). The 2007 cyber attacks against Estonia and international law on the use of force: an informational approach. *Law, Innovation and Technology*, 9(2):159-189.

Halfond WG, Viegas J, Orso A. (2006, March). A classification of SQL-injection attacks and countermeasures. Proceedings of the IEEE İnternational Symposium on Secure Software Engineering, Piscataway, New Jersey, 13-15.

Hathaway OA, Crootof R, Levitz P, Nix H, Nowlan A, Perdue W, Spiegel J. (2012). The law of cyber-attack. *California Law Review*, 100:817-885.

Hatipoğlu O. (2021). Kamu politikası analizi açısından Türkiye'de kripto para politikalari. *Maliye ve Finans Yazıları*, 116:171-201.

Hekim H, Başıbüyük O. (2013). Siber suçlar ve Türkiye'nin siber güvenlik politikalari. *Uluslararası Güvenlik ve Terörizm Dergisi*, 4(2):135-158.

Hemsley KE, Fisher E. (2018). *History of industrial control system cyber incidents* (No. INL/CON-18-44411-Rev002). Idaho National Lab (INL), Idaho Falls, USA.

Herzog S. (2011). Revisiting the Estonian cyber attacks: Digital threats and multinational responses. *Journal of Strategic Security*, 4(2):49-60.

Holat O. (2021). Yeni medya ve siber savaş kavramları bağlamında Stuxnet saldırısı örneğinin incelenmesi. *Abant Kültürel Araştırmalar Dergisi*, 6(11):105-121.

Kara İ. (2019). Kaba kuvvet saldırı tespiti ve teknik analizi. *Sakarya University Journal of Computer and Information Sciences*, 2(2):61-69.

Kara Ş, Zengin A, Hızal S. (2023). Ağ sistemlerinin güvenliği için siber saldırıların ayrık olaylı sistem tanımlama tabanlı modellenmesi ve simülasyonu. *Mühendislik Bilimleri ve Araştırmaları Dergisi*, 5(2):186-202.

Karaarslan E, Akbaş MF. (2017). Blok zinciri tabanlı siber güvenlik sistemleri. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, 3(2):16-21.

Karaarslan E. (2019). *Ulusal Güvenlik Için Blokzinciri Tabanlı Siber Güvenlik Modeli*. Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, Yüksek Lisans Tezi, Eskişehir: Anadolu Üniversitesi.

Karakaya A, Canbay Y, Bülbül H, Tuğlular T, Irmak E, Kavun EB, Takçı H. (2020). *Siber Güvenlik ve Savunma: Biyometrik ve Kriptografik Uygulamalar (Vol. 4)*. Ankara: Nobel Akademik Yayıncılık.

Karasoy H, Gezici HS. (2023). Bombalardan baytlara: siber güvenliğin ulusal güvenlikteki rolü ve yapay zekânin siber güvenlikteki önemi. *Uluslararası Yönetim Akademisi Dergisi*, 6(1):173-188.

Karasoy HA, Babaoğlu P. (2021). Türkiye'de siber güvenlik: yasal ve kurumsal altyapi. *Yasama Dergisi*, (44):123-155.

Karataş A. (2020). The comparative analysis of national cyber security policies: United States, United Kingdom and Türkiye examples. *Journal of Academic Social Resources*, 5(19):737-751.

Katole RA, Sherekar SS, Thakare VM. (2018). Detection of SQL injection attacks by removing the parameter values of SQL query. *2nd International Conference on Inventive Systems and Control (ICISC)*, India, 736-741.

Kenney M. (2015). Cyber-terrorism in a post-Stuxnet world. *Orbis*, 59(1):111-128.

Khader M, Karam M, Fares H. (2021). Cybersecurity awareness framework for academia. *Information*, 12(10):417.

Khidzir NZ, Ismail AR, Daud KAM, Afendi MS, Ghani A, Ibrahim MAH. (2016). Critical cybersecurity risk factors in digital social media: Analysis of information security requirements. *Lecture Notes on Information Theory*, 4(1):18-24.

Kim K, Kim I, Lim J. (2017). National cybersecurity enhancement scheme for intelligent surveillance capacity with public IoT environment. *The Journal of Supercomputing*, 73:1140-1151.

Kiraz OZ. (2021). *Siber Güvenlik Bağlamında Yeni Tehdit Algılamalarının Türkiye'nin Güvenlik Politikalarına Etkileri*. Sosyal Bilimler Enstitüsü, Siyaset Bilimi ve Uluslararası İlişkiler Anabilim Dalı, Yüksek Lisans Tezi, Batman: Batman Üniversitesi.

Kişman ZA, Güleç Ö. (2021). Uluslararası ilişkiler açısından siber güvenlik ve NATO'nun siber güvenlik stratejileri. *Akademik Açı*, 1(1):127-154.

Köksoy F. (2020). Avrupa Birliği'nin siber güvenlik politikasi: kurumsalcilik mi tutarlilik mi? *Güvenlik Stratejileri Dergisi*, 16(35):635-674.

Korhan S. (2017). Siber uzayda aktör-güç ilişkisi. *Cyberpolitik Journal*, 2(4):75-104.

Köseoğlu Ö, Aydın İ. (2022). Devlet ilkokullarinda sosyal medya politikasi ve yönetimine ilişkin nitel bir arastirma. *Journal of Political Administrative and Local Studies*, 5(1):1-25.

Kostyuk N, Wayne C. (2019). Communicating cybersecurity: citizen risk perception of cyber threats. https://www.semanticscholar.org/paper/Communicating-Cybersecurity%3A-Citizen-Risk-of-Cyber-Kostyuk-Wayne/e737e116ed2b540a8d35ed627cb228358aed3f42. 14.

Kumar G. (2016). Denial of service attacks–an updated perspective. *Systems Science & Control Engineering*, 4(1):285-294.

Kurnaz S, Önen SM. (2019). Avrupa Birliği'ne uyum sürecinde Türkiye'nin siber güvenlik stratejileri. *International Journal of Politics and Security*, 1(2):82-103.

Labuschagne WA, Burke I, Veerasamy N, Eloff MM. (2011). Design of cybersecurity awareness game utilizing a social media framework. Information Security for South Africa, Johannesburg, 1-9.

Lawson ST, Yeo SK, Yu H, Greene E. (2016). The cyber-doom effect: The impact of fear appeals in the US cybersecurity debate. *8th International Conference on Cyber Conflict (CyCon)*, Tallinn, 65-80.

Li Y, Liu Q. (2021). A comprehensive review study of cyber-attacks and cybersecurity; Emerging trends and recent developments. *Energy Reports*, 7:8176-8186.

Loftus N, Narman HS. (2023). Use of machine learning in interactive cybersecurity and network education. *Sensors*, 23(6):2977.

Luiijf HAM, Besseling K, Spoelstra M, De Graaf P. (2013). Ten national cyber security strategies: A comparison. *Critical Information Infrastructure Security: 6th International Workshop, CRITIS 2011, Lucerne, Switzerland, September 8-9, 2011, Revised Selected Papers 6*, Springer Berlin Heidelberg, 1-17.

Marecki P. (2019). Atari, creative making & zombie computers: Robbo. Solucja. *Journal of Creative Writing Studies*, 4(1):1-21.

Mason RO. (1986). Four ethical issues of information age. *MIS Quarterly*, 10(1):5-11.

McCormack T. (2015). The Sony and OPM double whammy: international law and cyber attacks. *SMU Science & Technology Law Review*, 18:379.

Medeiros BP, Goldoni LRF. (2020). The fundamental conceptual trinity of cyberspace. *Contexto internacional*, 42:31-54.

Mete M. (2021). *Enformasyon Savaşında İletişim Yönetiminin Rolü: Güvenlik Güçleri İçin Bireysel Sosyal Medya Kullanımı*. Sosyal Bilimler Enstitüsü, Halkla İlişkiler ve Tanıtım Anabilim Dalı, Doktora Tezi, İstanbul: Marmara Üniversitesi.

Mohurle S, Patil M. (2017). A brief study of wannacry threat: Ransomware attack 2017. *International Journal of Advanced Research in Computer Science*, 8(5):1938-1940.

Mutlu T, Korkut-Owen F. (2017). Sosyal bilişsel kariyer kurami açisindan bilim, teknoloji, mühendislik ve matematik alanlarindaki kadinlar. *Elektronik Sosyal Bilimler Dergisi*, 16(60):87-103.

Nurse JR, Creese S, Goldsmith M, Lamberts K. (2011). Trustworthy and effective communication of cybersecurity risks: A review. *1st Workshop on Socio-Technical Aspects in Security and Trust (STAST)*, Milano, Italy, 60-68.

Ocak HS. (2021). *İç Denetimin Gelişen ve Değişen Dünyasında: Siber Güvenlik ve Denetim*. Sosyal Bilimler Enstitüsü, İşletme Anabilim Dalı, Yüksek Lisans Tezi, İstanbul: Marmara Üniversitesi.

Öcal A. (2022). *Uluslararası Ilişkilerde Değişen Güvenlik Anlayışı ve Türkiye'nin Siber Güvenlik Stratejileri*. Sosyal Bilimler Enstitüsü, Uluslararası İlişkiler Anabilim Dalı, Yüksek Lisans Tezi, Edirne: Trakya Üniversitesi.

Özdemirci F, Torunlar M. (2018). Bilgi-değişim-siber güvenlik-bağımsızlık. *Bilgi Yönetimi*, 1(1):78-83.

Öztürk MS. (2018). Siber saldirilar, siber güvenlik denetimleri ve bütüncül bir denetim modeli önerisi. *Journal of Accounting and Taxation Studies*, Special Issue:208-232.

Öztürk S, Yıldız Ö. (2019). *Türkiye'de Bilgi ve İletişim Teknolojileri Sektörünün 2000 Yılı Sonrası Makroekonomik Etkileri*. Sosyal Bilimler Enstitüsü, İktisat Anabilim Dalı, Yüksek Lisans Tezi, Nevşehir: Hacı Bektaş Veli Üniversitesi.

Pappas C, Lee T, Reischuk RM, Szalachowski P, Perrig A. (2019). Network transparency for better internet security. *IEEE/ACM Transactions on Networking*, 27(5):2028-2042.

Pipyros K, Mitrou L, Gritzalis D, Apostolopoulos T. (2014). A cyber attack evaluation methodology. *Proceedings of the 13th European Conference on Cyber Warfare and Security*, Piraeus, Greece, 264-270.

Polat E, Bülbül Hİ. (2023). SQL enjeksiyonu saldirilarinin makine öğrenmesi ile tespiti. *TÜBAV Bilim Dergisi*, 16(1):16-23.

Quigley K, Burns C, Stallard K. (2015). 'Cyber Gurus': A rhetorical analysis of the language of cybersecurity specialists and the implications for security policy and critical infrastructure protection. *Government Information Quarterly*, 32(2):108-117.

Raiyn J. (2014). A survey of cyber attack detection strategies. *International Journal of Security and Its Applications*, 8(1):247-256.

Ramirez R, Choucri N. (2016). Improving interdisciplinary communication with standardized cybersecurity terminology: A literature review. *IEEE Access*, 4:2216-2243.

Romanosky S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, 2(2):121-135.

Sabillon R, Serra-Ruiz J, Cavaller V. (2021). An effective cybersecurity training model to support an organizational awareness program: The Cybersecurity Awareness TRAining Model (CATRAM). A case study in Canada. In: Information Reso Management Association (eds.), *Research Anthology on Artificial Intelligence Applications in Security*. USA, Information Science Reference, 174-188.

Sağıroğlu Ş, Alkan M. (2018). *Siber Güvenlik ve Savunma*. Ankara, Grafiker Yayınları.

Salahdine F, Kaabouch N. (2019). Social engineering attacks: A survey. *Future internet*, 11(4):89.

Sayedi OS. (2020). *Ulusal Siber Güvenlik Stratejisi Oluşturma Süreç Analizi ve Türkiye ile Afganistan'ın Ulusal Siber Güvenlik Stratejisinin Değerlendirilmesi*. Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, Yüksek Lisans Tezi, Edirne: Trakya Üniversitesi.

Schmidt A. (2012). At the boundaries of peer production: The organization of Internet security production in the cases of Estonia 2007 and Conficker. *Telecommunications Policy*, 36(6):451-461.

Sertçelik A. (2015). Siber olaylar ekseninde siber güvenliği anlamak. *Medeniyet Araştırmaları Dergisi*, 2(3):25-42.

Singh M, Verma C, Juneja P. (2020). Social media security threats investigation and mitigation methods: A preliminary review. *Journal of Physics: Conference Series*, 1706(1):012142.

Stoddart K. (2016). Live free or die hard: US–UK cybersecurity policies. *Political Science Quarterly*, 131(4):803-842.

Swedberg R. (2020). Exploratory research. In C Elman (ed.), *The Production of Knowledge: Enhancing Progress in Social Science*. Oxford, Cambridge University Press, 17-41.

Tabansky L. (2011). Critical infrastructure protection against cyber threats. *Military and Strategic Affairs*, 3(2):61-78.

Tate R. (2022). Transparent cyber deterrence. *Joint Force Quarterly*, 107:39-49.

Tek S. (2022). *Türkiye ve Dünyada Gerçekleştirilen Siber Saldırı Yöntemlerinin ve Bu Saldırılara Karşı Alınan Önlemlerin İncelenmesi*. Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, Yüksek Lisans Tezi, Edirne: Trakya Üniversitesi.

Tekke A, Lale A. (2021). Sosyal medyada etik, bilgi manipülasyonu ve siber güvenlik. *Akademik İncelemeler Dergisi*, 16(2):44-62.

Terzi M. (2018). Bilgi ve iletişim teknolojilerine dayali oluşumlar ile bu oluşumlarin uluslararasi ilişkilere güvenlik bağlamindaki etkisi: siber terörizm. *Kara Harp Okulu Bilim Dergisi*, *28*(1):73-108.

Tobin P, Mahrouqi A, Abdalla S, Kechadi T. (2015). Simulating SQL-injection cyber-attacks using GNS3. *International Journal of Computer Theory and Engineering*, 8(3):213-217.

Toğaçar M. (2023). Kötü amaçli yazilim türlerinin tespitinde kullanilan 1B verilerin 2B barkod türlerine dönüştürülerek derin ağlarla analizlerinin gerçekleştirilmesi. *Mühendislik Bilimleri ve Araştırmaları Dergisi*, 5(1):169-177.

Topçu SH. (2022). Rusya Federasyonu'nun siber güvenlik stratejisi: Kırım örneği. *Uluslararası İlişkiler Çalışmaları Dergisi*, 2(1):19-35.

Torun NK, Torun T. (2022). Kötü amaçlı yazılımların e-ticaret içerisinde siber güvenlik açısından incelenmesi. *Sakarya İktisat Dergisi*, 11(1):1-16.

Tuğal İ, Almaz C, Sevi Mİ. (2021). Üniversitelerdeki siber güvenlik sorunları ve farkındalık eğitimleri. *Bilişim Teknolojileri Dergisi*, 14(3):229-238.

Ünal AN, Ergen A. (2018). Siber uzayda yeterince güvenli davranıyor muyuz? İstanbul ilinde yürütülen nicel bir araştırma. *Manisa Celal Bayar Üniversitesi Sosyal Bilimler Dergisi*, 16(2):191-216.

Ünal S. (2015). Siber uzama yönelik güvenlikçi söylemin inşası: Sony Pıctures'a yönelik siber saldiri haberlerinin analizi. *Journal of International Social Research*, 8(41):1308-1320.

Ünal S. (2021). Siber uzama yönelik politik söylemde iletişim güvenlik yakinsamasi: ABD, AB ve Türkiye örneği. *Akademik Hassasiyetler*, 8(17):369-399.

Ünver GN. (2017). Ulusal siber güvenlik strateji belgelerinde insan haklari. *Cyberpolitik Journal*, 2(3):101-126.

Ünver M, Canbay C, Mirzaoğlu AG. (2009). *Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler*. Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı Raporu, BTK, Ankara.

Valeriano B, Maness R. (2014). Cyberwar and rivalry: The dynamics of cyber conflict between antagonists, 2001-2011. *Journal of Peace Research*, 51:4.

Van der Walt E, Eloff JH, Grobler J. (2018). Cyber-security: Identity deception detection on social media platforms. *Computers & Security*, 78:76-89.

Van Niekerk B. (2017). An analysis of cyber-incidents in South Africa. *The African Journal of Information and Communication*, 20:113-132.

Venkatachary SK, Prasad J, Samikannu R. (2017). Economic impacts of cybersecurity in energy sector: A review. *International Journal of Energy Economics and Policy*, 7(5):250.

Wang P, Park SA. (2017). Communication in cybersecurity: a public communication model for business data breach incident handling. *Issues in Information Systems*, 18(2):136-147.

Waters CK. (2007). The nature and context of exploratory experimentation: An introduction to three case studies of exploratory research. *History and Philosophy of the Life Sciences*, 29(3):275-284.

Wazid M, Katal A, Goudar RH, Singh DP, Tyagi A, Sharma R, Bhakuni P. (2013). A framework for detection and prevention of novel keylogger spyware attacks. *7th International Conference on Intelligent Systems and Control (ISCO)*, Coimbatore, India, 433-438.

Wilson KS, Kiy MA. (2014). Some fundamental cybersecurity concepts. *IEEE Access*, 2:116-124.

Wood AK, Ravel AM. (2017). Fool me once: Regulating fake news and other online advertising. *Southern California Law Review*, 91:1223.

Yan Y, Qian Y, Sharif H, Tipper D. (2012). A survey on cybersecurity for smart grid communications. *IEEE Communications Surveys & Tutorials*, 14(4):998-1010.

Yanarışık O. (2022). Terörizmin finansmaninda siber tehditler ve kripto paraların rolü. *Üçüncü Sektör Sosyal Ekonomi*, 57(4):3229-3241.

Yavanoğlu U, Sağıroğlu Ş, Çolak İ. (2012). Sosyal ağlarda bilgi güvenliği tehditleri ve alınması gereken önlemler. *Politeknik Dergisi*, 15(1):15-27.

Yıldırım EY. (2018). Bilişim sistemlerine yönelik siber saldırılar ve siber güvenliğin sağlanması. *Mesleki Bilimler Dergisi*, 7(2):24-33.

Yılmaz O. (2018). Küreselleşme sürecinde dönüşen güvenlik algisi ve siber güvenlik. *Cyberpolitik Journal*, 2(4) :22-43.

Yohanandhan RV, Elavarasan RM, Manoharan P, Mihet-Popa L. (2020). Cyber-physical power system (CPPS): A review on modeling, simulation, and analysis with cybersecurity applications. *IEEE Access*, 8:151019-151064.

Yurttaş HG, Güzel A. (2023). Kablosuz ağa bağlı tıbbi cihazlarda siber güvenlik açıkları ve çözüm önerileri. *Uluslararası Sağlık Yönetimi ve Stratejileri Araştırma Dergisi*, 9(2):269-283.

Zahra SR, Chishti MA, Baba AI, Wu F. (2022). Detecting Covid-19 chaos driven phishing/malicious URL attacks by a fuzzy logic and data mining based intelligence system. *Egyptian Informatics Journal*, 23(2):197-214.

Zeebaree S, Ameen S, Sadeeq M. (2020). Social media networks security threats, risks and recommendation: A case study in the kurdistan region. *International Journal of Innovation, Creativity and Change*, 13(7):349-365.

Zhang XA, Borden J. (2020). How to communicate cyber-risk? An examination of behavioral recommendations in cybersecurity crises. *Journal of Risk Research*, 23(10):1336-1352.