TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Adil Atalay Hamamcıoğlu 194483IVSB

Improving Turkey's National Cyber Security Framework

Bachelor Thesis

Supervisor: Valdo Praust
MsC

Tallinn 2023

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Adil Atalay Hamamcıoğlu 194483IVSB

Türgi riikliku küberjulgeoleku raamistiku täiustamine

bakalaureusetöö

Juhendaja: Valdo Praust
MsC

Tallinn 2023

Author's declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Adil Atalay Hamamcıoğlu

14.05.2023

Abstract

By comparing Turkey's national cyber security strategy (NCSS) to those of Greece, Germany, the United Kingdom, and Estonia, the thesis sought to enhance Turkey's NCSS. The study examined pertinent national documents and regulations, as well as the national cyber security plans of the five nations.

The study found significant differences in each of the studied countries' definitions, objectives, priorities, and stakeholder involvement. In order to gauge the country's level of cyber security awareness and education, the study also carried out a survey of Turkish citizens. According to the findings, Turkey could enhance its NCSS by addressing new cyber threats and technologies, fostering stakeholder collaboration, and raising public awareness of and educational standards for cyber security.

Eight useful suggestions were made as part of the study to enhance Turkey's NCSS. Among these suggestions are addressing new cyber threats and technologies, fostering stakeholder collaboration, taking a practical approach, laying out more specific and concrete goals, and enhancing cyber security awareness and education.

Overall, the study provides insightful information about the distinctions and overlaps among national cyber security strategies in the chosen nations and offers useful suggestions for enhancing Turkey's NCSS. The methodology and results of this study can aid in improving our understanding of how national cyber security strategies affect the safeguarding of vital assets and the advancement of secure digital transformation.

The thesis is written in English and is 98 pages long, including 7 chapters, 13 figures and 8 tables.

List of abbreviations and terms

2FA	2-Factor Authentication
AI	Artificial Intelligence
APT	Advanced Persistent Threat
AR	Awareness Raising
BEC	Business Email Compromise
BKA	Federal Criminal Police Office
BSI	Federal Office for Information Security
CBDDO	Presidential Digital Transformation Office
CCDCOE	The NATO Cooperative Cyber Defence Centre of Excellence
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CI	Critical Infrastructure
CIP	Citical Infrastructure Protection
CS	Cyber Security
CSIRT	Computer Security Incident Response Team
DoS	Denial of Service
DDoS	Distributed Denial of Service
eID	Electronic Identification/Identity
ENISA	European Union Agency for Cybersecurity
EU	European Union
HMG	His Majesty's Government
HTTP	Hyper-Text Transfer Protocol
HTTPS	Hyper-Text Transfer Protocol Secure
ICS	Industrial control system
ICT	Information and Communications Technology
ID	Identity/Identification
IP	Internet Protocol
ISP	Internet Service Provider
IoT	Internet of Things
IT	Information Technology
KVKK	Personal Data Protection Agency
MITM	Man-In-The-Middle
MÜREN	National Production Integrated

NATO	North Atlantic Treaty Organization
NCSR	National Cyber Security Council
NCSS	National Cyber Security Strategy
PC	Personal Computer
R&D	Research and Development
SHA	Secure Hash Algorithm
SMART	Specific, Measurable, Achievable, Realistic and Timely
SME	Small and Medium-sized Enterprises
SMS	Short Message Service
SOC	Security Operations Center
SSL	Secure Sockets Layer
SWIFT	The Society for Worldwide Interbank Financial Telecommunication
TEDAŞ	Turkey Electricity Distribution Company
TOBB	Union of Chambers and Commodity Exchanges of Turkey
TRT	Turkey Radio Television Organization
TÜBİTAK	Scientific and Technological Research Council of Turkey
UK	United Kingdom
URL	Uniform Resource Locator
UAB	Ministry of Transport and Infrastructure
US	United States
USA	United States of America
USB	Universal Serial Bus
USD	United States Dollar
USOM	National Computer Emergency Response Team of Türkiye
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
Wi-Fi	Wireless Fidelity
WWW	World Wide Web

Table of Contents

List of Figures

List of Tables

1 Introduction

Cyber security is a topic of increasing importance [1]. Cyber attacks not only pose a significant threat to national security, but they also have severe social and economic impacts.

1.1 Background And Motivation

Cyber attacks can lead to the loss of sensitive information, including personal and financial data, and can result in financial losses for individuals and companies [2] [3]. Additionally, cyber attacks can undermine public trust in government and private institutions and can cause significant disruptions to critical infrastructure and essential services. Therefore, it is imperative that Turkey's national cyber security framework (NCSS) is comprehensive and effective in protecting against cyber threats to mitigate these potential impacts.

In Turkey, several high-profile cyber attacks have occurred in recent years, highlighting the need for effective national cyber security frameworks to protect against these threats. These attacks have affected individuals, businesses, and government agencies, causing financial losses, disruption of services, and loss of sensitive information [4].

Individuals are particularly vulnerable to cyber attacks, as they often lack the technical expertise and resources to protect themselves against sophisticated threats [5]. Cyber attacks can lead to identity theft, financial fraud, and invasion of privacy, among other harms.

Given the significant risks associated with cyber attacks, it is crucial that governments take steps to protect their citizens and businesses against these threats. The motivation for this thesis is to contribute to the improvement of Turkey's NCSS, with the ultimate goal of protecting individuals, businesses, and government agencies from the negative consequences of cyber attacks.

1.2 Research Questions And Objectives

The primary aim of this thesis is to examine the current state of Turkey's national cyber security framework and compare it with the cyber security frameworks of selected European

countries. In order to achieve this aim, the following research questions will be addressed:

1. What are the key elements of Turkey's national cyber security framework, and how effective are they in preventing cyber attacks?
2. What are the main differences and similarities between Turkey's national cyber security framework and the cyber security frameworks of selected European countries, particularly Estonia, Germany, Greece, and the United Kingdom?
3. What are the strengths and weaknesses of the national cyber security frameworks in the selected European countries, and how can these be applied to improve Turkey's national cyber security framework?

The primary objectives of this thesis are as follows:

1. To analyze the cyber security strategies, and cyber security awareness and education initiatives in Turkey's national cyber security framework, and assess their effectiveness in addressing cyber threats.
2. To compare Turkey's national cyber security framework with the cyber security frameworks of selected European countries, using Estonia, Germany, Greece, and the United Kingdom as case studies.
3. To identify the strengths and weaknesses of the national cyber security frameworks in the selected European countries, and recommend best practices and strategies that could be applied to improve Turkey's national cyber security framework.

By addressing these research questions and objectives, the aim of this thesis is to contribute to the development of a more effective NCSS in Turkey, which can better protect individuals, businesses, and the country's critical infrastructure against the growing threat of cyber attacks.

1.3 Scope

This thesis will focus on national cyber security frameworks of Turkey and selected European countries, including Estonia, Germany, the United Kingdom, and Greece. The analysis will cover three main aspects of the frameworks: cyber security strategies, and cyber security awareness and education initiatives. The time frame for the study is limited to the past six years (2016-2022). The study will include a review of relevant academic literature, official documents, and reports.

1.4 Limitations

This study has several limitations that must be acknowledged. First, due to time and resource constraints, the data collection will be limited to publicly available reports, articles, and other relevant online resources. This may limit the scope and depth of the analysis. Furthermore, the availability of sources and references in English may be limited, especially when it comes to Turkey's NCSS and past incidents. Therefore, some of the sources and references used in this study may be in Turkish, which may limit the accessibility of the findings to a wider audience.

It should also be noted that due to the unavailability of official cyber security incident reports, relying on Turkish news websites targeting the general public is the only option for gathering information on cyber incidents in Turkey. While this limitation may affect the accuracy and completeness of the information gathered, it is necessary to use these sources to gain insight into the cyber threat landscape in Turkey.

Second, this study will only focus on the cyber security strategies, and cyber security awareness and education aspects of national cyber security frameworks in Turkey and several European countries. Other aspects, such as technical implementations, legal framework, or incident response protocols, will not be included in this analysis.

Third, the proposed improvements to Turkey's NCSS are based on the analysis of publicly available information. The actual implementation and effectiveness of these improvements may vary depending on factors that are beyond the scope of this study.

Fourth, due to the limited academic analysis available, it should be noted that some of the more recent cyber security strategies, such as those adopted in 2022, have difficulties being addressed in the literature review. The lack of literature on these strategies can be attributed to their recent adoption and the brief period of time that has passed since their implementation. To provide a comprehensive understanding of the fundamental concepts and current developments in cyber security strategies, the literature review may primarily draw on older studies and analyses.

When interpreting the results, it is important to consider the "Cyber Security Awareness and Education Level in Turkey Assessment" survey's limitations, which were used in this thesis. The survey's substantial limitations include its small sample size of only 55 respondents. The survey may not be representative of Turkey as a whole due to the small number of participants, as there may be significant regional and demographic differences in cyber security awareness and education levels. As a result, the findings' accuracy might

not be as good as it could be. Additionally, because this survey was conducted online, there may be selection bias. Results from the survey may be skewed if respondents are more likely to participate if they are already aware of cyber security issues. As a result, it is important to acknowledge these limitations and proceed with caution when interpreting the results and considering their generalizability.

Finally, the comparison of Turkey's NCSS with the frameworks of other countries will be limited to publicly available information and may not reflect the complete picture of the current state of cyber security in these countries. Despite these limitations, this study will provide valuable insights into Turkey's NCSS and offer recommendations for improvement based on a comparison with other European countries' frameworks.

2 Background Information

Cyber security can be defined as the practice of protecting electronic devices, network systems, and sensitive data from unauthorized access, theft, damage, and other cyber threats. It encompasses a broad range of measures taken to secure the confidentiality, integrity, and availability of electronic data and systems. [6]

A cyber attack refers to a malevolent endeavor to take advantage of weaknesses in a computer or network infrastructure with the aim of inflicting harm or obtaining unauthorized entry to confidential data. Perpetrators with criminal motives, cybercriminals, can initiate it either individually or through organizations, often utilizing advanced hacking methods, malware, or social engineering strategies. Upon a successful attack, the cybercriminal may potentially obtain unauthorized access to confidential information or cause interference with the normal functioning of the system. The severity and extensive consequences of a cyber attack render it a crucial issue for both individuals and organizations. [7]

National cybersecurity strategies are policy frameworks that guide a country's approach to protecting against cyber threats. Such strategies are designed to enhance a country's cybersecurity capabilities, through the implementation of a comprehensive set of actions targeting the most critical components of its infrastructure. These strategies are typically developed by governments to establish a set of principles and guidelines for ensuring cyber resiliency and protection of national security interests. They outline the roles and responsibilities of key stakeholders, the identification and management of risks, incident response strategies, and the promotion of best practices to improve cybersecurity posture at both the national and individual levels. [8]

2.1 Common Cyber Attacks In Cyber Warfare

Cyber warfare refers to the use of digital technology to disrupt or damage computer systems, networks, and information resources with the aim of achieving political, economic, or military objectives [9]. Cyber warfare can take many forms:

1. **Advanced Persistent Threat (APT) attacks** - Nation-state actors often use APT attacks to steal sensitive information and gain access to critical infrastructure systems. These attacks are sophisticated, well-funded, and often last for months or even years.

2. **Industrial control system (ICS) attacks** - These attacks target systems that control critical infrastructure like power grids, water treatment facilities, and transportation systems. ICS attacks can result in significant damage and service disruptions.
3. **Cyber espionage** - Government-sponsored hackers may attempt to infiltrate other nations' computer systems to gather sensitive information like military or economic secrets.
4. **Distributed Denial of Service (DDoS) attacks** - Nations may use DDoS attacks to disrupt communications, shut down websites or networks, or cause economic damage.
5. **Malware attacks** - Cybercriminals can plant malware in critical systems to disrupt or damage their operations.
6. **Ransomware attacks** - Ransomware attacks can be used to encrypt critical systems, making them unusable until a ransom is paid.
7. **Social engineering attacks** - Nation-state actors may use social engineering tactics to trick government officials into divulging sensitive information or executing malicious code.

These attacks can cause damage to critical infrastructure, disrupt communication networks, and compromise sensitive information. They can also lead to the loss of revenue, intellectual property, and public trust. Furthermore, cyber attacks can be used to achieve military objectives, such as disabling radar systems or disrupting military communications.

2.1.1 Denial Of Service Attacks

Denial of Service (DoS) attacks involve flooding a network or website with traffic, rendering it inoperable. These attacks can be carried out using tools that overload the target system with traffic.

Distributed Denial of Service (DDoS) attacks on the other hand, uses botnets, or a network of devices as a means of to overload the target system with traffic. [10]

2.1.2 Social Engineering Attacks

Social engineering attacks are a type of cyber attack that targets users' psychology and emotions rather than technical vulnerabilities to obtain unauthorized access to sensitive information or systems [11]. Hackers use social engineering techniques to manipulate users into performing actions that compromise system security, like sharing login credentials or downloading malware.

A type of social engineering attack is pretexting. In a pretexting attack, the attacker imper-

sonates someone else to gain access to sensitive information or systems. For example, a hacker may impersonate a company's IT staff and ask employees for their login credentials in order to "fix" a supposed problem with the company's systems.

Another type of social engineering attack is baiting, where the attacker leaves a tempting object like a USB drive in a public place. The USB drive contains malware and is marked with an enticing label like "Company Salaries" in order to entice someone to plug it into their computer and inadvertently execute the malware program.

Social engineering attacks extend beyond the realm of digital environments. An individual with malicious intent can assume the guise of an information technology specialist within a company, thereby obtaining entry to the electronic devices or accounts of the personnel or management. Unauthorized access to locked or closed doors can be accomplished through various means such as tailgating, which involves following an authorized individual to gain entry. Another method is the "coffee trick," whereby a perpetrator holds two cups of coffee to deceive unsuspecting authorized individuals into opening the door for them. Following the attacker's successful physical infiltration of the organization, the act of document theft becomes a readily available and uncomplicated course of action.

Organizations are not the only ones who are in danger when it comes to physical social engineering attacks. Valuable information such as passwords, email addresses, and full names may be obtained by a cybercriminal through shoulder surfing, where personal property is viewed by the attacker over the victim's shoulder. The risk of information exposure is still present even if items are thrown in the trash, as dumpster diving is often utilized by cyber criminals to retrieve improperly discarded classified documents or credit cards. [12]

Social engineering attacks can be particularly dangerous because they exploit human vulnerabilities rather than technical ones. To prevent social engineering attacks, education and training are important. User awareness of these attacks and how to spot them can go a long way in preventing successful attacks [11].

Phishing

One of the most common cyber attacks is phishing, which involves the use of emails or other electronic communication to trick individuals into providing sensitive information, such as passwords or credit card numbers. This is often done through the use of well-crafted emails that appear to be legitimate, but in fact are not. The victims are then referred

to a website where they are requested to give sensitive information, which are then used for fraudulent activities. [13]

Another type of phishing attack, known as whaling, involves targeting high-profile individuals, such as CEOs or executives, who have access to sensitive company information. This attack is more elaborate than traditional phishing attacks and often involves the use of a forged or spoofed email address to make it appear as if the email is coming from a trusted source. These attacks are often tailored to the victim's role and utilize personalization to gain the victim's trust. Whaling attacks may pose as legal subpoenas, bank transfers, or CEO fraud. [13]

Spear-phishing is another type of phishing attack that targets specific individuals or organizations. This type of attack is highly targeted, with cybercriminals often conducting research on their targets in order to create highly personalized and convincing messages. The goal of spear-phishing attacks is to obtain sensitive information that can be used to gain unauthorized access to an organization's systems or to carry out financial fraud. [13]

Smishing involves the use of text messages or SMS to trick a user into divulging personal information or clicking on malicious links. The attackers typically use social engineering techniques, such as posing as a legitimate organization or government agency, to gain the trust of the victim. Once the victim clicks on the malicious link, it can lead to the installation of malware or ransomware on their device, or direct them to a fake website that appears legitimate but is designed to steal their personal information. [14]

Vishing, on the other hand, involves the use of voice calls or VoIP to trick the user into providing personal or financial information. The attacker will pose as a legitimate source, such as a bank, and persuade the user to provide sensitive information such as banking login credentials or credit card details. The attacker may additionally use tactics like manipulating caller ID to give the impression of authenticity. [14]

Business Email Compromise (BEC) Attacks

Business Email Compromise (BEC) is a type of social engineering attack where an attacker impersonates a trusted business partner, like a supplier or CEO, and trick the victim into transferring money or sensitive information to the attacker's account. BEC attacks can be highly sophisticated and are often successful because they rely on established relationships and a sense of trust between the organizations [15].

BEC attacks can take many forms, including spoofed emails and fake invoices. In some cases, the attacker may use malware to compromise an email account and perform wire transfer fraud. Some attackers also use spear-phishing emails to target specific individuals who are likely to have access to sensitive information like bank account numbers.

Watering Hole Attacks

Watering Hole attacks involve the attacker compromising a website that is frequently visited by the target organization and infecting the website with malware. When a member of the target organization visits the site, they inadvertently download the malware, which then compromises the user's computer and gains access to sensitive information or systems [16].

Watering Hole attacks can be particularly effective because they exploit the trust that the target organization has in its business partners and customers. Additionally, they can be difficult to detect because the malware is often disguised as a legitimate program or application.

Fake News And Deepfake Attacks

Fake news is a phenomenon where false or misleading information is spread widely through digital media with the intention of deceiving the public or manipulating public opinion. Fake news can have significant negative consequences, including affecting political and social stability, reducing trust in institutions, and creating public panic or fear [17].

Fake news can spread through social media platforms like Twitter and Facebook, which allow users to quickly and easily share stories and articles with a large audience. Fake news is often used as a propaganda tool to influence public opinion and promote specific political or economic agendas. Additionally, fake news is often accompanied by sensational headlines and images to attract attention and create an emotional response in the viewer [18].

Deepfake attacks involve the use of artificial intelligence (AI) technology to create fake or manipulated media content, including videos, images, and audio recordings. Deepfakes can be used to discredit individuals, spread false information, and damage reputations. For example, deepfakes can be used to impersonate individuals in sensitive positions, like

politicians or business leaders, and make false statements or promises [19].

2.2 Common Cyber Attacks

Threat actors utilize prevalent cyber attacks as a means to compromise the security of digital systems. The consequences of data breaches are commonly characterized by the harm inflicted on individuals and organizations, such as financial losses and other disruptive effects that carry substantial weight. The importance of implementing strong cyber security measures to safeguard digital assets is underscored by the significance of such attacks.

2.2.1 Zero-day

A zero-day attack is when a software vulnerability or flaw is exploited without the software vendor or developer being aware of it. This gives the attacker the advantage of launching the attack before a patch or security update is created to stop such an attack. These attacks take place before the software vendor or developer is aware of the vulnerability, giving the attacker a chance to take advantage of the bug before a fix is created.

The phrase "zero-day" describes a software vulnerability that is used on the first day it is discovered by the attacker but goes unnoticed by the software vendor or developer.

Zero-day attacks are regarded as a serious cybersecurity threat due to their very nature, necessitating proactive security measures and incident response protocols to lessen their effects.

2.2.2 Trojan, Malware, Spyware, And Ransomware

A Trojan is a type of malware that disguises itself as a legitimate program or file. Once installed on a system, it can give attackers access to sensitive information, allow for remote control of the system, or download additional malware. [20]

Malware is defined as harmful software that can be used to damage, disable, or gain unauthorized access to computer systems. It is typically introduced into a computer or network system through various channels, such as email attachments, infected websites, or USB devices, without the user's knowledge or consent. Once the malware has been installed, it can be used to compromise the system's security, steal sensitive information, or cause disruption to system operations. Its effects can be severe and widespread, making it a significant threat to cyber security. [21]

Spyware is a type of malicious software that is designed to covertly gather information

about a computer user's activities without their knowledge or consent. It can be installed on a computer through various means, such as email attachments, software downloads, or malicious websites. Once installed, spyware can monitor and log keystrokes, take screenshots, capture passwords and other sensitive information, record online browsing activity, and even remotely control a computer without the user's knowledge. This type of software is often used by cybercriminals for financial gain or to steal personal information for identity theft purposes. It can also be used by governments or corporations for surveillance or espionage purposes, raising significant privacy and ethical concerns. [22]

Ransomware is a type of malware that encrypts the victim's data and demands payment in exchange for the decryption key. These attacks can result in significant financial losses and data breaches. [23]

2.2.3 Brute Forcing Attacks

Brute Forcing is an attack in which an attacker uses a repetitive trial-and-error approach to guess passwords or encryption keys. This approach involves using software to systematically enter possible combinations until the correct one is found. [24]

2.2.4 Man In The Middle Attacks

Man In The Middle (MITM) attacks involve intercepting the communication between two parties and potentially altering or stealing sensitive information. These attacks often occur through public Wi-Fi networks or compromised routers. [25]

2.2.5 Identity Theft/Impersonation

Identity Theft involves the use of stolen personal information, such as social security numbers or credit card details, to gain access to sensitive information or make fraudulent purchases [26].

Impersonation attacks involve pretending to be someone else, such as a bank or service provider, to trick individuals into providing sensitive information [27].

2.3 Emerging Technologies

It is impossible to understate the effect of emerging technologies on cyber security. New vulnerabilities are produced as new technologies are introduced. It is generally agreed upon that the digital era has made it simpler for attackers to use security flaws in a number of different ways.

As these emerging technologies continue to evolve and be adopted in various industries, it is crucial to be aware of the potential cyber threats and to implement appropriate security measures to prevent or mitigate them.

2.3.1 5G/6G

The fifth and sixth generations of wireless mobile communication systems are referred to as 5G and 6G, respectively. Compared to 4G, these technologies offer more bandwidth, less latency, and faster speeds. There are a plethora of potential uses for 5G and 6G, including the Internet of Things (IoT), augmented and virtual reality, and even self-driving cars.

But the introduction of 5G and 6G also brings new cybersecurity dangers. These networks' quick speeds and low latency make it easier for cybercriminals to launch attacks. Because of the increased bandwidth, DDoS attacks, for instance, might be more successful on 5G and 6G networks. IoT device proliferation also increases the possibility of security flaws that could be used to launch cyberattacks.

Additionally, the expanded use of 5G and eventual adoption of 6G networks may result in new security rules and difficulties. As more data is transmitted over these networks, privacy issues regarding the gathering, storing, and sharing of consumer data may surface. [28]

2.3.2 Artificial Intelligence (AI)

Cyber security is significantly impacted by the rapidly developing field of AI. It refers to the creation of computer programs and systems that are capable of carrying out operations that ordinarily call for human intelligence, such as perception, logic, learning, and judgment. [29] New cyber threats are developing as a result of the expanding use of AI technology across many industries, including finance, healthcare, and defense. [30]

Cyber attacks based on AI are becoming more sophisticated, and as technology develops, the risks posed by these attacks are also likely to rise. AI has the potential to automate attacks, making them more swift and efficient, as well as to produce practical social engineering techniques. AI can also be used to find and take advantage of weaknesses in computer systems. [31]

The potential for AI models to be hacked or poisoned is one of the biggest cyber threats related to AI. By providing false data to AI models, attackers can compromise the accuracy of the results. Since there is a chance that an AI model might be unable to react appropri-

ately in a novel situation, more serious security breaches could result from the use of AI in detecting and responding to security incidents. [32]

2.3.3 Blockchain

Blockchain is a distributed database technology that dispenses with the need for a reliable central authority to store and transfer data securely. Each member of the blockchain network has a copy of the database, and any changes to the database require the agreement of all members of the network. [33]

Blockchain's cryptographic mechanisms, which guarantee the information's integrity and prevent unauthorized changes, are what give it its security. However, blockchain is not immune to cyber threats, just like any other technology.

The 51% attack, where a single participant or group of participants controls the majority of the network's computing power and can influence the consensus process to their advantage, is one of the potential threats to blockchain. Another danger is the development of "smart contracts" that have security flaws that can be used to steal assets or jeopardize the blockchain's integrity.

Additionally, hackers might try to take advantage of flaws in the connections between blockchain and other systems, like web browsers or mobile apps. Because transactions on a blockchain can be seen and tracked, privacy issues may arise. [34]

2.3.4 Cloud Computing

Instead of relying on local servers or computer hard drives, cloud computing is a technology that enables users to store, access, and manage their data and applications over the internet. Cloud computing is a new technology that has gained popularity because of its scalability, flexibility, and affordability. Users must be aware of the new cyber threats that this technology also brings about. [35]

Data breaches are one of the most urgent cyber threats relating to cloud computing. Attacks on cloud systems can result in significant data loss or theft because of how much sensitive data is stored there. Serious repercussions could follow, from monetary losses to reputational harm. Furthermore, because cloud computing uses shared infrastructure, it is simpler for attackers to find and exploit holes and gain unauthorized access to numerous systems.

DoS/DDoS attacks are another online danger connected to cloud computing, making it

unavailable to authorized users. Particularly for companies whose operations depend on cloud services, this could have serious repercussions. [36]

2.3.5 Electronic Identity (eID)

The term "electronic identity" (eID) refers to a person's digital representation of their identity, which can be used to verify their identity during online communications and transactions. eIDs use a person's personal information or biometric data to confirm their identity.

While the use of personal identifying information raises concerns about cyber threats, eIDs have a number of potential advantages, including increased efficiency and security in online transactions. Insecure eID systems can be used by cybercriminals to steal personal data and commit identity theft. Additionally, when eID providers store user data, data breaches could happen and expose sensitive information.

Hacking eID systems, phishing attacks, and social engineering tactics designed to persuade users to divulge their eID credentials are some examples of online threats related to eIDs. It is essential that businesses and individuals implement the necessary security measures to protect people's personal information as eIDs proliferate in the digital economy. It is important to note that the creation of uniform eID regulations and schemes at the national and international levels can aid in raising the security requirements for eID implementations. [37]

2.3.6 Internet of Things (IoT)

The Internet of Things (IoT) is a network of actual physical objects like furniture, cars, home appliances, and other things that can connect to each other and share data thanks to electronics, software, sensors, and connectivity. The cyber threat landscape is growing as IoT devices gain popularity, with attackers using these connected devices to launch more complex and extensive attacks. IoT devices have built-in security flaws like weak passwords, outdated software, and inadequate encryption that can be used by hackers to access or take control of these devices without authorization. [38]

The proliferation of cyber threats is facilitated by the increasing interconnectedness of IoT devices and their frequently lax security. The potential for Internet of Things-based cyberattacks is enormous given that billions of devices are anticipated to be connected to the internet in the upcoming years [39]. Data theft, botnets, ransomware attacks, DDoS attacks, and others are some of the most frequent cyber threats connected to IoT devices. In order to reduce their exposure to these threats, it is crucial for both businesses and

individuals to take proactive steps to secure their IoT devices.

2.3.7 Quantum Computing

An emerging technology called quantum computing has the potential to have a big impact on the cyber security industry. Quantum computing, in contrast to conventional computing, is based on the idea that a particle can be in multiple states at once according to the laws of quantum mechanics. This enables quantum computers to carry out some computations much faster than conventional computers. [40]

Quantum sensing, which makes use of quantum mechanics to precisely detect and measure a variety of physical phenomena, is one application of quantum computing that has the potential to improve cyber security. This has applications in the creation of more secure systems using quantum sensing, such as in the fields of communications and cryptography. [41]

Post-quantum cryptography, a branch of quantum computing that aims to create encryption techniques that can withstand attacks from quantum computers, is another area of quantum computing that is relevant to cyber security. Quantum computers are capable of attacking conventional cryptographic techniques and breaking the underlying mathematical algorithms upon which these techniques are based. Post-quantum cryptography seeks to create substitute strategies that can fend off assaults from quantum computers. [42]

Although there are many challenges and issues to be resolved, quantum computing has the potential to significantly improve cyber security. Quantum computing, for instance, might also present fresh cyber threats, like the capacity to circumvent previously impenetrable encryption systems. Additionally, new cyberattacks that are challenging to defend against using conventional techniques may be made possible by the development of quantum computing and related technologies [43]. Therefore, careful thought and additional research are needed regarding the effects of quantum computing on cyber security.

2.4 Virtual Private Networks

A VPN, or virtual private network, is a tool that allows users to create a secure and encrypted connection over a public network. This can be useful in a variety of scenarios where privacy and security are important, such as remote work, online banking, or accessing sensitive information.

VPNs work by routing a user's internet traffic through a secure and private network,

effectively hiding their IP address and encrypting their data. This means that users can access the internet as if they are in a different location, which can be helpful for bypassing geographic restrictions or accessing content that may be blocked in certain regions.

In addition to providing a secure connection, VPNs can also be used to protect against tracking and monitoring by third-party entities, such as marketing firms or government agencies. This is because a VPN effectively shields a user's online activity from prying eyes, making it more difficult for others to collect personal data or track online behavior.

Overall, VPNs provide a valuable layer of protection for internet users who prioritize privacy and security. By using a VPN, individuals can take control of their online experience and protect themselves against various online threats. [44]

2.5 National Cyber Security Strategies In The European Union

The critical challenge posed by the increasing number and complexity of cyber threats to the security and resilience of its Member States has been recognized by the European Union (EU). Consequently, many EU countries have developed their own national cyber security frameworks to address specific challenges and ensure the protection of critical infrastructure, digital assets, and personal data.

2.5.1 Germany

Germany's new 2021 Cyber Security Strategy [45] aims to provide a strategic framework for federal government policies on cyber security for the next five years, and is based on an assessment of the increasing threat of cyber attacks.

The strategy focuses on four action areas; prevention of cyber attacks, detecting and responding to cyber attacks, increasing cyber resilience, and promoting international cooperation.

Within action area 3, the government stakeholders involved in cyber security are addressed, with objectives relating to cooperation, enhancement of skills and powers, and new challenges faced in cyberspace.

The active role of Germany in European and international cyber security policy is addressed in action area 4, with strategic objectives relating to harmonizing regulations, strengthening international law, and promoting bilateral cooperation.

The strategy concludes with a transparent method for its implementation, reporting, and strategic controlling, with emphasis on continual tracking, review, and systematic preparation for future evaluations.

2.5.2 United Kingdom

The UK Government published a National Cyber Security Strategy 2022 [46], outlining its plan to tackle cyber threats over the next decade. The strategy reflects the changing nature of cyber threats and the evolving risks faced by the UK, in particular, those posed by hostile state actors and organised criminal groups.

The National Cyber Security Strategy 2022 identifies four main goals: shaping a resilient UK, ensuring that the UK is a responsible cyber actor, securing the digital economy, and building global alliances. To achieve these goals, the government has set out seven strategic priorities, which include developing and using cutting-edge technology, building a diverse and skilled cyber workforce, and fostering innovation and growth in the cybersecurity industry.

1. **Pillar 1: Strengthening the UK cyber ecosystem** - To improve the UK's cyber capabilities, this pillar focuses on investing in people and skills, and enhancing partnership between government, academia, and industry. This will help in developing a more robust UK cyber ecosystem.
2. **Pillar 2: Building a resilient and prosperous digital UK** - The second pillar aims to reduce cyber risks and build a resilient, prosperous digital UK. This will enable businesses to maximize the economic benefits of digital technology, while ensuring that citizens are more secure online and confident in the protection of their data.
3. **Pillar 3: Taking the lead in the technologies vital to cyber power** - The third pillar focuses on taking the lead in vital cyber technologies, building industrial capability and developing frameworks to secure future technologies.
4. **Pillar 4: Advancing UK global leadership and influence** - To promote UK's global leadership and influence, this pillar aims to work with government and industry partners, sharing UK cyber power expertise.
5. **Pillar 5: Detecting, disrupting and deterring our adversaries** - The final pillar aims to detect, disrupt, and deter adversaries to enhance UK security in cyberspace, making potential use of the UK's full spectrum of levers.

Overall, the strategy aims to maintain the UK's position as a leading cyber power, and to build a secure and resilient digital future for all.

2.5.3 Estonia

Estonia's Cyber Security Strategy 2019 - 2022 [47] aims to strengthen the country's cyber defense capabilities and secure cyberspace for increased digital innovation and economic growth. The strategy focuses on developing new technologies, enhancing cooperation between stakeholders, and raising awareness of the importance of cybersecurity.

The Estonian Cyber Security Strategy sets out four main goals:

1. Ensure effective governance and efficient management of cyber security
2. Build up the necessary cyber defense and response capabilities
3. Foster innovation and development of cutting-edge digital technology
4. Increase awareness of cyber security issues among the public and private sectors.

To achieve these goals, the strategy sets out a number of specific objectives, such as enhancing critical information infrastructure protection, increasing the country's cyber defense capabilities, developing new technologies for cyber security and fostering innovation in the cybersecurity industry.

In addition, the strategy highlights the importance of international cooperation in tackling cyber threats, and aims to strengthen partnerships with international organizations and other countries.

The Estonian Cyber Security Strategy 2019 - 2022 was developed in response to the evolving nature of cyber threats and the growing importance of cybersecurity in Estonia's digital economy. The strategy was approved by the Estonian government in 2019 and is valid until the end of 2022.

2.5.4 Greece

The Greek government formulated a comprehensive Cyber Security Strategy aiming to enhance the country's cyber security measures. The strategy focuses on four main areas including cyber security governance, capabilities enhancement, critical infrastructure protection, and international cooperation promotion. This Cyber Security Strategy was developed after the country faced several cyber attacks in the past. Its draft version was published in 2019 which underwent public consultation and officially released in 2020 [48].

Greece aims to provide a comprehensive and coordinated approach to cyber security, with the objective of protecting the critical infrastructure and enhancing the country's

cyber resilience. The strategy sets out a number of action areas, including risk management, incident response, awareness raising, international cooperation, and research and innovation.

The National Cyber Security Strategy of Greece [49] highlights the need for a comprehensive and coordinated approach to cyber security, which involves all stakeholders, including the government, private sector, and civil society.

The strategy identifies seven main action areas:

1. **Governance and coordination** - The strategy establishes a national governance structure and sets out a framework for coordination and information sharing among different stakeholders.
2. **Risk management** - The strategy aims to identify, assess, and manage cyber risks to critical infrastructure, and to promote a culture of cyber security risk management.
3. **Incident response** - The strategy sets out a coordinated incident response mechanism, which involves public and private sector organizations, and includes measures for early warning, reporting, and recovery.
4. **Awareness raising and training** - The strategy aims to increase public awareness of cyber security risks and best practices, and to provide training and capacity-building for different sectors.
5. **International cooperation** - The strategy emphasizes the importance of international cooperation and information sharing, and aims to build strategic partnerships with international organizations and other countries.
6. **Research and innovation** - The strategy supports research and innovation in the field of cyber security, with a focus on developing new technologies and solutions for enhancing the country's cyber resilience.
7. **Legal and regulatory framework** - The strategy aims to strengthen the legal and regulatory framework for cyber security, and to enhance the enforcement of cyber security standards and regulations.

Overall, the National Cyber Security Strategy of Greece aims to provide a comprehensive and coordinated approach to cyber security, with a focus on protecting critical infrastructure, enhancing the country's cyber resilience, and promoting international cooperation and partnerships.

2.6 The Cyber Security Strategy Of Turkey

The National Cyber Security Strategy of Turkey for 2020 - 2023 [50] aims to build and strengthen cybersecurity mechanisms in order to protect Turkey's interests against cyber threats. To achieve this, the strategy has outlined a number of objectives:

1. Establishing mechanisms to ensure the security of national information infrastructure, support the security of digital society, and strengthen cyber defense capabilities.
2. Creating a cyber-ecosystem dependent on domestic sources and made secure with domestic capabilities.
3. Promoting the adoption of a risk-based approach to cybersecurity management, both in public and private sectors.
4. Promoting national scientific research and innovation in cybersecurity fields, and the development of a cybersecurity workforce.
5. Developing a strong and secure information and communication infrastructure that supports the needs of society.
6. Increasing institutional and technical capacity in incident response and digital evidence collection and analysis to facilitate cybercrime investigations.
7. Strengthening cooperation and collaboration with international partners to combat global cyber threats and participate in international policy-making processes.
8. Raising awareness among citizens, institutions, and other stakeholders in society about strategies, policies, and measures aimed at cyber safety and sharing best practices for cybersecurity.

These objectives, if achieved, will be critical in safeguarding Turkey's interests against cyber threats and ensuring the safety and security of its citizens, information infrastructures, and economy.

2.7 Past Cyber Security Incidents In Turkey

In Turkey, there have been several cyber security incidents [51], but no publicly available official incident reports exist with in-depth analyses and responses. Only major incidents that make news headlines are reported, and the sources of information are Turkish news websites that target the general public, which may lack details.

Turkey has a history of censoring technology and social platforms to curb dissent, as well as issuing nationwide website blocks [52]. On October 8th, 2016, an attempt was made to block access to technology and cloud services in Turkey, including Dropbox, Microsoft OneDrive, and Google Drive, in response to leaked emails allegedly from a high-ranking

government official [53]. The impacted services, including the popular developer platform GitHub, were found to be issuing SSL errors, indicating interception at a national or ISP level. Foreign visitors in Turkey were still able to access the cloud platforms, as their data was tunneled to the country of origin. Google Drive later complied with take-down demands from the government, and access was restored. Dropbox also appears to have been restored. A massive trove of 57,623 emails from the Turkish government dating as far back as 2000 was leaked, exposing how pro-establishment social media trolls were silencing criticism and targeting the opposition. The hackers demanded that the Turkish government release a number of leftist dissidents, but the government chose to ban news outlets and suspend accounts circulating the leak. Courts in Ankara confirmed the legitimacy of the email leak in legal orders that discussed the investigation of suspected RedHack members.

In December 2016, an attack targeting Akbank via the SWIFT global money transfer system was confirmed by the bank [54]. It was not established whether any financial assets were stolen from the third-largest listed bank in Turkey, while confirming that no customer data was compromised. The financial loss was estimated up to $4 million, which would be covered by insurance. Akbank stated immediately that preventive measures were taken and authorities were informed. Despite the fact that the bank's systems were operating correctly throughout the attack, this incident has added to the growing number of cyber attacks in global banking.

In March 2021, according to media reports, the municipality of Konya in central Turkey was the target of a cyber attack resulting in the theft of personal information from approximately 1 million individuals [55]. The scale of the attack was not disclosed by the municipality official, although Sözcü newspaper claims that personal information, including ID numbers, of those who had sent emails to the municipality were stolen and put in a database on a hacker forum by a suspect known as Maxim Gorki. The municipality reported the attack to law enforcement on March 29th and also disclosed that they are frequently targeted by cyber attacks. The official stated that the latest attack resulted in access to access logs of public data published on their websites and a limited number of email addresses and phone numbers.

It was announced by Yemeksepeti, the most popular food delivery service in Turkey, on March 25th that they had fallen victim to a cyber attack [56] [57]. The stolen information, including users' full names, birth dates, registered email addresses, SHA-256 hashed passwords, registered phone numbers, and registered addresses, was disclosed via their official Twitter account by Yemeksepeti.

In 2022, the Turkey Electricity Distribution Company (TEDAŞ) has reported a cyber attack

resulting in a data breach affecting both employees and citizens [58]. The breach was reported to the Personal Data Protection Agency (KVKK) and affected 208,000 individuals, with leaked information including names, email addresses, and phone numbers. The breach occurred due to an unknown party obtaining the login credentials of a TEDAŞ employee, which they then used to send the stolen data to an external email address. The breach was detected as a result of intelligence work carried out by the Cyber Security Operations Center on the Dark Web.

In September 2022, according to a report released by Chinese cybersecurity firm NSFOCUS, Turkish defense industry projects are being targeted by a new advanced persistent threat (APT) hacking group named Muren Shark. The group primarily targets institutions such as the Scientific and Technological Research Council of Turkey (TÜBİTAK) and the Turkish Naval Forces Command using phishing documents and online attack services to infiltrate the networks and steal critical information. The attackers delivered Turkish phishing documents to attack specific targets in Turkey using data stolen during previous cyber attacks. Muren Shark used Yakın Doğu College in northern Cyprus as a command control and data transfer server to avoid detection during the attack. The hackers embedded a secret spyware into documents obtained from TÜBİTAK and the Turkish Navy and sent these documents to employees of both institutions. It remains unclear how the hackers obtained the documents from TÜBITAK and the Turkish Navy. [59]

In the aftermath of a devastating earthquake that hit Turkey and Syria in early 2023 [60], cyber scammers took advantage of the situation to launch various types of cyber frauds. According to reports, scammers utilized fake charity pages on social media to collect donations meant for the earthquake victims. Furthermore, hackers lured unsuspecting individuals into clicking on malicious links or emails that either obtained personal information or installed malware in their devices. [61]

In February 2023, a disruptive DDoS attack was carried out on the satellite and communication systems of the North Atlantic Treaty Organization (NATO) in Turkey. Killnet, a loosely organized group of pro-Kremlin activists who endeavors to impede the functioning of military and governmental websites of nations that endorse Ukraine through APT, has claimed responsibility for the DDoS attacks. The attack came at a time when NATO was engaged in relief operations following a devastating earthquake in Syria. The attack caused significant delays and communication difficulties for those involved in the operation [62]. This incident highlights the vulnerability of critical infrastructure and the potential for cyber attacks to cause significant disruptions not only to the organizations targeted but also to the broader society.

3 Methodology

In this study, the NCSS of Turkey is compared with those of the selected countries. The aim of this study is to gain insights into how Turkey's NCSS compares to those of other selected countries, and to identify best practices that could be implemented to improve the effectiveness of Turkey's NCSS.

3.1 Research Design And Approach

This study employs a descriptive research design to examine Turkey's NCSS. A descriptive research design is appropriate for this study as it seeks to provide an accurate portrayal of the state of cyber security in Turkey by analyzing past incidents, cyber security strategies, and the level of cyber security awareness and education.

The research approach used in this study is qualitative. Qualitative research is appropriate for this study as it seeks to provide an in-depth understanding of the NCSS in Turkey through the analysis of reports, official documents, and a short survey.

3.2 Data Collection And Analysis

The data collection process for this study involves collecting and analyzing various sources of data related to the national cyber security frameworks of selected countries. These sources include news articles, reports, official legal documents, and a short survey.

The survey aims to shed light on the level of cyber security awareness and education among Turkish people by posing inquiries about password security, email security, anti-virus software, 2FA, hazards associated with public Wi-Fi, VPNs, and password management.

The analysis of data collected for this study will be done using content analysis. Content analysis is appropriate for this study as it allows for the systematic examination of the collected data in order to identify patterns and themes related to the cyber security strategies, and level of cyber security awareness and education in Turkey.

3.2.1 Preparation Of The Custom Search Engine

A custom search engine was created using Google's Programmable Search Engine tool[1] [63] for the purpose of data collection and research for the thesis. 32 different URL patterns[2] were utilized as the source for the search engine. Additional keywords such as *cyber, security, national, strategy, framework, Europe, European Union, Turkey, Estonia* were incorporated to ensure the search engine provided relevant and focused results. By applying such a method, materials such as articles, sources, reports, news, papers, blogs, and citations pertaining to the thesis topic could be easily identified and analyzed.

The URLs used for the custom search engine were chosen from trustworthy and well-known sources that have been referenced in many other studies, with some being governmental websites. By utilizing such reputable sources, it was possible to ensure that the resulting materials obtained through the search engine were accurate and reliable.

However, it is important to keep in mind that the quality and effectiveness of the search engine's results are only as good as the search criteria and indexed content on the websites included in the search. Therefore, it is necessary to augment the search engine's results with additional research, while simultaneously employing a critical evaluation of the sources obtained through it.

3.2.2 Preparation Of The Survey

The survey aims to provide insights into the level of cyber security awareness and education among Turkish individuals by posing inquiries about various aspects of cyber security. These topics include password security, email safety, anti-virus software, 2FA, risks associated with public Wi-Fi, VPNs, and password management. These topics were selected as they represent common everyday technological activities related to personal privacy and data security.

The survey is comprised of 11 brief questions[3] and is designed to capture the attention of the respondents as it has been studied that the average attention span of people has decreased from 12 seconds to 8 seconds, which is even lower than that of a goldfish [64].

By analyzing the responses to these questions, the study aims to identify the level of awareness and education among Turkish individuals regarding cyber security. The survey's limitations should be considered when interpreting the results. The survey's 55 respondents

[1] The custom search engine can be accessed here, or through the URL `https://cse.google.com/cse?cx=d4ea6ab17af2546e0`

[2] The list of the URL patterns can be found in Appendix 2 - chapter 7.3

[3] The survey is available in Appendix 3 - chapter 7.3

were one of its biggest drawbacks. Thus, the data may not represent Turkey's entire population, preventing demographic and regional analysis. This restriction may compromise the findings' accuracy and generalizability. Because respondents self-selected online, the survey may have been biased. It's possible that more cyber security-savvy respondents completed the survey, skewing the sample.

3.3 Analysis Framework

To analyze and compare the national cyber security strategies of the selected countries, the following 9 topics, inspired by another study by H.A.M. Luiijf et al. (2013) [65], were used:

1. Is the definition of "Cyber Security" the same between different NCSS?
2. What is the mission and vision of various NCSS?
3. What are the perceived threats that the various NCSS address?
4. What is the scope of the various NCSS?
5. What are the strategic objectives and guiding principles of the NCSS?
6. Which stakeholders are addressed?
7. What are the key planned actions?
8. What emerging threats are covered?
9. What are the planned actions for raising cyber security awareness and education?

4 Literature Review

The studies utilized in this research project were identified through utilization of a custom search engine, as specified in chapter 3.2.1. Selection criteria involved inclusion of any of the relevant keywords in the title, abstract, or keywords of the materials. Materials that were deemed outdated or irrelevant were excluded, and only recent or still relevant studies were included in the analysis.

4.1 Cyber Security Awareness And Education

There has been research on the factors affecting cyber security awareness and education among individuals. Alqahtani (2022) assessed the cyber security awareness among the university students based on three fundamental aspects: browser security, password security, and social media. Based on the research Alqahtani (2022) conducted, it was concluded that knowledge of browser security, password security, and social media activities significantly influence cyber security awareness in university students, causing them to realize the importance of cyber security awareness. However, Alqahtani (2022) pointed out that in practice; "students' levels of cybersecurity awareness are still lacking, especially when it comes to password security." [66]

Likewise, in a study by Zwilling et al. (2022), research was conducted on cyber security awareness, knowledge, and behavior. It was observed in this study that most individuals possess only a rudimentary understanding of cyber security, do not comprehend the significance of VPNs and strong passwords, but are aware that they compromise some of their privacy when using the internet [5].

4.2 Cyber Security And Human Nature

The susceptibility of individuals to phishing attacks has been extensively studied in the literature, with several factors identified as contributing to one's vulnerability. Human nature, in particular, has been identified as a crucial factor in this regard as phishing attackers often play on individuals' psychological and emotional triggers, as well as technical vulnerabilities [67] [68]. Authority cues within emails, for instance, can lead individuals to click on a link within an email [69]. PhishMe (2017) reported that curiosity and urgency were the most common emotional motivators for individuals to respond to

phishing attacks [70].

However, later studies identified entertainment, social media, and reward/recognition as top emotional triggers behind successful phishing attacks. Stress can also impair one's decision-making abilities, leading them to make rash decisions [71], and everyday stress can weaken areas of the brain that control emotions [72].

Several studies have also examined the relationship between demographic variables and susceptibility to phishing attacks. For example, Williams et al. (2018) found that individuals between 18 and 25 years old were more susceptible to phishing attacks than other age groups due to their greater trust in online communication and impulsivity [73]. Women have also been found to be more susceptible than men to phishing attacks, with lack of technical know-how and experience being the primary reason for this [74].

A survey conducted by Ong in 2014 found that smartphone malware attacks are more likely to target men than women, according to the report released by the antivirus company Avast [75]. This result was also confirmed by a study conducted by Hadlington in 2017, which found that men are more susceptible to mobile phishing attacks [76]. The reason behind this is that men are generally more comfortable and trusting when using mobile online services. Demographic characteristics of individuals and their ability to correctly detect a phishing attack were studied in Iuga et al.'s 2016 research [77]. The study revealed that participants who used PCs frequently were better able to identify phishing efforts more accurately and rapidly than other participants. Hadlington's (2017) study showed that internet addiction, attentional and motor impulsivity positively predict risky cybersecurity behaviors, while a positive attitude toward cybersecurity in business was negatively related to such behaviors. Moreover, the trustworthiness of people in some web sites/platforms is one of the vulnerabilities that scammers or crackers exploit, particularly when it is based on visual appearance that could deceive the user. For instance, Hadlington (2017) noted that fraudsters take advantage of people's trust in a website by replacing a letter from the legitimate site with a number, for example, goog1e.com instead of google.com [76].

Other studies have focused on specific attributes that make individuals more likely to fall for phishing attacks. Iuga et al. (2016) showed that those with higher levels of personal computer usage tend to accurately identify phishing attempts more often than others [77]. Additionally, Hadlington (2017) found that trustworthiness of websites is an exploitable gap for scammers and crackers, with individuals often falling prey to familiar-looking websites with minor alterations [76]. Yeboah-Boateng and Amanor (2014) highlighted the susceptibility of college students to phishing attacks, emphasizing that younger students are more vulnerable than older ones. Furthermore, they noted that many students lack

ICT knowledge, with terms like phishing, SMishing, and Vishing being unfamiliar to them [78]. Full-time work, however, has been identified as a protective factor against phishing [79]. Hadlington (2017) found that internet addiction, attentional and motor impulsivity, and positive attitude towards cybersecurity in business are positively related to risky cybersecurity behaviors, while a negative attitude towards cybersecurity is negatively associated with risky cybersecurity behaviors [76].

4.3 Effects Of Cyber Attacks On Individuals And SMEs

In a study by Huaman et al. (2021), 5,000 computer-assisted telephone interviews were conducted with representatives of small and medium-sized enterprises (SMEs) in Germany to understand their experiences with cybercrime, management of information security, and risk perception [80]. It was found that SMEs often lack awareness and resources to deploy extensive information security measures, and many guidelines and recommendations encourage companies to invest more into their information security measures. Despite this, many basic security measures have been deployed in the majority of companies. Differences in reporting cybercrime incidences were uncovered based on industry sector, company size, and security awareness.

Another study was conducted by López et al. (2020), on intelligent detection and recovery from cyber-attacks for small and medium-sized enterprises [81]. It was found that cyber-attacks are becoming more sophisticated and damaging, and SMEs are particularly affected due to their economic resources. The study proposes an intelligent cybersecurity platform that uses proactive security techniques, machine learning, and block-chain to optimize detection and recovery from attacks. The proposal is part of a project that aims to provide security in each phase of an attack to help SMEs in prevention, detection, containment, and response.

4.4 National Cyber Security Frameworks

New cyber security strategies have been adopted by several countries since the studies were conducted, including Estonia for the 2019-2022 period [47], the United Kingdom for the 2022-2030 period [46], Germany in 2021 [82], and Turkey in 2020 [83]. Various studies have been conducted to analyze the national cyber security frameworks of different countries, however due to the recent adoption of new national cyber security strategies, there are not many up to date studies on NCSS.

One study by H.A.M. Luiijf et al. (2013) analyzed the national cyber security frameworks

of ten countries, including Germany and the United Kingdom, and found that there were significant differences, and gaps in their implementation and effectiveness. H.A.M. Luiijf et al. (2013) prepared 9 topics to look at in order to analyze the differences between various NCSS, some of which are also used in this study[1] in order to compare the NCSS of the selected countries. [65]

1. "What does the notion 'Cyber Security' mean to nations?"
2. "What are the perceived threats that the various NCSS address?"
3. "What is the scope of the various NCSS?"
4. "Is there a relationship with other national strategies?"
5. "What are the strategic objectives and guiding principles of the NCSS?"
6. "Which stakeholders are addressed and how are they addressed?"
7. "What are the key action lines and planned actions?"
8. "Are emerging threats covered?"
9. "How are national functions institutionalised by the various NCSS?"

As a result of analyzing various NCSS using the topics above, H.A.M. Luiijf et al. (2013) made 13 observations in their study [65]:

1. "An internationally accepted and harmonized definition of 'Cyber Security' is lacking."
2. "A global harmonised definition and understanding of 'cyber security' (and related terminology framework) would be beneficial to all nations."
3. "Some NCSS are restricted to Internet-connected ICT only leaving the protection of other ICT that might very well be hampered out-of-scope."
4. "Most of the ten nations mention the cyber threat to their CI. Their NCSS, however, lack to clarify the relationship of existing national and international CIP strategies and the national cyber security strategy."
5. "Most NCSS address the general cyber crime and e-espionage type of threats. Only a small set of nations consider threats to their national defence, economy, and public confidence."
6. "The NCSS do not show a common understanding of the terrorist threat in cyberspace."
7. "Only the UK addresses the jamming, signal modification and high-power transmission threats in its national cyber security approach."
8. "All but one NCSS lack a strategic objective which reflects the need for agile adaption to emerging cyber security threats."

[1] These topics are mentioned in chapter 3.3 of this study

9. “The NCSS of France, Japan and New Zealand lack guiding principles/ framework conditions for their cyber security actions and activities.”
10. “The NCSS lack a notion of collaborative international detection and response capabilities.”
11. “The Japanese NCSS takes a wide view to cyber security and includes an agile adaptation to emerging cyber security threats.”
12. “The Netherlands requests international action to enhance the software security quality globally by promoting software liability.”
13. “Only one of the ten NCSS defines its set of planned actions in a SMART way. Therefore, most nations are unable to measure and determine afterwards whether their strategy is a success and where strengthening is required by taking additional measures.”

Moreover, a study by Štitilis et al. (2016) analyzed the EU and NATO cyber security strategies, and came to a similar conclusion as H.A.M. Luiijf et al., stating that “a number of similarities were found. However, there were many more differences or discrepancies between national cyber security strategies according to the selected criteria” [84].

Another study by Olena et al. (2021) conducted a research on the economical and legal aspects of cybercrime, and proved that “there is a relationship between a country’s income level and the negative economic impact of cybercrime, forasmuch as the economically richer a country is the greater its costs and losses from cybercrime are” [85]. In the same study, it has also been determined that there are more cyber attacks worldwide each year.

Lastly, a study conducted by CCDCOE and Emre Halisdemir (2021) [86] offers a comprehensive overview of the National Cyber Security Strategy and Action Plan 2020-2023 of Turkey [87].

Overall, these studies provide valuable insights into the state of national cyber security frameworks, the economic and social impacts of cyber attacks, and the factors affecting cyber security awareness and education among individuals.

5 Cyber Security Strategies Analysis

5.1 Definition Of "Cyber Security"

Table 1 shows the different ways various NCSS define and describe "cyber security". Greece's and Turkey's NCSS provides a description instead of a definition, while United Kingdom's NCSS provides both a short definition and clarifying description for "cyber security". Germany's NCSS, on the other hand, provides a short definition for "cyber security", whereas Estonia's NCSS states that "The relevant terms and definitions are summarised in Appendix 1.", however, the appendix mentioned is not a part of the NCSS, nor it is accessible on the internet.

As the study by H.A.M. Luiijf et al. (2013) [65] and another study by Schatz et al. (2017) [88] has stated, the change in terminology usage is creating some problems because "cyber security" does not have the same definitional clarity as, say, "Computer Security." If parties have different ideas about what the term means, this could cause confusion and misunderstanding. As all NCSS include international collaboration in cyber security field as one of their strategic objectives, agreeing on an internationally accepted definition of "cyber security" will help not only Turkey, but other countries as well in achieving this objective.

Schatz et al. (2017) has come up with a new definition "that captures key components and respects community adhesion" for "cyber security" in their study:

"The approach and actions associated with security risk management processes followed by organizations and states to protect confidentiality, integrity and availability of data and assets used in cyber space. The concept includes guidelines, policies and collections of safeguards, technologies, tools and training to provide the best protection for the state of the cyber environment and its users." [88]

Suggestion 1. Turkey, and all other countries with international collaboration in mind should agree on a common definition and description for "cyber security". Improved inter-country alignment and effective communication will result in countries cooperating internationally coming to an agreement on a common definition and description of the term "cyber security". This will improve the efficiency of cross-country cooperation, and will improve countries cyber capabilities. One of the ways this improvement can be measured

by is the increased consistency and clarity in cyber security efforts and strategies across borders.

Table 1. *Definition/Description of "cyber security" in various NCSS*

Country	**Definition/Description**
Estonia	*States that definitions are provided in Appendix 1, which does not exist*
Germany	"The IT security of all information technology systems which are and could be interconnected at data level in cyberspace."
Greece	"The term 'cyber security' refers to all the appropriate actions and measures that must be taken in order to ensure the protection of cyberspace from such threats that are directly linked to cyberspace itself and which can cause damage to inter-dependable information and communication technology (ICT) systems."
Turkey	"All activities that involves protecting the information technologies which constitutes the cyberspace from attacks, ensuring the confidentiality, integrity and availability of those systems, detecting attacks and cyber incidents, activating response mechanisms against those, and restoring the systems back to pre-cyber incident conditions."
United Kingdom	"The protection of internet-connected systems (to include hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures or being manipulated into doing so."

The NCSS of Greece, Turkey, UK, Germany, and Estonia all define and describe "cyber security" differently from one another. While the UK offers both a definition and a clarifying description for "cyber security," Greece and Turkey only offer a description. Germany, however, only offers a brief explanation. Estonia makes reference to an appendix that provides a glossary of important terms, but it is not a part of the NCSS and is not available online.

5.2 Mission And Vision

Table 2 shows the mission and vision stated explicitly by various NCSS. When it comes to the mission, only United Kingdom and Turkey's NCSS explicitly state the mission, while the UK's NCSS mission is closer to being an objective rather than mission; as for the vision, Germany and Greece lack an explicit statement.

Based on a study by the consulting company Bain and Company, 90% of the 500 surveyed companies publish mission and vision statements in some capacity [89]. With the caveat that they were only related to effectiveness when strategy, goals and objectives were also aligned with them, it has also been demonstrated that "firms with clearly communicated, widely understood, and collectively shared mission and vision" [89] perform better than those without them. Although the main focus of this study were firms, the same statement can be made for the NCSS as governmental and non-governmental organizations will be the ones carrying out the actions and plans stated in the NCSS.

According to an article by the University of Minnesota (2015), "A mission statement communicates the organization's reason for being, and how it aims to serve its key stakeholders.", and "A vision statement, in contrast, is a future-oriented declaration of the organization's purpose and aspirations." [90]. The same article perfectly represents the importance of mission and vision using Figure 1:

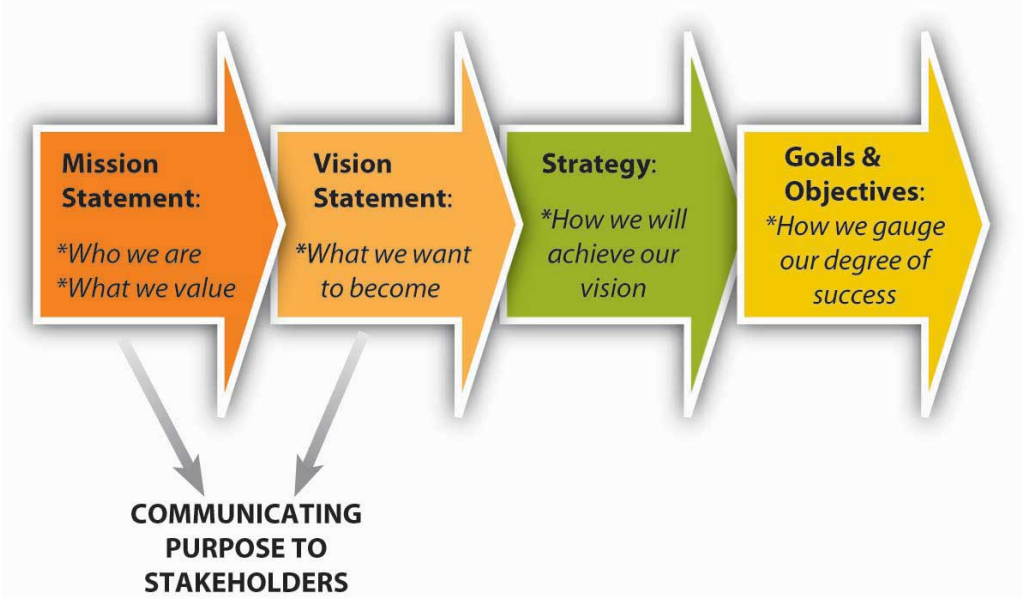

Figure 1. *Key Roles of Mission and Vision [90]*

Suggestion 2. Turkey should have a more detailed and concrete vision, like Estonia and the UK. As for the mission, other countries should take Turkey's mission statement as an example because only Turkey's NCSS mission statement adheres to the definition of a mission statement. Having a more detailed and concrete vision will result in increased stakeholder buy-in and effectiveness of cyber security improvement efforts. This improvement could be measured by potentially observing improved investors' buy-in.

Table 2. *Mission and vision of various NCSS*

Country	**Mission**	**Vision**
Estonia	*Not explicitly stated*	"Estonia can cope with cyber threats as a secure and undisrupted digital society, relying on the indivisibility of national capabilities, a well-informed and engaged private sector, and an outstanding research and development competence. Estonia is an internationally recognised leader in cybersecurity, a standing which supports national security and contributes to the growth of global competitiveness of companies operating in the domain. The Estonian society perceives cybersecurity as a shared responsibility in which everyone has a role to play."
Germany	*Not explicitly stated*	*Not explicitly stated*
Greece	*Not explicitly stated*	*Not explicitly stated*
Turkey	"With the understanding that cyber security is an integral part of the national security, work in coordination with all stakeholders to protect the assets in cyberspace especially critical infrastructures from threats and reduce possible impacts of cyber incidents."	"Acquire a secure cyber environment and become an international brand in the field of cyber security to support the economic development of the country, social life and national security."
United Kingdom	"Government's critical functions to be significantly hardened to cyber attack by 2025, with all government organisations across the whole public sector being resilient to known vulnerabilities and attack methods no later than 2030."	"This strategy seeks to ensure that core government functions - from the delivery of public services to the operation of National Security apparatus - are resilient to cyber attack, strengthening the UK as a sovereign nation and cementing its authority as a democratic and responsible cyber power."

When it comes to the mission, only the NCSS of the United Kingdom and Turkey declare it directly; nonetheless, the mission of the NCSS of the United Kingdom is closer to being an objective rather than a mission. When it comes to the vision, the NCSS of Germany and Greece do not include an explicit statement.

5.3 Perceived Threats

As mentioned in chapter 2, there are many cyber threats and many more emerging with new technologies. It is crucial for the national cyber security of a country to be prepared for as many attack vectors as possible. Comparable to the human body, the more viruses and bacteria the immunity system is prepared for, the easier it is for the body to prevent or recover from an illness caused by one of those viruses or bacteria [91].

Table 3 shows the perceived threats by various NCSS. With the exception of Greece, which has only (indirectly) mentioned ICS attacks, all NCSS seem to perceive 3 common cyber threats; malware, ransomware, and ICS attacks. Germany's NCSS, by far, is the one with the most number of perceived threats, covering threats such as; DDoS, cyber espionage/sabotage, and fake news/disinformation.

In 2021, during the joint opening meeting of the "National Strategic Communication Policy," Presidential Communications Director Fahrettin Altun stated that "In Germany, only nine out of 100 news stories are fake, 15 in England, 12 in France. When we look at this point, we see that Turkey is the country that experiences this global disinformation problem the most," [92]. Even though Turkey has addressed the fake news/disinformation problem by passing an opposed law in 2022 [93], which will undoubtedly increase the problem of censorship in the country, Turkey's NCSS lacks any mention of fake news or disinformation.

Suggestion 3. Turkey should address cyber threats that have been found to be as damaging as the others, such as fake news/disinformation, DDoS, and cyber espionage/sabotage. Addressing common cyber threats like fake news/disinformation, DDoS, and cyber espionage/sabotage will result in improved critical asset and sensitive information protection. This improvement can be measured by a decreased number of successful attacks and a strengthened national cyber security infrastructure.

Table 3. *Perceived threats addressed by various NCSS*

Country	**Perceived Threats**
Estonia	■ Malware ■ Ransomware ■ DDoS ■ ICS attacks
Germany	■ Malware ■ Ransomware ■ Cyber sabotage/espionage ■ Zero-day attacks ■ APTs ■ DDoS ■ Fake news/Disinformation ■ ICS attacks
Greece	■ ICS attacks
Turkey	■ Malware ■ Ransomware ■ Phishing ■ Zero-day attacks ■ APTs ■ ICS attacks
United Kingdom	■ Malware ■ Ransomware ■ ICS attacks

There are differences between NCSS in terms of how they view cyber threats. While most NCSS perceive malware, ransomware, and ICS attacks as common threats, some nations

also see DDoS, cyber espionage/sabotage, and fake news/disinformation as potential dangers. In comparison to other nations, Germany's NCSS perceives the most perceived threats. The emphasis on fake news and disinformation varies as well, with Turkey's NCSS making no mention of it despite having serious issues with disinformation.

5.4 Scope

Table 4 shows the scope stated by various NCSS. Apart from Greece, all NCSS explicitly state their scope.

Estonia's NCSS is a thorough framework that outlines the guiding principles and goals for ensuring efficient communication among Estonia's cybersecurity stakeholders and successfully defending critical assets from online threats. A number of important stakeholders, including government agencies, academic institutions, think tanks, and the private sector, participated in the development of the strategy. In order to ensure that the agreed-upon principles and objectives are carried out through a combination of all parties involved and processes, it aims to create a comprehensive picture, prevent duplication of effort and overlapping efforts. Estonia's national cyber security strategy uses a cooperative and comprehensive approach to provide a framework for efficient cybersecurity governance that can help safeguard vital assets from online threats.

Germany's NCSS outlines the framework for Federal Government cyber security activities, encouraging openness and understanding for all stakeholders, facilitating their active participation, taking into account EU specifications, enshrining reporting and controlling at the strategic level, and methodically preparing for upcoming evaluations and ongoing strategy refinement.

A wide range of goals are included in Turkey's NCSS to defend the nation from cyber threats. Public information systems, critical infrastructure information systems run by both the public and private sectors, small and medium-sized businesses, and all national cyberspace components are included. This strategy applies to all natural and legal persons in Turkey and emphasizes the need to provide each person and entity with a secure online environment.

The UK's NCSS includes local governments, government departments, agencies, and organizations from the broader public sector. These entities all participate in the delivery of core governmental functions. Lead government departments are in the best position to comprehend the distinctive qualities of the organizations that fall under their purview and enhance their macro-level cybersecurity posture by evaluating and articulating any

necessary improvements. The strategy recognizes various degrees of autonomy outside of central government and takes into account the diversity and complexity of public sector organizations.

Table 4. *Scope of various NCSS*

Country	**Scope**
Estonia	"The Cybersecurity Strategy is a horizontal document regarding agreements and coordination in the field of cybersecurity, which all the most important Estonian cybersecurity stakeholders helped to draft: government institutions, academia and think tanks and the private sector. The strategy does not provide detailed coverage of all necessary activities for ensuring cybersecurity, of which a key part has already become a natural part of the planning processes in various sectors. The purpose of the Cybersecurity Strategy is to form the big picture, as it were, avoid redundancy and overlapping efforts, and ensure that the principles and objectives agreed upon during drafting the strategy are implemented through a combination of all parties and processes."
Germany	"The Cyber Security Strategy" ■ "sets out the framework for Federal Government cyber security activities;" ■ "creates transparency and comprehensibility for all stakeholders in government, private industry, the research community and society;" ■ "facilitates the active, target-oriented involvement of all these stakeholders;" ■ "takes into account EU specifications;" ■ "enshrines reporting and controlling at the strategic level; and" ■ "systematically prepares for future evaluations and the ongoing refinement of the strategy"
Greece	*Not explicitly stated*
Turkey	"The scope of the National Cyber Security Strategy and Action Plan (2020-2023) includes public information systems, information systems of critical infrastructures operated by public and private sector, small and medium-sized enterprises, and all components of cyberspace at national level including all natural and legal persons."

Continues...

Table 4 – *Continues...*

Country	Scope
United Kingdom	"Core government functions are delivered by many diverse public sector organisations, including government departments, arms-length bodies, agencies, local authorities, and other wider public sector organisations. This strategy therefore considers all such public sector organisations. In doing so it recognises the breadth, complexity and varying degrees of autonomy of these organisations, particularly those beyond central government. Lead government departments are best placed to understand the unique characteristics of the organisations within their purview, including their arms-length bodies and agencies, as well as other government bodies and wider public sector organisations. The focus is therefore placed on enabling lead government departments to assess and articulate the macro cyber security posture of those organisations, driving improvements as necessary."

Estonian, German, Turkish, and British national cyber security strategies all seek to offer a comprehensive framework for facilitating efficient coordination among cybersecurity stakeholders and protecting crucial assets from cyber threats. However, each strategy has particular priorities and focuses. Turkey's strategy emphasizes protecting both natural and legal persons from cyber threats, Estonia's emphasizes avoiding redundancy and encouraging collaboration, Germany's emphasizes transparency and understandability, the UK's emphasizes enabling lead government departments to assess and articulate macro cybersecurity posture. Despite these variations, each strategy emphasizes the value of teamwork and comprehensive approaches to cybersecurity governance.

5.5 Strategic Objectives And Guiding Principles

Table 5 shows the strategic objectives of various NCSS. Estonia and Turkey take a generalized approach to strategic objectives, providing brief objectives. Greece expands the strategic objectives by explaining them in a bit more detail, whereas Germany and the UK list many strategic objectives grouped under different pillars and action areas, thus they have been included in Appendix 4 - Chapter 7.3.

A national cyber security strategy that includes multiple strategic objectives for various situations can be deemed as superior for defending against various cyber threats. Multiple goals will enable a more thorough and specialized approach to addressing various cyber threats and cyber security issues.

Suggestion 4. Turkey should take Germany and the UK's NCSS strategic objectives as an example to prepare a more in-depth, all encompassing understanding of objectives. Improvements in better alignment and effective communication between stakeholders and authorities will be seen by adopting Germany's and the UK's NCSS strategic objectives as an example through developing a more detailed and in-depth objective collection. This improvement can be measured by more consistent responses to cyber threats, and quicker detection, response, and remediation of cyber threats.

Table 5. *Strategic Objectives of various NCSS*

Country	**Strategic Objectives**
Estonia	1. "A sustainable digital society" 2. "Cybersecurity industry, research and development" 3. "A leading international contributor" 4. "A cyber-literate society"
Germany	*Included in Appendix 4 - Chapter 7.3*

Continues...

Table 5 – *Continues...*

Country	**Strategic Objectives**
Greece	1. "To upgrade the level of prevention, evaluation, analysis and deterrence of threats against the security of ICT systems and infrastructure" 2. "To enhance the ability of public and private sector stakeholders to prevent and handle cyber security incidents and to improve the resilience and recoverability of ICT systems following a cyber-attack" 3. "To create an effective coordination and cooperation framework by determining the individual competences and roles of the various public and private sector stakeholders involved in the implementation of the National Cyber Security Strategy" 4. "To ensure the active participation of Greece in international cyber security initiatives and actions by international organizations, for the enhancement of national security" 5. "To make all social institutions aware and to inform users regarding the secure use of cyberspace" 6. "To continuously adapt the national institutional framework to new technological requirements and to EU directions for effective handling of illegal acts linked to cyberspace activity" 7. "To promote innovation, research and development in security issues and cooperation between the stakeholders involved" 8. "To make use of best international practices"
Turkey	1. "Protecting Critical Infrastructure and Increasing Resilience" 2. "National Capacity Building" 3. "Organic Cyber Security Network" 4. "Security of New Generation Technologies" 5. "Fighting against Cybercrime" 6. "Developing and Fostering National and Domestic Technologies" 7. "Integrating Cyber Security into National Security" 8. "Improving International Cooperation"
United Kingdom	*Included in Appendix 4 - Chapter 7.3*

In the specialized and in-depth approach to strategic objectives, NCSS differ from one another. While Greece builds on these objectives by outlining them in more detail, Estonia and Turkey generalize their strategic objectives and provide brief objectives. Germany and the UK, in contrast, list a large number of strategic objectives categorized under various pillars and action areas. Therefore, a national cyber security strategy with multiple strategic objectives for various scenarios can be deemed superior for countering different cyber threats, enabling a more thorough and specialized approach to dealing with cyber security issues.

Table 6 shows the guiding principles of various NCSS. The corporateness, continuity, and sustainability guiding principles form the foundation of Turkey's national cyber security strategy. They emphasize the significance of cyber security as an essential component of national security, highlighting effective stakeholder coordination and communication as essential components to all studies pertaining to cyber security policies. The guidelines also emphasize the necessity of risk management in cyberspace, which must be established and handled effectively while adhering to basic guidelines for cyber security like confidentiality, integrity, and availability. The strategy also highlights the advantages of utilizing domestic and national goods and services through R&D, creativity, and a solid understanding of technological infrastructure. Last but not least, it is believed to be crucial to build cyber security on solid legal foundations and continuous service delivery, especially for critical infrastructure, is crucial.

In Estonia's national cyber security strategy, fundamental rights and freedoms are regarded as being significant for both physical space and cyberspace. Cyber security is acknowledged as a facilitator and amplifier of Estonia's socioeconomic and digital development. For Estonia's digital ecosystem, the security of cryptographic solutions is regarded as exceptional and crucial. Last but not least, open communication is vowed to, and transparency and public trust are emphasized as fundamental principles for the digital society.

The principles of collective effort and digital sovereignty among the government, private industry, the research community, and society are the cornerstones of Germany's national cyber security strategy. It highlights the significance of securing digital transformation, which calls for the establishment of measurable and open goals. The plan seeks to strengthen digital sovereignty by establishing thorough information security measures. The ultimate objective is to create efficient cyber security tools and processes to safeguard vital infrastructure, reduce risks, and promote a secure online environment.

Greece's NCSS is guided by the guiding principles of creating a safe and resilient cyberspace in accordance with national, EU, and international laws, standards, and practices.

By making use of the resources available in the academic community and from other stakeholders, this includes promoting a security culture among citizens and in the public and private sectors. With a focus on critical infrastructure and the protection of operational continuity, emphasis is put on constantly improving capabilities for protection against cyberattacks. To lessen the impact of cyber threats, the strategy places a priority on the institutional defense of the national cyber security framework and the efficient handling of cyber attack incidents. The ultimate objective is to establish a safe online environment where stakeholders and citizens can work together under the guidance of principles like justice, freedom, and openness.

The five guiding principles that serve as the foundation of the UK's NCSS. The ability of individuals and organizations to conduct business safely and securely online while exercising their legal and democratic rights is given top priority. Second, it opposes the push for fragmentation and their notion of internet sovereignty in favor of an open and interoperable internet as the best model for promoting prosperity and well-being on a global scale. The strategy places a strong emphasis on the necessity of using cyber capabilities in a legal, appropriate, and responsible manner while holding those who act irresponsibly in cyberspace accountable. Fourth, the strategy employs every available tool to combat the criminal use of the internet. Last but not least, it promotes a diverse, inclusive approach to discussions about the future of cyberspace and digital technology, protecting human rights and thwarting attempts at digital authoritarianism and state control.

There is clearly room for improvement when comparing Turkey's NCSS to those of other countries. Firstly, while Turkey acknowledges the value of cyber security as a crucial component of national security, it is important to emphasize the collaboration and digital sovereignty among the government, business sector, academic community, and general public. In order to effectively handle incidents of cyber attack, Turkey's NCSS could benefit from a stronger emphasis on the institutional shielding of the national cyber security framework. Additionally, Turkey's national strategy could prioritize and emphasize the growth of a strong security culture among the populace as well as in the public and private sectors, perhaps through collaboration with pertinent stakeholders and academic communities to better utilize pertinent capabilities. Finally, upholding the principle of open communication could promote greater transparency and public trust. In general, strengthening these designated areas of focus within Turkey's national cyber security strategy could lead to a more secure and resilient cyberspace for citizens and stakeholders to operate in safely and securely, maximizing economic and societal benefits while protecting human rights and thwarting cyber threats.

Suggestion 5. Turkey should concentrate on collaborative efforts and digital sovereignty

among stakeholders, institutional shielding of the national cyber security framework, the development of a strong culture of security, and enhancing transparency and public trust through adherence to the principle of open communication. Adopting the SMART approach, like Germany did, will be helpful for the future NCSS as well. Improvements will be seen in increased stakeholder involvement, effective stakeholder-authority communication, and better measurement and management of cyber threats by focusing on the strategic objectives mentioned.

Table 6. *Guiding Principles of various NCSS*

Country	**Guiding Principles**
Estonia	1. "We consider the protection and promotion of fundamental rights and freedoms as important in cyberspace as in the physical environment" 2. "We see cybersecurity as an enabler and amplifier of Estonia's rapid digital development, which is the basis for Estonia's socioeconomic growth. Security must support innovation and innovation must support security" 3. "We recognise the security assurance of cryptographic solutions to be of unique importance for Estonia as it is the foundation of our digital ecosystem." 4. "We consider transparency and public trust to be fundamental for digital society. Therefore, we commit to adhere to the principle of open communication."
Germany	1. "Establishing cyber security as a joint task for government, private industry, the research community and society" 2. "Reinforcing the digital sovereignty of government, private industry, the research community and society" 3. "Making digital transformation secure" 4. "Setting measurable, transparent objectives"

Continues...

Table 6 – *Continues...*

Country	**Guiding Principles**
Greece	1. "The development and establishment of a secure and resilient cyberspace which will be regulated in accordance with national, EU and international rules, standards and good practices and in which citizens, and public and private sector stakeholders can be active and interact securely, as per the values that govern the rule of law such as, indicatively, those of freedom, justice and transparency." 2. "The continuous improvement of our capabilities for protection against cyberattacks, with emphasis on critical infrastructure and the safeguarding of operational continuity" 3. "The institutional shielding of the national cyber security framework, for effective handling of cyber-attack incidents and the minimization of impact by cyberspace threats." 4. "The development of a strong culture of security in citizens and the public and private sectors, by utilizing the relevant capabilities of the academic community and of other public and private sector stakeholders."

Continues...

Table 6 – *Continues...*

Country	**Guiding Principles**
Turkey	1. “Cyber security is an integral part of national security. Full achievement of national security is only possible through reaching the goals determined in the field of cyber security” 2. “Cyber security studies are conducted in accordance with corporateness, continuity and sustainability principles from past to future, in terms of all achievements, objectives, programs and projects” 3. “In order for digitalization to be successful and sustainable, cyber security must be regarded as vitally significant” 4. “All studies related to implementation of cyber security policies are conducted with efficient communication, coordinated cooperation between stakeholders and appropriate methodologies” 5. “Stakeholders carry out their responsibilities for risk management in cyberspace with respect to transparency, accountability and ethical values” 6. “Cyber security risks are determined and managed in an efficient way” 7. “It is essential to deliver services especially the ones on critical infrastructures in a continuous and efficient manner” 8. “Cyber security is the essential component in all phases of service and product development, from design to the distribution” 9. “Adherence to basic cyber security principles such as "confidentiality-integrity-availability" balance and "need-to-know" basis is essential” 10. “It is essential to build the cyber security on strong legal foundations” 11. “Use of national and domestic products/services is encouraged with R&D, innovativeness and strong technological infrastructure understanding”

Continues...

Table 6 – *Continues...*

Country	**Guiding Principles**
United Kingdom	1. "We will prioritise the ability of citizens and businesses to operate in cyberspace safely and securely so they can maximise the economic and societal benefits of digital technology and exercise their legal and democratic rights" 2. "We will work to uphold an open and interoperable internet as the best model to support global prosperity and wellbeing, resisting the pressure of authoritarian states towards fragmentation and their idea of internet sovereignty" 3. "We will make lawful, proportionate and responsible use of our cyber capabilities, supported by clear oversight and engagement with the public and our allies, and we will hold others to account for reckless or indiscriminate behaviour in cyberspace" 4. "We will take action against the criminal use of cyberspace by all means available, calling out those who use criminal proxies or harbour criminal groups in their territories and working to prevent the proliferation of high-end cyber capabilities to criminals" 5. "We will champion an inclusive, multistakeholder approach to debates about the future of cyberspace and digital technology, upholding human rights in cyberspace and countering moves towards digital authoritarianism and state control"

There are differences between NCSS in terms of guiding principles and focus areas. In addition to emphasizing corporateness, continuity, and sustainability of cyber security, Turkey's national cyber security strategy places a high priority on effective stakeholder coordination, risk management, utilizing domestic goods and services, having strong legal foundations, and ongoing service delivery. The strategy of Estonia places a strong emphasis on fundamental freedoms and rights, the security of cryptographic solutions, open communication, and transparency. Germany's strategy emphasizes teamwork, digital sovereignty, open goals that are measurable, information security measures, effective cyber security tools and processes, and risk mitigation. Greece's cyberspace policy places a high priority on institutional defense, effective incident response, the promotion of security culture, protection of critical infrastructure, and reducing the impact of cyber threats. Last but not least, the UK's strategy places a high priority on being able to conduct business in a safe and secure manner, fighting internet fragmentation, using cyber capabilities ethically

and legally, preventing criminal use of the internet, and advancing diversity and inclusion in cyberspace discussions.

5.6 Stakeholders

Table 7 lists various stakeholders addressed by different NCSS. While Turkey and Germany list a variety of stakeholders, Estonia, Greece, and the UK list a few stakeholders. None of the NCSS explicitly address ISPs as a stakeholder, however, Estonia, Germany, Greece, and the UK implicitly address service providers. Among the various NCSS, only Greece explicitly addresses CERTs and CSIRTs, and only UK explicitly addresses SMEs as a stakeholder.

The importance of ISPs, CERTs and CSIRTs cannot be overlooked when it comes to cyber security as they are the main stakeholders responsible for defending and responding to cyber attacks. SMEs are equally important for Turkey as SMEs, numbering more than 3.2 million, constitute more than 99% of enterprises in Turkey based on a research by TOBB in late 2020 [94]. Even though SMEs are mentioned in the scope, they have not been explicitly addressed in the NCSS.

Suggestion 6. Turkey should explicitly address service providers, CERTs/CSIRTs, and SMEs as crucial stakeholders. Explicitly addressing service providers, CERTs/CSIRTs, and SMEs as crucial stakeholders will result in more comprehensive and coordinated response to cyber threat, as well as more easily understandable and clearer NCSS, resulting in more widespread adoption and adherence to NCSS. This improvement can be measured by the lessened fragmentation of the cyber security landscape and better coverage of cyber security risks.

Table 7. *Stakeholders addressed by various NCSS*

Country	**Stakeholders**
Estonia	■ “Government institutions” ■ “Academia and think tanks” ■ “Private sector”

Continues...

Table 7 – *Continues...*

Country	**Stakeholders**
Germany	■ "Government institutions" ■ "Research community" ■ "Private industry" ■ "Civil society" ■ "Associations" ■ "Foundations" ■ "Independent voluntary experts"
Greece	■ "The National Cyber Security Authority" ■ "Computer Security Incident Response Teams - CSIRTs, also known as Computer Emergency Response Teams – CERTs of public and private sector"
Turkey	■ "Public institutions" ■ "Private sector institutions and organizations, mainly the ones operating critical infrastructures" ■ "Universities" ■ "Non-governmental organizations" ■ "Research communities" ■ "Individuals in the country" ■ "International stakeholders"
United Kingdom	■ "Public and private sectors" ■ "SMEs" ■ "Academics" ■ "Other experts"

It is possible to see differences between the NCSS in terms of the stakeholders they address. In Estonia, the private sector, academic institutions, and think tanks are all addressed. In Germany, civil society, the research community, associations, foundations, and independent voluntary experts are also addressed in addition to governmental bodies and private sector

organizations. Greece primarily focuses on the public and private sector CSIRTs/CERTs and the National Cyber Security Authority. Institutions from the public and private sectors, universities, non-governmental organizations, research communities, local citizens, and external stakeholders are all addressed in Turkey. The UK addresses both the public and private sectors as well as SMEs, academics, and other professionals.

5.7 Key Planned Actions

According to Turkey's NCSS, "The complementary document of the Strategy, National Cyber Security Action Plan (2020-2023) includes in detail; the description of an action and institutions responsible for each action, institutions with which to cooperate, goals of actions and sub-actions, methods to follow while realizing those and time periods of their realization."

The key planned actions of various national cyber security strategies cannot be compared and analyzed due to the nonexistence/inaccessibility of the complementary document containing the planned actions of Turkey's national cyber security strategy.

5.8 Emerging Threats/Technologies

As mentioned in chapter 2, there are many emerging technologies. These emerging technologies will pave the way for new cyber threats, including a variety of zero-day attacks.

Table 8 lists various emerging threats and technologies addressed by different NCSS. While Greece's NCSS does not mention any, blockchain, IoT, and AI are addressed by all other NCSS. UK's NCSS covers the biggest variety of emerging technologies and threats, including even 6G, the successor of 5G.

Turkey's NCSS fails to address quantum computing (including post-quantum cryptography), big data, new semiconductor/microprocessor technologies, and eID technology even though being in the process of migrating to eID framework [95].

Suggestion 7. Turkey should address at the least quantum computing, big data, and eID as emerging technologies and threats. Addressing quantum computing, big data, and eID as emerging technologies and threats will result in enhanced preparedness and mitigation of cyber threats and protection of sensitive information. This can be measured, for example, by looking at how well the countermeasures to the perceived threats are working and will

work in the future.

Table 8. *Emerging threats/technologies covered by various NCSS*

Country	**Emerging Threats/Technologies**
Estonia	■ Blockchain ■ Cryptography ■ AI ■ eID
Germany	■ Blockchain ■ IoT ■ AI ■ 5G ■ Cloud computing ■ Quantum computing and big data ■ eID
Greece	*No emerging technologies addressed*
Turkey	■ Blockchain ■ IoT ■ AI ■ 5G ■ Cloud computing

Continues...

Table 8 – *Continues...*

Country	**Emerging Threats/Technologies**
United Kingdom	■ Blockchain ■ IoT ■ AI ■ 5G and 6G ■ Cloud computing ■ Quantum technologies (quantum computing and quantum sensing) ■ Cryptography and post-quantum cryptography ■ eID ■ "Semiconductors, microprocessor chips, microprocessor architecture, and their supply chain, design, and manufacturing process"

Based on the emerging technologies that are viewed as threats or opportunities, differences in NCSS can be seen. The Estonian NCSS is particularly interested in eID, AI, and cryptography. Blockchain, IoT, AI, 5G, cloud, quantum, big data, and eID are all covered by the German NCSS. The Greek NCSS, in contrast, does not discuss any cutting-edge technologies. The NCSS in Turkey also covers cloud computing, blockchain, IoT, AI, and 5G. Inclusion of quantum technologies (quantum computing and quantum sensing), cryptography and post-quantum cryptography, semiconductors, microprocessor chips, microprocessor architecture, and their supply chain, design, and manufacturing process distinguishes the NCSS of the United Kingdom. Furthermore, both 5G and 6G technology are covered by the UK's NCSS.

6 Cyber Security Awareness and Education Analysis

This chapter of this thesis aims to present the findings of the survey, mentioned in chapter 3.2.2, assessing the cyber security awareness and education level of Turkish citizens. The decision to target Turkish citizens was made due to the lack of up-to-date statistics on cyber security awareness and education in Turkey, whereas ENISA has recently published a report on Europe's cyber security awareness and education including references to statistics for various European countries including Estonia and Germany, and highlighting methods to improve it [96].

When interpreting the findings, it is important to keep in mind the limitations of the survey. One of the survey's biggest flaws was the 55 respondents. Thus, demographic and regional analysis cannot be done because the data might not fully represent Turkey's population. The accuracy and generalizability of the findings could be hampered by this restriction. Online self-selection of respondents may have influenced the survey's results. The sample may have been skewed if more respondents with knowledge of cyber security responded to the survey.

6.1 State Of Cyber Security Awareness And Education In Turkey

The survey was answered by 55 people. Figure 2 shows the distribution of generation of the responders. While baby boomers (born between 1946-1964), generation X (born between 1965-1980), and generation Z (born between 1997-2012) share an almost equal distribution of around 30%, generation Y (born between 1981-1996) and the alpha generation (born after 2013) make up only a small portion of the answers.

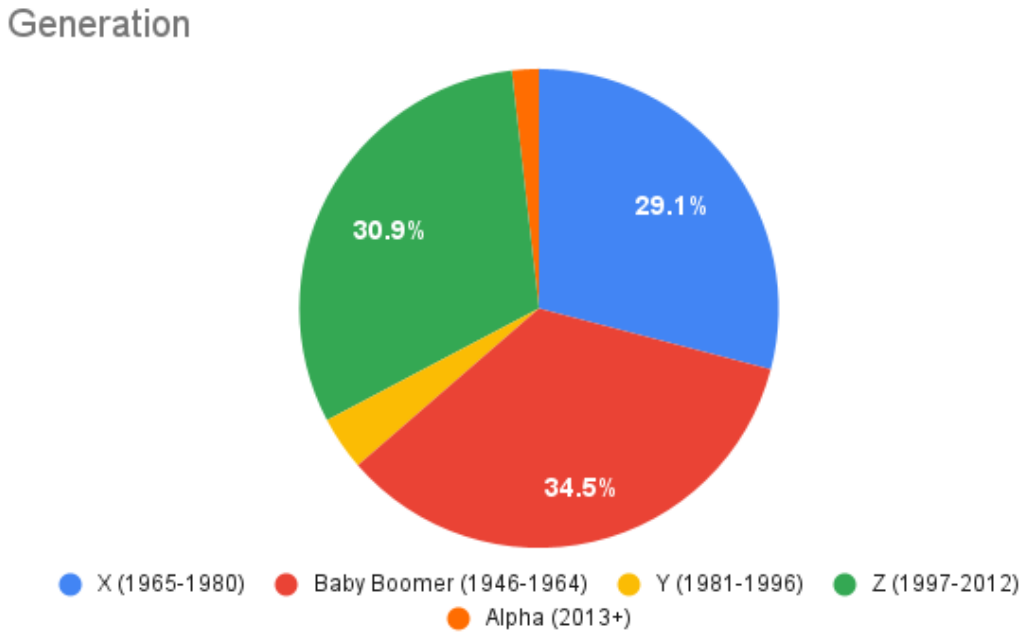

Figure 2. *Responders' generation distribution*

One of the most important and basic cyber security knowledge a person should have is the minimum requirements for a secure password. As computers and processors get faster each year, the increase in processing speed also increases the speed of brute force attacks, forcing everyone to use longer and more complex passwords. A report by Speedster IT and Hive Systems [97] show the time it takes a cyber criminal to brute force a password, displayed in Figure 3 below.

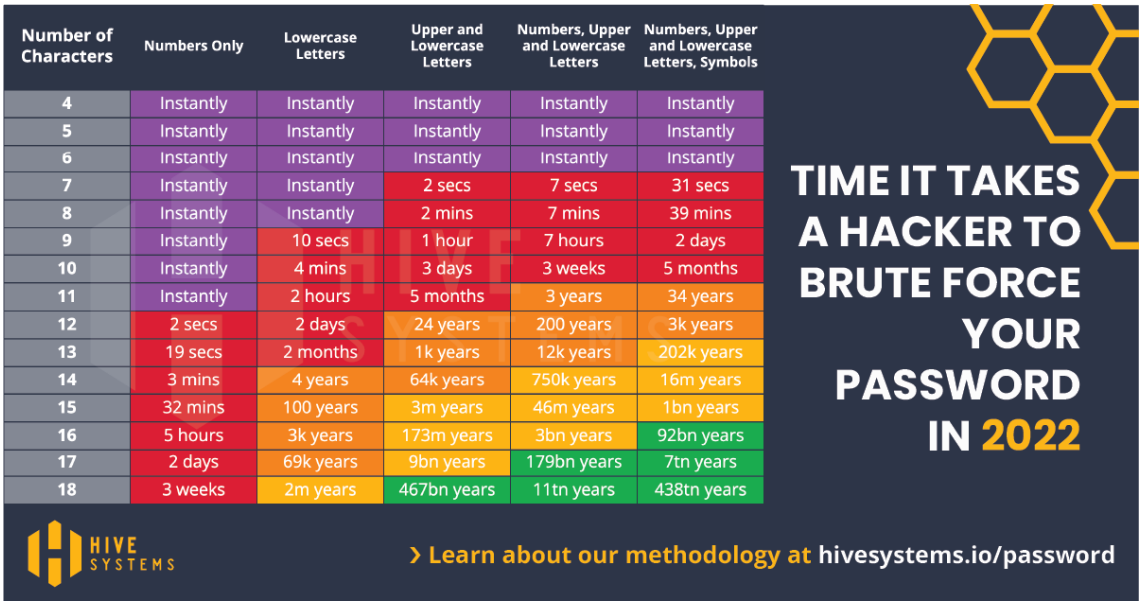

Figure 3. *Time it takes a cyber criminal to brute force a password*

Responders were asked to choose one or more options in the topic of password security. People who chose the “All of them” option, or chose all of the options manually were deemed knowledgeable in terms of minimum password security requirements. Figure 4 shows the distribution of responders who are knowledgeable when it comes to password security, 80% of responders were aware of minimum requirements for password security.

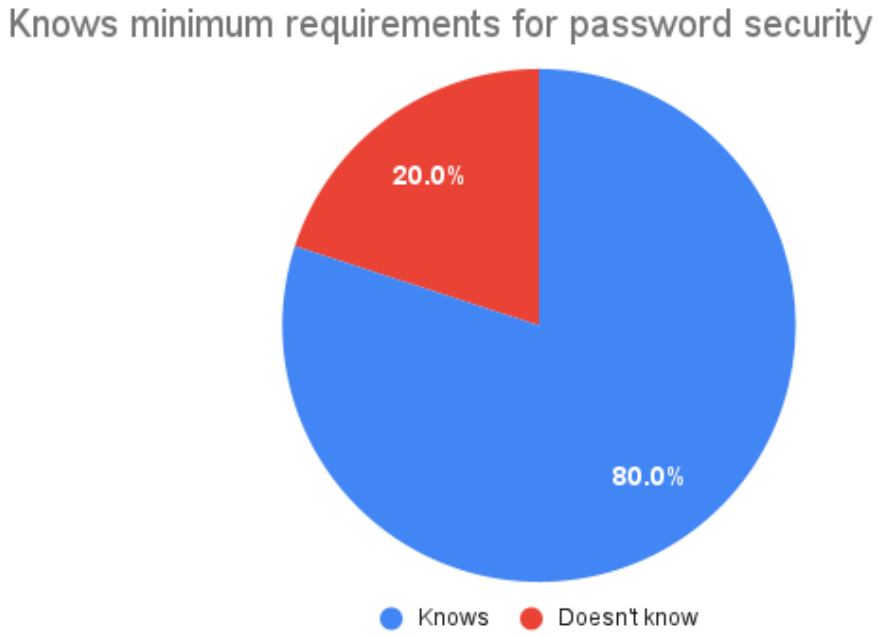

Figure 4. *Distribution of responders who know the minimum requirements for password security*

On top of the minimum requirements for password security question, responders were asked if they use the same password for more than 1 account, and what password storage method they use. It is important to use unique passwords for all important accounts as a data breach compromising a password used in multiple accounts can give the attacker easy access to all other accounts that use the same password.

Figure 5 shows the distribution of responders who use the same password for their accounts. 20% of responders stated that they use unique passwords for all of their accounts, while 49.1% stated that they use the same password for only unimportant accounts. Unfortunately, 30.9% of responders admitted that they use the same password for all/most of their accounts.

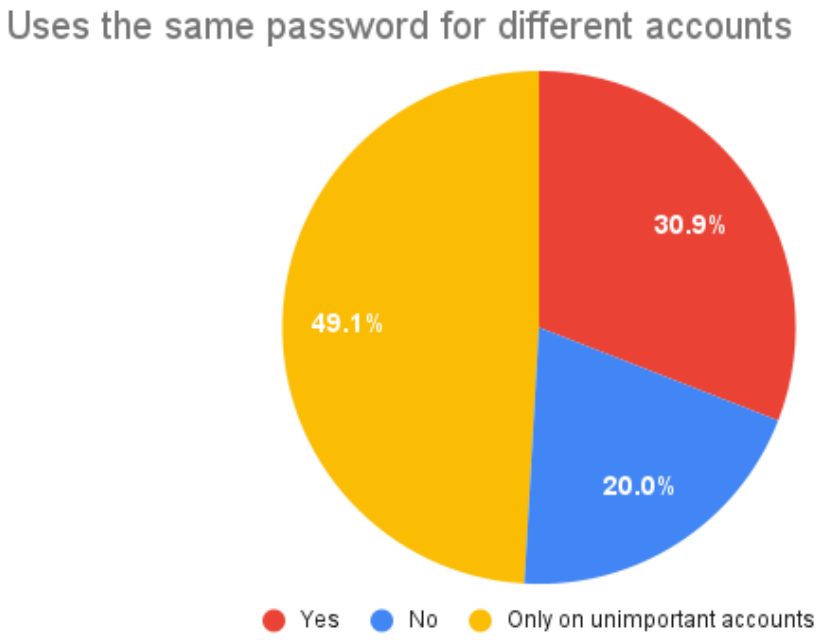

Figure 5. *Distribution of responders who use the same password for different accounts*

Figure 6 shows the distribution of password storage methods used by the responders. The majority of responders (45.5%) keep their passwords in their mind, while 30.9% write down their passwords on a piece of paper/notebook. Only 16.4% of responders use a proper password manager such as Bitwarden, whereas a surprising 7.3% of responders use the “forgot password” option each time.

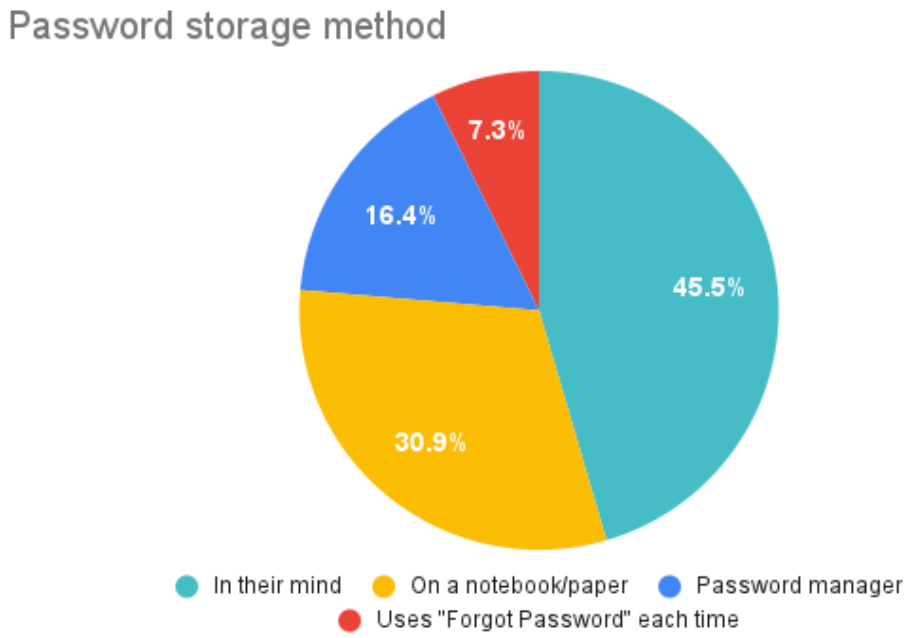

Figure 6. *Distribution of password storage methods used by responders*

A separate method of protecting online accounts is to use 2FA. Using 2FA, excluding SMS verification as it has been proven to be vulnerable [98], mitigates the risks of brute forcing, phishing and spear-phishing attacks [99]. Responders were asked if they use 2FA for their accounts other than bank accounts (normal accounts). Bank accounts were excluded from this question as all banking applications require 2FA nowadays. Figure 7 shows the percentage of responders who use 2FA for their normal accounts. While 16.4% admitted that they do not know what 2FA is, and 34.5% stated that they do not use 2FA, the remaining 49.1% stated that they use 2FA for their normal accounts.

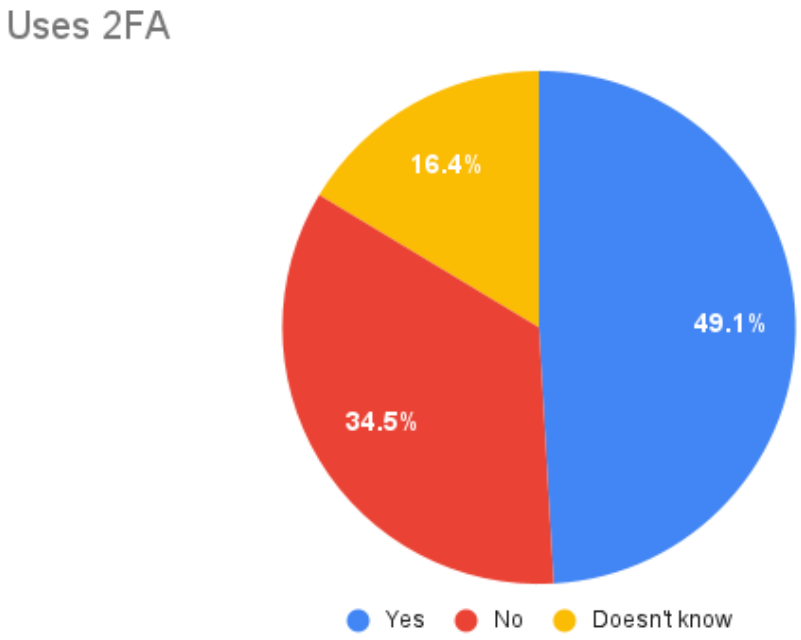

Figure 7. *Distribution of responders who use 2FA*

The main way a person can protect themselves from phishing and email-based attacks is checking the sender of an email, and not opening/reporting the email if it is from an untrustworthy or unknown source. Responders were asked if they check the sender of an email. Figure 8 shows the distribution of answers. While only a very small portion of responders do not, or just sometimes check the sender, 80% of responders stated that they always check the sender of an email. 14.5% of responders stated that they check the sender of an email only if the email looks suspicious.

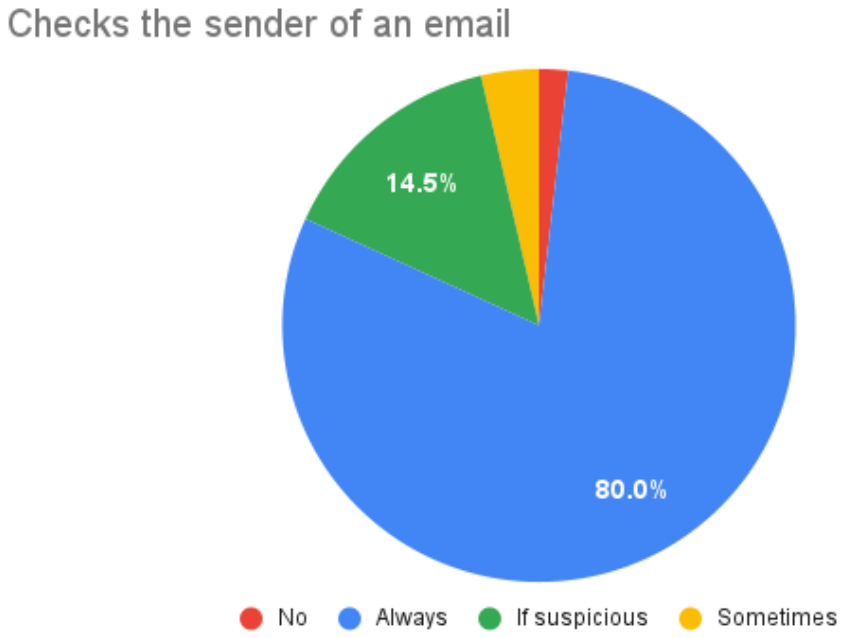

Figure 8. *Distribution of responders who check the sender of an email*

One of the primary methods of keeping a device secure is the usage of an anti-virus software. Figure 9 shows the percentage of responders who use an anti-virus software. 29.1% of responders declared that they do not use any anti-virus software, while the remaining 70.9% declared otherwise.

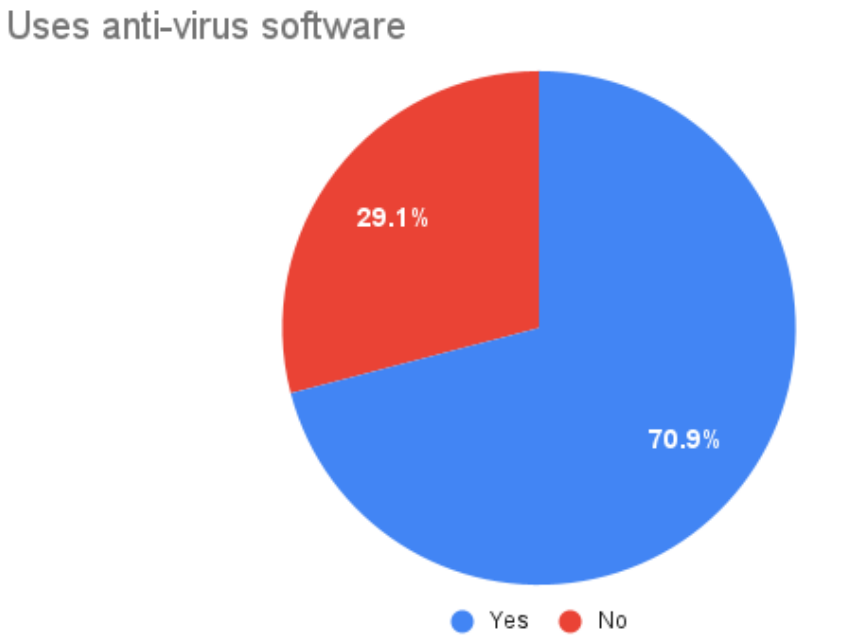

Figure 9. *Distribution of responders who use anti-virus software*

Another way of keeping a device secure, even without the use of an anti-virus software, is to scan the files downloaded from the internet using an anti-virus software or an online tool such as VirusTotal. Figure 10 shows the distribution of responders who scan downloaded files. The majority of responders, 47.3%, stated that they scan downloaded files only if the website they have downloaded the file from was untrustworthy, while 38.2% admitted that they do not scan downloaded files at all. Only 14.5% stated that they scan all of the downloaded files.

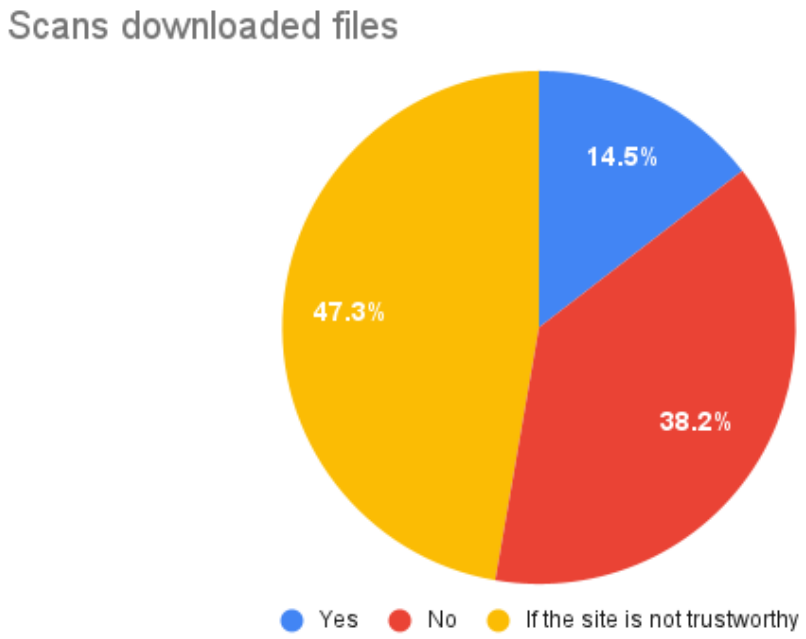

Figure 10. *Distribution of responders who check the sender of an email*

Furthermore, it is important to be aware of the risks associated with public Wi-Fi networks, such as MITM attacks. Responders were evaluated using a multi-choice question to see if they were familiar with the risks associated with public Wi-Fi usage. Responders who chose "All of them" option, or chose all of the options manually were deemed knowledgeable when it comes to the risks associated with public Wi-Fi networks. Figure 11 shows the percentage of responders who were deemed fully knowledgeable. More than half of the responders, 50.9%, were knowledgeable about the risks, while 43.6% were partially correct. Only 5.5% of responders failed to determine the risks.

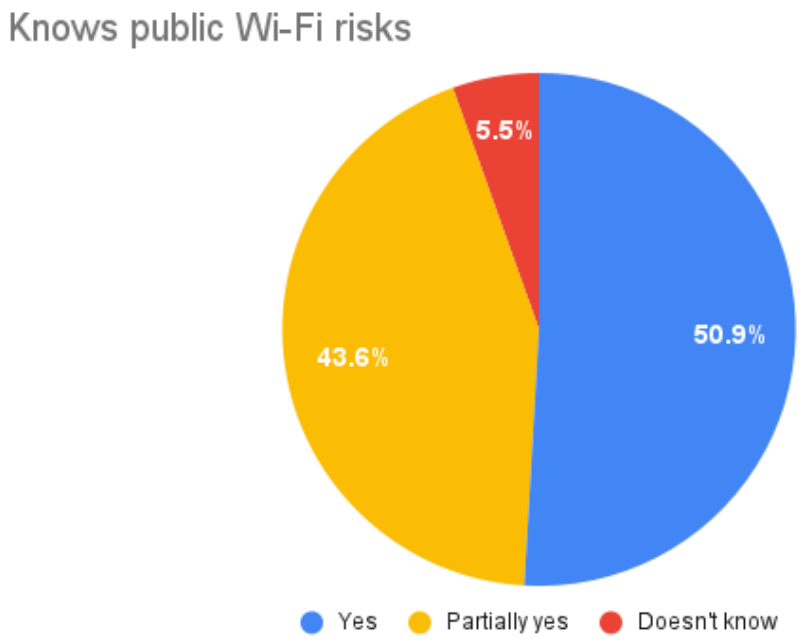

Figure 11. *Distribution of responders who know the risks associated with public Wi-Fi usage*

The primary method of protection while using a public Wi-Fi network is the usage of a VPN, as a reliable VPN software encrypts the data before it leaves the device, removing the risk of MITM attacks. Even though it is legal to use VPN in Turkey, many of the VPN providers are currently blocked by the government [100], thus responders were only asked if they knew what a VPN is. Figure 12 shows the distribution of responders who know what a VPN is. Only 14.5% of responders were unfamiliar with the term VPN, while the remaining 85.5% were familiar with the term.

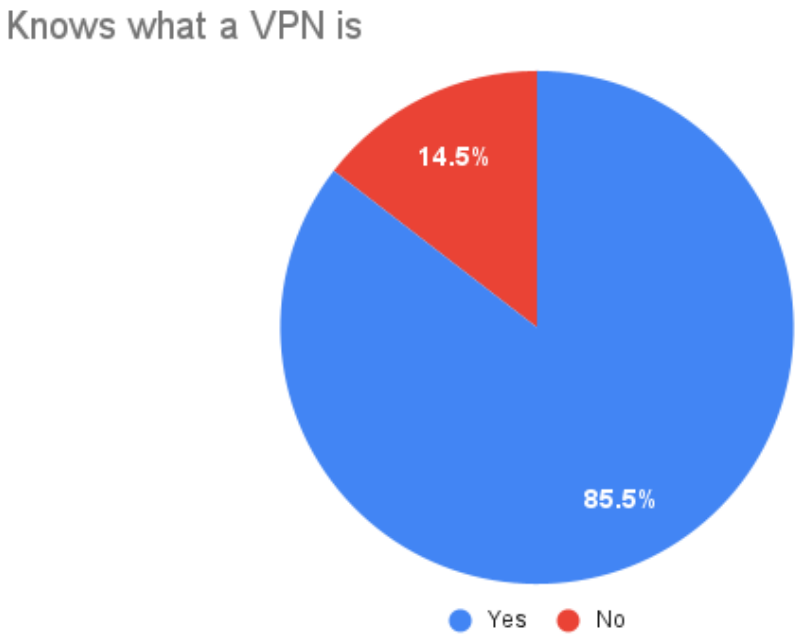

Figure 12. *Distribution of responders who know what a VPN is*

Lastly, responders were asked if they have received cyber security awareness education at school or work. Figure 13 shows the percentage of people who have, or have not received cyber security awareness education. More than two thirds of responders, 69.1%, stated that they have not received such education at school nor work. 14.5% stated that they have received it only once, while 16.4% stated that they have received it more than once.

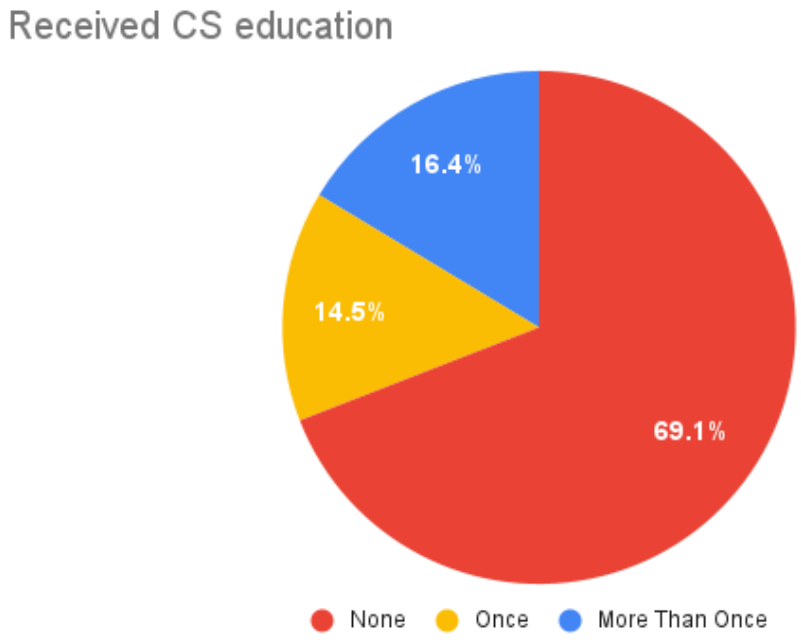

Figure 13. *Distribution of responders who have received cyber security awareness education at school or work*

6.2 Suggestions For Raising Cyber Security Awareness And Education In Turkey

From the result of this survey and the last question of the survey, it can be concluded that Turkey is lacking in cyber security awareness and education, even though the NCSS includes cyber security awareness education.

ENISA has already prepared a report on raising the cyber security awareness and education in Europe [96]. The following recommendations were stated in the report:

- "building capacities for cybersecurity awareness"
- "regular assessments of cybersecurity trends and challenges,"
- "measuring cybersecurity behaviour, and"
- "planning for cybersecurity awareness campaigns."

Simply following these recommendations and consulting experts will have a dramatic impact on cyber security awareness and education in Turkey, however, an extra step can be taken by implementing Awareness Raising in a Box (AR-in-a-BOX) package in SMEs.

Suggestion 8. Turkey should take experts' opinions and ENISA's recommendations into

account while planning the cyber security awareness education in the country, increasing the budget allocated for campaigns and education if needed. Preparation of a package similar to AR-in-a-BOX for SMEs in Turkey will contribute immensely in achieving a proper cyber security awareness and education level in the country. Improvements will be seen in increased awareness and education efforts if the country plans cyber security awareness education in accordance with the opinions of experts and ENISA's recommendations and creates a package similar to AR-in-a-BOX for SMEs. This can be measured by increased understanding and adoption of cyber security best practices among the public, businesses, and other stakeholders in Turkey, for example, by utilizing regular surveys, drills, etc.

7 Discussion And Conclusion

In order to improve Turkey's NCSS, this thesis examined the NCSS of Greece, Turkey, the UK, Germany, and Estonia and identified differences in cybersecurity definitions, objectives, priorities, perceived threats, emerging technologies, and stakeholder involvement. This section discusses potential improvements, as well as proposes methods to measure and formalise the results of the suggestions.

7.1 Summary Of Findings

The results show that there are significant differences between the NCSS definitions and descriptions of cyber security, with some nations providing a thorough framework for stakeholder coordination and asset protection while others take a more specialized and in-depth approach to strategic objectives. Similar to priorities, national priorities have different focus areas and guiding principles. Emerging technologies and identified stakeholders vary across nations as well. Overall, it can be said that NCSS have different strategies for dealing with cyber threats and governance.

Another finding of the thesis is that, despite including cyber security awareness education in its national cyber security strategy, Turkey's level of cyber security awareness and education was found to be low based on survey data. This suggests that Turkey's efforts to implement cyber security education and develop more successful awareness campaigns could use some improvement.

Despite these variations, the thesis emphasized the value of collaboration and all-encompassing strategies for cybersecurity governance. The thesis emphasized that NCSS should give priority to effective stakeholder coordination, risk management, transparency, and the capacity to conduct business in a safe and secure manner regardless of different priorities and objectives. The study acknowledges the significance of tailored approaches to cybersecurity governance given that every country will have different cybersecurity priorities and challenges, necessitating the creation of an NCSS tailored to each country's particular requirements. The conclusions of this thesis urge further investigation in order to strengthen and clarify the observed differences in NCSS.

7.2 Implications And Contributions

As a result of these findings, 8 suggestions were made in various areas with the objective of improving Turkey's NCSS:

- **Suggestion 1.** Turkey, and all other countries with international collaboration in mind should agree on a common definition and description for "cyber security". Improved inter-country alignment and effective communication will result in countries cooperating internationally coming to an agreement on a common definition and description of the term "cyber security". This will improve the efficiency of cross-country cooperation, and will improve countries cyber capabilities. One of the ways this improvement can be measured by is the increased consistency and clarity in cyber security efforts and strategies across borders.
- **Suggestion 2.** Turkey should have a more detailed and concrete vision, like Estonia and the UK. As for the mission, other countries should take Turkey's mission statement as an example because only Turkey's NCSS mission statement adheres to the definition of a mission statement. Having a more detailed and concrete vision will result in increased stakeholder buy-in and effectiveness of cyber security improvement efforts. This improvement could be measured by potentially observing improved investors' buy-in.
- **Suggestion 3.** Turkey should address cyber threats that have been found to be as damaging as the others, such as fake news/disinformation, DDoS, and cyber espionage/sabotage. Addressing common cyber threats like fake news/disinformation, DDoS, and cyber espionage/sabotage will result in improved critical asset and sensitive information protection. This improvement can be measured by a decreased number of successful attacks and a strengthened national cyber security infrastructure.
- **Suggestion 4.** Turkey should take Germany and the UK's NCSS strategic objectives as an example to prepare a more in-depth, all encompassing understanding of objectives. Improvements in better alignment and effective communication between stakeholders and authorities will be seen by adopting Germany's and the UK's NCSS strategic objectives as an example through developing a more detailed and in-depth objective collection. This improvement can be measured by more consistent responses to cyber threats, and quicker detection, response, and remediation of cyber threats.
- **Suggestion 5.** Turkey should concentrate on collaborative efforts and digital sovereignty among stakeholders, institutional shielding of the national cyber security framework, the development of a strong culture of security, and enhancing transparency and public trust through adherence to the principle of open communi-

cation. Adopting the SMART approach, like Germany did, will be helpful for the future NCSS as well. Improvements will be seen in increased stakeholder involvement, effective stakeholder-authority communication, and better measurement and management of cyber threats by focusing on the strategic objectives mentioned.

- **Suggestion 6.** Turkey should explicitly address service providers, CERTs/CSIRTs, and SMEs as crucial stakeholders. Explicitly addressing service providers, CERTs/CSIRTs, and SMEs as crucial stakeholders will result in more comprehensive and coordinated response to cyber threat, as well as more easily understandable and clearer NCSS, resulting in more widespread adoption and adherence to NCSS. This improvement can be measured by the lessened fragmentation of the cyber security landscape and better coverage of cyber security risks.
- **Suggestion 7.** Turkey should address at the least quantum computing, big data, and eID as emerging technologies and threats. Addressing quantum computing, big data, and eID as emerging technologies and threats will result in enhanced preparedness and mitigation of cyber threats and protection of sensitive information. This can be measured, for example, by looking at how well the countermeasures to the perceived threats are working and will work in the future.
- **Suggestion 8.** Turkey should take experts' opinions and ENISA's recommendations into account while planning the cyber security awareness education in the country, increasing the budget allocated for campaigns and education if needed. Preparation of a package similar to AR-in-a-BOX for SMEs in Turkey will contribute immensely in achieving a proper cyber security awareness and education level in the country. Improvements will be seen in increased awareness and education efforts if the country plans cyber security awareness education in accordance with the opinions of experts and ENISA's recommendations and creates a package similar to AR-in-a-BOX for SMEs. This can be measured by increased understanding and adoption of cyber security best practices among the public, businesses, and other stakeholders in Turkey, for example, by utilizing regular surveys, drills, etc.

These suggestions cover a range of topics, including standardizing terminology used in cyber security, creating a clear vision, addressing new cyber threats, improving transparency, and stepping up efforts in awareness and education. Additionally, while addressing emerging technologies and threats, the suggestions encourage participation of key stakeholders such as service providers, CERTs/CSIRTs, and SMEs. Together, these suggestions could help foster cooperation, digital sovereignty, and a culture of security, all of which could help Turkey's NCSS become better and more efficient.

7.3 Limitations And Future Research Directions

The scope of the study is primarily responsible for this thesis's limitations. In particular, neither the legal considerations of national cyber security strategies nor the implementation of the thesis' suggestions were addressed. Additionally, it did not thoroughly examine the NCSS's primary planned actions due to them being unavailable, which could have revealed more information about their overall strategies.

To better comprehend the full scope of national cyber security strategies, future research directions may explore these areas of limitation. Research might also look at how legal frameworks might affect how NCSS are implemented and how much they are actually used in daily life. Additional analysis could look at the implementation procedure and results, as well as the efficacy of the suggested interventions for enhancing national cyber security strategies.

When interpreting the findings, it is important to be aware of the limitations of the survey used for this thesis. The survey's small sample size, which consisted of only 55 respondents, is one of its biggest limitations. As a result, it is possible that the data are not representative of Turkey's entire population, and chances for demographic and regional analysis are lost. As a result, this restriction may jeopardize the findings' accuracy and generalizability. Furthermore, because the survey was conducted online, there may have been a bias in the selection of respondents because they self-selected. It's possible that respondents who were more knowledgeable or interested in cyber security were more likely to complete the survey, producing a sample that is skewed.

Future studies in this field might take into account these drawbacks and try to fix them. A larger and more varied sample size of respondents could be used in subsequent studies, enabling a better representation of the population and a higher likelihood of conducting regional and demographic analysis. Alternative sampling methods, such as stratified or random sampling rather than self-selection, may also aid in addressing issues with selection bias. Last but not least, it would be helpful to conduct a follow-up study to evaluate any changes in cyber security education and awareness levels as a result of any NCSS advancements and awareness campaigns launched after the thesis.

The future of national cyber security strategies may be impacted by emerging technologies and cyber threats, so more research may be required to understand this. Research could focus on the potential benefits and dangers brought about by new technologies as well as how NCSS can adjust to meet these challenges. Finally, to gain a deeper understanding of the crucial role stakeholders play in national cyber security strategies, research could look

at the complexity of stakeholder involvement, including partnerships and collaboration between public and private entities.

References

[1] *Kaspersky cyberthreat real-time map*, en. [Online]. Available: https://cybermap.kaspersky.com/stats.

[2] Panlogic, *Cyber crime*, en-GB, Apr. 2023. [Online]. Available: https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime.

[3] *Impact of cyber attack on your business*. [Online]. Available: https://www.nibusinessinfo.co.uk/content/impact-cyber-attack-your-business.

[4] *Significant cyber incidents*, en. [Online]. Available: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

[5] M. Zwilling, G. Klien, D. Lesjak, Ł. Wiechetek, F. Cetin, and H. N. Basim, "Cyber security awareness, knowledge and behavior: A comparative study," en, *Journal of Computer Information Systems*, vol. 62, no. 1, pp. 82–97, Jan. 2022, ISSN: 0887-4417, 2380-2057. DOI: 10.1080/08874417.2020.1712269. [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/08874417.2020.1712269.

[6] *What is cyber security?* en. [Online]. Available: https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security.

[7] *What is a cyber attack?* en-US. [Online]. Available: https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cyber-attack/.

[8] *Enisa and cyber security strategies*, en, Page. [Online]. Available: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-ncss.

[9] *What is cyber warfare?* en. [Online]. Available: https://www.fortinet.com/resources/cyberglossary/cyber-warfare.

[10] *Denial of service (dos) guidance*, en. [Online]. Available: https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection.

[11] *What is a social engineering attack in cybersecurity?* en. [Online]. Available: https://www.cisco.com/c/en_uk/products/security/what-is-social-engineering.html.

[12] *Physical social engineering attacks: How ready are you?* en, Jan. 2020. [Online]. Available: https://welcomegate.com/physical-social-engineering-attacks-how-ready-are-you/.

[13] Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, "Phishing attacks: A recent comprehensive study and a new anatomy," *Frontiers in Computer Science*, vol. 3, p. 563 060, Mar. 2021, ISSN: 2624-9898. DOI: 10.3389/fcomp.2021.563060. [Online]. Available: https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060/full.

[14] *10 common social engineering attacks*, en. [Online]. Available: https://www.beyondtrust.com/blog/entry/top-social-engineering-attacks.

[15] *Business email compromise (bec) - the different types of attacks*, en-US. [Online]. Available: https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-email-security/business-email-compromise-bec/.

[16] *Watering hole attacks*, en. [Online]. Available: https://www.ncsc.gov.uk/collection/supply-chain-security/watering-hole-attacks.

[17] K. Matthews, *What does fake news have to do with cybersecurity? a lot*, en-US, Jun. 2019. [Online]. Available: https://securityboulevard.com/2019/06/what-does-fake-news-have-to-do-with-cybersecurity-a-lot/.

[18] D. De Beer and M. Matthee, "Approaches to identify fake news: A systematic literature review," en, in *Integrated Science in Digital Age 2020*, T. Antipova, Ed. Cham: Springer International Publishing, 2021, vol. 136, pp. 13–22, ISBN: 9783030492632. DOI: 10.1007/978-3-030-49264-9_2. [Online]. Available: http://link.springer.com/10.1007/978-3-030-49264-9_2.

[19] *What is deepfake*, en. [Online]. Available: https://www.fortinet.com/resources/cyberglossary/deepfake.

[20] *What is a trojan horse and what damage can it do?* en-gb, Apr. 2023. [Online]. Available: https://www.kaspersky.co.uk/resource-center/threats/trojans.

[21] *What is malware?* en. [Online]. Available: https://www.malwarebytes.com/malware.

[22] *What is spyware?* en-gb, Apr. 2023. [Online]. Available: https://www.kaspersky.co.uk/resource-center/threats/spyware.

[23] *What is ransomware?* en-gb, Apr. 2023. [Online]. Available: https://www.kaspersky.co.uk/resource-center/threats/ransomware.

[24] *What is a brute force attack?* en. [Online]. Available: https://www.fortinet.com/resources/cyberglossary/brute-force-attack.

[25] *Man-in-the-middle*, en, Page. [Online]. Available: https://www.enisa.europa.eu/topics/incident-response/glossary/man-in-the-middle.

[26] *What is identity theft?* en-US. [Online]. Available: https://terranovasecurity.com/what-is-identity-theft/.

[27] *What is an impersonation attack?* en. [Online]. Available: https://www.upguard.com/blog/impersonation-attack.

[28] *5g/6g wireless networks*. [Online]. Available: https://www.dhs.gov/science-and-technology/5g6g.

[29] *What is artificial intelligence (ai)?* en-us. [Online]. Available: https://www.ibm.com/topics/artificial-intelligence.

[30] R. Hastings, *Examples of artificial intelligence (ai) in 7 industries*. [Online]. Available: https://emeritus.org/blog/examples-of-artificial-intelligence-ai/.

[31] M. Anderson, *The impact of ai on cybersecurity*, en-US, Mar. 2020. [Online]. Available: https://www.computer.org/publications/tech-news/trends/the-impact-of-ai-on-cybersecurity/.

[32] *Data poisoning: When attackers turn ai and ml against you*, en-US. [Online]. Available: https://securityintelligence.com/articles/data-poisoning-ai-and-machine-learning/.

[33] *What is blockchain technology?* en-us. [Online]. Available: https://www.ibm.com/topics/blockchain.

[34] *8 blockchain security issues you are likely to encounter*, en, May 2023. [Online]. Available: https://cybersecurity.att.com/blogs/security-essentials/8-blockchain-security-issues-you-are-likely-to-encounter.

[35] *What is cloud computing?* en-us. [Online]. Available: https://www.ibm.com/topics/cloud-computing.

[36] *Top cloud security issues, threats and concerns*, en-US. [Online]. Available: https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/top-cloud-security-issues-threats-and-concerns/.

[37] D. Walkowski Shahnawaz Backer, *Digital identity is an increasingly popular attack vector for cybercriminals*, en, Aug. 2020. [Online]. Available: https://www.f5.com/labs/learning-center/digital-identity-is-an-increasingly-popular-attack-vector-for-cybercriminals.

[38] *What is the internet of things (iot)?* en-GB. [Online]. Available: https://www.oracle.com/uk/internet-of-things/what-is-iot/.

[39] *Iot connected devices worldwide 2019-2030*, en. [Online]. Available: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/.

[40] *What is quantum computing?* en-us. [Online]. Available: https://www.ibm.com/topics/quantum-computing.

[41] *Quantum sensing applications*, EN. [Online]. Available: https://www.cambridgeconsultants.com/insights/opinion/what-is-quantum-sensing.

[42] *How will quantum technologies change cryptography?* en. [Online]. Available: http://scienceexchange.caltech.edu/topics/quantum-science-explained/quantum-cryptography.

[43] *The quantum computing impact on cybersecurity*, en, Jan. 2020. [Online]. Available: https://quantumxc.com/blog/quantum-computing-impact-on-cybersecurity/.

[44] *What is vpn?* en, Apr. 2023. [Online]. Available: https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn.

[45] *Cyber security strategy for germany 2021*, en, 2021. [Online]. Available: https://www.bmi.bund.de/SharedDocs/downloads/EN/themen/it-digital-policy/cyber-security-strategy-for-germany2021.pdf;jsessionid=055F743A5C83903AA13FB8B6392419AB.1_cid322?__blob=publicationFile&v=4.

[46] *National cyber strategy 2022 (html)*, en. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1049825/government-cyber-security-strategy.pdf.

[47] *Cybersecurity strategy*, 2019. [Online]. Available: https://www.mkm.ee/media/703/download.

[48] 499, *Greece cyber security strategy*, en. [Online]. Available: https://www.trade.gov/market-intelligence/greece-cyber-security-strategy.

[49] *National cyber security strategy*, 2020. [Online]. Available: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/GRNCSS_EN.pdf.

[50] *National cybersecurity strategy and action plan*. [Online]. Available: https://cbddo.gov.tr/en/national-cybersecurity-strategy/.

[51] Surfshark, *Data breach statistics by country: First quarter of 2022*, en-US, Apr. 2022. [Online]. Available: https://surfshark.com/blog/data-breach-statistics-by-country.

[52] *Incident reports and news*, en-US. [Online]. Available: https://turkeyblocks.org/reports/.

[53] J. Murdock, *Turkey blocks google, microsoft and dropbox services to "suppress" mass email leaks*, en, Oct. 2016. [Online]. Available: https://www.ibtimes.co.uk/turkey-blocks-google-microsoft-dropbox-services-suppress-mass-email-leaks-1585655.

[54] C. Sezer and B. Altayli, *Turkey's akbank faces $4 million hit from attempted cyber heist*, en. [Online]. Available: https://www.thefiscaltimes.com/latestnews/2016/12/16/Turkeys-Akbank-says-targeted-hackers-no-security-breach.

[55] *Cyberattack steals info of one million in turkey's konya*, en-US, May 2021. [Online]. Available: https://www.dailysabah.com/turkey/investigations/cyberattack-steals-info-of-one-million-in-turkeys-konya.

[56] en. [Online]. Available: https://twitter.com/yemeksepeti/status/1375764826241314818.

[57] *Yemeksepeti hacklendi mi?* tr, Mar. 2021. [Online]. Available: https://www.hurriyet.com.tr/ekonomi/yemeksepetinden-siber-saldiri-aciklamasi-41773352.

[58] D. Çağıl, Ed., *Tedaş'a siber saldırı*, tr. [Online]. Available: https://www.tgrthaber.com.tr/gundem/tedas-siber-saldiriya-maruz-kaldi-2837280.

[59] F. Yurtsever, "[analysis] turkey's critical defense projects under cyber attack," en, Feb. 2022. [Online]. Available: https://turkishminute.com/2022/09/02/defense-projects-under-cyber-attack/.

[60] *2023 turkey-syria earthquake*, en-US, Apr. 2023. [Online]. Available: https://disasterphilanthropy.org/disasters/2023-turkey-syria-earthquake/.

[61] *Cyber scams are exploiting türkiye-syria earthquake relief efforts*, en, Feb. 2023. [Online]. Available: https://www.weforum.org/agenda/2023/02/cyber-scams-exploit-turkey-syria-earthquake-relief/.

[62] J. Kilner and D. Millward, "Russian hackers disrupt turkey-syria earthquake relief," en-GB, *The Telegraph*, Feb. 2023, ISSN: 0307-1235. [Online]. Available: https://www.telegraph.co.uk/world-news/2023/02/12/russian-killnet-hackers-disrupt-natos-turkey-syria-earthquake/.

[63] *Programmable search engine by google*, en. [Online]. Available: https://programmablesearchengine.google.com/about/.

[64] *Attention Spans*. Canada, 2015, p. 52. [Online]. Available: https://dl.motamem.org/microsoft-attention-spans-research-report.pdf.

[65] H. A. M. Luiijf, K. Besseling, M. Spoelstra, and P. de Graaf, "Ten national cyber security strategies: A comparison," in *Critical Information Infrastructure Security*, S. Bologna, B. Hämmerli, D. Gritzalis, and S. Wolthusen, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 1–17, ISBN: 978-3-642-41476-3.

[66] M. A. Alqahtani, "Factors affecting cybersecurity awareness among university students," *Applied Sciences*, vol. 12, no. 5, p. 2589, Mar. 2022, ISSN: 2076-3417. DOI: 10.3390/app12052589. [Online]. Available: http://dx.doi.org/10.3390/app12052589.

[67] *Phishing simulator*. [Online]. Available: https://keepnetlabs.com/wp-content/uploads/2022/02/Phishing-Simulator-v1.3.pdf.

[68] C. Crane, *The dirty dozen: The 12 most costly phishing attack examples*. [Online]. Available: https://www.thesslstore.com/blog/the-dirty-dozen-the-12-most-costly-phishing-attack-examples/#:~:text=At%20some%20level,%20everyone%20is%

20susceptible%20to%20phishing,outright%20trick%20you%20into%20performing%20a%20particular%20task.

[69] S. Furnell, "An assessment of website password practices," en, *Computers & Security*, vol. 26, no. 7, pp. 445–451, Dec. 2007, ISSN: 0167-4048. DOI: 10.1016/j.cose.2007.09.001. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404807001083.

[70] *Enterprise phishing resiliency and defense report*, publisher: PhishMe, Inc., 2017. [Online]. Available: https://cofense.com/wp-content/uploads/2017/11/Enterprise-Phishing-Resiliency-and-Defense-Report-2017.pdf.

[71] R. Lininger and R. D. Vines, *Phishing: cutting the identity theft line*. Indianapolis, IN: Wiley Pub, 2005, ISBN: 9780764584985.

[72] G. Keinan, "Decision making under stress: Scanning of alternatives under controllable and uncontrollable threats.," en, *Journal of Personality and Social Psychology*, vol. 52, no. 3, pp. 639–644, 1987, ISSN: 1939-1315, 0022-3514. DOI: 10.1037/0022-3514.52.3.639. [Online]. Available: http://doi.apa.org/getdoi.cfm?doi=10.1037/0022-3514.52.3.639.

[73] E. J. Williams, J. Hinds, and A. N. Joinson, "Exploring susceptibility to phishing in the workplace," en, *International Journal of Human-Computer Studies*, vol. 120, pp. 1–13, Dec. 2018, ISSN: 1071-5819. DOI: 10.1016/j.ijhcs.2018.06.004. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1071581918303628.

[74] *Caught on the net!* en-GB. [Online]. Available: https://www.getsafeonline.org/personal/news-item/caught-on-the-net/.

[75] S. Ong, *Avast survey shows men more susceptible to mobile malware*. [Online]. Available: https://www.mirekusoft.com/avast-survey-shows-men-more-susceptible-to-mobile-malware/.

[76] L. Hadlington, "Human factors in cybersecurity; examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours," en, *Heliyon*, vol. 3, no. 7, e00346, Jul. 2017, ISSN: 24058440. DOI: 10.1016/j.heliyon.2017.e00346. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S2405844017309982.

[77] C. Iuga, J. R. C. Nurse, and A. Erola, "Baiting the hook: Factors impacting susceptibility to phishing attacks," en, *Human-centric Computing and Information Sciences*, vol. 6, no. 1, p. 8, Jun. 2016, ISSN: 2192-1962. DOI: 10.1186/s13673-016-

0065-2. [Online]. Available: https://doi.org/10.1186/s13673-016-0065-2.

[78] J. Lin, S. Amini, J. I. Hong, N. Sadeh, J. Lindqvist, and J. Zhang, "Expectation and purpose: Understanding users' mental models of mobile app privacy through crowdsourcing," in *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*, ser. UbiComp '12, Pittsburgh, Pennsylvania: Association for Computing Machinery, 2012, pp. 501–510, ISBN: 9781450312240. DOI: 10.1145/2370216.2370290. [Online]. Available: https://doi.org/10.1145/2370216.2370290.

[79] E. Yeboah-Boateng and P. Amanor, "Phishing, smishing & vishing: An assessment of threats against mobile devices," English, *Journal of Emerging Trends in Computing and Information Sciences*, vol. 5, no. 4, pp. 297–307, Apr. 2014, ISSN: 2079-8407.

[80] N. Huaman, B. von Skarczinski, D. Wermke, *et al.*, "A large-scale interview study on information security in and attacks against small and medium-sized enterprises," in *In 30th USENIX Security Symposium*, 2021.

[81] M. A. Lopez, J. M. Lombardo, M. López, *et al.*, "Intelligent detection and recovery from cyberattacks for small and medium-sized enterprises," en, *International Journal of Interactive Multimedia and Artificial Intelligence*, vol. 6, no. 3, p. 55, 2020, ISSN: 1989-1660. DOI: 10.9781/ijimai.2020.08.003. [Online]. Available: https://www.ijimai.org/journal/sites/default/files/2020-08/ijimai_6_3_7.pdf.

[82] *Cyber security strategy for germany*, en. [Online]. Available: https://www.bmi.bund.de/EN/topics/it-internet-policy/cyber-security-strategy/cyber-security-strategy-artikel.html;jsessionid=9B7B3D4CC08C9CD39998DB71D47C03FD.1_cid364?nn=16825398.

[83] *Turkey reveals its three-year cybersecurity plan*, en. [Online]. Available: https://www.trtworld.com/magazine/turkey-reveals-its-three-year-cybersecurity-plan-42820.

[84] D. Štitilis, P. Pakutinskas, and I. Malinauskaitė, "Eu and nato cybersecurity strategies and national cyber security strategies: A comparative analysis," en, *Security Journal*, vol. 30, no. 4, pp. 1151–1168, Oct. 2017, ISSN: 0955-1662, 1743-4645. DOI: 10.1057/s41284-016-0083-9. [Online]. Available: http://link.springer.com/10.1057/s41284-016-0083-9.

[85] O. V. Sviatun, O. V. Goncharuk, C. Roman, O. Kuzmenko, and I. V. Kozych, "Combating cybercrime: Economic and legal aspects," en, *WSEAS TRANSACTIONS ON BUSINESS AND ECONOMICS*, vol. 18, pp. 751–762, Apr. 2021, ISSN: 2224-2899, 1109-9526. DOI: 10.37394/23207.2021.18.72. [Online]. Available: https://wseas.com/journals/bae/2021/b465107-1330.pdf.

[86] E. Halisdemir, *National Cybersecurity Organisation: TURKEY* (National Cybersecurity Organisation), en. Tallinn, 2021, p. 19. [Online]. Available: https://ccdcoe.org/uploads/2018/10/TUR_country-report_final-ver-for-publication_August-2021.pdf.

[87] Republic of Turkey Ministry of Transport and Infrastructure, 2020. [Online]. Available: https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/national-cyber-security-strategy-2020-2023.pdf.

[88] D. Schatz, R. Bashroush, and J. Wall, "Towards a more representative definition of cyber security," *The Journal of Digital Forensics, Security and Law*, 2017, ISSN: 15587223. DOI: 10.15394/jdfsl.2017.1476. [Online]. Available: https://commons.erau.edu/jdfsl/vol12/iss2/8/.

[89] C. K. Bart, "The relationship between mission statements and firm performance: An exploratory study," en, *Journal of Management Studies*, vol. 35, no. 6, pp. 823–853, Nov. 1998, ISSN: 0022-2380, 1467-6486. DOI: 10.1111/1467-6486.00121. [Online]. Available: https://onlinelibrary.wiley.com/doi/10.1111/1467-6486.00121.

[90] A. r. a. r. o. o. Publisher, "4.3 the roles of mission, vision, and values," en, Oct. 2015. [Online]. Available: https://open.lib.umn.edu/principlesmanagement/chapter/4-3-the-roles-of-mission-vision-and-values/.

[91] *How does the immune system work?* en. Institute for Quality and Efficiency in Health Care (IQWiG), Apr. 2020. [Online]. Available: https://www.ncbi.nlm.nih.gov/books/NBK279364/.

[92] D. SABAH, *Turkey most exposed country to fake news globally: Altun*, en-US, Dec. 2021. [Online]. Available: https://www.dailysabah.com/politics/turkey-most-exposed-country-to-fake-news-globally-altun/news.

[93] R. Michaelson, "Turkey: New 'disinformation' law could jail journalists for three years," en-GB, *The Guardian*, Oct. 2022, ISSN: 0261-3077. [Online]. Available: https://www.theguardian.com/world/2022/oct/13/turkey-

new-disinformation-law-could-jail-journalists-for-3-years.

[94] *SMEs of Turkey*. 2020. [Online]. Available: https://www.tobb.org.tr/KobiArastirma/Documents/SMEs%5C%20of%5C%20Turkey%5C%20Report%5C%202020.pdf.

[95] *Digital türkiye*. [Online]. Available: https://cbddo.gov.tr/en/faq/digital-turkey.

[96] *Raising awareness of cybersecurity*, en, Report/Study. [Online]. Available: https://www.enisa.europa.eu/publications/raising-awareness-of-cybersecurity.

[97] S. IT, *How long to brute force a password 2022 2023 | speedster it*, en-GB, Jan. 2023. [Online]. Available: https://www.speedster-it.com/how-long-to-brute-force-a-password-in-2022/.

[98] T. Shyamsundar, *What is sms authentication and is it secure?* en-GB, 2020. [Online]. Available: https://www.okta.com/uk/blog/2020/10/sms-authentication/.

[99] *What is two factor authentication | pros and cons of 2fa | imperva*, en-US. [Online]. Available: https://www.imperva.com/learn/application-security/2fa-two-factor-authentication/.

[100] M. Shanice Basa, *Are vpns legal in turkey? the definitive guide (2023)*, en. [Online]. Available: https://www.wizcase.com/blog/are-vpns-legal-in-turkey-definitive-guide/.

Appendix 1 – Non-exclusive license for reproduction and publication of a graduation thesis[1]

I, Adil Atalay Hamamcıoğlu

1. Grant Tallinn University of Technology free license (non-exclusive license) for my thesis "Improving Turkey's National Cyber Security Framework", supervised by Valdo Praust
   1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
   1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive license.
3. I confirm that granting the non-exclusive license does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

14.05.2023

[1]The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.

Appendix 2 - Custom Search Engine URL Pattern List

The programmable search engine compiles a list of search results from the following URL patterns, eliminating the need to check the source of every information to make sure they are from a trustworthy source.

1. ncsi.ega.ee/*
2. www.sev.org.gr/*
3. *.mindigital.gr/*
4. www.trade.gov/*
5. *.tubitak.gov.tr/*
6. *.ebrary.net/*
7. *.edam.org.tr/*
8. www.inss.org/*
9. www.oxfordcyberacademy.com/*
10. www.dailysabah.com/*
11. www.academicapress.com/*
12. hgm.uab.gov.tr/*
13. *.cbddo.gov.tr/*
14. www.cyberwiser.eu/*
15. *.ccdcoe.org/*
16. www.trt.com.tr/
17. www.trtworld.com/
18. www.mkm.ee/*
19. www.bmi.bund.de/*
20. *.gov.tr/*
21. *.gov.uk/*
22. www.academia.edu/*
23. *.archive.org/*
24. www.researchgate.net/*
25. link.springer.com/*
26. *.ieeexplore.ieee.org/*
27. www.mdpi.com/*
28. www.csis.org/*
29. www.enisa.europa.eu/*
30. citeseer.ist.psu.edu/*
31. scholar.google.com/*
32. www.databreaches.net/*

Appendix 3 - Cyber Security Awareness and Education Level in Turkey Assessment Survey

The English translation of the survey questions and answers are as follows:

1. Which of the following properties should a password have in order for it to be considered secure nowadays?
   - Minimum 1 lowercase letter (a-z)
   - Minimum 1 uppercase letter (A-Z)
   - Minimum 1 digit (0-9)
   - Minimum 1 special character (!@)
   - Minimum 8 characters of length
   - All of them
2. Do you check the sender of an email before you open links or attachments?
   - Yes, always
   - Yes, only if the email looks suspicious
   - No, never
   - Sometimes
3. Were you given cyber security education during your school/work life?
   - Yes, more than once
   - Yes, only once
   - No, never
4. Do you use an anti-virus program?
   - Yes
   - No
   - I do not know what it is
5. Do you use 2 factor authentication for your accounts other than bank accounts?
   - Yes
   - No
   - I do not know what it is
6. Do you scan the files you have downloaded from the internet using an anti-virus program?
   - Yes
   - Yes, only if the website looks not trustworthy

- No

7. Which of the following are the risks of connecting to a public Wi-Fi?
    - There are no risks
    - Account information (emails, passwords) theft
    - Personal information (chats, data entered in websites) theft
    - Getting hacked
    - All of them
8. Do you know what a VPN is?
    - Yes
    - No
9. Where do you store sensitive information such as passwords?
    - In my mind
    - In a notebook
    - In a password management tool
    - I use "Forgot password" option each time
10. Do you use the same password for multiple accounts?
    - Yes, always
    - Yes, if the account is not important
    - I use a different password for each account
11. From which generation are you from?
    - Alpha generation (2013 and later)
    - Gen Z, Zoomer (1997 - 2012)
    - Gen Y, Millenial (1981 - 1996)
    - Gen X (1965 - 1980)
    - Baby boomers (1946 - 1964)
    - Silent generation (1928 - 1945)
    - I do not want to specify

Appendix 4 - Strategic Objectives

.1 Germany

1. **Action Area 1** - Remaining safe and autonomous in a digital environment
   (a) Promoting digital literacy among all users
   (b) Increasing the user-friendliness of security solutions
   (c) Expanding government measures to protect consumers in the digital world
   (d) Establishing uniform European security requirements
   (e) Guaranteeing secure electronic identities
   (f) Protecting the authenticity and integrity of algorithms, data and documents, and the electronic identities of people and things in the broader sense
   (g) Creating the conditions for secure electronic communication and safe web offerings
   (h) Responding responsibly to vulnerabilities – promoting coordinated vulnerability disclosure
   (i) Using encryption – a prerequisite for self-determined, autonomous action – across the board
   (j) Guaranteeing IT security through AI and for AI
2. **Action Area 2** - Government and private industry working together
   (a) Reinforcing the coordination function of the NCSR in the cyber security landscape
   (b) Improving cooperation between government, private industry, the research community and civil society on matters of cyber security
   (c) Establishing a cooperative platform for government, private industry, the research community and society to enable communication about cyber attacks
   (d) Protecting businesses in Germany
   (e) Strengthening Germany's digital economy
   (f) Creating a uniform European regulatory framework for businesses
   (g) Promoting research and development into more resilient, more secure IT products, services and systems for the EU single market
   (h) Strengthening the security of future technologies and key enabling technologies through security by design
   (i) Providing IT security through quantum technology
   (j) Harmonising testing and approval processes with innovation cycles (time to market)

(k) Improving the protection of critical infrastructures
(l) Cyber security certification
(m) Securing the telecommunications infrastructure of the future

3. **Action Area 3** - Strong and sustainable cyber security architecture for every level of government
   (a) Improving the options available to the Federal Government for threat prevention in case of cyber attacks
   (b) Equipping the technical and operational divisions of the BSI for the future and creating a network for them
   (c) Strengthening institutionalised cooperation between the BSI and the states
   (d) Developing the National Cyber Response Centre
   (e) Strengthening cyber and information security in the federal administration
   (f) Stepping up cyber security associated with elections
   (g) Ramping up law enforcement in cyberspace
   (h) Expanding central skills and services of the BKA for combating cyber crime
   (i) Providing security through encryption, and security despite encryption
   (j) Fostering responsible handling of zero-day vulnerabilities and exploits
   (k) Increasing the digital sovereignty of the security authorities by expanding the Central Office for Information Technology in the Security Sector
   (l) Raising the level of cyber security through increased preventive intelligence gathering
   (m) Strengthening defence aspects of cyber security
   (n) Adapting telecommunications and telemedia law and other specialist legislation to technological progress
4. **Action Area 4** - Germany's active role in European and international cyber security policy
   (a) Actively shaping effective European cyber security policy
   (b) Shaping cyber security and defence in NATO
   (c) Strengthening international law and the legislative framework for cyberspace and working towards responsible state behaviour
   (d) Promoting confidence-building measures
   (e) Strengthening bilateral and regional support and cooperation for cyber capacity building
   (f) Strengthening international law enforcement cooperation and combating international cyber crime
   (g) Working jointly in the EU on innovative solutions for combating crime more effectively

.2 United Kingdom

1. **Pillar 1** - Strengthening the UK cyber ecosystem
   (a) Strengthen the structures, partnerships and networks necessary to support a whole-of-society approach to cyber
   (b) Enhance and expand the nation's cyber skills at every level, including through a world class and diverse cyber profession that inspires and equips future talent
   (c) Foster the growth of a sustainable, innovative and internationally competitive cyber and information security sector, delivering quality products and services, which meet the needs of government and the wider economy
2. **Pillar 2** - Building a resilient and prosperous digital UK
   (a) Improve the understanding of cyber risk to drive more effective action on cyber security and resilience
   (b) Prevent and resist cyber attacks more effectively by improving management of cyber risk within UK organisations, and providing greater protection to citizens
   (c) Strengthen resilience at national and organisational level to prepare for, respond to and recover from cyber attacks
3. **Pillar 3** - Taking the lead in the technologies vital to cyber power
   (a) Improve our ability to anticipate, assess and act on the science and technology developments most vital to our cyber power
   (b) Foster and sustain sovereign and allied advantage in the security of technologies critical to cyberspace
   (c) Preserve a robust and resilient national Crypt-Key enterprise which meets the needs of HMG customers, our partners and allies, and has appropriately mitigated our most significant risks including the threat from our most capable of adversaries
   (d) Secure the next generation of connected technologies and infrastructure, mitigating the cyber security risks of dependence on global markets and ensuring UK users have access to trustworthy and diverse supply
   (e) Work with the multistakeholder community to shape the development of global digital technical standards in the priority areas that matter most for upholding our democratic values, ensuring our cyber security, and advancing UK strategic advantage through science and technology
4. **Pillar 4** - Advancing UK global leadership and influence
   (a) Strengthen the cyber security and resilience of international partners and increase collective action to disrupt and deter adversaries
   (b) Shape global governance to promote a free, open, peaceful and secure cyberspace
   (c) Leverage and export UK cyber capabilities and expertise to boost our strategic

advantage and promote our broader foreign policy and prosperity interests

5. **Pillar 5** - Detecting, disrupting and deterring adversaries
   (a) Detect, investigate and share information on state, criminal and other malicious cyber actors and activities in order to protect the UK, its interests and its citizens
   (b) Deter and disrupt state, criminal and other malicious cyber actors and activities against the UK, its interests, and its citizens
   (c) Take action in and through cyberspace to support our national security and the prevention and detection of serious crime

Appendix 5 - National Cyber Security Strategy URLs

Estonia - *CYBERSECURITY STRATEGY* can be found here, or through the URL: `https://www.mkm.ee/media/703/download`

Germany - *Cyber Security Strategy for Germany 2021* can be found here, or through the URL: `https://www.bmi.bund.de/SharedDocs/downloads/EN/themen/it-digital-policy/cyber-security-strategy-for-germany2021.pdf?__blob=publicationFile&v=4`

Greece - *NATIONAL CYBER SECURITY STRATEGY - Version 3.0* can be found here, or through the URL: `https://ccdcoe.org/uploads/2018/10/Greece_National-Cyber-Security-Strategy-ver.3.0_EN.pdf`

Turkey - *National Cyber Security Strategy 2020-2023* can be found here, or through the URL: `https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/national-cyber-security-strategy-2020-2023.pdf`

United Kingdom - *National Cyber Strategy 2022* can be found here, or through the URL: `https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1049825/government-cyber-security-strategy.pdf`