TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Anamul Hoque Shihab 176136IVBS

Lessons from Estonia: A Cyber Security Awareness Strategy for Bangladesh

Bachelor Thesis

Supervisor: Kaido Kikkas
Ph.D.

Tallinn 2020

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Anamul Hoque Shihab 176136IVBS

Õppetunnid Eestist: Küberturvalisuse Teadlikkuse Strateegia Bangladeshile

Bakalaureusetöö

Juhendaja: Kaido Kikkas
Ph.D.

Tallinn 2020

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: Anamul Hoque Shihab

07.01.2020

Abstract

The government of Bangladesh has introduced a National Cybersecurity Strategy (NCSS) to secure its cyberspace from threats but is lagging in the proper implementation of the strategy. This study was aimed at identifying the drawbacks of the NCSS (National Cybersecurity Strategy) of Bangladesh by comparing it with the world's one of the best cyber-secure country Estonia and propose recommendations for possible policy changes to build more secure cyberspace. The study examines the various initiatives taken by Estonia to raise awareness in various sectors. After conducting a survey based on semi-structured interview (questionnaire) the author has got a clear overview of the need for an awareness strategy for Bangladesh. From lessons learned from Estonian initiatives, the author has suggested an awareness strategy approach that could be developed and implemented in Bangladesh to be successful in raising awareness among its citizens.

This thesis is written in English and is 38 pages long, including 5 chapters, 5 figures, and 1 table.

Abstract in Estonian

Bangladeshi valitsus on küberruumi kaitseks loonud Rahvusliku Küberturbestrateegia (NCSS), kuid selle elluviimine on takerdunud.Käesoleva lõputöö eesmärgiks on leida NCSSi kitsaskohad, võrreldes seda Eesti kui maailma ühe edukama küberturberiigiga, ning pakkuda välja võimalikke muudatusi ja täiendusi. Töös on uuritud Eestis läbi viidud tegevusi, mille abil küberteadlikkust eri sektorites edendatakse. Uuringus on kasutatud poolstruktureeritud intervjuusid. Eesti kogemuse põhjal on autor pakkunud välja küberteadlikkuse parandamise strateegia, mille abil saaks Bangladeshi elanike teadlikkust tõsta.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 38 leheküljel, 5 peatükki, 5 joonist ja 1 tabelit.

List of abbreviations and terms

BCC	*Bangladesh Computer Council*
BGD e-GOV CIRT	*Bangladesh e-Government Computer Incident Response Team*
BSI	*Information Security of Germany*
CCA	*Cyber Crime Awareness Foundation*
CDU	*Cyber Defense Unit*
CERT	*Cyber Emergency Response Team*
CI	*Critical Infrastructure*
CIO	*Computer Information Officer*
CIRT	*Cyber Incident Response Team*
CISO	*Computer Information Security Officer*
CMM	*Cybersecurity Capability Maturity Model*
CTO	*Commonwealth Telecommunications Organisation*
DoS	*Denial of Service*
EGA	*E-Governance Academy*
EU	*European Union*
GCI	*Global Cybersecurity Index*
GCSCC	*Global Cyber Security Capacity Centre*
HITSA	*Information Technology Foundation for Education*
HARNO	*Education and Youth Authority*
ICT	*Information and Communication Technology*
IDB	*Inter-American Development Bank*
IT	*Information Technology*
ITU	*International Telecommunication Union*
MPTIT	*Ministry of Posts, Telecommunications, and Information Technology*
NATO	*North Atlantic Treaty Organization*
NATO CCD COE	*NATO Cooperative Cyber Defence Centre of Excellence*
NCSI	*National Cybersecurity Index*
NCSS	*National Cybersecurity Strategy*
OSCE	*Organization for Security and Cooperation in Europe*
R&D	*Research and Development*
RIA	*Riigi Infosüsteemi Amet*
TUT	*Tallinn University of Technology*

Table of contents

1 Introduction 10
1.1 Problem statement and motivation 10
1.2 The rationale of the study 12
1.3 Objectives of the study 12
1.4 Scope of the study 12
1.5 Thesis overview 13
2 Literature Review 15
2.1 Cyberspace in the modern era 15
2.2 The dark side of cyberspace 16
2.3 Cybersecurity 17
2.4 Global cybersecurity strategy 17
2.5 National cybersecurity strategy 18
2.6 National Cybersecurity Strategy of Bangladesh 19
2.7 National Cybersecurity Strategy of Estonia 20
3 Research Methodology 22
3.1 Research Design 22
3.2 Basis of comparison 22
3.3 Comparison framework 23
3.4 Comparison Metrics 24
3.5 Comparison of NCSS of Bangladesh and Estonia 25
3.6 Policy recommendation based on comparative analysis 33
4 Data analysis and recommendation 35
4.1 Cybersecurity awareness initiatives in Estonia 35
4.2 Cybersecurity awareness initiatives in Bangladesh 36
4.3 Survey introduction 38
4.4 Response analysis 38
4.5 A cybersecurity awareness strategy for Bangladesh 42
5 Conclusion 49
References 50
Appendix 1 – Questionnaire 54
Appendix 2 – Non-exclusive license for reproduction and publication of a graduation thesis 57

List of figures

Figure 1: Five stages of NCSS maturity (Created by the author, based on [35]) 23
Figure 2: Cybersecurity knowledge level of the respondents 38
Figure 3: Knowledge of the development of National Cybersecurity Strategy 39
Figure 4: Percentage of respondents who received cybersecurity training 40
Figure 5: Satisfaction level with the current existing measurements 41

List of tables

Table 1: Key differences between Estonia & Bangladesh regarding NCSS development 32

1 Introduction

This chapter discusses the motivation and problem statement, the rationale of the study, the research's objectives, and the scope of the study. The overall organization of the study is also presented in this section.

1.1 Problem statement and motivation

In this era of 'Global Village', the whole world is connected through the internet. Production, income, working opportunities in all spheres of life, are accelerated because of the use of the internet. Every aspect of our life is controlled by the internet providing ease to our daily life. Uses of the Internet in both public and private sectors have been increasing rapidly because of the flexibility it provides. The Internet has opened new aspects of business and through the internet, the nations can govern online smoothly. The International Telecommunication Union (ITU) estimates that at the end of 2019, 53.6percent of the global population, or 4.1 billion people, are using the Internet [1]. The Internet has also become a popular space among criminals and the number of cybercrimes is also on the rise because of the ease of access and anonymity it provides. Cyberspace has numerous adverse effects including electronic fraud, theft of confidential property and personal information, financial crime, and damage or destruction of property. Cyber-attacks are increasing rapidly ranging from minor intrusion attempts to planned attacks sponsored by states. The losses caused by cyber-attacks in physical and financial levels are more prominent than physical terrorism [2].

Many countries have encountered the evilest side of cyberspace by facing unexpected cyber-attacks. For instance, the attacks on Estonia's internet infrastructure in 2007, the cyberwar in 2008 between Georgia and Russia which was initially a physical war, the attack on Iran's nuclear program in 2010 through Stuxnet worm [3]. These incidents made the nations realize the tier need for cyber-capability at the federal level. To protect the national cyberspace from malicious attacks, the nations have taken a high-level strategic plan namely the National Cyber Security Strategy (NCSS).

Bangladesh, A small developing country in South Asia, has also been affected by numerous cyberattacks. 26 government organizations were hacked in 2012, hackers carted away US$250,000 without making any fuss from Sonali Bank (a government bank)

in 2013 [4] and the most significant one is the 2016 central bank heist which was one of the world's largest bank heist of cybercrime [5]. Though Bangladesh Government has published the National Cyber Security Strategy in 2014, There is no noticeable improvement in their cyberspace. Bangladesh has developed its first NCSS based on the framework provided by the International Telecommunication Union (ITU), thus ensuring the inclusion of international policies [6]. Where the developed countries such as UK, Netherlands, Czech Republic, and Estonia have published several iterations of their National Cyber Security Strategy, with the USA assessing and updating their documents most frequently [7], the interest to analyze the efficiency of NCSS in Bangladesh is not worth mentioning. The nature of cyber threats is changing rapidly and to defend against those attacks' modification and update of the NCSS of Bangladesh needs to be the utmost priority of the government for ensuring the safety of public and critical infrastructure.

The attempts that had been made to assess the strategic strength of the NCSS (National Cybersecurity Strategy) of Bangladesh through a cross-comparison with the NCSS (National Cybersecurity Strategy) of different nations are very negligible. This study aims to analyze the current state of the NCSS (National Cybersecurity Strategy) of Bangladesh and recommend necessary amendments and inclusions through a comparative analysis with the NCSS (National Cybersecurity Strategy) of Estonia. The current state of the NCSS of Bangladesh could be thoroughly analyzed if compared with the best cybersecurity practices in the world. According to the NCSI (National Cybersecurity Index), Estonia ranked 3rd in the National Cyber Security Index and 5th in the Global Cybersecurity index where the position of Bangladesh is 74th and 78th respectively [8] [9]. Besides, Estonia is the role model in the world for the establishment of e-Governance services. Bangladesh's government has also published the e-Government master plan for 'Digital Bangladesh' [10]. Thus, a cross-comparison with Estonia's NCSS in this study will find out the required area of amendments in the NCSS (National Cybersecurity Strategy) of Bangladesh by providing an overview of the experiences Estonia has, describing how it has dealt with the threats of cyberspace and, how their policies and legal frameworks have evolved according to the advance of cyber threats. It will also serve as a useful guide to other countries to develop their national approaches to cybersecurity.

1.2 The rationale of the study

In 2014, Bangladesh declared its first National Cybersecurity Strategy (NCSS), however, since then the country has suffered several large-scale cyber-attacks. The concept of Critical Infrastructures (CI) has been acknowledged in the NCSS but there is no guideline to define which infrastructures are key and how they are part of CI (Critical Infrastructure) [11]. Cooperation between government and organization bodies concerning the threats and vulnerability in cyberspace is also absent [11]. The NCSS of Bangladesh needs a thorough analogy to mitigate all these lacking and achieve the goal to be a digital nation, but there is very insignificant research in this regard. Also, awareness among its public and private sectors' people in protecting personal information is very poor [12]. This study will identify the shortcomings in the NCSS and will recommend the required modifications given the cross-comparison with the NCSS of Estonia.

The comparative analysis mentioned in this paper is relevant to the national need of Bangladesh. The recommendations in this study comply with the required change in the National Cyber Security Strategy of the country. The suggestions made in this paper are set following the socio-economic and national development process to encompass cyber threats.

1.3 Objectives of the study

The objectives of the study are given below:

- Analyze and compare the cybersecurity strategies of Bangladesh with a developed country Estonia.
- Propose policy recommendations for NCSS (National Cybersecurity Strategy) of Bangladesh based on the comparative analysis findings.
- Propose a cybersecurity awareness strategy for Bangladesh in the view of Estonia.

1.4 Scope of the study

This comparative study will help developing countries like Bangladesh to understand the difference between their approach to NCSS with the developed and more secure

countries. The recommendations will be proposed according to the socio-economic and national development process of Bangladesh. Thus, there is a scope to change the proposed suggestions to meet the criteria of the study country.

The implementation of the proposed awareness strategy solely depends on the will of the government. While poor policymaking and corruption are hindering the success of the existing strategies, implementing new ones is nothing but a daydream. Because of the wide use of the internet, people have become more aware of their rights and participating in the online discussion of the government's activities. The government is afraid of losing power because of this mass movement. There is an example of blocking Facebook and YouTube nationwide and restricting upload speeds by the government. The government in Bangladesh put behind the broader success of ensuring internet access and cybersecurity to hold onto power. It will not be an exception if the government does not implement the proposed strategy to resist people from the potentials of the internet and stimulate power practice. They are also unwilling in expanding the e-governance services because corruption will be reduced a great deal if does so.

1.5 Thesis overview

Chapter 1 This chapter discusses the motivation and problem statement, the rationale of the study, the research's objectives, and the scope of the study. The overall organization of the study is also presented in this section.

Chapter 2 This chapter deals with the theoretical background related to the study. A brief conceptual discussion on technical terms such as cybersecurity, cyberspace, the dark side of cyberspace, national cybersecurity strategy, has been presented here. A discussion on the global cybersecurity strategy, the existing national cybersecurity strategy for Bangladesh are discussed then. Lastly, there will be an overview of the NCSS (National Cybersecurity Strategy) of Estonia.

Chapter 3 This chapter explains the framework and methodology followed to achieve the research objectives. It contains the comparative analysis of the NCSS (National Cybersecurity Strategy) of Bangladesh

and Estonia by term to term. There will be a proposal of policy recommendations for Bangladesh at the end of the chapter.

Chapter 4 There is a discussion on the responses found from the survey and recommendations on which awareness strategies are best suited for Bangladesh. The Cybersecurity awareness strategies of both Bangladesh and Estonia will also be discussed. The limitations and future research scope will be discussed at the end.

Chapter 5 In this chapter, the overall findings and conclusion of the study have been discussed.

2 Literature Review

This chapter deals with the theoretical background related to the study. A brief conceptual discussion on technical terms such as cybersecurity, cyberspace, the dark side of cyberspace, national cybersecurity strategy, has been presented here. A discussion on the global cybersecurity strategy, the existing national cybersecurity strategy for Bangladesh are discussed then. Lastly, there will be an overview of the NCSS of Estonia.

2.1 Cyberspace in the modern era

The Internet has offered unparalleled opportunities and has an everlasting impact on every aspect of human life. People use the internet for various purposes, from communication to business, education as well as entertainment. Because of the convenience internet posed in our day-to-day life, more and more people are using the internet. Cyberspace is always ready to serve all the possible needs a person can require. The ex-president of the United States of America, Barack Obama, defines cyberspace as a world of its own, space where every level of human life depends on functioning in the best way. [13].

Cyberspace is acting as a means of international communication by connecting billions of people from all around the world. It has caused a significant change in human behaviour. People are more likely to communicate through the electronic medium rather than meeting up physically [14], thus saving time and effort and making life easier. For instance, Physical letters have been replaced by emails. Cyberspace has a great impact on social life too. It has offered a platform (i.e., Facebook, WhatsApp, Twitter) through which we can connect and socialize with people from any part of the world. It is a great platform for businesses to advertise their products.

The Internet has made the way of academic and professional research easier than ever. Internet is more of a digital library serving not only the students but also teachers and other professionals from different sectors. All the journals and databases are available online which has simplified the way of finding scholarly articles. Besides, researchers can easily find and distribute their research findings to a broader audience [15]. Besides, people can gather any kind of information by simply typing the keywords in any search engine. E-commerce has enabled people to run their businesses even sitting at home. It can be defined as a medium for buying and selling products online. A plethora

of start-ups have been launched in recent years only because of the wide array of opportunities offered by the internet.

2.2 The dark side of cyberspace

Cyberspace can be considered as a double-edged sword [16]. Though the blessings of the internet are inevitable, it also has its dark side. Not only criminals are using cyberspace for committing crimes but also nations are using cyberspace as an alternative to physical war. There are so many examples of state-sponsored intrusions that have a devastating effect on the attacked nation. However, cyberspace causes numerous threats to individuals, organizations, and above all to the whole nation. The dark side of cyberspace affects every user within it, both direct and indirect user.

At the individual level, an individual may experience several types of cyber-attacks. Identity theft, financial fraud, cyberbullying, online child grooming, etc are the most common. Perpetrators collect personal information available in different online services such as social media without the slight notice of that individual. They impersonate the individual and commit a crime like financial fraud. Phishing is one of the ways to collect personal information by sending out bulk emails. These emails cause the recipient to willingly disclose personal information. The use of cyberspace in bullying has a more harmful effect than the physical one because the criminal can bully the victim without the constraints of time and location [17]. Online bullies feel unassailable because there is no face-to-face interaction which allows the criminal to say anything to the victim [18]. Children are also vulnerable to the threats of cyberspace. By child grooming, sexual predators manipulate children to engage them in sexual conversations.

At the organizational level, criminals attack the computer system with the help of viruses, i.e., worms, trojan horses, and by DoS (Denial of Service) attacks. Financial organizations often lose huge amounts of money as criminals attack their computer system and heist the money.

Cyber terrorism, cyber warfare, hacking important information from the governmental site are the dark side of cyberspace at the national level. Many nations have encountered major cyber-attacks. For example, the attacks on Estonia's internet infrastructure in 2007,

the cyberwar in 2008 between Georgia and Russia which was initially a physical war, the attack on Iran's nuclear program in 2010 through Stuxnet worm [3].

2.3 Cybersecurity

The International Telecommunication Union (ITU) estimates that at the end of 2015 more than 51% of the global population are using the Internet [19]. The Internet has also become a popular space among criminals and the number of cybercrimes is also on the rise because of the ease of access and anonymity it provides. The importance of cybersecurity is undoubtedly a major concern because of the increasing dependency on Information and communication technology. [20]

According to the ITU, the illicit use of cyberspace potentially affects the economy, public health, the safety of the individuals, and the overall security of a nation [21]. As the security of the nation and its citizens is the utmost priority of the government, thus cybersecurity is also the duty of the government. Government and individuals depend on cyberspace for different purposes; therefore, cybersecurity must be a national priority. For this thesis, the definition of cybersecurity that the International Telecommunication Union (ITU) provided will be used and is as follows:

"Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: Availability, Integrity, which may include authenticity and non-repudiation, and Confidentiality [22]."

2.4 Global cybersecurity strategy

For the socio-economic development of the country, cybersecurity is a fundamental aspect of the government. Despite the tier need of NCSS, according to the ITU Global

Cybersecurity Index (GCI) 2017 [23], only 76 countries have published their NCSS. In 2018, ITU published a guide to developing the NCSS with coordination to the World Bank, Commonwealth Secretariat (ComSec), the Commonwealth Telecommunications Organisation (CTO), and NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), thereafter (IGOs) [24]. It is one of the most comprehensive guides about the constitution of a successful cybersecurity strategy. [24].

The guide provided by ITU aims to act as a framework for a country to implement their NCSS considering the country's specific socio-economic aspects [24]. The Guide is a unique resource, as it provides a framework that has been agreed on by organizations with demonstrated and diverse experience in cybersecurity and builds on their prior work in this space. As such, it offers the most comprehensive overview to date of what constitutes successful national cybersecurity strategies [24].

States must follow the guide to achieve desired economic growth and national security goals by balancing security risks associated with the rapidly evolving ICT-infrastructure.

2.5 National cybersecurity strategy

National cybersecurity strategy can be of varying forms and level of detail depending on the priorities and objectives to combat cyber threats. Some country focuses on CI related risks, others may prioritize protecting intellectual property or raising public awareness, or a combination of all of these. Thus, there is no established definition of the constitution of the National Cybersecurity Strategy. Depending on existing research in this area, the guide to develop a national cybersecurity strategy by ITU [24], encourages stakeholders to think of a National Cybersecurity Strategy as:

- an expression of the vision, high-level objectives, principles, and priorities that guide a country in addressing cybersecurity.
- an overview of the stakeholders tasked with improving the cybersecurity of the nation and their respective roles and responsibilities; and
- a description of the steps, programs, and initiatives that a country will undertake to protect its national cyber-infrastructure and, in the process, increase its security and resilience.

2.6 National Cybersecurity Strategy of Bangladesh

In 2014, The People's Republic of Bangladesh published its National Cybersecurity Strategy (NCSS) to combat cyber threats. The central goal of the strategy was "working collaboratively home and abroad, to manage all major cyber risks that affect the country directly irrespective of their origin and type, thereby creating a safe, secure and resilient critical national information infrastructure for the economy and society" [6]. A total of 11 actions were described in the NCSS which includes the development of a national cybersecurity framework, raising public awareness, critical infrastructure protection, cybercrime mitigation, the establishment of incident response capability, securing government infrastructure, cybersecurity skills, and training development, and establishment of public-private partnership [6]. Possible risks and threats were also listed in the strategy.

According to the review report on cybersecurity capacity of Bangladesh conducted by the Global Cyber Security Capacity Centre (GCSCC) in collaboration with NRD CS (NRD Cybersecurity) in 2018 using the Cybersecurity Capability Maturity Model (CMM), the NCSS of Bangladesh is in the Formative-Established level, which means few aspects have begun to grow and be formulated, some are in place and functioning; there is no well-thought-out consideration of the relative allocation of resources [11]. No authority was assigned in the NCSS for the design, implementation, monitoring, and revision of the strategy, but the Ministry of Posts, Telecommunications, and Information Technology (MPTIT) had been leading the whole procedure [11]. The strategy is now under review and has not yet got any update and iteration considering the rapidly evolving cyber threats.

Though Bangladesh has established an NCSS in 2014, it is still in its infant state. Critical Infrastructure was recognized in the strategy but there was no guideline in place to identify which infrastructures are key and should be the part of CI [11]. People associated in both the public and private sector have very little, in some cases no knowledge of handling personal information. They do not know what steps can be taken and where to report if any violation is caused. Currently, there is no national computer-related incident response organization and the authority that serves as the coordinating body for the reporting and management of cybersecurity incidents in the public sector is the Bangladesh e-Government Computer Incident Response Team

(BGD e-GOV CIRT) [11]. But people remain in confusion about how to report an incident. The BGD e-GOV CIRT as part of Bangladesh Computer Council (BCC) has designed awareness campaigns and adapted some of the Stop.Think.Connect materials and publishes material on its website but they are not targeted to specific groups and people hardly know about their website and available materials [25].

In Bangladesh, there is not enough legislation to ensure the security of ICT infrastructures. Though BCC has published an information security guidance, ministries do not comply with it. Each ministry decides on its security policies and there is no authority for auditing the level of compliance [11]. Uses of unlicensed software is very common in Bangladesh. A study performed by the government of United states reported that about 90% of the business software in Bangladesh are unlicensed and downloaded from unauthorized websites. [26] This practice is illegal and a serious security threat. Even there is free alternatives available (I.e. Linux operating systems, Libra Office, GIMP) most people are not aware they exist.

2.7 National Cybersecurity Strategy of Estonia

Estonia is among the first countries to develop a National Cybersecurity Strategy. After the major cyberattacks in its cyberspace, Estonia developed its first national cybersecurity strategy in 2008 that recognized the interdisciplinary nature of cybersecurity and the need for coordinated action in the area [27]. The government of Estonia updated its first national cybersecurity strategy in 2014 for the period 2014-2017 and the third iteration has been published recently for the period 2019-2022. The latest strategy is built on its predecessors but re-assesses its overall process considering changes in the threat environment. The 2019-2022 Estonian cybersecurity strategy has several objectives includes: support cybersecurity Research and Development, Advancing cooperation with international partners, and developing experts in both public and private sector [27].

The introduction of e-Governance services in all aspects of government and public services has brought great advantages for the people of Estonia, but also put them to the threats of cyberspace. With a high level of dependence on the internet, Estonia dealt with cyber threats through the successful implementation of its strategy. Estonia introduced different organizations in support of its cybersecurity strategy. Ensuring

cooperation between agencies and monitoring the implementation of the strategy is imposed upon the Cybersecurity Council, which was a part of the Security Committee of the ministerial body of Government of the Republic [27]. The responsibility of the protection of the government network is given to the Estonian Information System Authority *(Riigi Infosüsteemi Amet*, or RIA) with the required power and resources [27]. A critical infrastructure mapping project was undertaken by RIA with the motive of identifying services that rely on cyberspace [28].

A well-established emergency response team is a major component of the cybersecurity strategy. To handle cyber incidents Estonia has the Cyber Emergency Response Team (CERT-EE) which operates under the framework of RIA (*Riigi Infosüsteemi Amet*). CERT-EE prioritizes cases according to four principles [29]:

- the number of affected users,
- the significance of the incident,
- origin and destination of the attack,
- the resources required to handle the incident.

Estonia has a worldwide reputation for its advanced e-government services. Estonia is a leader in e-governance for introducing the digital authentication of identity. Its electronic ID card is the key to get access to Estonia's e-government services. The Information Technology Foundation for Education (HITSA) operates as the main source of cybersecurity training and awareness campaigns in Estonia [28].

To combat cyber threats, Estonia has developed a series of legislations and acts including the Emergency Act of 2009 (amended 2016) [30], The State Secrets and Classified Information of Foreign States Act of 2007 [31], The Electronic Communications Act 2004 (amended in 2011) [32], Personal Data Protection Act 1996 (amended in 2010) [33], etc. All these legislations are enforced properly according to the type of crime.

International cooperation within the regional and global organization is a core part of Estonia's cybersecurity strategy. Estonia has regional partnerships with the Baltic and Nordic states, in addition to this, Estonia is an active participant within the frameworks of NATO), the European Union (EU), the UN Group of Government Experts, and the Organization for Security and Cooperation in Europe (OSCE) [28].

3 Research Methodology

This chapter explains the framework and methodology followed to achieve the research objectives. It contains the comparative analysis of the NCSS (National Cybersecurity Strategy) of Bangladesh and Estonia by term to term. There will be a proposal of policy recommendations for Bangladesh at the end of the chapter.

3.1 Research Design

To achieve the objective of the study, the author has followed a two-step strategy. At the first step, there will be a comparative analysis of the cybersecurity strategies of Bangladesh and Estonia. Estonia has been chosen because of its success in implementing the National Cybersecurity Strategy and for being the leader in the world in ensuring e-governance services. Based on the comparison, the author will propose several policy recommendations for the NCSS of Bangladesh.

In the second step, the author has surveyed through a questionnaire (semi-structured interviews) to collect data from the targeted group of people. This survey was targeted to the youth of Bangladesh who is currently studying at the graduate or undergraduate level in the universities. Upon completion of the study, this targeted group of people will join the public and private sectors' organizations and are liable to ensure the cybersecurity of their companies. The response from them has revealed the success scenario of the awareness measures taken by the government. The author got an idea of which awareness programs and additional strategies could be added to the NCSS from the collected response. After analyzing the collected data, the author has recommended some steps for implementation as a cybersecurity awareness strategy.

3.2 Basis of comparison

To analyze the maturity of the NCSS is not an easy task. Several stakeholders from the public and private sectors are associated with the development and implementation of the NCSS. It is surely a challenge for a random person or organization to analyze and review the cybersecurity capacity of a nation without a thorough consultation with the associated stakeholders. The author of this paper could not review the cybersecurity capacity of Estonia and Bangladesh on one hand. The author depends on the only review report available on the maturity of cybersecurity capacity

of Bangladesh which was conducted by the international firms NRD CS (NRD Cybersecurity) and Global Cyber Security Capacity Center (GCSCC) of the University of Oxford at the invitation of the Bangladesh Computer Council (BCC). The analysis of the cybersecurity capacity of Bangladesh was conducted based on the Cybersecurity Capability Maturity Model (CMM). Stakeholders from both public and private sectors participated in a roundtable consultation, over the period 2-4 July 2018 [11]. The CMM model has been widely used by at least 80 countries since 2015 [34].

For comparison of the cybersecurity capacity of Bangladesh with that of Estonia, the author follows the review report, "Advanced Experiences in Cybersecurity Policies and Practices - An Overview of Estonia, Israel, South Korea, and the United States" conducted by Inter-American Development Bank (IDB) in 2016 [28]. According to the author James Andrew Lewis of this report, "Of the four countries reviewed in this publication, Estonia comes closest to having a 'dynamic' approach to cybersecurity". The author specifically chooses this review report because this analysis is also based on the CMM Model developed by GCSCC of the University of Oxford [35].

Therefore, the comparison between the maturity level of cybersecurity capacity of Bangladesh and Estonia will be conducted based on the CMM Model.

3.3 Comparison framework

According to the definition of the CMM model provided by the Global Cyber Security Capacity Centre (GCSCC), there are five stages of maturity, ranging from the start-up stage to the dynamic stage. The start-up stage implies an ad-hoc approach to capacity, whereas the dynamic stage represents a strategic approach and the ability to dynamically adapt or change against environmental considerations [35].

Figure 1: Five stages of NCSS maturity (Created by the author, based on [35])

3.4 Comparison Metrics

The following set of five metrics has been defined by GCSCC (Global Cyber Security Capacity Centre) to gauge the maturity level of the cybersecurity capacity of any nation [35].

- **Cybersecurity Policy and Strategy:** This dimension discusses the development of cybersecurity policy and strategy. Also, the supportive factors like emergency incident response, crisis management policy, identification of critical infrastructures that influence the success of the development of policy and strategy are included in this dimension.

- **Cybersecurity culture and society:** This dimension assesses the growth of cybersecurity culture among individuals and the society by a thorough discussion on the understanding of cybersecurity aspects of the individuals, reliance on internet services, and knowledge on protecting personal data.

- **Cybersecurity education, training, and skills:** The success of the existing awareness-raising programs is analyzed in this dimension by evaluating the availability, quality, and uptake of educational and training offerings for various groups in the public and private sectors.

- **Legal and regulatory framework:** The design and enforcement of all the cybersecurity-related laws and legislations such as personal data protection, IT infrastructure security, etc are discussed in this dimension. The capacity of law enforcement authorities like police and prosecutors are also analyzed.

- **Standards, organizations, and technologies:** The efficacy of the cybersecurity technologies in ensuring personal, organizational, and above all the national security is evaluated in this sector by specifically examining the success of implemented cybersecurity standards and good practices along with the development of required technologies to reduce risks related to cyberspace.

The author of this paper will carry out the comparative analysis of the cybersecurity capacity of Bangladesh with that of Estonia, with respect to these metrics described above.

3.5 Comparison of NCSS of Bangladesh and Estonia

Most of the information in this section is collected from "Cybersecurity Capacity Review Bangladesh" [11] for Bangladesh and "Advanced Experiences in cybersecurity policies and practices" [28] in the case of Estonia. The comparison will be done based on the following metrics described by the CMM model [35].

i) **Cybersecurity Policy and Strategy:** The National Cybersecurity Strategy (NCSS) of Bangladesh is at the Formative-Established level and after 6 years of developing the strategy, no iteration has been conducted to cope up with the rapidly evolving cyberspace. In stark contrast, Estonia comes closest to having a "dynamic" approach to cybersecurity, and the NCSS of Estonia already has undergone three iterations from the time of development.

   Estonia introduced significant organizational approaches to support its cybersecurity strategy. The Cybersecurity Council is tasked with the responsibility to monitor the overall implementation of Estonia's cybersecurity strategy. It is supported by the Ministry of Economic Affairs and Communications, which cooperates among government agencies, civil society, companies, and educational institutions for the implementation of cybersecurity policy. All authorities involved in cybersecurity submit an annual report to the Ministry of Economic Affairs and Communications on measures they have adopted and their performance. In the case of Bangladesh, responsibility for the design, implementation, monitoring, and revision of the strategy was not formally assigned, but the process had been and continues to be led by the Ministry of Posts, Telecommunications and Information Technology (MPTIT). Some progress has been noticed in certain aspects of the implementation of the strategy, mostly those that are the responsibility of the MPTIT. Other implementation aspects of the National cybersecurity strategy are lagging as they fall within the responsibility of other government ministries or agencies and the MPTIT has no legal authority to monitor their progress.

   The Estonian Information System Authority (*Riigi Infosüsteemi Amet*, or RIA), which is given additional powers and resources for the protection of government

networks [27]. Within the RIA, Estonia created a "Department of Critical Information Infrastructure Protection." The RIA undertook a critical infrastructure-mapping project to identify vital services that rely on cyber means and formed a commission to promote public-private cooperation. On the other hand, the concept of cybersecurity in critical infrastructure (CI) in Bangladesh is still in its infant state. The NCSS recognizes CI but there no official measures to categorize which infrastructures are key and should be considered as part of CI. Coordination within CI and between CI and the government, for cybersecurity threat and vulnerability disclosure, is absent. There are no formal or informal channels for incident disclosure and reporting of incidents is not mandatory for any sector.

Estonia has cyberunit both in police and Border Guard Board and it merged the two units in 2012 forming PBGB. To bring the private sector expertise to the government sector, Estonia has created a Cyber Defense Unit (CDU) in 2011 as part of the Estonian Defense League [36]. Cyber defense capacity in Bangladesh is at the formative stage. Currently, there is a cyber defense strategy. There are is a little ray of hope in the way the military functions in ensuring cybersecurity. The Ministry of Defence has established a military CERT.

Estonia's Cyber Emergency Response Team (CERT-EE) manages cyber incident response at the national level and coordinates between public and private sector response teams. In Bangladesh, currently, there is no national computer-related incident response organization and the authority that serves as the coordinating body for the reporting and management of cybersecurity incidents in the public sector is the Bangladesh e-Government Computer Incident Response Team (BGD e-GOV CIRT). At the private level, only a very limited number of organizations have established security operations centres (SOCs) to respond to incidents in the financial and telecommunications sectors. There is no coordination between the private and public sectors for incident response.

ii) **Cybersecurity culture and society:** People in Bangladesh have little, or no understanding of how personal information is handled online and the measures for the protection of personal information. Most Internet users

are not aware of their privacy rights and how to secure personal information when they use technologies like mobile phones, online services, and social media. There is no existing data protection legislation in Bangladesh and the country has no well-established tradition of protecting personal information. The public has a minimal recognition of a cybersecurity mindset.

According to the 2015 cybersecurity survey conducted by the European Commission, 47 percent of Estonian residents admitted that they felt well informed about the risks of cybercrime [37]. The introduction of e-Governance services in all aspects of government and public services has brought great advantages for the people of Estonia. Estonia is the leader in e-governance. Its electronic ID card is the key to getting access to Estonia's e-government services. Through the ID card citizens gain access to the systems for Internet voting, online tax returns, e-prescriptions, and online health records [38]. The ID also serves as the repository of e-tickets for public transportation. Internet voting has become a stocktaking measure for the degree of confidence that citizens place in cybersecurity [39]. The consultation team of the review report [11], could not get a clear scenario on to which extent the Bangladesh government is offering e-services. There is no specific authority for monitoring the e-government services and to introduce new services according to the need.

iii) **Cybersecurity education, training, and skills:** Estonia has created educational programs from the elementary school to the university levels. The Information Technology Foundation for Education (HITSA) functions as the primary source of training and awareness campaigns in Estonia, beginning its training programs with pre-school age children. HITSA (The Information Technology Foundation for Education) organizes different competitions and training programs for students to inspire the next generation of cybersecurity professionals. Recently HITSA (The Information Technology Foundation for Education) has been merged with the Education and Youth Authority (HARNO) along with Foundation Innove, Foundation Archimedes and Estonian Youth Work Center. HARNO (Education and Youth Authority) operates under the supervision of Ministry of Education and Research [40]. The goal of HARNO (Education and Youth Authority) is to provide equally adaptable educational facilities that are modern and competent in coordination with 11 departments [40]. The Violence

Prevention Strategy for 2015-2020 focuses on ensuring that children and teens use media and the internet safely to protect them from dangers including cyberbullying, and planning activities for the prevention of online violence against children [27]. The strategy is supported also by the Children and Families Development Plan 2012-2020 which deals with providing advisory service to the parents on internet security and running an information hotline for reporting illegal content and activities instantaneously [27].

The E-Governance Academy (EGA) is a consultation and think tank centre for an information society that supports other nations in implementing Estonia's digital (including cybersecurity) solutions [27]. Estonian universities are enriched with cybersecurity courses both at the graduate and undergraduate levels. The Tallinn University of Technology offers a Cybersecurity Engineering course at the undergraduate level and a joint MA program with the University of Tartu. In 2016, the University of Tartu launched an IT law training and research program aimed at providing highly qualified lawyers for working in the ICT and cybersecurity sector [27].

Now, if we focus on Bangladesh, we will observe an opposite scenario in this regard. The government has not yet realized the action item of the NCSS, and a coordinated National Cybersecurity Education Framework is not yet introduced. There are a few master's programs available in some private universities and Dhaka University provides a degree in Information Security. Though many children and teenagers use smartphones and computers, at primary and secondary education level students have only one course in ICT, which is does not cover any cybersecurity-related topic.

The BGD e-GOV CIRT as part of Bangladesh Computer Council (BCC) has designed awareness campaigns and adapted some of the Stop.Think.Connect materials and publishes material on its website but they are not targeted to specific groups and people hardly know about their website and available materials [25]. Several projects were prevailing that were supported by international partners but have been discontinued. No awareness campaigns for executives have been yet initiated. Some training offerings by international partners, including Cisco,

Symantec Australia, and the government of Korea which provided numbers of training for government officials need to be mentioned.

iv) **Legal and regulatory framework:** Estonia has developed a series of legislation and regulation to combat cybercrimes. The most important of these is the Emergency Act of 2009 (amended 2016) [30]. This regulation requires CI (Critical Infrastructure) providers to report cyber incidents and submit reports to the Estonian Information System Authority. The State Secrets and Classified Information of Foreign States Act of 2007 calls for an annual assessment of the digital storage security of government documents classified as 'top secret' and 'secret' [31]. The Electronic Communications Act 2004 (amended in 2011) [32] authorizes the Technical Surveillance Authority of Estonia to request ICT service providers to conduct security assessments of their systems. The processing of correspondence and personal information is governed by the Personal Data Protection Act 1996 (last amended in 2010) [33]. The Act implements EU data protection standards, distinguishes between 'personal data' and 'sensitive personal data', and places 'sensitive personal data' under extended protection. Cybersecurity Act is providing a basis for evaluating and managing risks and determining responsibility at the company level [27].

In Bangladesh, the main legal framework at present is the Information and Communication Technology (ICT) Act, 2006 which has two amendments in 2009 and 2013 respectively, defines and amends certain parts of the law relating to legal acknowledgment and security of information and communication technology and related matters.

Besides that, the Bangladesh Penal Code, 1860 [41], the Pornography Control Act, 2012 [42], and the Bangladesh Telecommunication Act, 2001 exists but they are not specifically related to cybercrime. The Digital Security Act has been highly criticized by civil society organizations and human rights advocates because it lacks transparency. Consumer protection is enacted through 2009 [43], Consumers' Right Protection Act which doesn't define how to handle online fraud related cybercrime. Intellectual property protection is governed by the Customs Act (2016), Copyrights Act (2005) [44], Patents and Design Act (1911) [45], and Trademarks Act (2009) [46], but they do not contain a specific provision

for the protection of intellectual property of online products and services. Child protection is enacted through the Children's Act (2013) [47], but it does not contain provisions for children's online protection.

Though Bangladesh has identified its CI (Critical Infrastructure), legal and regulatory frameworks are in the 'start-up' stage of development and implementation.

v) **Standards, organizations, and technologies:** Estonia, despite its small size and location, has cooperation with international organizations and it is a core part of its cybersecurity strategy. Estonia uses international cooperation to improve its security and to increase its international influence. Estonia has regional partnerships with the Baltic and Nordic states, in addition to this, Estonia is an active participant within the frameworks of NATO (North Atlantic Treaty Organization), the European Union (EU), the UN Group of Government Experts, and the Organization for Security and Cooperation in Europe (OSCE).

Estonia developed its own IT security standard (ISKE) modelled on the *IT-Grundschutz* (IT Baseline Protection Manual) developed by the Federal Office for Information Security of Germany (BSI). Compulsory for the public sector since 2008 (updated in 2018), the ISKE assesses an entity's security requirements through a three-level standard (high, medium, low). The standard seeks to balance confidentiality, integrity, and the availability of data [48].

Estonia has also taken initiatives to promote opensource tools, there is a repository https://koodivaramu.eesti.ee/ which provides the opensource solutions for public use [49].

In Bangladesh, the main reason behind the absence of ICT standards in all ministries is the limited budget allocated to IT (Information Technology) and the insufficient cybersecurity experts. A central institution tasked to mandate the implementation of a unified set of standards for all ministries and to execute regular audit controls is long overdue. Although BCC (Bangladesh Computer Council), in collaboration with NRD CS (NRD Cybersecurity), has developed an information security manual and promotes a uniform application of these practices across all ministries, they lack the mandate to enforce these standards.

For all financial institutions, ICT policy guidelines are available by the regulator, but for other sectors' organizations, there is no guideline. Across other sectors, there are no requirements for organizations to ensure specific standards within them nor regulators have the mandate to enforce specific ICT security policies and monitor compliance. There are standards for procurement of software in the public & private sector, however, these do not include guidelines for cybersecurity. The lack of standards is evident from the practice of using unlicensed software's in public and private sector. A plethora of bilateral training agreements with neighbouring countries are in action, however, collaboration with NATO members have been unsuccessful till now.

Where all the dimensions of the NCSS of Estonia are in the dynamic stage, the dimensions of the NCSS of Bangladesh are still in the start-up to formative stage only with the exception in the development of NCSS laying in the 'Established' stage. An extensive set of measures should be taken urgently to protect the national cyberspace of Bangladesh to cope up with the rapidly evolving cyber environment.

Table 1 shows the key differences between Estonia and Bangladesh:

Table 1: Key differences between Estonia & Bangladesh regarding NCSS development

Indicators	**Estonia**	**Bangladesh**
NCSS development	Published its first NCSS in 2008 and updated in 2014 & 2019	Published its first NCSS in 2014, Since then no updates.
Organization to monitor the progress of NCSS	The Cyber Security Council of Estonia was established in 2009 to monitor the goals of NCSS and ensuring communication between different institutions.	No authority was assigned formally, Currently, the Ministry of Posts, Telecommunications, and Information Technology is acting as a responsible authority
Authority for Critical Infrastructures protection	Department of CI protection a part of the Estonian Information System Authority (RIA)	There is no specific authority for Critical Infrastructures protection
Cyber Defense capacity	Estonia has cyberunit both in police and border guard (PBGB). Estonian Defense League – A voluntary organization has a cyber defense unit.	Bangladesh Police runs a cybercrime unit and the Military has a cyber defense unit. There is no coordination between the public and private sectors.
Cybersecurity Education availability	The Education and Youth Authority (HARNO) functions as the primary source of training and awareness campaigns in Estonia. Cybersecurity courses are available from primary education to the master's degree level.	There are no cybersecurity-related courses in primary, secondary, and higher secondary education. At the bachelor's and master's level there are few degree courses available related to Information Security.
Personal Data protection	personal information is governed by the Personal Data Protection Act 1996.	There is no Act regarding Personal Data protection
IT Security Standard	Estonia developed its own IT security standard (ISKE) – mandatory for public sector	No national security standard available

3.6 Policy recommendation based on comparative analysis

The author has recommended some policies with respect to initiatives of the Estonia government to provide advice and steps aimed to increase the existing cybersecurity capacity of Bangladesh. They are as follows:

i) The NCSS of Bangladesh needs to be revised, which should include the current state of cybersecurity, identify the critical infrastructures, specific objectives, and the parties involved in implementing the strategy. A central government agency should be established to monitor the implementation of the NCSS and coordinate with other stakeholders.

ii) Measures to monitor and evaluate the efficiency of all CIRTs needs to be taken. Besides, collaboration with CERT-EE (Estonian Cyber Emergency Response Team) and other international bodies should be augmented. National CIRT should clearly define their main goals, types of support they provide, collaborate with private sector CIRT teams.

iii) An initiative to promote the use of open-source applications should be established to reduce the use of unlicensed applications. Educational institutes can teach students using opensource applications which can greatly reduce the cost of buying commercial software license. Government should enforce the law against pirated software as it's a criminal offense.

iv) A list of CIs' (Critical Infrastructures) needs to be developed concerning identified risk-based priorities. Adequate technical security measures should be taken to ensure security for CI's (Critical Infrastructures).

v) A cyber defense component in the national cybersecurity strategy needs to be developed.

vi) New legislative measures need to be developed through consultation with the liable stakeholders on personal data protection, online children's safety, consumer protection, intellectual property & human rights. The law enforcement authority must be trained adequately to build trust in the confidentiality of the reports thus encouraging victims to report cybercrimes.

vii) A nationally accepted IT Security Standard should be established and good practice of this standard in both public and private sectors must be strictly ensured. A secure Identity Access management should be developed for government critical network infrastructures.

4 Data analysis and recommendation

There is a discussion on the responses found from the survey and recommendations on which awareness strategies are best suited for Bangladesh. The Cybersecurity awareness strategies of both Bangladesh and Estonia will also be discussed. The limitations and future research scope will be discussed at the end.

4.1 Cybersecurity awareness initiatives in Estonia

In this chapter, the author will discuss the cybersecurity awareness initiatives taken by Estonia in the public & private sectors, for children's online safety and in Education.

i) **In the public & private sector:** Estonia established a support network, named *Look@World Foundation*, in collaboration with international service providers to organize awareness programs and training, and for safeguarding the use of ICT (Information and Communication Technology) devices [28]. The Children and Families Development Plan 2012-2020 deals with providing advisory service to the parents on internet security and running an information hotline for reporting illegal content and activities instantaneously [27]. Estonia's Cyber Emergency Response Team (CERT-EE) also organize awareness programs for the public and train them on reporting cyber incidents.

   Estonian Association of Information Systems Auditors organizes seminars and training sessions for professionals to raise awareness on cybersecurity measures and required steps to combat cyber threats. The E-Governance Academy (EGA) promotes the safe implementation of e-governance services and train the public sector employers for this. The Cyber Olympic Project organizes seminars and conferences for teachers, IT officials, entrepreneurs [50].

ii) **For children online safety:** The Violence Prevention Strategy for 2015-2020 focuses on ensuring that children and teens use media and the internet safely to protect them from dangers including cyberbullying, and planning activities for the prevention of online violence against children [27]. Estonia initiated Safer Internet Project, e-Safety hotline for children and parents, the e-police initiative focused on children and awareness, e-course on e-safety for teachers supported by Tiger Leap Foundation's ICT [51] to promote the safe use of the internet,

especially for children. For ensuring safe cyberspace for children Estonia has a wide range of projects and educational programs at the school level such as Look@World Foundation's Smart Lab Project, Samsung Digital Turn Project for school, using Raspberry Pi-s at school with the support of TransferWise, Microsoft's Partners in Learning projects and so on [52]. The Cyber Olympic Project has also taken a lot of initiatives for children.

iii) **In educational institutions:** Estonia has created educational programs from the elementary school to the college levels. Estonia has established the Education and Youth Authority (HARNO) as the leading organization for training and awareness-raising programs which has activities on every education level, from kindergarten to university [40]. HITSA (The Information Technology Foundation for Education) organizes different competitions and training programs for students. Estonian universities are enriched with cybersecurity courses both at the graduate and undergraduate levels. The Tallinn University of Technology offers a Cybersecurity Engineering course at the undergraduate level and a joint MA program with the University of Tartu. In 2016, the University of Tartu launched an IT law training and research program aimed at providing highly qualified lawyers for working in the ICT and cybersecurity sector [27]. The Centre for Innovation in Education at Tallinn University, the *Pedagogicum* at the University of Tartu has the project Network of Innovation Schools, the Tallinn University of Technology's project *Mektory* Innovation [52], are some projects from universities of Estonia to support the safe use of cyberspace.

4.2 Cybersecurity awareness initiatives in Bangladesh

In this chapter, the author will discuss the initiatives taken by Bangladesh in the public & private sectors, for children's online safety and in Education.

i) **In the public & private sector:** People in Bangladesh are very novice in handling personal information, and they have almost zero knowledge of the measures for the protection of personal information. Although some awareness-raising programs exist, they are either very ad-hoc or not specified for different targeted groups. The BGD e-GOV CIRT (Bangladesh e-Government Computer Incident Response Team) as part of Bangladesh Computer Council (BCC) has designed

awareness campaigns and adapted some of the Stop.Think.Connect materials and publishes material on its website but they are not targeted to specific groups and people hardly know about their website and available materials [25]. The parents are still in the darkness and do not know how to protect their children from cybercrimes. Cyber Crime Awareness Foundation (CCA Foundation) is a private voluntary organization that is engaged in educating public and private sector personals through events and campaigns for raising awareness about Cyber Security and increasing the resiliency of the nation in combating cyber-incidents [53].

Several projects were prevailing that were supported by international partners but have been discontinued. No awareness campaigns for executives have been yet initiated. The private sector officials have little knowledge of cyber risks and threats and cybersecurity is not considered as the main concern [11]. In organizations, cybersecurity knowledge is focused on the officials of the IT (Information Technology) sector and other staff are not aware of cybersecurity at all. Also, Chief Information Security Officers (CISO) or Chief Information Officers (CIOs) are a very rare figure in different organizations.

ii) **For children's online safety:** Though many children and teenagers use smartphones and computers, at the primary and secondary school level students have one lesson in ICT, which is not over cybersecurity. There is no specific authority for organizing awareness-raising programs and competitions for the children. No online safety programs have been introduced yet for making children capable of securing themselves from cyber grooming, cyberbullying, and other cybercrimes.

iii) **In educational institutions:** There are only two private universities that offer a master's degree in Information Security [54] [55]. Also, there are no public or private universities where Bachelor or diploma degree courses are available. Despite the government taken different initiatives to increase the number of cybersecurity experts, universities are lagging in offering courses. Though almost every public and private university have Computer Science and Engineering courses both at the graduate and undergraduate level, these are not focused on cybersecurity at all.

4.3 Survey introduction

The author will analyze the responses that are collected from a survey (semi-structured interview) targeted at university students to validate the proposed awareness strategy for Bangladesh. Data were collected for a variety of aspects that are needed to be updated or launched to strengthen the cybersecurity awareness strategy of Bangladesh. From the survey, the author got an in-depth insight of the existing strategies in practice for raising awareness which enables to understand the lacking in the strategy and suggest some recommendations in view of the strategies introduced in Estonia.

There was a total of 22 questions (attached in the appendix) of varying types. The author collected a total of 91 responses.

4.4 Response analysis

The majority of the responses were made by the age group 18-30 years with educational qualifications of either a bachelor's or a master's degree. The author put questions to thoroughly understand the knowledge about the cybersecurity of the respondents. It was surprising to know that even graduates from universities do not have a satisfactory level of cybersecurity knowledge though most of them asserted in the response that they possess a moderate level of knowledge. Figure bellow shows knowledge of cybersecurity, where 1 represents no knowledge and 5 means very good knowledge.

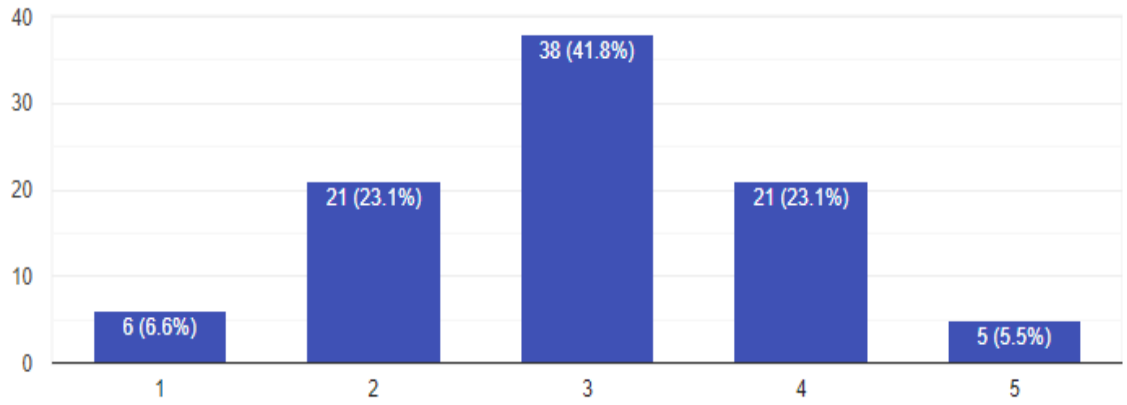

Figure 2: Cybersecurity knowledge level of the respondents

It became more justified when they replied in the negative on knowing about the National Cybersecurity Strategy developed by the Bangladesh government in 2014. Even most of them do not know what does 'NCSS' stands for. They got introduced to the term merely from this survey.

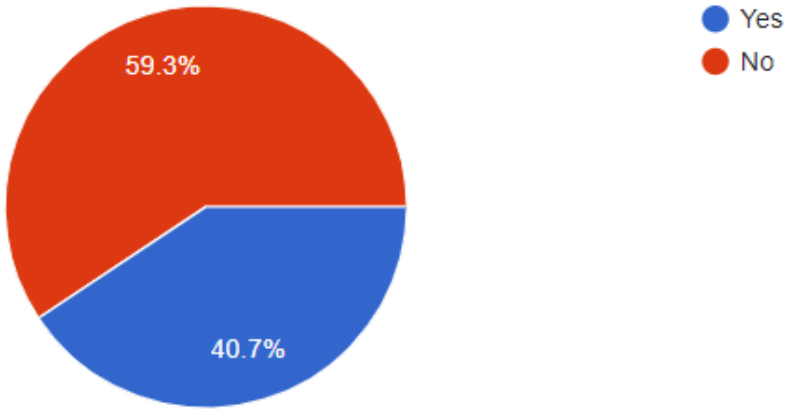

Figure 3: Knowledge of the development of National Cybersecurity Strategy

Despite not knowing what is 'NCSS', the respondents maintained that protecting cyberspace against security threats should be the main purpose of the National Cybersecurity Strategy.

Though Bangladesh is highly vulnerable to cyber threats, there is hardly any mentionable awareness-raising program available in educational institutions, workplaces, or online. It became evident when most of the participants said that they have not got any cybersecurity training from these authorities. It is an urgent need to introduce cybersecurity courses and training in educational institutions, workplace, and most importantly online platform.

As shown in the figure below most participants have not received any cybersecurity training in their workplace or educational institutions.

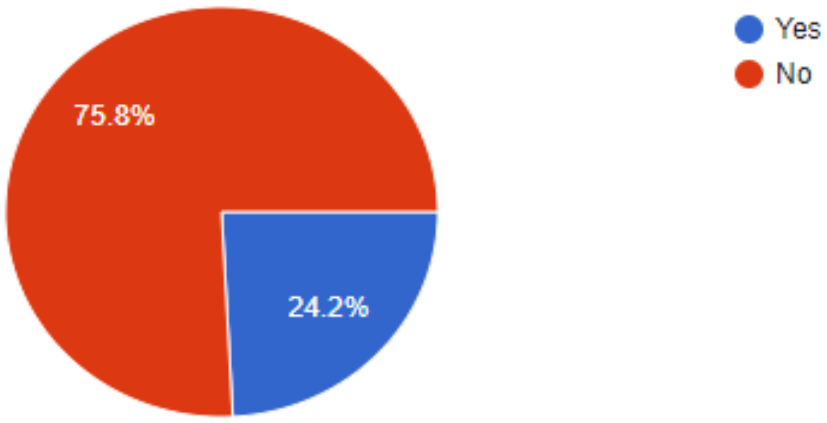

Figure 4: Percentage of respondents who received cybersecurity training

The survey responses also show that raising awareness should be the priority of the government to combat cyberthreats. When asked if the respondents would be willing to take cybersecurity training, over 80 % of them answered that they are willing to take courses if they are available.

While cyber experts are the main catalysts in fighting against cyberthreats, Bangladesh is lagging in this sector. The respondents feel that Bangladesh needs more and more cyber experts in both the public and private sectors. They are also 'Somewhat Okay' with the e-governance services taken by the government but feel an urgent need for additional up-to-date services like online tax system, e-voting etc. Introduction of cybersecurity related degree programs in universities and investment in cybersecurity research programs can greatly help to increase the number of experts in this field.

As it was discussed in the previous chapter, Bangladesh is taking some measurements like awareness campaign by BGT e-GOV CIRT or providing some cybersecurity materials on their website. However, as the figure below shows, most respondents are not satisfied with the current existing measurements.

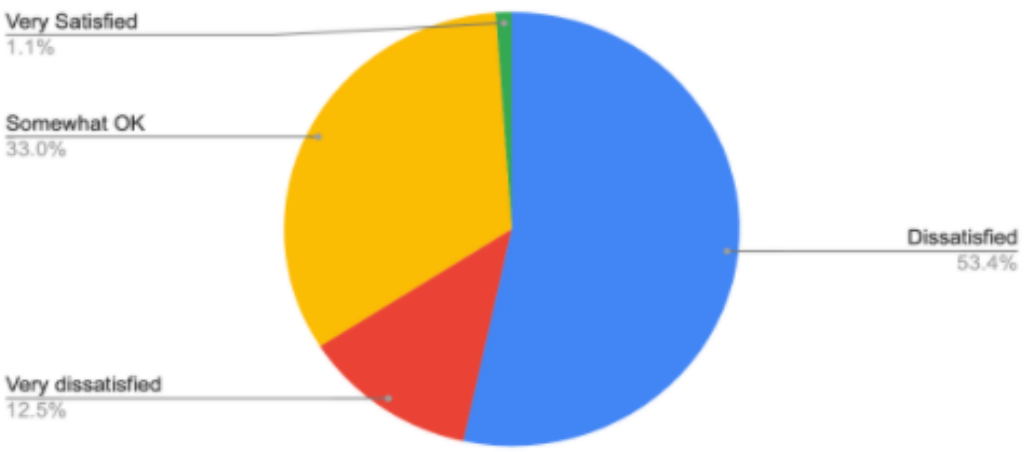

Figure 5: Satisfaction level with the current existing measurements

The Bangladesh police have little expertise in handling cybercrimes. They hardly know how to collect evidence for this kind of crime. There is no specialized branch in police to deal with cyber threats. But in most cases, people contact the police when they face any cybercrime. They do not know about the BGD e-GOV CIRT (Bangladesh e-Government Computer Incident Response Team) where they can report and get justice.

The overall scenario of the responses refers to the need for developing an effective cybersecurity awareness strategy. The majority of the respondents have neither got any training on cybersecurity nor have any cybersecurity course in their university. Almost all the participants asserted the government should take urgent steps for raising awareness of cybersecurity. They are also not satisfied with the initiatives taken by the government. They asked for more experts with proper cybersecurity knowledge in all sectors.

4.5 A cybersecurity awareness strategy for Bangladesh

i) **Lessons from Estonia:** Estonia has been successful in raising awareness of people from all sectors, especially the students from schools and universities. Estonia has a wide range of programs, training, and initiatives providing unparalleled opportunities in raising awareness and educating people. According to the 2015 cybersecurity survey conducted by the European Commission, 47 percent of Estonian residents admitted that they felt well informed about the risks of cybercrime [37]. The Education and Youth Authority (HARNO) (previously known as HITSA) operates as the leading organization for training and awareness-raising programs which has activities on every education level, from kindergarten to university [38]. HARNO (Education and Youth Authority) is a joint organization of Foundation Innove, Foundation Archimedes, Information Technology Foundation for Education (HITSA) and Estonian Youth Work Centre with 11 departments tasked with individual responsibilities. In June 2015, HITSA (Information Technology Foundation for Education) organized a cybersecurity contest for the students from secondary school and the top five contestants were awarded a visit to the Ministry of Défense, NATO Cooperative Cyber Defence Centre of Excellence (CCDCoE), the CDU (Cyber Defense Unit), and the Estonian Information System Authority [28]. 70 participants from all over the world, including faculty members from the University of California, Berkley, Oxford University, and University College London, took part in the first cybersecurity summer school organized by HITSA (Information Technology Foundation for Education) [56]. The Centre for Innovation in Education at Tallinn University is providing teachers training and project days; the *Pedagogicum* at the University of Tartu has the project Network of Innovation Schools and providing their training and solutions; the Tallinn University of Technology's project *Mektory* Innovation provides students and teachers a training about science [52]. The Ministry of Defence and the School of Information Technologies at Tallinn University of Technology together run the Cyber Olympic Project. Under the project a variety of initiatives has been taken such as CyberPin – a test for 7-12 years old students about logic, crypto, and IT problem-solving challenges; CyberCracker – a digital safety awareness program for 10-15 years old students; CyberSpike – for making 14-24 years old children to participate

in European Cyber Security Challenge and many other hacking challenges around the world, providing higher level hacking competition and training program; most importantly this project is providing supporting curriculum and materials to Estonian schools starting from the 1st grade with the goal to gamified cybersecurity (introduced Cybersecurity Game) education and making it more practical [50].

Estonia launched the project Safer Internet Centre in Estonia – Smartly on the Web, in 2010. The project's activities are mainly focused on three sectors, i.e. awareness-raising, hotline activity, and Helpline activity regarding the child helpline 116 111 [57]. The awareness-raising project is run by the Tiger Leap Foundation under this project [57]. The e-course on e-safety initiated by the Foundation is aimed at giving a clearer overview of the inter safety issue to common teachers. There were 7 main objectives: to teach how to protect a computer from viruses, to make familiarize with various websites that are focused on e-safety, smart use of the internet, familiarizing with various social networking sites, teaching how to choose secure passwords, raising awareness on cyberbullying and learn how to react as well as learn how to teach students about these matters [51]. The hotline activity is advising children, their parents, and other officials on safe internet issues by providing training for parents and children on identifying computer addiction, limiting child's computer usage, handling child's computer addiction; identity theft on social networks; competence imbalance on internet, recommendations for children in using the Internet; cyber grooming; sexual harassment; advice in case of cyberbullying; unnecessary internet/mobile broadband bills; annoying contacts; potential harmful content, etc [57]. The child helpline 116 111 is appointed with the responsibility to answer parents' and children's questions regarding Internet usage and other networking technologies via both phone and web [57]. NPO Estonian Union for Child Welfare coordinates the whole project of the child helpline and operates the Hotline work [57]. A report about materials on the Internet containing sexual abuse of children can be submitted to the Hotline webpage (*www.vihjeliin.ee*) [57]. Other initiatives of the 'Safer Internet Centre in Estonia – Smartly on the Web' project includes documentaries named 'Life in the Virtual World' on ETV2, a special edition of the magazine

"*Märka last*" in the newspaper "*Postimees*", Student competition: 'Let's discover the digital world together...safely!', and introducing learning materials such as Play & Learn workbook for children aged 4-8, Study games: 'Discovering Real Life' & 'Odd and Even', the animated film 'Bunny-Johnny in the Internet world', Web-based game 'Nastix', and these are very successful in the specific sectors [57].

ii) **Recommendations for Bangladesh:** A private organization named Cyber Crime Awareness Foundation (CCA) in Bangladesh published a research report on 29th September 2019 on "The trend of cybercrime in Bangladesh" [58]. In this report, the organization suggested 10 steps for reducing cybercrimes and ensuring cybersecurity. The suggestions include declaring the month October as 'Cyber Awareness Month', introducing the existing 'Digital Security Act' to mass people as most people has no idea of this act, using electronic media more effectively as a medium of raising awareness, inclusion of 'Cyber Lessons' in the curriculum of primary and secondary schools, the proposed "Cyber Gym" at the Military Institute of Science and Technology (MIST) should be established as soon as possible to meet the urgent need of cybersecurity specialists in the country, appointing cybersecurity specialists in private and public sectors, etc [58]. But CCA (Cyber Crime Awareness Foundation) did not provide any guideline on which projects and programs could be added to the awareness-raising initiatives domain. The author is suggesting the following inclusions in the awareness strategy based on the successful initiatives taken by Estonia:

- An authority like the Education and Youth Authority (HARNO) should be established to act as the primary source for monitoring and implementing the awareness-raising strategy. This authority should host competitions and campaigns both at the national and international level in cooperation with similar authorities from other countries.

- The top public universities in Bangladesh should come forward with a motive of helping in developing the awareness strategy and supporting the strategy with the development of required materials. The universities can get an idea of the required projects and materials from the successful projects of Estonia's top universities i.e., Tallinn

University of Technology, University of Tartu, Tallinn University, and if needed can collaborate with the Estonian universities.

- The students from primary and secondary schools should be inspired to take cybersecurity as a career motive. The best way to do this is to host regular competitions as Estonia did and doing till now. Though different international Olympiads are organized in Bangladesh regularly, an Olympiad like the Cyber Olympic Project would be the best inclusion for students to inspire them. Competitions like CyberPin, CyberCracker, CyberSpike, or similar ones should be held regularly.

- Most of the children use smartphones and other electronic devices for gaming and social networking. If proper steps could be taken to gamify the cybersecurity awareness strategy, then the student would practically learn the aspects of cybersecurity. Bangladesh Computer Council (BCC) can take an eye to the existing games developed by different countries and should take the step to develop one for children in Bangladesh.

- An integrated project like the "Safer Internet Centre in Estonia- Smartly on the Web" should be introduced with the cooperation of all the related authorities. A project like Safer Internet Centre in Estonia is a crying need in Bangladesh since neither the parents nor the children know how to be secured online.

- The teachers at primary and secondary school levels need to be trained for the successful implementation of the initiative. An e-course on e-safety like Estonia would be the best solution for this.

- Police are the only widely known authority for reporting all kinds of crime. But they are not well trained for handling cybercrimes, especially the ones that occur with children. E-police initiatives like Estonia could be introduced in this regard.

- Hotline Activity, which includes children, their parents, and other officials from the public and private sector in the awareness-raising program, could

be developed by the government for making the related personals aware of the cybersecurity measures.

- Organizations from the private sector can also help the government with a budget and take initiatives for raising awareness. They can take an idea from the successful initiatives from Estonia like the Smart Lab Project sponsored by Look@World Foundation, Samsung Digital Turn Project for school, using Raspberry Pi-s at school with the support of TransferWise, Microsoft's Partners in Learning projects [52]. The government cannot be successful with the awareness strategy without the help of private and public sectors' stakeholders.

- A child helpline needs to be initiated with the responsibility to answer parents' and children's questions regarding Internet usage and other networking technologies via both phone and web.

- All the projects and campaigns, the related authorities, and the implementation of the awareness strategy should be monitored by one authority. But, unfortunately, the Bangladesh government has developed a National Cybersecurity Strategy which does not assign any authority for implementing the strategy. Thus, it is a suggestion to revise the National Cybersecurity Strategy of Bangladesh for the needed inclusions and development.

iii) Challenges for Bangladesh to implement the proposed awareness strategy: The author of this study has suggested an awareness strategy for Bangladesh. However, Bangladesh will require to develop and introduce the required authorities, websites, training facilities, and study materials. Also, the financial capability of Bangladesh will be another factor to study if these strategies are implementable.

The cultural discrepancies between Estonia and Bangladesh will be the most challenging hinder in implementing the strategy proposed by the author. When Estonia has a cyber-aware population spontaneously reporting cybercrime whenever faced, the Bangladeshi people always think about social respect above getting justice. No matter how severely a person is victimized by cyberbullying

or harassment, both the parents and the victim prefer to negotiate with the criminal to uphold the honour in society. The victim suffers hundreds of times greater than the criminal. This mindset will bar the success of the proposed strategy.

Another factor is the variation of crimes in Estonia and Bangladesh. While cyber gambling is a crime in Bangladesh, even the leaders from government parties have been accused of cyber gambling and put into jail; it is not a crime in Estonia if got a license from the Estonian Tax and Customs Board. The government should take these cultural variations into account before extravagantly executing the lessons learned from Estonia.

While the Estonian people supports and cooperates in executing the initiatives taken by the government in combating cybercrimes, the people of Bangladesh takes the step negatively if it goes against their interest. Thus, the government fails to act adequately in this mere concept. For instance, in Bangladesh liberty of the press is highly practiced. The journalists can criticize the government and come up with their opinion on a specific matter. But more often, the newspapers cross the thin line of constructive criticism. If the government tries to put a halt to this kind of independence, people take this negatively and criticize the government. They are indifferent to follow the rules and regulations that are not as per their interest. People think of their interests above the greater benefits of the nation. No nation will be successful with its cybersecurity strategy having a population of this attribute.

Besides, government officials are not helpful enough in analyzing the drawbacks of the existing awareness strategy and establishing new ones. The author tried to contact the officials from the Bangladesh Computer Council (BCC), The BGD e-GOV CIRT (Bangladesh e-Government Computer Incident Response Team), and the Adviser to Hon'ble Prime Minister for ICT Affairs to know the existing measures and strategies for raising awareness, but nobody was willing to provide any information on this. The research and development sector in cybersecurity is lagging in Bangladesh due to these unsupportive officials.

iv) **Future Research Scope:** This study can be a guideline for further study in developing and implementing the awareness-raising strategy of Bangladesh.

The success of the proposed measures should be analyzed keeping in mind the socio-economic and demographic status of Bangladesh. the author proposed the awareness strategy based on the successful awareness-raising initiatives of Estonia but these need to be analyzed thoroughly before implementation. An integrated and successful awareness strategy could be developed by not only studying the initiatives of Estonia but also other countries.

5 Conclusion

The study has found that the National Cybersecurity Strategy (NCSS) of Bangladesh has not been properly designed and implemented. The study also points out that Bangladesh doesn't have a responsible authority to monitor and implement their NCSS goals. From the comparative analysis, it's also established that Bangladesh doesn't have specific laws and regulations in place to combat cybercrime. An extensive set of measures should be introduced and developed to be successful with the NCSS (National Cybersecurity Strategy). From the survey, it is also evident that the Bangladesh government has not taken proper measures for raising the cyber awareness of people. Even graduates from universities don't have sufficient knowledge of cyber threats and cybersecurity. The BGD e-GOV CIRT should be more engaged in raising awareness and establish cooperation with organizations in the private sector.

This study proposed a series of recommendations that will help in the improvement of the National Cybersecurity Strategy (NCSS). Finally, an awareness strategy that could be developed and implemented in Bangladesh to be successful in raising the cyber awareness of people has been proposed.

References

[1] International Telecommunication Union, "Statistics," [Online]. Available: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx. [Accessed 05 September 2020].

[2] World Economic Forum, "Global Risks Report Eighth Edition," 2013.

[3] Ü. Tatar, O. Çalik, M. Çelik and B. Karabacak, "A Comparative Analysis of the National Cyber Security Strategies of Leading Nations," in *9th International Conference on Cyber Warfare & Security.*, 2014.

[4] M. J. Schwartz, "Bangladesh Probes 2013 Bank Hack via SWIFT," Bank Info Security, 2016.

[5] K. Sarker, H. Rahman, F. Khandaker, M. S. Arman, S. Biswas and T. Bhuiyan, "A comparative analysis of the cybersecurity strategy of Bangladesh," *International Journal on Cybernetics & Informatics (IJCI)*, Vols. 8, No. 2, 2019.

[6] "Department of Printing and Publications, Government of the People's Republic of Bangladesh," [Online]. Available: http://www.dpp.gov.bd/upload_file/gazettes/10041_41196.pdf. [Accessed 3 September 2020].

[7] N. Shafqat and A. Masood, "Comparative Analysis of Various National Cyber Security Strategies," *(IJCSIS) International Journal of Computer Science and Information Security,* Vols. 14, No.1, 2016.

[8] International Telecommunication Union, "Global Cybersecurity Index 2018".

[9] e-Governance Academy Foundation, "NCSI National Cybersecurity Index," [Online]. Available: https://ncsi.ega.ee/ncsi-index/. [Accessed 2 September 2020].

[10] A. Maumdar and H. H. Alharahsheh, "Digital Bangladesh -Vision 2021: What is the Digital Bangladesh Concept?," *South Asian Research Journal of Engineering and Technology,* vol. 2, no. 1, 2020.

[11] "Cybersecurity Capacity Review Bangladesh," Global Cyber Security Capacity Center, 2018.

[12] N. Ahmed, U. Kulsum, M. I. B. Azad, Z. Momtaz, E. Haque and S. Rahman, "Cybersecurity awareness survey: An analysis from Bangladesh perspective," 2017.

[13] "Remarks by the president on securing our nation‘s cyber infrastructure," 2009. [Online]. Available: https://obamawhitehouse.archives.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure. [Accessed 13 September 2020].

[14] J. J. Duderstadt, D. E. Atkins and D. V. Houweling, "Higher education in the digital age: Technology issues and strategies for American colleges and universities.," Rowman & Littlefield Publishers, 2002.

[15] J. Q. Anderson, J. L. Boyles and L. Rainie, in *Higher Education: Experts Expect More Efficient Collaborative Environments and New Grading Schemes; They Worry about Massive Online Courses, the Shift Away. Pew Internet & American Life Project*, http://www.eric.ed.gov/ERICWebPortal/recordDetail?accno=ED534048, 2012, pp. 1-43.

[16] M. G. Nardoianni, The Cyber Security Challenge: A Comparative Analysis, Rome, Italy: LUISS University, 2016.

[17] M. K. Swartz, "Cyberbullying: An extension of the schoolyard," *Journal of Pediatric Health Care,* Vols. 23, NO. 5, pp. 281-182, 2009.

[18] Q. Li, "New bottle but old wine: A research of cyberbullying in schools," *Computers in Human Behavior,* vol. 23, pp. 281-282, 2007.

[19] ITU, "Statistics," [Online]. Available: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx. [Accessed 4 September 2020].

[20] The International Telecommunication Union (ITU), "https://www.itu.int," [Online]. Available: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx. [Accessed 15 October 2020].

[21] F. Wamala, "ITU National Cybersecurity Strategy Guide," 2011.

[22] ITU, "Series x: data networks, open system communications and security. Overview of cybersecurity. Recommendation ITU-T X.1205," ITU, 2008.

[23] "Global Cybersecurity Index (GCI)," International Telecommunication Union (ITU), 2017.

[24] "Guide to Developing a National Cybersecurity Strategy –Strategic engagement in cybersecurity," International Telecommunication Union (ITU), 2018.

[25] "BGD e-GOV CIRT | Bangladesh e-Government Computer Incident Response Team|," [Online]. Available: https://www.cirt.gov.bd/.

[26] www.thefinancialexpress.com.bd, [Online]. Available: https://www.thefinancialexpress.com.bd/trade/90pc-business-software-in-bangladesh-is-pirated-us-report-1601632144. [Accessed 5 January 2020].

[27] Ministry of Economic Affairs and Communications, Republic of Estonia, Republic of Estonia, Ministry of Economic Affairs and Communication, 2008. [Online]. Available: https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf?fbclid=IwAR2fxD0WtfVFLMcsgS7iAlWyfI5_qBHZL7geUzdyjfkXxb73zvo1INAM740. [Accessed 7 September 2020].

[28] J. A. Lewis, "Advanced Experiences in cybersecurity policies and practices," Inter-American Development Bank (IDB), 2016.

[29] "Activities of CERT Estonia," [Online]. Available: https://www.ria.ee/en/cyber-security/cert-ee.html. [Accessed 20 October 2020].

[30] *Emergency Act, Republic of Estonia, RT I 2009, 39,262, as last amended by RT I, 30.06.2015, 4.*

[31] *State Secrets and Classified Information of Foreign States Act, Republic of Estonia, RT I 2007, 16, 77, as last amended by RT I,22.12.2011, 2.*

[32] *Electronic Communications Act, RT I 2004, 87, 593, Republic of Estonia, as last amended by RT I, 25.03.2011, 1.*

[33] *Personal Data Protection Act, Republic of Estonia, RTI 2007,24, 127, as last amended by RT I, 30.12.2010, 2.*

[34] Global Cyber Security Capacity Centre (GCSCC), University of Oxford, [Online]. Available: https://gcscc.ox.ac.uk/the-cmm. [Accessed 02 September 2020].

[35] "The CMM | Global Cyber Security Capacity Centre," Global Cyber Security Capacity Centre, [Online]. Available: https://gcscc.ox.ac.uk/the-cmm.

[36] K. Kaska, A.-M. Osula and L. J. Stinissen, "The Cyber Defence Unit of the Estonian Defence League," NATO CCDCoE," 2013.

[37] "Special Eurobarometer 423, "Cybersecurity Report," survey conducted by TNS Opinion & Social at the request of the European Commission," Directorate-General for HomeAffairs, 2015.

[38] "e-Estonia," [Online]. Available: http://estonia.eu/about-estonia/economy-a-it/e-estonia.html..

[39] D. Springall, T. Finkenauer, Z. Durumeric, J. Kitcat, H. Hursti, M. MacAlpine and J. A. Halderman, "Security Analysis of the Estonian Internet Voting System," in *The 21st ACM Conference on Computer and Communications Security (CCS '14)*.

[40] "Haridus- ja Noorteamet," [Online]. Available: https://harno.ee/en/about-us. [Accessed 05 January 2020].

[41] "Bangladesh Panel Code 1860," 6 October 1860. [Online]. Available: http://bdlaws.minlaw.gov.bd/act-11.html. [Accessed 11 October 2020].

[42] Ministry of Law, Justice and Parliamentary Affairs, Bangladesh, "Bangladesh Pornography Control Act, 2012," 8 March 2012. [Online]. Available: http://bdlaws.minlaw.gov.bd/act-1091.html. [Accessed 11 October 2020].

[43] *Directorate of National Consumer Rights: Consumers' Right Protection Act 2009.*

[44] Ministry of Law, Justice and Parliamentary Affairs, Bangladesh, "WIPO: Bangladesh Copyright Act," [Online]. Available: http://www.wipo.int/wipolex/en/details.jsp?id=11172. [Accessed 11 October 2020].

[45] *Patents and Design Act (1911).*

[46] *WIPO: Bangladesh Trademarks Act*, 2009.

[47] Ministry of Law, Justice and Parliamentary Affairs, Bangladesh, "International Labour Organization: BangladeshChildren's Act," 2013. [Online]. Available: https://www.unicef.org/bangladesh/sites/unicef.org.bangladesh/files/2018-07/Children%20Act%202013%20English.pdf. [Accessed 10 October 2020].

[48] The Information System Authority (RIA), "Estonian Security System Overview," 2012. [Online]. Available: https://www.ria.ee/sites/default/files/content-editors/kuberturve/eisa_on_cyber_security_2012.pdf. [Accessed 6 October 2020].

[49] "e-government code repository," [Online]. Available: https://e-estonia.com/code-repository-for-e-governance/.

[50] "ECSC Eesti eelvoor - About the Project," [Online]. Available: https://sites.google.com/view/kyberolympia/eng/about-the-project?authuser=0.

[51] B. Lorenz and K. Kikkas, "Lessons Learned from the Safer Internet Program," e-Learning Papers, 2012.

[52] B. Lorenz, K. Kikkas and M. Laanpere, Digital Turn in the Schools of Estonia: Obstacles and Solutions, Springer International Publishing Switzerland, 2016, pp. 1-10.

[53] "CCABD - Cyber Crime Awareness Foundation," [Online]. Available:https://ccabd.org/.

[54] BANGLADESH UNIVERSITY OF PROFESSIONALS, "Masters in Information SystemsSecurity(MISS),"[Online].Available: https://bup.edu.bd/programs/22/details-academics?department_id=17. [Accessed 1 November 2020].

[55] United International University, "MSCSE(MAJOR CYBER SECURITY)," [Online]. Available:http://cse.uiu.ac.bd/graduate-program/mscsemajor-cyber-security/. [Accessed 1 November 2020].

[56] "Information Technology Foundation for Education," [Online]. Available: http://www.hitsa.ee/about-us/news/.

[57] "Targalt Internetis," 2011. [Online]. Available: http://www.targaltinternetis.ee. [Accessed 13 November 2020].

[58] Cyber Crime Awareness Foundation, "CCABD," 2019. [Online]. Available: https://ccabd.org/wp-content/uploads/2019/09/Research_Report_Cybercrime_2019_CCAFoundation.pdf.

Appendix 1 – Questionnaire

1. Rate your knowledge about cybersecurity (0- None, 5- Very Good)
2. Are you satisfied with the measures taken by the government to secure the national cyberspace?
    a. Very satisfied
    b. Satisfied
    c. Somewhat OK
    d. Dissatisfied
    e. Very satisfied
3. Have you heard of any cyberattack on a public or private organization in Bangladesh?
4. In your opinion, how vulnerable is Bangladesh to cyber threats? (0- Not vulnerable, 5 – Highly vulnerable)
5. Do you know of any measures taken by the government to protect cyberspace?
6. Are you aware that the government has developed a National Cybersecurity Strategy in 2014?
    a. Yes
    b. No
7. What is the purpose of a national cybersecurity strategy (NCSS)? (Select all that applies)
    a. Protecting cyberspace against security threats
    b. To enact laws to deter and prosecute cybercrime.
    c. Identifying the information infrastructures that are vulnerable to cyber threats
    d. Making people aware of the need for cybersecurity
    e. I don’t know
    f. Other:
8. Are there enough cybersecurity experts in Bangladesh?
    a. Yes
    b. No
    c. More specialists are needed

9. Have you ever received any cybersecurity training from your educational institution, workplace, or online?
    a. Yes
    b. No
10. Should educational institutions introduce cybersecurity courses?
    a. Yes
    b. No
11. Please select if you have experienced any of the following (Select all that applies)
    a. I have had a virus or unwanted software on my device
    b. The computer was hijacked/taken over
    c. I have been a victim of online fraud/I lost money
    d. I was blackmailed
    e. Other
12. What step will you take if you encounter a cybercrime? (Select all that applies)
    a. Contact the police
    b. Try to negotiate with the criminal considering social respect
    c. Do nothing at all
    d. Tell friends
    e. Other
13. Are you satisfied with the e-government services?
    a. Very satisfied
    b. Satisfied
    c. Okay
    d. Dissatisfied
    e. Very satisfied
14. What additional e-government services can be added to the domain?
    a. Electronic id cards
    b. Digital signature
    c. Internet voting
    d. Online tax returns
    e. Other
15. In your opinion, are the laws in effect can control cybercriminals?
    a. Strongly agree
    b. Agree

c. Neutral
d. Disagree
e. Strongly disagree

16. Should the government take initiative to create awareness programs for all age groups?
    a. Yes
    b. No
17. Should the Bangladesh government collaborate with international organizations to improve its cyberspace?
    a. Yes
    b. No
18. Were you familiar with the term 'NCSS' before taking this survey?
    a. Yes
    b. No
19. Do you have any suggestions on how to improve the cybersecurity situation in Bangladesh?

20. What gender do you identify as?
    a. Male
    b. Female
    c. Oher
    d. Prefer not to say
21. How old are you?
    a. Below 18
    b. 18-30 years
    c. 31-40 years
    d. above 40
22. What is the highest degree or level of school you have completed?
    a. High school graduate, diploma or the equivalent
    b. Bachelor’s degree
    c. Master’s degree
    d. Doctorate

Appendix 2 – Non-exclusive license for reproduction and publication of a graduation thesis[1]

I Anamul Hoque Shihab

1. Grant Tallinn University of Technology free license (non-exclusive license) for my thesis “Lessons from Estonia: A cybersecurity strategy for Bangladesh”, supervised by Kaido Kikkas
   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 the 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 licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

07.01.2020

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.