CYBER SECURITY CAPACITY BUILDING OF PAKISTAN

By

Maryam Khalid

A thesis submitted to the faculty of Information Security Department, Military College of Signals, National University of Sciences and Technology, Rawalpindi in partial fulfillment of the requirements for the degree of MS in Information Security

June 2018

CERTIFICATE

This is to certify that Maryam Khalid Student of **MSIS-13** Course Reg.No: **NUST201362682MMCS25213F** has completed her MS Thesis title **"Formulation of National Strategy for Cyber Security Capacity Building"** under my supervision. I have reviewed her final thesis copy and am satisfied with her work.

_____

Thesis Supervisor

(Asst Prof Dr. Rabia Latif)

Dated: _____

ABSTRACT

Cyberspace is an integral aspect in evolution of a country as it is growing at a rapid pace. Digital infrastructure used today has inherent vulnerabilities and the cyber attacks are becoming more sophisticated with each passing day. A powerfully built cyber capacity is required for smooth operations in a country where development of various sphere like social, economic and political is dependent on cyberspace. Cyber capacity building is aimed to facilitate the individuals and to provide them with adequate knowledge and skill set to combat against cyber attacks/threats or generally countries have plans and processes in place to raise awareness among the masses in this regard.

This research aims to provide comparative analysis of National Cyber Security Strategies of twenty different countries based on the measures taken for advancement of cyber capacity building. The major observation concluded from this analysis is that those developed nations are mostly equipped with technology and policy alongside some developing countries for cyber capacity building unlike other nations that have yet to set their priorities for building cyber capacities. The second step in this research was to conduct a survey to assess the level of cyber maturity among masses. The results of the survey and the analysis will lead to developing the cyber security strategy for Pakistan while depending on the comparison this research generate and specifies recommendations that can be adopted by counties striving to construct their cyber capacity building culture in an advanced and adequate manner.

ACKNOWLEDGMENTS

I am writing this acknowledgement to reflect on the people who have supported and me and provided their guidance so much throughout my research and year of study at Military College of Signals. I must express my profound gratitude to all my professors at MCS while my masters in IS. I would like to acknowledge efforts of my supervisor Rabia Latif for her guidance.

A special mention and thankyou to my co-supervisor Brig Tugral for guiding in my initial stages. I would like to show gratitude to my committee members for reading my thesis and providing me with beneficial feedback. I would like to thank my HoD IS for his efforts. The way he motivated me for completion of my thesis by conducting monthly progress meetings.

I would like to particularly single out my committee member Lec Narmeen Shafqat and thank her for her excellent cooperation. Her door was always open for me and she guided me in the right direction, aiding me with relevant documents and providing me her valuable time.

Finally, I would thank my parents, husband, friends and special mention to my brother for providing me with their continuous encouragement and unfailing support through my research process and in ,my year of study. I could not have accomplished this task without these people.

TABLE OF CONTENTS

ABSTRACT ..... **iii**
ACKNOWLEDGMENTS ..... **iv**
TABLE OF CONTENTS ..... **v**
LIST OF FIGURES ..... **ix**
LIST OF TABLES ..... **x**
ACRONYMS ..... **xi**
INTRODUCTION **1**
1.1 Introduction **1**
1.2 Problem Statement **2**
1.3 Research Objective **2**
1.4 Scope of Research **2**
1.5 Areas of Application **2**
1.6 Significance of Research **3**
1.7 Research Methodology **3**
1.7.1 Comparative Analysis 3
1.7.2 Survey 4
1.7.3 Strategy Development 4
1.8 Thesis Outline: **4**
CAPACITY BUILDING **6**
2.1 Introduction **6**
2.2 Defining Capacity Building: **6**
2.2.1 Capacity Building Importance: 6
2.2.2 Target Audience 7
2.2.3 Initiator In Capacity Building 8
2.2.4 Aim Of Cyber Security Capacity Building 8
2.2.5 Obstacles in Effective Cyber Security Capacity Building Plan 9
2.3 Factors affecting CCB **10**
2.4 Pakistan's Cyber Space: **12**
2.4.1 Pakistan Initiatives In CCB 13
2.5 Conclusion **14**
COMPARATIVE ANALYSIS OF DIFFERENT COUNTRIES **15**
3.1 Introduction **15**
3.2 Literature Review **15**

3.2.1 Itu Framework....16
3.3 Selection Of Countries....16
3.3.1 Developed Countries....17
3.3.2 Developing Countries....18
3.4 Comparison Metrics....18
3.5 Highlighted Metrics Comparison....19
3.5.1 Definition of Capacity Building....19
3.5.2 Manpower Development....20
3.5.2.1 Raising Cyber Awareness:....20
3.5.2.2 Building Cyber Security Culture....21
3.5.3 Participation in International Organizations Activities....22
3.5.3.1 National Cyber Security Awareness Month (NCSAM)....22
3.5.3.2 Privacy Awareness Week (PAW)....23
3.5.3.3 European Cyber Security Month (ECSM)....23
3.5.4 Standardization Development....24
3.5.5 Building Cyber Workforce....25
3.5.5.1 Cyber Ex:....25
3.5.5.2 C-Save:....25
3.5.6 Cyber Security Training....26
3.5.7 Cyber Security Education:....29
3.5.7.1 Cyber Security Formal Education....29
3.5.7.2 Online Cyber Security Degree Programs....29
3.5.8 Research and Development....30
3.5.8.1 Homegrown Indigenous Industry:....31
3.5.9 Cyber Security Capacities:....32
3.5.9. 1 Capacity Building Program for International Cyber Security Negotiations:....33
3.5.10 Cyber Security Spending....33
3.5.11 National Cyber Security Awareness Training Program For The Internet Users....34
3.5.12 CCB in Pakistan....34
3.5.13 Recommendation....35
3.5.12.1 Recommendations for Initiating Countries:....36
3.5.12.2 Recommendations for Maturing Countries:....36
3.5.12.3 Recommendations for Leading Countries:....37
3.6 Conclusion....38
***DATA ANALYSIS AND FINDINGS*....39**
4.1 Introduction....39
4.2 Response rate:....39

4.3 Survey Results: **40**
4.3.1 Question 1 41
4.3.2 Question 2: 42
4.3.3 Question 3: 43
4.3.4 Question 4: 43
4.3.5 Question 5: 44
4.3.6 Question 6: 44
4.3.7 Question 7: 45
4.3.8 Question 8: 47
4.3.9 Question 9: 48
4.5 Conclusion: **49**
CYBER SECURITY CAPACITY BUILDING STRATEGY **50**
5.1 Introduction **50**
5.2 Guiding Principles **50**
5.3 Vision **51**
5.4 Framework Summary **51**
5.5 Roles And Responsibilities: **53**
5.5.1 Strategy Head: 53
5.5.2 Chief Information Security Officer: 53
5.5.3 Program Manager: 54
5.5.4 Manager: 54
5.5.5 Users: **55**
5.5.5.1 Types of Users: 55
5.6 Awareness **55**
5.6.1 Guiding Principles 56
5.6.2 Awareness medium: 56
5.6.3 Developing Awareness Material: 58
5.6.3.1 Choosing Awareness Topics: 58
5.6.4 Cyber Awareness Week: 60
5.7 Training: **61**
5.7.1 Training Life Cycle: 61
5.7.2 Training Course: 62
5.7.3 Training Types: 62
5.7.3.1 Video Training: 62
5.7.3.2 Web-Based Training : 63

5.7.3.3 Instructor-Led Training : 63
5.7.3.4 Level Of Training According To User Type: 63
5.7.4 Training Outcomes (Cyber Scout) 64
5.8 Education: 64
5.8.1 Middle School: 65
5.8.2 High School (9-12) 66
5.8.3 Graduate: 66
5.8.4 PostGraduate: 69
5.9 Research And Development 70
5.10 Home Grown Industry 71
5.11 Implementation 72
5.11.1 Immediate Actions- Phase A: 72
5.11.2 Mandatory Actions- Phase B: 72
5.12 Conclusion 73
***CONCLUSION* 74**
6.1 Introduction 74
6.2 Objective Achieved 74
6.3 Limitation 74
6.4 Future Directions 75
6.5 Concluding Remarks 77
Appendix "A" –Cyber Maturity Assessment Questionnaire 78
BIBLIOGRAPHY 80

LIST OF FIGURES

FIGURE 4.1: GENDER DISTRIBUTION 40
FIGURE 4.2: AGE DISTRIBUTION 40
FIGURE 4.3: UNDERSTANDING OF TERM “CYBER” 41
FIGURE 4.4 SURVEY RESULT OF FOUR QUESTIONS 42
FIGURE 4.5 URL USED TO OPEN FACEBOOK 45
FIGURE 4.6 SECURE PASSWORD 46
FIGURE 4.7 CIRCUMSTANCES TREATED AS SUSPICIOUS 47
FIGURE 4.8 NATIONAL ORGANIZATION CONTACTED WHEN FACEBOOK PROFILE HACKED 48
FIGURE 6.1 CYBER SECURITY CAPACITY BUILDING STRATEGY 76

LIST OF TABLES

TABLE 3.1 LEADING COUNTRIES WITH HIGH ITU RANKING 16
TABLE 3.2 LEADING COUNTRIES WITHOUT REVIVED CAPACITY BUILDING RANKING 17
TABLE 3.3 DIFFERENT AWARENESS CAMPAIGNS 20
TABLE 3.4 SUMMARY OF STANDARDIZATION BODY OF COUNTRIES 24
TABLE 3.5 TRAININGS OF SELECTED COUNTRIES 26
TABLE 3.6 HOME GROWN INDIGENOUS PRODUCTS 31
TABLE 3.7 CCB ACTIVITIES IN PAKISTAN 34
TABLE 5.1 FRAMEWORK FACTORS WITH THEIR DESCRIPTIONS 51
TABLE 5.2 LEVEL OF TRAINING ACCORDING TO USER TYPE 64
TABLE 5.3 LIST OF GRADUATE COURSES WITH THEIR DESCRIPTION 66
TABLE 5.4 LIST OF DIFFERENT SECURITY AREAS WITH COURSE DESCRIPTION 67
TABLE 5.5 LIST OF POSTGRADUATE COURSES WITH THEIR DESCIPTION 69

ACRONYMS

CERT	Computer Emergency Response Team
FIRST	Forum for Incident Response and Security Team
ITU	International Telecommunication Union
ENISA	European Union Agency for Network and Information Security
OAS	Organization of American State
CCB	Cyber capacity building
ICT	Information And Communication Technologies
NCSS	National Council for the Social Studies
NCSA	National Cyber Security Alliance
NCSAM	National Cyber Security Awareness Month
PAW	Privacy Awareness Week
APPA	Asia Pacific Privacy Authorities
ECSM	European Cyber Security Month
ASD	Australian Signals Directorate
NERC	North American Electric Reliability Corporation
ANSSI	National Agency Of IT Security
MITS	Management of Information Technology Security
NIST	National Institute of Standards and Technology
ETSI	European Telecommunications Standards Institute
FIPS	Federal Information Processing Standards
PCIDSS	Payment Card Industry Data Security Standard
NICERC	National Integrated Cyber Education Research Center
GRENA	Georegian Research and Education Networking Association
ACSRI	Australian Cyber Security Institute
VOIP	Voice over Internet Protocol
PECA	Prevention of Electronic Crime Act
CCB	Cyber Capacity Building
CS	Cyber Security
IS	Information Security
PISA	Pakistan Information Security Association

Chapter 1

INTRODUCTION

1.1 Introduction

Cyberspace is blooming at a rapid speed that is unprecedented by any of the world's other commodity. According to [1] nearly estimated fifty billion digital devices will be connected in cyberspace. The growth in cyberspace is happening in countries considered to be emerging economies. Cyber Security is still an alien concept in some parts of the world in this day and age. It is the new field of study that is attracting a wide range of audience and as internationally it is getting recognition. The cybercrime today is the latest and perhaps the most daunting problem in the cyber world. The world is becoming more dependent on the digital technology day by day and it is arousing new threats and new ventures for the cybercriminals to exploit. In this day and age, it is not just the technical battle to fight as the consequences of these cyber attacks damage the normal human activities. Only taking security measures are not the only solution to this increasing problem, a cyber capacity building is a solution in this case. To combat these cyber threats the developed and some underdeveloped countries have taken initiatives mentioned in their cyber strategies whereby providing pieces of training and by means of a certain voluntary code of practices capacity development can be achieved as these notions are considered as a foundation to augment the cybersecurity capability among the masses.

Countries need to evolve or grow at the same pace as that of the rest of the world and in this century every country is dependent on other countries for resources so one cannot practice obsolete methods and for that matter ignore the security measures because in that case the rest of the world will isolate the nation as the threat posed to their technology will reflect on the country trading or cooperating with the particular country. Cyber defense is not the priority at the moment in Pakistan. Due to the lack of cybersecurity strategy in Pakistan, there is at least an emergent need to devise a national CCB strategy. As in the past year, Prevention of Electronic Crime Act (PECA) [2] was passed but the general population of the country is not even aware of the punishments and consequences of cyber crimes. In this research a national strategy is formulated that includes numerous means and techniques to enhance the awareness level nationwide, build cyber

professional workforce and provide procedures that inculcate cyber consciousness among the masses to combat against cybercrime. Initiatives and campaigns of the international world can be adopted by the government for ensuring the cyber security in the country.

1.2 Problem Statement

As evident from the previously mentioned facts, there is lack of cybersecurity strategy in Pakistan, therefore, there is at least an emergent need to draft a national cybersecurity capacity building strategy

1.3 Research Objective

The aforementioned problems can be addressed by achieving the following listed research objectives. The main objectives of the thesis are to:

a) Assess the maturity level in accordance with cybercrime IT security and security in Pakistan
b) Comparative analysis of capacity building regime of different countries
c) Formulate the national strategy for cybersecurity capacity building

1.4 Scope of Research

Cyber Security is the need for the hour as the national Cyber Space is vulnerable to cyber attacks [3]. One way to ensure cybersecurity is to enhance the workforce by capacity building on a national level. As mentioned above cybersecurity capacity building is a national need in this age so the proposed strategy will serve the purpose in an adequate manner. Military organizations have done little with cybersecurity capacity building so this proposed strategy can be a stepping stone in this regard.

1.5 Areas of Application

a) Utilization for Industry: The proposed strategy can be implemented in the industry to mitigate its security risk. Cybercrime is the most imminent threat to the industry as business suffers mainly due to cyber attacks. In our society, most people working in industry are not even aware that they are cyber victims. This capacity building regime will aid the industry users to operate in a more secure environment.
b) Utilization for Military: Military organizations have done little with cybersecurity capacity building so this proposed strategy can be a stepping stone in this regard.

1.6 Significance of Research

This research will address the issue that is not been discussed openly or any counteractive plan has been devised on a national level. In a country like Pakistan which is under the radar every time it is an essential fact to formulate a cybersecurity strategy to combat cybercrime. Strategy development definitely requires the involvement of different stakeholders that are discussed later in chapter 2 but by developing a cybersecurity building strategy a step is taken towards attaining the unachievable goal in the current scenario.

The main advantages of this research on a national level are:

a) It will facilitate the authorities to develop cybersecurity strategy for Pakistan.
b) It will ensure national defense against crime in cyberspace by developing the cyber army.
c) It will minimize the human threat factor in cyber crimes by raising the awareness level of professionals and regular citizens.
d) It will broaden the horizons for homegrown cybersecurity products and as a result flourishing the industry.
e) By eliminating ignorance to security it can boost the economy of the state as these day millions are lost due to cyber attacks.

1.7 Research Methodology

The research will commence with the brief analysis of capacity building capacity building and factors affecting its success or failure. As the research is concentrating on Pakistan so a brief description of the current cyber threat landscape of Pakistan will be highlighted. The subsections provide the detailed view of the entire research methodology being adopted.

1.7.1 Comparative Analysis

The comparative analysis will unfold with providing the audience the top-ranked countries in ITU standings [4] as to develop a strategy for Pakistan there is a need to critically analyze the procedures and practices of countries that are internationally recognized for their capacity building efforts. ITU has developed some security factors with the help of researchers, scientist and security professionals on basis of which the cybersecurity index is formulated and standings in the tables internationally and

regionally are decided. Ten comparators are decided for the comparison where a few ITU factors are considered and along with them some new factors are being under consideration for the comparison of these countries and as result, recommendations are provided to upgrade the practices.

1.7.2 Survey

Surveys regarding the following will be conducted.

a. Cybersecurity maturity level of the general audience will be assessed by conducting a survey based on some specific security questions in a different environment.
b. The results will have compiled that will further facilitate the research in formulating the cybersecurity capacity building strategy.

1.7.3 Strategy Development

In accordance with the recommendations provided at the end of comparative analysis and the survey conducted the strategy is developed keeping the factors affecting its success and failure in mind.

1.8 Thesis Outline:

The thesis is presented in five chapters and the organization is provided as follows:

Chapter 1 provides the introduction of the research while highlighting the reason for research and mentioning its significance in different spheres.

Chapter 2 discusses the definition of capacity building in the cyber world and list down the factors that contribute to the success of capacity building strategy. The Cyberthreat landscape of Pakistan is also mentioned in this chapter.

Chapter 3 focus on the capacity building activities adopted internationally in cybersecurity. It provides the comparative analysis of the selected countries and lists down a few recommendations for such countries.

Chapter 4 presents the survey conducted to assess the cybersecurity maturity level of the general audience.

Lastly, in Chapter 5 cybersecurity capacity building strategy is formulated and its implementation is provided.

Chapter 2

CAPACITY BUILDING

2.1 Introduction

The chapter defines the concept of capacity building by addressing certain questions that describe the whole phenomenon of capacity building in cyberspace. It also highlights the factors that contribute to success and failure of cybersecurity capacity building. A holistic view of Pakistan cyberspace in recent times is also provided in this chapter as the theme of the research is to formulate a strategy for Pakistan.

2.2 Defining Capacity Building:

Capacity building circle's some key questions that need to be answered where cybersecurity capacity building activities are concerned. These questions are used to clarify the concept comprehensively.

2.2.1 Capacity Building Importance:

According to [5] a critical theme in numerous developed communities in any aspect is capacity development. Governments across the world are making cyber capacity development a prominent pillar while approaching their policy's as to provide a pathway where their nation can reap the benefits of the internet and cyberspace. Pakistan is combating a security crisis at the present time so its nation should also be aware of the cyber warfare tactics and counteractive measures to retain and guard their personal security. As mentioned in the above section Pakistan threat landscape highlights the urgency to implement a cybersecurity capacity building program as it is a necessity in this time and age where every developed nation is equipped with cybersecurity tools. Several potential benefit areas can be deduced from the breadth of capacity building fora of cybersecurity. Formulating policy for cybersecurity capacity building will enhance the overall coordination and implementation of efforts among different internal and external departments. Raising awareness level of society in cybersecurity initiatives will generate debates and discussion among masses that will depict that while developing policies society's values are considered. Formal training and education in cybersecurity will ensure

social growth by developing a more sophisticated and technically sound skilled workforce that can combat cybercrime as a single unit like a cyber army.

2.2.2 Target Audience

The answer is quite uncomplicated as every single person requires security so any particular group of people can not only be the target of capacity building. The thematic focus of capacity building is skill building of the community [6]. Knowledge sharing will increase as heterogeneous stakeholders from various walks of life are involved in capacity building strategy which will result in improved communication and understanding among cybersecurity capacity building is deduced as different angles are involved: law, technology, economy, diplomacy, the private sector and societal perspective. Some individuals are enlisted below who are the primary focus of cybersecurity capacity building.

a. Policy Makers
b. Leaders
c. Scientists and researchers
d. Academia
e. Public and private sector
f. Individual consultants
g. Defense Sector
h. Transportation
i. CERT/teams
j. Health sector

The skill of community leaders or the decision makers needs to be developed as they have to approve any policy, strategy or initiative regarding cybersecurity and can eventually become a hindrance in cyberspace security growth if they are neglected in capacity development. An effective cybersecurity capacity building program should strive for the researchers and scientist attention. Beneficial results for the entire society can be produced if these individuals will put in their efforts and talent to develop security solutions and product. Youth in any nation has significant importance where the development of a nation is considered so educating them about cyber security will play a vital role capacity building. Private companies are the financers or in majority cases the owners of security products so they are one of the most eminent stakeholders in capacity

building as their employers are the victims. Defense sector in every country is the responsible agency for security so the cybersecurity domain lies under its umbrella. Developed nations [7] like America and Israel have their homeland department leading major cybersecurity activities. CERTS are the medium of providing cybersecurity practice guidelines to the audience. In totality, all above discussed individuals can play an effective role in cyber security so their capacity development is included in this research.

2.2.3 Initiator In Capacity Building

As cybersecurity capacity building is a national level concern and as mentioned above it circles different professionals and individuals so the initiator of such activities should be any government ministry in an ideal case. It is mentioned in the answer to question 1 that in majority countries responsibility is given to any government department of government and according to [8] mainly countries like Canada, Germany, and Malaysia have defense ministries leading cybersecurity activities while the USA has its head of state and Australia, Japan and UK have cabinet office in this respect. If any national level activity needs to be planned so government full support and coordination is essential as it is evident from other countries strategies discussed in detail in chapter 3. There are different international organizations that several areas of expertise and work for the enhancement of cyber security capacity building. All resources are invested in the development of CIRT by ITU and FIRST. Capacity development is the prime activity of these CIRTs. ENISA [8] and OAS [9] have dwelled their efforts in crisis management and formulating cybersecurity strategy. Global Cyber Security Capacity Centre has designed a maturity model and an online repository for cybercrime which is accessible to other nations for guidelines. In a country like Pakistan where no strategy is operating the guidelines from the international organization are vital to set up a strong foundation.

2.2.4 Aim Of Cyber Security Capacity Building

a. To spread awareness of cybersecurity threats and trends in an audience.
b. To inculcate the cybersecurity culture by educating individuals about cybersecurity norms.
c. To build a skilled workforce that can combat cybercrime by providing technical ad-hoc training.
d. To change the general attitude and mindset regarding adopting and practicing security guidelines and measures.

e. To encourage scientist, researchers, and students towards cyber security so ultimately security products are developed and homegrown industry is grown.
f. To provide forums and guidelines to users and aware them about their rights provided by the state in cybercrime bill.

2.2.5 Obstacles in Effective Cyber Security Capacity Building Plan

Unfortunately while implementing a successful capacity building program a barrage of obstacles need to be faced in a country like Pakistan. It is an exhausting task to formulate and execute cybersecurity capacity building strategy in a state where cybersecurity strategy is not operating or developed at a national level. Cybersecurity is an afterthought in this country at the moment as it is facing tremendous security crises of its own. As in Pakistan products and services are installed and are not upgraded on a frequent manner so just by guiding individuals to update will not convince them to actually do it as it is said that new tricks are hard to teach to an old dog. It is a general perspective that cybersecurity is the sole duty of the information technology sector. To break through this perception a draining effort is required because individuals are not easily receptive to change of habits or thought process. Another factor is that a single technique may not be appropriate for every audience member because one size cannot fit all so dynamic thinking and approach is required. Lack of resources is the major element in an underdeveloped country [7] as it cannot spend enough on issues that are not treated as urgent so to launch the strategy and implement it in the desired manner will need massive support from the government.

Another challenge is to get the right message across the appropriate audience and in the format that is easily accessible and understandable to them. As in a country like Pakistan where there are no targeted communication processes available to spread the message will be a strenuous effort. Lack of organization can prove to be an obstacle in progress of such plans as no management infrastructure is present to style cybersecurity capacity building plan and deliver to the user by engaging its interest and grabbing the attention for a while. A common pitfall is a failure to follow up in capacity building activities. The success of any project is finally decided on the feedback of its users and then cultivating their response in the gap analysis of the plan.

2.3 Factors affecting CCB

a) CCB is the continuous process of a marathon.

International organizations, governments, and private sectors have acknowledged the significance of cybersecurity capacity building in cyber landscape. The urgency to attain quick gains can be clouded by the short-term goals while ignoring the ultimate goal. A chain process of cyber capacity building small initiatives and efforts is required that lead and assist in larger projects. The objectives of CCB should change with the developing cyber frameworks while the activities involved in the capacity building like training, education, and awareness can all be achieved by gradual progression and growth.

b) Cybersecurity capacity building would not be successful if it uses diversity in language.

Capacity building in cyberspace requires a common language as reliance on ICT has increased in all spheres of life and it can impact the transformation of society and governing system. As it is a generic concern so it should be part of mainstream issues in social debates on the development of agriculture, transportation, energy, and technology. The concept of the cyber capacity building is often confused with cyber defense and cybercrime where individuals are unable to differentiate its actors involved, process and responsibilities with those of other two mentioned. Capacity building is not about just fighting cybercrime but to provide a safe environment to the nation in which they can develop and excel

c) Cybersecurity capacity building impacts the economic and social development of society.

The ultimate goal of the cyber capacity building is to develop a resilient ICT domain where nations can progress both socially and economically. CCB is not only about security as a large number of countries are reliant on ICT and internet for delivery of services online so any efforts to improve security is directly related to services like e-health, online banking, e-government and online education which are responsible for social and economic growth eventually. The link of social growth on ICT is even provided in Millennium Development Goals of UN in 2015[10].

d) The obstacles and demons faced by everyone in cyber capacity building activities are different.

The challenges can be categorized as of donors and beneficiaries in the cyber capacity building. Challenges faced by donors include designing scalable models and developing a strategic framework for cybersecurity capacity building. Engaging the decision makers and ministers at the top level is a significant task along with coordinating local and traditional level partners. Challenges faced by beneficiaries include attaining harmony despite the complexity in any region, highlighting the reality of cybercrime to leaders, to prioritize the CCB activities and in the end moving the plans from development to execution.

e) **The priorities set by individuals with regard to cybersecurity capacity building are not the same.**

The wish list of donors is different from that of beneficiaries where priorities are concerned. The former's priorities include elongated internet access, to improve user's ability of utilizing the web, developing local products and content, to promote the secure and open internet model, creating trusted and reliable infrastructure, compliance to legal framework that safeguards human rights of security and freedom while the latter's priorities include training, skill development, knowledge building, provision of tailored programs and equipment.

f) **International coordination is required for smooth operation of cybersecurity capacity building activities.**

International coordination is required mainly due to the reasons that cyberspace and cyber attacks are not limited or confined within any boundaries or borders. The Investment required for CCB projects on extravagant scale exceeds the capability of a single country. On the international level, both donors and beneficiaries impart all efforts on adopting good practices, developing a communication channel for information sharing and coordination of resources. For an efficient practice, the peer countries should have equivalent security posture. The guiding principles can easily be implemented in the upper scenario. Information sharing between actors within government is essential in identifying needs, gap analysis and a better understanding of failures. Monitoring of resource allocation can be facilitated by establishing a platform where both parties can update about their CCB activities and centrally all activities are monitored and the activities are observed in a controlled environment.

g) **Stakeholders input and validation is essential is developing cybersecurity capacity building activities.**

A clear understanding of objectives is the way to yield desirable results from the multi-stakeholder approach. Unfortunately these days private sector is playing a more crucial role in raising cyber security awareness than the government. The private sector can enlighten the government about cybersecurity issues and influence them in decision making regarding cyber laws and policies. Reporting an incident is another challenge faced in CCB as trust is the main issue so a trusted third party is required for sensible reporting.

h) **The Cyber capacity building is the need of the time so it should be a priority which it is not the case for a majority of countries.**

Every country is facing its own pressing issues like sanitation, food, poverty, illiteracy, infrastructure development and security where cybersecurity might not be a priority in political issues. But as it is mentioned above that social and economic development of any nation depends on CCB so prioritizing it is an intelligent choice. The risks involved in cybersecurity are not that visible but that does not mean they are non-existent. Cybersecurity is significantly valued in societies where applications are installed that are dependent on technology and any disruption can cause major damage and loss. CCB is dropped from the government's agenda where risk assessment of technology is not in practice.

2.4 Pakistan's Cyber Space:

According to [11] Global Security Intelligence Report presented by Microsoft in 2017, one out of four personal computers is infected with malware. After Bangladesh, it has the highest average in this regard and worms like Win32/Nuqel, Win32/Tupym and Ippedo were reported to be the most common. 0.8% to 0.12% computers of Pakistan were infected by ransomware[12]. The report discloses that 84% of computers in the country are not security software enabled which is the main cause of such malicious activity. Security dynamics are evolving constantly regionally and internationally every passing day and so, as a result, the threat spectrum is growing rapidly. The evolution of threat can be categorized from traditional to strategic level advanced persistent threat. In Pakistan [13] traditional security has a precise sphere and it is guarded ardently while non-traditional security is not even defined or for that matter guarded. Cyberspace has become the most recent battlefield as countries these days attack each other in this space like Indian hacker group Bl@Ck Dr@GoN defaced the official website of Pakistan People

Party(PPP) in 2014 [14] after its leader made a comment in Kashmir issue. Many other incidents were reported where Indian hackers have defaced official government websites of Pakistan which include the ministry of water and power, IT, Defense Law and justice and climate change [15]. This indicates that the official websites of Pakistan are not prone to these security attacks so there is a significant lack of security practices in these websites.

2.4.1 Pakistan Initiatives In CCB

PISA was formed in 2001 as it is a non-government organization comprising of cyber professionals for serving the sole purpose of developing a cyber secure Pakistan where the mission include cyber capacity building.

Cyber defense day:

PISA design an open platform to empower IS professionals to connect and share ideas about latest trends in cyber security on Pakistan's National Defense Day. It was inaugurated in 2015 and it is being celebrated for the past two years.

Cyber Secure Pakistan:

Cyber secure Pakistan is a conference that aims to cater the issue of sustainable development in cyber security and it involves speakers from Pakistan and China.

Incident response workshop:

A platform where organization can test their cyber security response procedures and seek advice from security experts on the topics like log analysis, data collection and forensic analysis, and incident response.

Cyber Scout:

It is an initiative by FIA to indulge students and professionals by providing them awareness on cyber security.

It can be concluded from the above mentioned information that all the efforts in CCB is targeted to special audience and there is no running program for the general audience regarding cyber security as other countries have mentioned in chapter 3.

2.5 Conclusion

Capacity building is a continuous process as states invest in cybersecurity practices and adoption of these measures. Capacity building is not only about providing technical capacities but it also inculcates capabilities in accord with cybersecurity defensive and offensive measures. Pakistan as a state is new to the cybersecurity environment as it is lagging behind in security practices and cyber capacity building as evident from its rank in cybersecurity index [4].

Chapter 3

COMPARATIVE ANALYSIS OF DIFFERENT COUNTRIES

3.1 Introduction

The cybercrime today is the latest and perhaps the most daunting problem in the cyber world [14]. To combat threats the developed and some underdeveloped countries have taken initiatives mentioned in their cyber strategies whereby providing training and by means of a certain voluntary code of practices capacity development is achieved as these notions are considered as the foundation to augment the cybersecurity capability among the masses. Different countries have developed heterogeneous approaches in cybersecurity capacity building a comparative analysis is provided in this chapter.

3.2 Literature Review

Cyber Security is still an alien concept in some parts of the world in this day and age. It is the new field of study that is attracting a wide range of audience and as internationally it is getting recognition. Cyberspace is blooming at a rapid speed that is unprecedented by any of the world's other commodity. The growth in cyberspace is happening in countries considered to be emerging economies. Cyber Security is still an alien concept in some parts of the world in this day and age. It is the new field of study that is attracting a wide range of audience and as internationally it is getting recognition.

Countries have cybersecurity strategies [15] in place that deal with cyberspace and its issues but a critical aspect in these strategies is capacity building. Capacity Building is defined as a process aimed at facilitating individuals by providing assistance to optimize their skills. According to the strategies [15] capacity building require time to have its impact and it should be applied on different systematic levels like an individual, organizational and institutional. The research study analysis cybersecurity strategy of seventeen countries based on the capacity building measures as the countries are from different continents and regions including USA, UK, France, Malaysia, Estonia, Georgia, Mauritius, Australia, Netherlands, Canada, Russia, Oman, Norway, Japan, Singapore, South Korea and Egypt.

3.2.1 ITU Framework

Global cybersecurity index project aims to assess the commitment level of ITU member states to cybersecurity by combining multiple indicators into single benchmark measure to compare and monitor the results [4]. The standings in an index are decided on five pillars that are identified by a group of experts. Five pillars are mentioned below:

a) Legal: Measures are analyzed on the basis of existing legal institutions along with regulations and compliance that deals with cybercrime and security.
b) Technical: These are measured on basis of existing technical institutions, response teams, standards and certifications that are created by the nation-state.
c) Organizational: The organizational measures are concluded on the existing policy and strategy designed by any government to cater cybersecurity risk.
d) Capacity building: Measured on the basis of performance indicators like manpower development, professional training, research, and education.
e) Cooperation: Measured on the basis of existing cooperate frameworks, public-private partnerships and information sharing networks.

Capacity building is intrinsic to legal, technical and organizational measures as understanding the risks to technology can lead to the development of efficient and satisfactory legislation and policies regarding cybersecurity.

3.3 Selection Of Countries

The countries selected are from the different continent and part of the world mainly based on the ITU ranking provided publically. All countries selected in this paper belong to leading countries category in cyber wellness profile document [4]. As the capacity building is a factor in deciding these rankings so the ranking does not entirely reflect that if a certain country is high in ranking so it is definitely fulfilling all the cybersecurity capacity building metrics designed in this research or provided internationally.

Table 3.1 Leading Countries with High ITU Ranking

Capacity building Ranking	Countries	Cyber Security Ranking
1	France	8
	America	2
	Malaysia	3
0.97	Singapore	1

0.95	Oman	4
0.94	Estonia	5
0.94	Australia	7
0.91	Mauritius	6
0.91	Russia	10
0.90	Georgia	8
0.82	Canada	9
0.80	Norway	11

Table 3.1 shows the countries with their capacity building ranking and cybersecurity index provided in ITU document [4]. The ranked were updated in 207 document but ranked of countries listed in Table 3.2 were not provided.

Table 3.2 Leading Countries without Revived Capacity Building Ranking

Japan	11
UK	12
Republic of Korea	13
Egypt	14
Netherlands	15

3.3.1 Developed Countries

This comprises of countries that are enlisted as developed according to [11] and are high in ITU ranking [4]. The reason for considering and analyzing such countries is to facilitate the strategy makers to design a cybersecurity capacity building strategy with the similar proof of concept in mind. As these countries are currently operating with these strategies and they are generating optimizing results. Countries that have yet to formulate their strategy can be benefited by the advanced cybersecurity practices.

USA and France are the countries whose efforts in cybersecurity capacity building are recognized by the entire world as it is evident from their ITU ranking in capacity building [4] and they all have standards and policies intact in this regard. Estonia, Norway, and the Netherlands are members of ENISA a CS expertise center which facilitates its member by providing guidelines for cybersecurity strategy development and capacity building.

These countries focus on safe and sound ICT and focus on preventing a cyber attack. UK is a member of ENISA and it has the largest online repository of cybersecurity in its cyber capacity building center. Japan has established active information security measures rather than passive.

3.3.2 Developing Countries

This category consists of developing countries that comprise of high ITU ranking [11]. The fastest growing cyberspace is of developing countries where the majority of the developing countries lack cyber capacity development but these selected countries have capacity building regimes equivalent to developed countries. Singapore is ranked first in cybersecurity as it is currently working on cybersecurity master plan. Malaysia is selected because it is an Asian country that has high ITU ranking even higher than most of the developed countries.

Developing countries are usually lacking in the Information Security development sector but Egypt, Mauritius, and Oman are three countries that have high ITU ranking in capacity building. Apart from Asian developing countries, the former two are included to analyze the security measures adopted by these developing countries being from the different continent. Russia and Georgia are two states selected because as their capacity building has increased from 0.37 and 0.25 to 0.91 and 0.90 respectively so they are definitely executing efficient plans for achieving such goals which should be analyzed. For a comparison based on capacity building, these countries are selected to analyze their excellence in cyberspace as these are not considered to be developed countries.

Pakistan is a developing country with cyber security global ranking as 67 and capacity building ranking as 0.3750.

3.4 Comparison Metrics

Cyber Security Strategy of every country is developed to attain similar goals as to reduce the threat in the cyber landscape can be one of them. However, every country considers different factors in designing their security strategy because of varying social, economic and political conditions. These comparison metrics are decided by analyzing the capacity building measures mentioned in the cybersecurity strategies of selected countries [15]. The metrics are mentioned below:

a. Definition of capacity building and in what context is it used or specified by each country

b. Manpower development: Raising Cyber awareness of societal actors and building a cybersecurity culture in the society
c. Participation in International Organizations Activities
d. Standards that are developed by any country in cybersecurity or to promote it.
e. To build cyber security workforce by providing cyber security education and developing skills.
f. Cybersecurity training and competitions
g. Research and development being carried out in cybersecurity
h. Cyber Security Spending: The dedicated budget that is allocated and spent on cybersecurity annually.
i. National cyber security awareness training program for the internet users
j. Cyber Security Capacities: Centers for cyber capacity building and short training courses on information security

3.5 Highlighted Metrics Comparison

The Cyber capacity building is considered as a dynamic process in this fast technological era as the demands of stakeholders involved are in the constant evolutionary process mentioned in a majority of the NCSS. Every country represents its disparate school of thought to address cybersecurity capacity building. The comparison is concluded on basis of the publically available strategy documents and information center online provided in this regard. English is the universal language used to write these strategies but European countries like Russia and France [15] have written in their native language but for the world to better understand their strategy all these countries have issued a daft in English. Successive subsection will provide the details of the comparison based on the metrics mentioned in section 3.4.

3.5.1 Definition of Capacity Building

Capacity building is a term introduced by United Nations Development Program in 1991 which was previously known as organizational development or institutional building in 1970 [16]. Countries have used this term as a more sophisticated option for development and awareness in Cyberspace security. Education, training, awareness raising, skill development, individual and organizational development all lie under the umbrella of the cyber capacity building. Capacity building term is used by the UK [4], Netherlands and

USA as it mentions continuously building national expert capacities to ensure cybersecurity. France, Estonia, Norway, Georgia, and Russia have mentioned awareness, training, and education in their NCSS.

3.5.2 Manpower Development

As mentioned in ITU cyber wellness profile ranking any effort by a state to promote cybersecurity by publicity campaigns, or making use of intuitions is included in manpower development.

3.5.2.1 Raising Cyber Awareness:

Cyber smart [17] a portal by Australia for raising awareness among children and parents. Stop.Think.Connect [18] is a national campaign to empower Americans to stay safe online. The UK has a program aimed to elevate masses awareness about cybersecurity. With you on the web is an initiative for the public to aware them for protecting their personal information. Get Cyber Safe [19] program educates Canadians about cybersecurity risks, deals with cyberbullying and provides latest related news. Amanak is a public awareness initiative for the youth, educators and the families.

Table 3.3 Different Awareness Campaigns

Awareness Campaigns/portal	Country
Cyber smart	Australia
Stop.Think.Connect	USA
Get safe online	UK
Get Cyber Safe	Canada
Amanak	Egypt
Raising public awareness about information society	Estonia
Information Security Outreach and Awareness Program	Japan
Expertise & Advice and Sharing knowledge	Netherlands
National Cyber Security Masterplan	Singapore
Waay	Oman

Estonia runs the program to educate and the aware public of its instrumental role in the development of information society. Mauritius created a portal with its Cert [20], to educate users about security issues of cyberspace. Georgia awareness campaign is under the supervision of the ministry of education and science which strives to familiarize the Georgian public with cyber crimes, online protection, and reporting mechanisms. Russia provides more technical awareness to users regarding cyber security features like phishing, social engineering, and spoofing etc. Center for cyber and information security Norway has the plan aimed to elevate awareness level to cyber threats and crimes. Japan Cert [21] has a program for education and training of cybersecurity incidents, trends, and vulnerabilities. Malaysian Communications and Multimedia Commission [22] provide a platform to the public for reporting cybersecurity incidents and deals with online content problems. Oman has Waay a campaign for government authorities to mitigate security risk. The Netherlands have knowledge sharing publications for the organizations to improve their digital security. Singapore Masterplan [23] aims to raise private and public sector awareness to adopt best security practices.

Awareness campaigns have common goals and practices adopted in achieving those goals are respective to the security stature of the particular country. The supervising authority of these campaigns differs as states like Mauritius, Oman, and Japan have their CERT while countries like America, Malaysia, Georgia, Singapore, Australia, Canada, and the UK has government ministries and department. Capacity centers are the responsible authority in states like Norway and Russia.

3.5.2.2 Building Cyber Security Culture

Raising awareness of Cybersecurity is a building step in creating and promoting cyber security culture. A cyber secure culture is developed when users left to right, top to bottom ruminate cybersecurity while carrying out any function in IT world. Every country that was selected for the comparison has accomplished successful awareness-raising campaigns but countries like Georgia, Mauritius, Japan, Singapore, UK, and the USA have gone an extra mile to build a culture of cybersecurity. Georgia has put in extra effort after the cyber attacks in Georgia-Russia war [24] when its websites were swamped with zombie computers as it is running Cisco regional networking academy for different security certifications. Mauritius CERT maintains a knowledge bank that has online safety videos, guidelines, e-newsletter, security tools, and antivirus resources.

Singapore has cybersecurity awareness and outreach program that explores new avenues in building cyberculture with help of broadcast media as popular videos of security competitions are posted on popular websites and cyber crimes are re-enacted on television shows for public education. The UK conducts cybersecurity contest to engage students in cybersecurity activity to test their skills, as a result, it plays a huge part in the development of young generation cyber defenders and the UK is operating a center for cultural development that is discussed later. Japan is operating an Information Security Human Resource Development Program [25] as it considers improving measures in information security as an urgent matter so the tasks are intensely examined before execution. The objective of the program is to improve capacity and awareness nationwide in several socioeconomic activities to publicize cybersecurity measures. National Cyber Security Alliance (NCSA) America [26] believes that cyber secure culture is developed by the fine-tuning of layer 8(the human factor) by promoting shared responsibility, embed security in every business process and employees are encouraged for learning.

A poor cybersecurity culture can open various floodgates to security attacks and vulnerabilities so these countries are trying their best to equip their nation with best security guidelines and cultivating the use of secure practices while dealing with ICT. It is analyzed that cybersecurity behavior, beliefs, and values regarding cybersecurity.

3.5.3 Participation in International Organizations Activities

The prioritization level of the capacity building in a country can be depicted by its participation in International activities. Three different international activities are discussed below:

3.5.3.1 National Cyber Security Awareness Month (NCSAM)

An initiative started in 2004 by the USA basically an annual campaign to educate its citizens about cybersecurity. Cyberspace has grown and so are the risks so the normal use of the internet has to know about the cyber threats and risks. October is the month every year this campaign is carried out with the intention to engage public and private sectors through events promoting the importance of cybersecurity, aid them with necessary tools to stay secure online and provide the user with cybersecurity guidelines and practices. The ultimate motive of the campaign is to increase the resiliency of citizens against cyber incidents. Canada is the other country observing this campaign as it focuses on the

computer users to be more vigilant and protective against cyber incidents. Different themes are provided to users relating cybersecurity during the whole month. USA and Canada also started a non-profit based public-private partnership in Jan 2008 known as Data Privacy Day for the promotion of trusted internet.

3.5.3.2 Privacy Awareness Week (PAW)

Asia Pacific Privacy Authorities (APPA) started an initiative in 2006 named as Privacy Awareness Week. It is held every year to address different privacy issues like protection and sharing of personal information on public platforms. The target audience of these organized events differs from individuals to various government and business organizations. Various member countries nominate a week in a certain month decided by APPA to carry out the events and activities according to their requirements. USA, Australia, Canada, Singapore, and Korea are the selected countries that celebrate PAW.

3.5.3.3 European Cyber Security Month (ECSM)

European Union launched ECSM campaign to promote cybersecurity among computer users of its member states in 2012. Cyber threats perception is changed through encouraging information security, educating the use of security practices and conducting competitions of cybersecurity. UK and Czech Republic were the pilot countries to participate in ECSM activities and conducted its events in their states. Generating awareness in the network and information security and to promote safe internet use among its user are the primitive objectives of this campaign. Netherlands have organized ECSM activities in 2016. All other European states selected in this research observe this month by the resources and materials provided by ENISA.

These international events bring together young scientist, students, researchers, university professionals and leading IT experts from all around the world to discuss the recent cybersecurity issues in a collaborative environment. The opportunity is provided to next generation for sharing their knowledge and discussing new ideas for improving cybersecurity. Participating in such events contribute to the cyber capacity building in a huge way as the young students and professionals are exposed to new cybersecurity concepts while IT experts gather new ideas and polish their skills in security services and product development.

3.5.4 Standardization Development

The comparator highlights the security standardization body of selected countries where standardization is considered an indicator to evaluate the maturity level of security. In this regard frameworks are developed to international standards by some countries others are striving to develop their own standards feasible to their cyber landscape. All seventeen countries are enlisted in table 3.4 with their standardization body.

Table 3.4 Summary of Standardization Body of Countries

Country	**Standardization body**
Singapore	Ministry of defense
America	North American Electric Reliability Corporation (NERC)
Malaysia	Standards Malaysia
Oman	Information technology authority
Estonia	Information system authority
Mauritius	Ministry of Information and Communication Technology
Australia	Australian Signals Directorate (ASD) by department of defense
Georgia	Data exchange agency that implements a framework to implement international standard according to law on information security document guideline
France	Anssi (National Agency Of It Security)
Canada	Management of Information Technology Security (MITS)
Russia	No standardization body but they are researching in developing standards
Norway	European Telecommunications Standards Institute
Japan	Information Security Measures Promotion Council
UK	Common criteria standardization group
Republic of Korea	Information Security Management system (ISMS)
Egypt	No recognized standardization body but central bank of Egypt responsible for cyber security regulation in banking
Netherlands	No standard present but guidelines are deduced from cyber security strategy

Every country develops its own framework but common approaches provided by international standards bodies like NIST, ETSI, ITU, FIPS, and PCI-DSS are used while developing regulations and standards.

.

3.5.5 Building Cyber Workforce

A Cyber workforce is built by standardizing roles and ensuring well-trained cybersecurity professionals. The Cyber workforce that is competitive globally and unrivaled is attained by the collaboration of academia private and government sector. A cyber workforce framework [27] is operating currently only in the USA that categorizes and describes abilities, task, skills, and specialty areas of cybersecurity. The comparative analysis shows that selected countries have majorly three mechanisms to build a cyber workforce. 1) By carrying out cybersecurity competitions 2) Cybersecurity education 3) Cybersecurity training. Enlisted below are the programs of different countries to create a cyber-secure workforce.

3.5.5.1 Cyber Ex:

It is a cyber exercise run by the states members of OAS (Organization of American States) Argentina, Brazil and Canada that strengthen the capacities against cyber incidents. A scenario based and interactive competition where the focus of the exercise is towards technical security and experts in ICT can shine in this exercise. A successful method to build cyber workforce as the experts will be disclosed, it will increase interest level of participant in pursuing cybersecurity career and capabilities of the cyber capacities will be exposed.

3.5.5.2 C-Save:

C-Save [28] is a volunteer program of USA to educate young individuals about cyber ethics and security. IT professionals take part to teach and in return, their own knowledge pool is enhanced.

3.5.5.3 Capture the Flag (CTF):

A CTF is a cybersecurity competition among security professionals or students of information security designed to serve as an educational exercise that challenges the

participants to decode cybersecurity problems and defend their systems. CTF competitions are treated as learning tools for everyone interested in cybersecurity as the event sharpens their tools skills in the process. These competitions were inaugurated by DEFCON in Las Vegas in 1996. With the passing time, these competitions became global and teams across the world started participating as the event was hosted on the internet. UK, Egypt, France, and Japan are conducting their internal CTF competitions and the winners of the contest are awarded and they qualify for the international CTF.

3.5.6 Cyber Security Training

Cybersecurity training is an essential component in achieving the strenuous task of building a cyber workforce. As pervasive risks are associated with cyber attacks so the demand of the hour is the proficient cyber skilled professionals. Every country strives to achieve the goal and in the table training of seventeen selected countries is discussed:

Table 3.5 Trainings Of Selected Countries

Country	Department/ center	Target Audience	Content	Outcome
Singapore	DigiSAFE cyber security center	Fresh professionals	Software security administration	Operation – centric training that prepares professionals in detecting and catering cyber attacks
America	Homeland security	Veterans and government personnel	malware analysis, surveillance, ethical hacking and risk management,	Online free security training develops technology skilled personnel
Malaysia	cyber security professional development	Information security practitioners	penetration testing and security posture	Cyber security competency is

	department		compliance	increased
Oman	CERT	Security officers, auditors	Ethical hacking mechanisms	A progressive training that provide its audience with different ethical hacking methodologies
Estonia	NATO CCD COE facilities	Cyber defenders	Malware and Exploit Essentials	Cyber defenders will get deep insight technical training and be familiar with vulnerability detection like fuzzing
Mauritius	CERT-MU	Local ICT professionals	Information security practices	ICT professionals adopt cyber security practices and inculcate them in normal software operations
Australia	IT Security Training(private company)	Employees of cyber security	Cyber threat analysis	Provides in house training according to company's need in developing cyber security skills
Georgia	State security agencies	Government employees/ cybercrime	Computer hygiene course/cyber	State agencies run programs to clean government

		professionals	crime and digital forensics	software and hardware
Canada	Ctc traincanada (security training center)	Government and IT sector	computer forensics, disaster recovery	security consultants with Real-world scenario training
Russia	knowBe4	Students, IT and infosec professionals	Social engineering, spear phishing, defense against ransomware attacks	A platform provided to audience for developing cyber defense skills
UK	GHCQ	Individuals and organizations	Cyber security and privacy essentials	A state security agency that trains and provide certified cyber security individuals
Republic of Korea	Net com learning	Cyber security companies	advanced persistent threats (APTs),	This private company structures smarter workforce in cyber security
Egypt	EC Council	Security experts, information security professionals and students	Certified ethical hacking	Trains its learners to be CEH certified

3.5.7 Cyber Security Education:

The prime focus of the analysis here is on the cybersecurity education practices that are present in selected seventeen countries. The most sophisticated and organized programs are running in USA and UK where various degrees offered are specially drafted in security areas. The main domains of cybersecurity are listed in a general list [29] developed by Nist in an initiative program of cybersecurity. Some countries still don't have formal education in cybersecurity even realizing its importance.

Academic institutions around the world are adopting various approaches regarding cybersecurity education. Formal education in cybersecurity starts from elementary school then high school and in the end university education.

In high school level USA has NICERC [30] a center that provides cybersecurity curriculum for teachers and their professional development.

3.5.7.1 Cyber Security Formal Education

Cybersecurity formal university education is on three levels:

a. **Undergraduate:** Information security courses are offered in mainstream computer science undergraduate programs or some universities offer full four year Bachelor program in cybersecurity mainly having courses in Basic Data Analysis, Cyber Defense and Threats, Introduction to Cryptography, Fundamentals of IT Systems, Networking Concepts, and Information Assurance
b. **Masters:** The degree programs usually offerd consist of defense in depth mechanisms and include legal, Policy, Ethics, and Compliance System Administration aspects of cybersecurity.
c. **Post Graduate:** The degree programs are specific in nature as they are research oriented and their domains are mainly network and computer security, digital forensic, Cyber Investigations Secure Embedded System, Systems Security Administration Security Incident Analysis and Response, Secure Cloud Computing and information security management and law.

3.5.7.2 Online Cyber Security Degree Programs

EC council provides world-class education in cybersecurity. Its online degree program helps the students from different backgrounds that range from new graduates to security managers and prepare them for a successful career in cybersecurity as their caliber is optimized by this formal qualification.

All the countries have cybersecurity institutions but top-ranked in the world are from the USA. Listed below are the top ten ranked universities

a. Carnegie Mellon University[31]
b. The University of Texas at San Antonio[32]
c. Norwich University[33]
d. Syracuse University[34]
e. Mississippi State University[35]
f. George Mason University[36]
g. Drexel University[37]
h. Rochester Institute of Technology[38]
i. Stanford University[39]
j. University of South Florida[40]

3.5.8 Research and Development

In developing reactive measures to cyber attacks every nation should devise a comprehensive approach where the paramount objective is to promote research and strengthen analysis capabilities as it will facilitate innovation to a further growing extent. The private sector in the Netherlands is a larger contributor to cybersecurity research. Georgian Research and Education Networking Association (GRENA) is a center operating in coordination with other state universities as it has expertise in mitigating cyber attacks. Oman Cert has national cyber clean projects which are funded by the states. Mauritius Cert conducts officially recognized research project and design preventive actions in order to reduce the impact of cyber incidents.

Australian Cyber Security Institute (ACSRI) has three themes as 1) to research about next-generation technologies 2) research projects on identification and authorization in cyber world 3) to develop an evidence base for policymakers. Defense Research and Development Canada (DRDC) have safety and security program that prioritize developing capabilities that contribute to cyber resiliency. Egypt has projects that are carried out by ICT sector and academic sector working in collaboration.

Estonia has security framework [41] as a national research program. Biometric and VOIP security are the research interest in Korea. Netherland has center researching in governance and policy. Homeland Security of the USA [42] has the cyber division for

cybersecurity research projects that include cyber economics, cyber analytics and resilience, cyber forensics and many more.

3.5.8.1 Homegrown Indigenous Industry:

Homegrown products are getting importance and countries all around the world are striving for their own industry of cyber security products as the light was brought on this issue when Edward Snowden released its report [43]. It claimed that NSA and GHCQ [44] were spying on other countries so the rest of the world felt a need for developing their own products that are secure and free of backdoors. In Table 3.6 the features are considered for comparative analysis as these factors can be the main target in cybersecurity attacks.

Table 3.6 Home Grown Indigenous Products

Country	Social networking site	Search engine	Chat service	Email service	Anti-virus
Singapore	Migme	Rednano	*	*	*
America	Facebook, Twitter, myspace	Google	Tango	Outlook, Gmail, Yahoo	Norton, McAfee
Estonia	*	Log.ee	Talkmaza	Hot.ee	*
Mauritius	*	Unabot	Wireclub	*	*
Australia	*	AusFind	*	Atmail	Clamwin, ikarus
France	Skyrock	*	*	Vmail , gandi	*
Canada	*	*	Kik , BBM	Hushmail, crypto heaven	*
Russia	Vkontakte	Yandex	*	*	Outpost antivirus, Dr web

Japan	Mixi, gree	Biglobe	Line	*	Titanium
UK	*	Google UK	*	*	Bull Guard, CYSEC, Sophos
Republic of Korea	Cyworld	Naver	Lakao talk	*	Ahnlab V3 internet security
Netherlands	Hyves	Vinden, llse	*	*	*

* = information not found

The USA is the leading country as it is developing every single aspect considered in this analysis. Facebook, Twitter, and Myspace are the top-ranked social networking sites in USA Australia, Canada, Mauritius, Norway, and Estonia while Malaysia has Friendster where the other countries have their own networking sites. Estonia, Mauritius, Japan, Republic of Korea, Russia and Netherlands have their own search engine alternative to Google.

Neither chat nor email services are being developed by Singapore, Malaysia, Russia, Netherlands, and the UK. Norway has only developed email service Runbox. Antivirus is the first line of defense as only America, UK, Korea, Russia and Australia have developed them. Georgia, Oman, and Egypt are three countries on the list that does not develop any cybersecurity products or features mentioned in the table. They acquire these services from prominent service providers and companies.

3.5.9 Cyber Security Capacities:

United Kingdom is running a Global Cyber Security Capacity Center (GCSCC) [44] whose objective is to provide cybersecurity practices not only in the UK but internationally. This center is the only capacity-building portal in the world while other countries like US and Netherlands have alliances and council but no such capacity center is present. As an international research center leading to the cyber capacity building provides quality initiatives across the world. It provides information to nations to plan better for their cybersecurity investment. Its partners are OAS, World Bank, and Commonwealth Communication organization. A cybersecurity capacity portal is

developed that is a resource globally available for capacity building. It is an online space to share experiences, new developments in the field and good practices of cybersecurity. GCSCC is designing a robust and holistic model to understand the damage experienced by states as they lack capacity and in result develop solutions for reducing the harmful effects. Many initiatives and conferences like Cycon are held to discuss cybersecurity among nations. A program is discussed below as its members are UK government, Switzerland, Netherlands, Singapore, US, Australia, Canada, Germany many of the selected countries in the research study:

3.5.9. 1 Capacity Building Program for International Cyber Security Negotiations:

The focus of the program is on cybersecurity diplomacy and the target audience is academia, government officials, and Diplomats. The objectives of the program are listed below:

a. A comprehensive understanding by diplomats, civil society representatives and public officials belonging from every region of the world of Confidence-building measures and collaboration in cyberspace.
b. Developing a sophisticated understanding of cybersecurity practices and policies at regional level.
c. A culture of alumni is built with lecturers and experts to provide the latest information on cybersecurity research, negotiation and debate.

The program conducts several workshops and conferences to attain these goals

3.5.10 Cyber Security Spending

The size of cybersecurity spending is directly proportional to the growth of cybersecurity workforce that concludes the priority level given to cybersecurity by a country or specific organization. The USA is considered to be the pioneer of development and recruitment as it is a huge cyber security spender. Israel and USA [45] are the largest exporters of cybersecurity tools and products as they have developed expertise and therefore are ahead of everyone in growing their cyber workforce.

South Korea allocates 10% of its every ministry budget to cyber security but does not disclose exact details. Technology and innovation ministry of Malaysia provides no exact figures for cybersecurity. Singapore [46], UK and Australia in 2016 released its cybersecurity strategy stating budget to be spent on cybersecurity. Countries don't usually

disclose their spending statistics publically so full analyses cannot be provided but it is evident that the countries high in ITU ranking are spending more on its cybersecurity infrastructure or in some cases to develop and nurture it.

3.5.11 National Cyber Security Awareness Training Program For The Internet Users

Awareness is the key component in capacity building as it is evident from the comparative study that countries have various programs in this regard. Internet users' awareness programs differ as they are specifically targeting the online users by providing them skills and resources to use the internet safely. Cyber-safe is Malaysia [28] outreach development and educating program to impart practical knowledge to users so they can have a positive experience while using the internet. Kids' online security is a program of Oman to promote healthy internet usage by adults and children as their website also informs about minor's sexual exploitation. Mauritius [47] has a website Safer Surfing for cybercrime prevention and internet safety. GoSafeOnline [48] is an online portal of Singapore that provides online security tips on how to secure your online device and the latter also provide reporting mechanism in case of any cyber threat or incident.

3.5.12 CCB in Pakistan

This section provides information about Pakistan on the comparison metrics mentioned in section 3.4. The Table 3.7 shows which of the metrices are present in Pakistan and which are not present.

Table 3.7 CCB activities in Pakistan

Comparison metric	**CCB in Pakistan**
Cyber security culture	A cyber secure culture lacks in the state as security is not given importance.
Manpower development	Cyber scout a small initiative by FIA
Standardization development	No standards are developed in cyber security where debates are going on about this issue
Cyber security training	ISAD is a project of PISA that used to provide training to cyber professionals.

Home grown industry	Cyber security products are usually imported or purchased from other countries
National awareness program	Cyber Defense Day is celebrated but no general awareness campaigns like other countries mentioned in above section is present in the state.
Cyber security capacity	Capacity center lacks in the state
Cyber security education	Universities offer Masters two year programs in Information security and some of the renowned universities are listed below a) Air University b) Bahria University,Islamabad c) Comsats Institute Of Information Technology [Isb] d) National University Of Science & Technology e) Riphah International University f) Military College Of Signals NUST and Riphah university offer Phd programs
Research and Development	As research is going on these universities related to cyber security but research programs on national levels are not being launched yet

3.5.13 Recommendation

Cyber threats are becoming more eminent and dangerous as the time is progressing and cybercriminals are launching more sophisticated cyber attacks. To cater this issue countries have devised cybersecurity strategy but as studies show that human factor is the biggest loophole in security so countries should devise efficient and effective capacity building plans. The recommendations provided here can guide a country that is strategizing new plans and it can also give optimizing results for a country that have existing plans in action.

These recommendations can be applied on yearly basis as after every three or five years. Different countries can adapt and apply this recommendation to upgrade its cybersecurity capacity building level or status. Recommendations in this research paper are arranged in the same manner as countries are categorized in ITU cyber wellness profile [6] 1) Initiating 2) Maturing 3) Leading.

3.5.12.1 Recommendations for Initiating Countries:

a. Initiating steps are to introduce the cybersecurity concepts to masses and running awareness campaigns on a lower level.
b. Internet users are the target of cyber attacks so they should be the target audience to educate about cybersecurity and how to safely conduct online activities. The goal can be achieved by online portals.
c. A communication platform should be present that can coordinate globally with other countries in order to increase the efficiency of the projects. Assistance can be required from the countries that will be operating the same CCB activities.
d. Developed countries should collaborate with the developing countries that lack CCB activities as the former would be a donor while the latter would be the recipient. ICT and internet have no geographical boundaries so a developed country will be reducing risk to its cyberspace by this collaboration.
e. All CCB activities should have institutional backing where the political support is also evident for the effectiveness of the project. Policymakers of high level should have the faith and trust in CCB activities for their smooth beginning and execution.
f. National agency of ICT should work in collaboration with education ministry to design a course of cybersecurity to increase the cyber literacy.
g. A country that is starting its cyber capacity building should be using established capacity building maturity models, cybersecurity indices, and methods that have given fruitful results to other countries but the conditions of economy and other geographical and infrastructural differences should be kept in mind.

3.5.12.2 Recommendations for Maturing Countries:

a. Develop a national approach to cyber capacity building and prioritizing it. The actors involved in this approach should be from the government for better understanding the urgency and importance of cybersecurity.
b. As evident from the comparison like England and Germany, every country should build their capacity pool in CCB. Experts and professionals in possession of appropriate skills should be engaged in CCB activities by the government.
c. The budget should be assigned to cyber capacity building with reference to the amount assigned to developments projects.

d. Internet steering committee should be established that recommends technical standards and good practices related to internet and its best security practices.
e. Already existing structures and capacities should be utilized for CCB activities to achieve efficient results rather than creating the capacities and structure from the scratch.

3.5.12.3 Recommendations for Leading Countries:

a. An office from the government should be designated for CCB activities and projects. All the roles and responsibilities should be clearly defined with no ambiguity in the strategy mandate.
b. The private sector should be involved in CCB activities by the government for the technical guidance and IT industry should work in collaboration with the government as to fulfill they cooperate social responsibility towards the society.
c. Cybersecurity education of leading countries should have a collaborative approach to initiating and maturing countries cannot address the entire range of issues, challenges, trends and different perspectives of cybersecurity on its own.
d. Any policy of the state regarding ICT infrastructure should be in line with cybersecurity practices as cyber attacks are an imminent threat.
e. Any country starting its CCB projects should have its capacity assessment prior to the beginning of the project to analyze the resources required for the project. Oxford Cyber Maturity Model can be helpful for this assessment but requirements can be adjusted according to the needs of the respective country.
f. As the result of the capacity assessment, the actors analyzing should draw a roadmap mentioning vision, strategy, concept, and target.
g. A country that is starting its cyber capacity building should be using an established method that has given fruitful results to other countries but the conditions of economy and other geographical and infrastructural differences should be kept in mind.
h. The evaluation process should be monitored and lesson learned should be documented to avoid the same mistakes in future.
i. An annual report on CCB projects should be disseminated highlighting all the projects, lesson learned, gap analysis and special mention to the emerging trends.

3.6 Conclusion

The objective of this research is to compare and analyze the initiatives and programs of cyber capacity building operating in these aforementioned countries and as mentioned in their cybersecurity document that is available publically. Residing on the comparison the research paper later provides recommendations that will facilitate the country that is designing its cyber capacity building strategy or other countries can include these points in their existing cybersecurity strategy.

Chapter 4

DATA ANALYSIS AND FINDINGS

4.1 Introduction

In this chapter, the results of the survey are analyzed and presented. The collection of data was droved by one basic goal to analyze security awareness level in masses regarding cybersecurity. In this regard, the fundamental security questions were asked from respondents to assess their cyber security knowledge base. Cybersecurity is still an alien term to individuals in our country that was evident from the response. The objective of the survey was accomplished by finalizing the results and however, the finding depicted the true essence of the cybersecurity culture in respondents and how they perceive security in general.

4.2 Response rate:

Due to the nature of survey four hundred surveys were initially sent to locals via email who are unfamiliar with or are does not directly linked to cybersecurity. Half of the above were sent to information technology and other engineering students and the remaining half were sent to the general public like high school students, housewives, office workers to assess the maturity level of cybersecurity. Four hundred survey forms were sent to cyber security students and professionals. Ten survey forms were unable to use because either there were blank spaces or in some cases, respondents filled survey with misleading information that was unsuited for this research.

The response rate of the survey was quite satisfactory as nearly all the surveys were filled with relevant information. The rate of male respondent was more than the female although an equal number of surveys was sent to male and female population evident from figure 4.1. The surveys were sent to audience from different age group to get the diverse view while the results in figure 4.2 show that majority of the surveys were filled by people ranging from 21-30 age group. The second age group that responded was of 31-40 and the rest of the age groups also responded but the ratio was quite low. The results drawn were according to the expectations as the majority of the population are not aware of basic cybersecurity terms and measures.

- **178 male**
- **222 female**

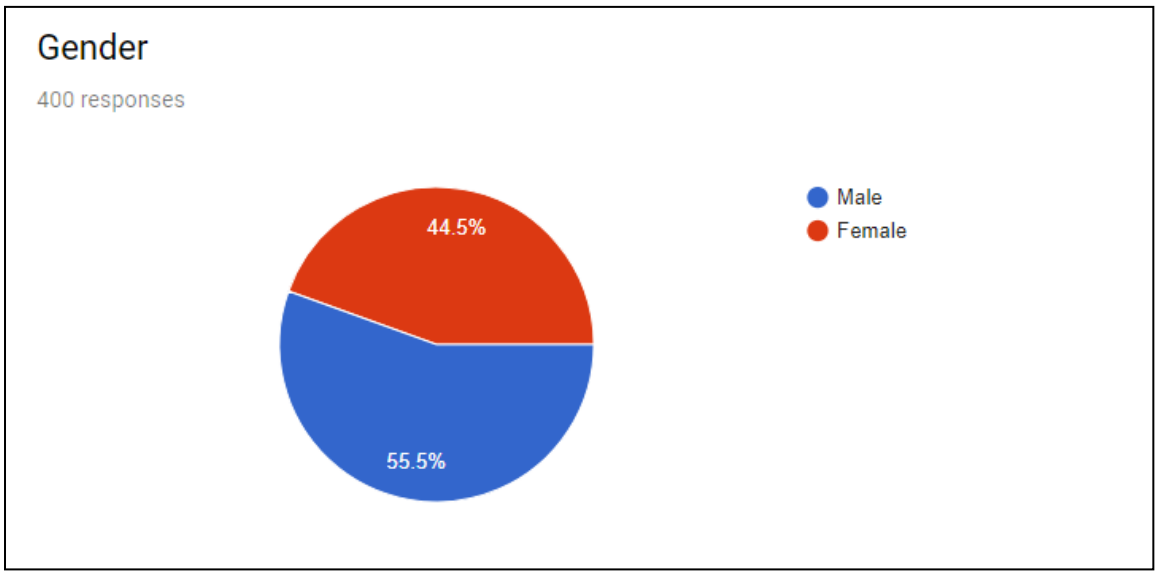

Figure 4.1: Gender Distribution

4.3 Survey Results:

In this section, survey questions are mentioned with their respective options provided to the audience. Every option that was included in the survey was serving a purpose so those reasons are also discussed. Observation and discussion are done on the basis of the results gained through the survey.

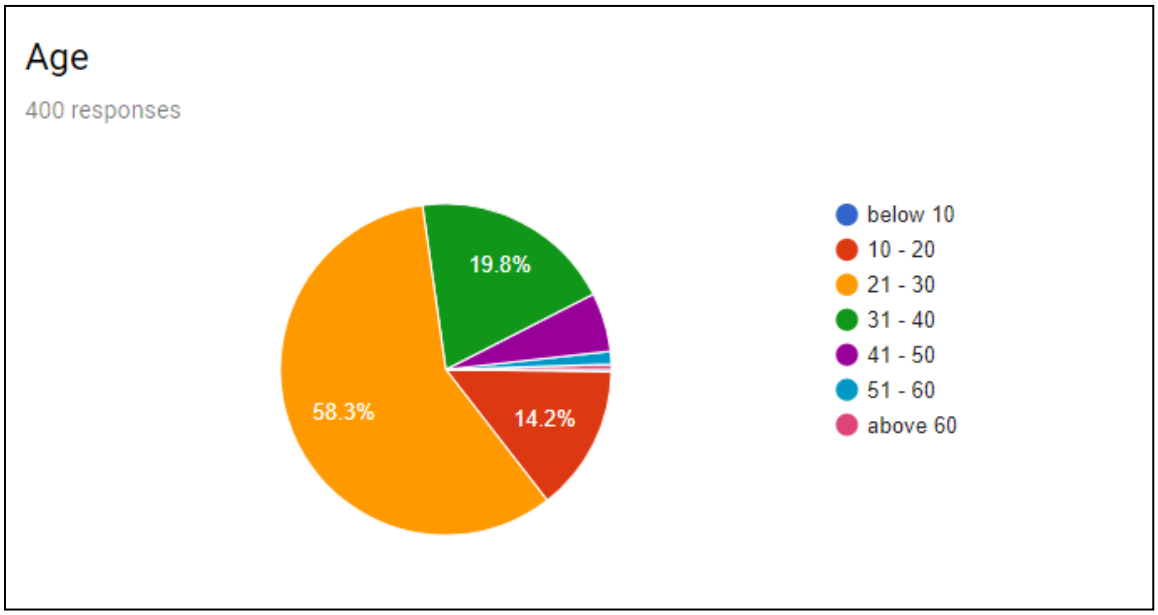

Figure 4.2: Age Distribution

4.3.1 Question 1

What is your understanding of the term CYBER in "cyber security"?

a) **First option: (Umm, No idea)**

It is evident that people who have opted out this option are not aware of the term cyber and never probably heard of this term which is surprising in this day and age. A vast majority has chosen this option as shown in figure 3 and the result can be drawn that these people do not even know what threats they are exposed to as they are not familiar with the fundamental term like cyber.

b) **Second option: (Not sure, but i guess it has something to do with information security)**

Respondents who have to opt out this option are confused as they are not sure of the correct answer. A thin line is present between CS and IS so respondents have heard this term but they are not certain. Generally, the context is same so confusion is justified for individuals, not related cybersecurity as its clear and accurate answer can be provided by security professionals.

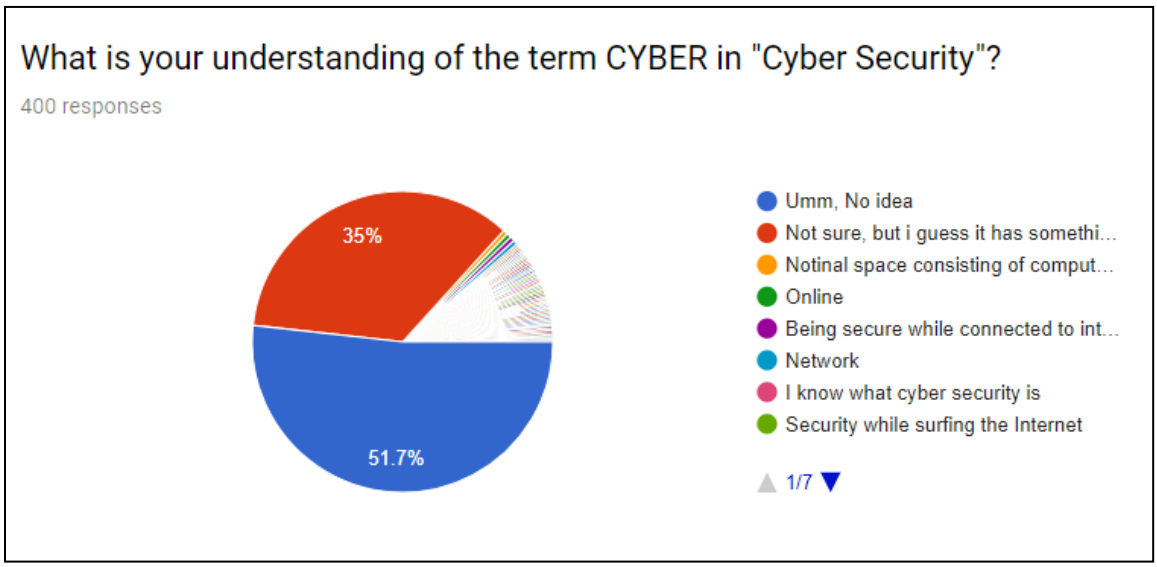

Figure 4.3: Understanding of Term "CYBER"

c) **Third option: (other)**

This option was provided to evaluate the understanding of this term by individuals. Different responses were submitted ranging from basic like online activity, security while

surfing the internet to more accurate like notional space consisting of computer networks. The very fact that someone has selected this option is evident enough to prove that they have no ambiguity related to term cyber as no appropriate option was available in the posed question.

4.3.2 Question 2:

Are you familiar with the Pakistan Electronic Crime Act (PECA 2016) enforced at the moment in Pakistan?

- 80 reacted to option 1
- 320 reacted to option 2

a) Option 1(YES):

Less than half of the respondents are familiar with PECA which is not a healthy sign of cybersecurity culture development. It was recorded that majority of the option was selected by cyber security students and professionals.

a) Option 2(NO):

Majority of the population does not know about PECA and its terms and conditions for any misconduct or cybercrime act. If people are not even aware of the cybercrime bill of their country then that will eventually result in more cyber crimes as individuals have no idea about cybercrime punishments.

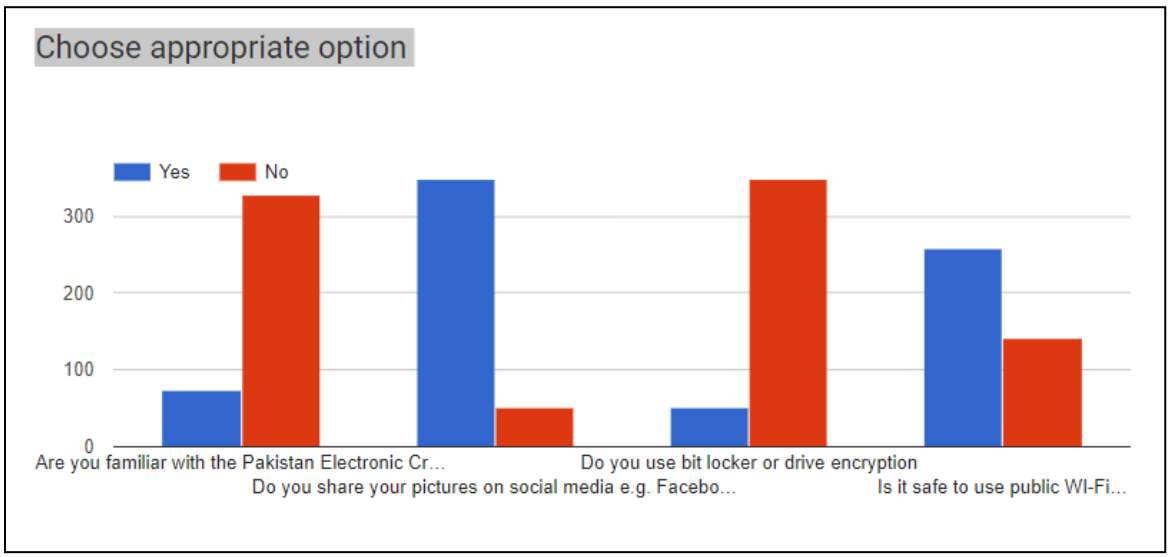

Figure 4.4 survey result of four questions

4.3.3 Question 3:

Do you share your pictures on social media e.g. Facebook ,Instagram etc?

- 350 reacted to option 1
- 50 reacted to option 2

a) Option 1(YES):

A large number of individuals upload their pictures on social media. This depicts the lack of awareness level as these pictures are a major target of cyber espionage and cyberbullying. Cybercriminals use these pictures to harass an individual online as a result of personal vendetta while people are openly providing their personal data online that is at risk all the time. This majority ratio of YES is evident enough to depict that people do not give importance to the security of their personal data or in some cases are unaware of the threat level of their information.

b) Option 2(NO):

People who are concerned about their privacy and are more conscious in nature are the ones who do not upload their pictures on social media. The low percentage of response shows that majority of the respondents does not consider uploading their pictures as a security threat.

4.3.4 Question 4:

Do you use bit locker or drive encryption?

- 50 reacted to option 1
- 360 reacted to option 2

a) Option 1(YES):

Individuals that opted option 1 depicted the mindset of a security professional where people considering protection of their drive as an important task. The statistics, however, shows that they are very less in number. Drive encryption is still an alien concept among masses.

b) Option 2(NO):

The results show similar ratio in respondents choosing to upload pictures on social media and using bit locker for drive encryption. It can be concluded that some individuals have selected this option as the security of personal data is not in their priority list. Not using bit locker exposes the drive to threats.

4.3.5 Question 5:

Is it safe to use public Wi-Fi at shopping malls, airport etc?

- 270 reacted to option 1
- 150 reacted to option 2

a) Option 1(YES):

These statistics shown in figure 4.4 lead to the result that individuals choosing this option are unaware of the risk caused by using open Wifi. These people are exposed to threat and easily become a potential victim of cyber crimes. Their choice illustrates that either this type of question was never posed to them or they have never heard of Wifi security. A minority of respondents have chosen this option which is a delightful sign of cyber awareness.

.

b) Option 2(NO):

The proportion of this response demonstrates the fact that respondents are well aware of the threats and risks in using public Wifi. In measuring the cyber maturity of masses this question is crucial as these days every activity is performed online and is ultimately dependent on Wifi so people use Wifi in public places but at least they are well informed with the threats and consequences. A vast majority of respondents have selected this option that does not conclude that they do not use open Wifi.

4.3.6 Question 6:

Which URL would you use to open Facebook?

a) Option 1: (http://facebook.com)

Facebook is the most used website in Pakistan so people are more likely to be familiar with its URL and a majority of respondents have selected option1 as they know that https is the secure connection but, in this case, they have neglected an extra letter in Facebook

and hackers usually misguide internet users into clicking such malicious links where they are under the illusion that they are choosing the secure URL without even realizing the truth.

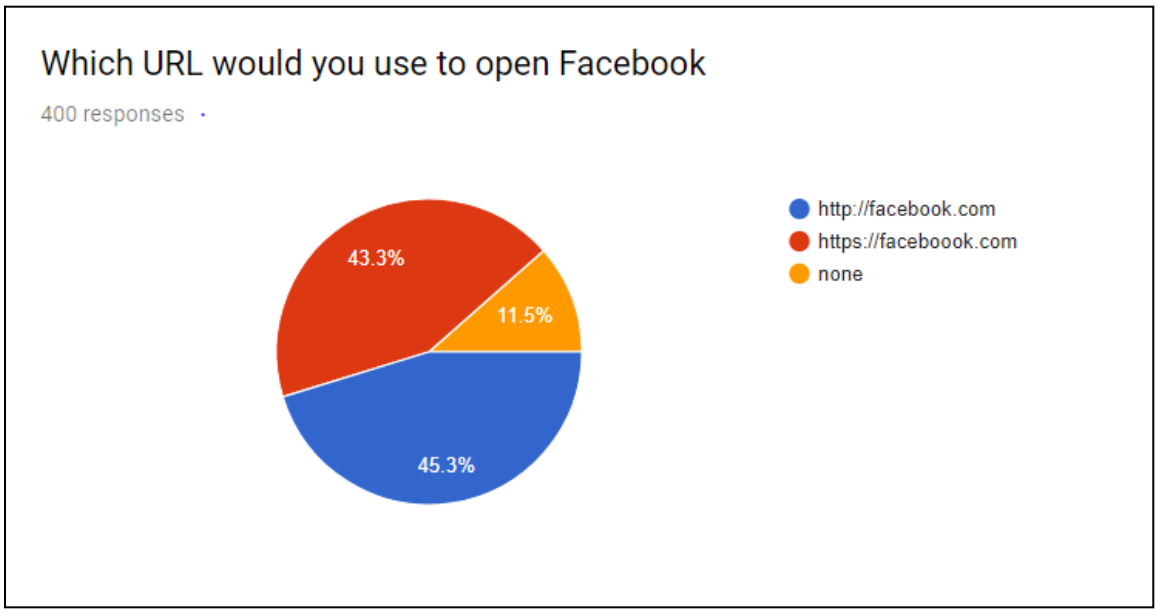

Figure 4.5 URL Used to Open Facebook

b) Option 2: (https://faceboook.com)

A very low percentage of respondents shown in figure 4.5 have selected this option which is the correct option and conclusion can be drawn that a few respondents are technically sound in cybersecurity as they were not misled by the URL but this situation is quite alarming as the statistics show very less number of responses to this option despite the fact that Facebook is a website which is actively used.

c) Option 3: (none)

A vast number of people are still not aware of the difference between an HTTP and https URL. The respondents of this option consider http:facebook.com the correct link as they are clueless about SSL and HTTP security. Many websites are still using HTTP URL so it is a common mistake by users as hackers can lure victims by sending HTTP links and directing them to its own malicious pages and extract personal information of victims.

4.3.7 Question 7:

Which of the given passwords is most secure?

a) Option 1: (Apple26Mango)

Computer users usually set the password that they can memorize easily and therefore use common language words. So this option was provided to test the respondents whether they consider it the most secure password but as the statistics show that only 10.6 of the total has selected the option which provides a clear picture that respondents are fully aware of password strength.

b) Option 2: (Uweplk&1)

Password strength is the most occurring security feature as whenever a user creates an account it is directed to choo se a strong password and these days it is mentioned that a strong password consists of numbers, alphabets, and special characters. 43.5% of respondents in figure 4.6 have chosen the right option that shows the awareness level of users in all aspects of strong passwords mainly due to the reason discussed above.

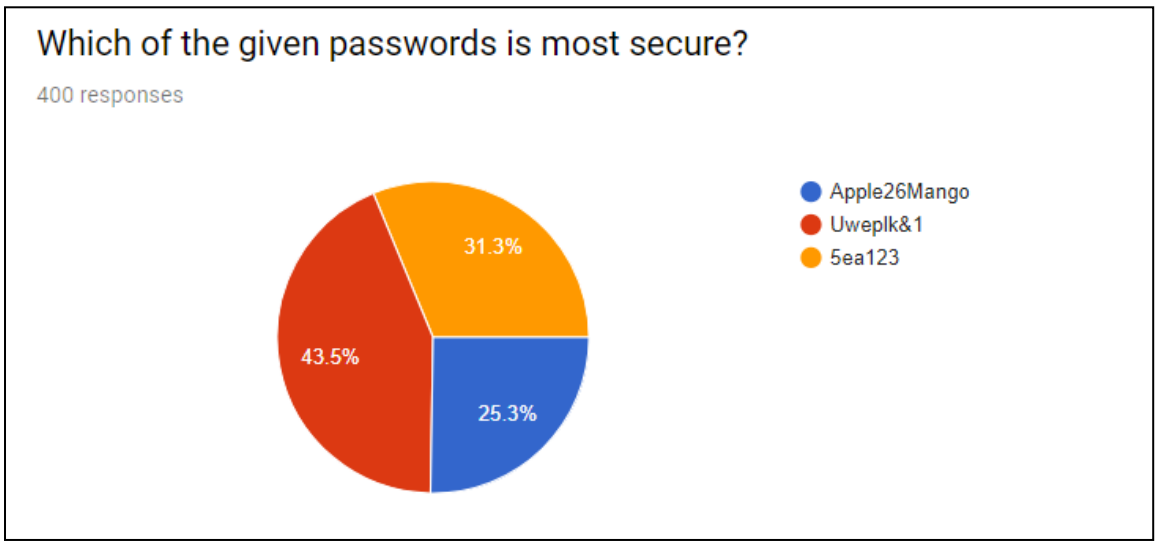

Figure 4.6 Secure Password

c) Option 3: (5ea123)

Option 1 and option 3 are not that distinctive in nature as option 1 was only larger in length. This option was provided to test whether the respondents are aware of the significance of password length.

4.3.8 Question 8:

Which of the following circumstances would you treat as suspicious?

a) **Option 1: (Email/ phone call from your bank's representative asking for credit card information)**

This is a suspicious circumstance as hackers these days use reconnaissance for any cyber attack and in case of online transactional activities, credit card information is crucial. The credibility of this email can be decided on the fact that whether the email is received from the same source as the user has received previous valid emails from the very source.

b) **Option 2: (Email from government employee with email address pak.gov@gmail.com)**

The second circumstance should also be treated as a threat or suspicious because a valid email from government employee will be received with a domain of the government office and not from @gmail.com. People choosing this option is familiar with this fact to decide between valid and suspicious emails.

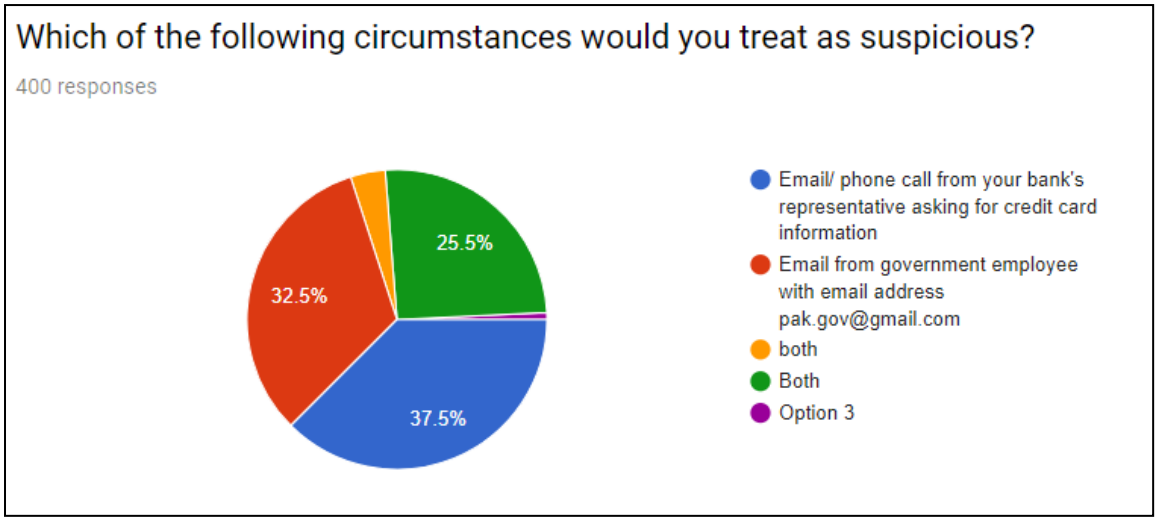

Figure 4.7 Circumstances Treated As Suspicious

c) **Option 3: (Both)**

The third option of both was provided to decide between individuals having knowledge about suspicious activities and those having in-depth technical details about recognizing suspicious circumstances.

4.3.9 Question 9:

Which national organization would you contact in case you find your Facebook profile hacked?

a) **Option 1: (No idea)**

The large ratio of responses provides an indication that majority of respondents are totally unaware of cybercrime unit of Pakistan which deals with such crimes. As they have opted an option where they openly accept of having no idea in this regard. The lack of awareness is the government responsibility as they have created a facility for its citizens to report crimes but the sad part is that people are unaware of the existence of such cybercrime units.

b) **Option 2: (There is no such national organization in Pakistan that can deal with it)**

The respondents selecting this option are even worse in cybersecurity than the first as they are confidently choosing a wrong option. This shows their negligence in the national organization and their initiative in cybersecurity.

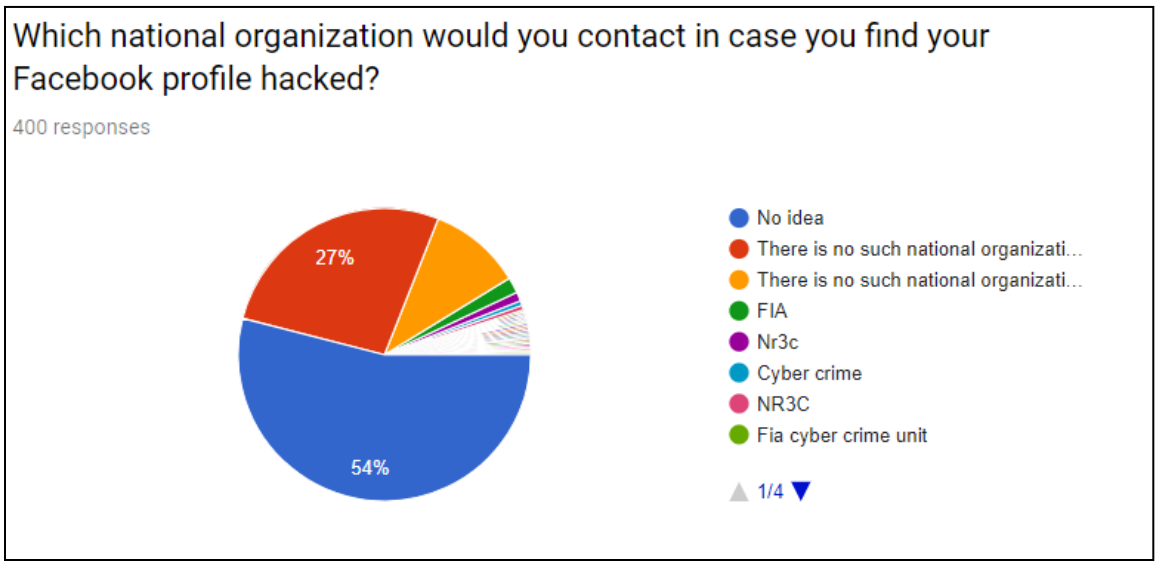

Figure 4.8 National Organization Contacted When Facebook Profile Hacked

c) **Option 3: (other)**

The third option is provided for individuals to mention if they know any such organization. NR3C is the national cybercrime unit of Federal Investigation Agency that

provides reporting mechanisms in these matters. Some respondents have written the correct answer but are more likely that the cybersecurity students and professionals have provided these answers.

4.4 Discussion of Results:

It is evident from the figure 4.2 of age distribution that people in the age group of 21 to 30 have mostly responded to this survey so results are concluded on the basis of respective people. As discussed above that the survey was conducted to assess the cyber awareness among people from different spheres of life and the results evidently show that only the cyber professionals have the idea of cyber security and are fully aware of the circumstances and vulnerabilities of cyberspace. The results of every posed question depict that respondents have opted or reacted to the wrong option mostly, and when there is another option where they can provide the right answer only the IS professionals have responded with the correct answer. In general, if we assess the situation so it can be concluded that young people are unaware of the terms related to cyber security and the basics involved in it. This conclusion is only drawn because of the way people reacted to the survey. As a growing economy, it is alarming if the youth is not aware of the threats to the cyber landscape as the users of the internet and digital medium is mostly the youth.

4.5 Conclusion:

The analysis depicts the true stature of cybersecurity in Pakistan as a very basic question about the topic were asked to the respondents and as shown by statistics a majority of respondents have selected the wrong option while in some cases the correct options are also provided. People ranging from the age 21-30 have mostly filled the survey so it can be analyzed that the lack of cyber security awareness is in the age group but on the whole, the level is below average. By analyzing the individual responses it is noticed that more men have chosen the right options as compared to females. The theme was achieved as this survey was conducted to assess the maturity level of the masses and in this case, the results are conclusive so the strategy for capacity building is the need of the hour as it is not the ultimate solution but a step in the right direction.

Chapter 5

CYBER SECURITY CAPACITY BUILDING STRATEGY

5.1 Introduction

The Cyber capacity building is a key factor in social and economic development as cybersecurity promotes it access in cyberspace and in result ensures that cyber criminals do not jeopardize the access by their predatory criminal behavior. Industrialized countries are working in collaboration with developing countries on different ICT projects over the internet and in most cases, the former is the donor while the latter is the recipient. Vulnerable software developed in one country can be a soft target of cyber attack while being installed in another country as cyberspace has no international borders so the developing countries suffer more in this aspect. The government of any developing country should have two potential capabilities while militating against cyber attacks. Firstly, well-structured information assurance national standards with proliferate cyber laws and policies in place. Secondly, the ability to respond operationally in dealing with cyber attacks and risks when assistance is required internationally.

On national level cyber capacity building seeks to enhance the performance and professional skill through rigorous planning and action that reflects in manpower development. Building national capacity generally involves four steps: 1) dissecting and analyzing what is missing 2) strategy planning 3) educate personnel 4) evaluation of results.

The proposal concentrates on establishing a general framework for assessing and delivering cyber capacity regimes. The framework provides rationale solutions while highlighting potential dimensions of capacity building for public and private organizations. This will conclude with recommendations for strategy makers and legal regulatory bodies for designing sophisticated cyber strategy

5.2 Guiding Principles

a. Existing local and national policy related to cybersecurity to be considered while strategizing the CCB.
b. Define the scope of the CCB strategy.

c. Roles and responsibilities should be defined as the person who should develop, design, implement, execute and maintain the cyber capacity building strategy. To ensure that the appropriate roles are assigned to capable individuals.
d. Achievable goals need to be defined for each aspect of the strategy (e.g. awareness, training, education, R&D, industry development etc).
e. To target and categorizes the appropriate audience for each aspect of the strategy.
f. Define the deployment methods to be used for each aspect of the cyber capacity building strategy.

   Documentation and feedback are the evidence of each aspect of strategy

5.3 Vision

a. The government of Pakistan should strive to create conditions within cyber landscape for the smooth functioning of the information society.
b. The strategy should aim at the rapid development of cybersecurity expertise and of capacities to resist the latest cyber threats.
c. The government shall cooperate with academia and the private sector in development activities that are concerned with the security of information systems.
d. The government shall encourage the development of a cybersecurity culture through raising awareness among citizens.

5.4 Framework Summary

Using the international capacity building framework this proposed structure is conceptualized for the assistance of government and the private sector in cybersecurity. This coordinated proactive approach will increase the cyber workforce of our country. Our country is vulnerable to cybersecurity attacks as mentioned above so it requires international collaboration to mitigate these risks. The details of the framework are mentioned in the tabular form

Table 5.1 Framework Factors With Their Descriptions

Topic	Description
Cyber Security	a. Increase the cyber literacy by designing cybersecurity

Education	course from grade one to ten b. Involve cybersecurity experts in designing the course material c. Universities offer degree programs in masters and PhD
Cybersecurity awareness	a. Encourage users to include cybersecurity practices while performing online activities b. Promote security awareness by conducting workshops, seminars, webinars, and conferences c. Collaborate with print, digital and social media to bring awareness among masses d. Establish a portal where the latest cyber security risks can be posted for the assistance of users
Professional training	a. Support skills training in cybersecurity at universities and colleges b. Promote international cooperation on training programs c. Private sector companies encourage their employees for professional training
Research and Development	a. Encourage the students to research in the security of critical infrastructure b. Invest in projects that will aid in maintaining updated national emergency responsiveness c. Indulge in proactive research techniques that will secure the internet in future d. Cybersecurity industry should research and develop innovative products
Homegrown industry	a. Develop homegrown products by encouraging research students in this field b. Establish government cert to develop products

5.5 Roles And Responsibilities:

While developing a strategy for a nation it is very crucial to define the roles and responsibilities of every stakeholder involved. The section will identify the responsible actors that need to perform for the smooth operation and execution of the cybersecurity capacity building strategy. Segregation of duties is an essential factor while designing a strategy nationwide as duties of every stakeholder differ according to its roles. To document the roles and responsibility will be helpful for the key position holders while developing a better understanding.

5.5.1 Strategy Head:

Strategy head needs to ensure that high priority is given to cybersecurity capacity building programs. Implementation of security program that is viable in nature is a key job that strategy head needs to monitor. The rest of the responsibilities are listed below:

a. Designate a chief information security officer to design the strategy keeping the tactics in mind.
b. Assign the duties to every stakeholder involved
c. To ensure that nationwide cybersecurity capacity building program is implemented, supported by budget and resources and is running smoothly.
d. To ensure that resources are well utilized and enough professional personnel is present to take care of it.

5.5.2 Chief Information Security Officer:

According to FISMA(CISO) are appointed to oversee such strategy tasks but in the present case the responsibilities of CISO should be revised according to the current need so the duties are listed below:

a. Design the overall strategy for the cybersecurity capacity building program while collaborating with another involved stakeholder.
b. Ensure that the strategy head, program manager, line manager and other stakeholders are understanding the initiatives taken for cybersecurity capacity building.
c. Ensure that the cyber security capacity building program is funded.
d. Ensure that the overall activity of program manager is monitored and enough personnel support is provided.

e. Ensure that reporting mechanisms are in place that is tracking the activities in an effective and efficient manner.

5.5.3 Program Manager:

The Program Manager has the tactical responsibility for the cybersecurity capacity building program development and situational awareness is the key utility that any program manager should uphold in order to achieve success in its role. In the capacity the program manager has the following role:

a. Ensure that the material for awareness and training program is timely developed and disseminated to the users.
b. User feedback on the cyber capacity program should be taken and it should be ensured that all the queries are addressed and the program is improved or adjusted to that feedback for future development.
c. To ensure that the process is reviewed periodically and amendments are made according to the situation.
d. To assist the CISO in developing a tracking and reporting structure for the cybersecurity capacity building strategy.

5.5.4 Manager:

All the practical labor is required of the manager as he is the one responsible for the operations and their smooth run. Time management is the key quality required of a manager as he will be dealing with numerous structures and processes at a time. Timely execution of events is the most important factor here. The responsibilities are listed below:

a. To work in collaboration with the CISO and the program manager to share the responsibility and meet the essential objective in time.
b. Training of users is the responsibility of the manager as they are the ones interacting with the users.
c. To promote the professional development of users by inculcating the cybersecurity culture in the best possible way by training, awareness and educating them.
d. Ensuring that every stakeholder in the hierarchy is appropriately trained about their security responsibility before granting them access.

e. Design the initial development plans for the users in a cost-effective way considering that the results will be according to the desire.

5.5.5 Users:

Anybody using ICT and digital devices for their personal and professional work is considered the user of cybersecurity as they are considered to be target audience while strategizing. As they maintain a large stake in the hierarchy so it is essential to define specified roles and responsibilities for them as they are listed below:

a. Provide honest feedback on the program for betterment and updation of services and products.
b. Report any issues faced by the authorities so they can update their program and take appropriate action to avoid such incidents in future.
c. Suggest any improvement in the training and awareness program for its success.
d. Promote the cause actively by adopting the guidelines provided and encouraging others to repeat the same act

5.5.5.1 Types of Users:

In this research, three types of users are specified for CCB strategy as later in the chapter different training are specified for the users so it is necessary to define the user type here so that the reader gets the clear image. The users are classified as below:

a) **Regular:** A normal computer user that has access to internet lie in this category where a person is using the technology for running its daily operations.
b) **Professionals:** A professional is defined as an individual who is the user of digital devices for its work purposes and personal both.
c) **IS specialist:** A professional who specializes in information security and have a fair amount of knowledge in cyber security.

5.6 Awareness

Cybersecurity awareness should focus on the entire population of users. Authorities should build the environment of proper IT security culture within the society. An awareness program is an effort that is aimed at all levels ranging from users to high-level officials and can be deployed and executed in the desired manner to reach the wanted

outcome. The effectiveness of the process is directly proportional to the effectiveness of efforts. Awareness is perhaps the most crucial aspect or component of cybersecurity capacity building as it is the medium for disseminating information and guidelines to users. As a result, the user should and will use this information to fulfill their responsibility in a secure manner and what is expected of them. Awareness is the vehicle in a cybersecurity capacity development program to communicate information security requirement across the masses in case a national development plan. An effective program should explain the proper rules of use of ICT to the audience.

The development of information security procedures, standards, guidelines or cybercrime law will be less effective if the users are unaware of these practices. As in this current scenario, the survey results presented in chapter 4 unveils that 61% of the audience was not even aware of the cybercrime bill acting in Pakistan and 50% were under the illusion that there is no active cybercrime unit working in Pakistan.

In co-operate, world security professionals sometimes fail to sell their perfect security products as they have not adequately marketed their product among numerous IT companies as in our country no one is really willing to invest money in security products as they lack the awareness level of security risk to their business.

5.6.1 Guiding Principles

Awareness, which is used to stimulate, motivate, and remind the audience what is expected of them

a. A way to carry the message to the cyberspace users for reinforcement of cybersecurity as a momentous concept.
b. To identify the responsible individuals for implementing such security programs.
c. Evaluate the criticality of cyber security applications, system, and infrastructure.
d. To ensure that goals and objectives of cybersecurity program are supported by the related government officials.
e. Identify the target audience

5.6.2 Awareness medium:

Different techniques are used by the world for disseminating information about cybersecurity across their particular countries. The techniques mentioned here are on the basis of resources and need assessment of the cybersecurity posture of the country. The

technique that is feasible and less complex should be adapted to freely disseminate cybersecurity awareness message. The techniques are listed below:

a. Posters
b. Banners
c. Newsletter
d. Home-to-home alerts
e. Nation-wide email messages
f. Web-based sessions
g. Computer-based seminars
h. Conferences
i. Seminars
j. Webinars
k. Games(crosswords, puzzles)
l. Competitions
m. Workshops
n. Media television
o. Print media
p. Social media

As described in chapter 3 section 3.5.3.2 across the world there are privacy awareness day and different events organized by ENISA, OAS and different entities to promote awareness about cybersecurity and its countermeasures. In our country, no such event is organized on a national level. Banners and posters can be designed by the information security students or companies and they can be disturbed among the masses. The Newsletter can be distributed in offices and companies designed by professionals in accordance with the international promotional material provided on the internet. The Government can generate alerts that can be disseminated on local levels like home-home alerts. This will raise awareness level and if one person will share the information with another and this chain

continues then beneficial and fast results can be achieved. A cyber cell can forward warning emails to people nation-wide. Conferences, workshops, and seminars can be held on different occasions and venues and the topics covered can be decided keeping the audience and their information security knowledge in mind. The Web-based session can

also be executed as they are in trend in the world and people usually consider going somewhere time-consuming so they can be fruitful for this scenario.

Games can prove to be an interactive way to aware the masses especially the young generation. It would have long-lasting and thought-provoking effects. Media whether social, print and television can play a vital role in spreading awareness. Dramas can be made on cybersecurity topics while highlighting the cyber crimes and they are after effect and how to deal with them. Social media in this day and age is the most powerful tool to spread awareness. Every country has their official accounts on twitter and facebook to spread awareness among its citizens mentioned in detail in chapter 3 section.

5.6.3 Developing Awareness Material:

The basic questions that need to be answered is awareness material development is that

Question: " What behavior do the authority wants to reinforce?"

Question: " What do the authority want the audience to be aware of regarding IT security?"

The strategy plan here is listing the topics that needs to be addressed in any awareness plan and they are mentioned in NIST guideline [53].

5.6.3.1 Choosing Awareness Topics:

A generic list of topics is provided and they can be discussed in any format selected for awareness. Topic distribution and selection is also dependent on the target audience and the responsible agency conducting that awareness exercise.

a) Lock your login
   - Apply strong authentication to your email and social networking account. Two-factor authentications are the best way forward.
   - Use a strong password for your accounts that contain alphabets, numbers, and symbols.
   - Use a different password for every account as using the same password increase the likeliness of a cyber attack.
   - Protect your password and never write your password on some file that is unprotected.

b) Be web smart:

- Keep updated and stay posted with current techniques to stay safe online. Visit trusted websites to stay vigilant for latest information and disseminate it to friends and family.
- A user should analyze the situation before acting on it like when an anonymous user asks for their personal information so users should be careful before giving way its information.
- Always have a backup of your critical work, document and personal data.

c) Connect to secure sites:
   - Don’t open any link that seems suspicious in your email that could lead to a phishing attack.
   - Connect to secure Wifi to avoid the risk of being a victim of cyber attacks
   - Protect your online activity as while shopping online and before providing your credit card information the security of the website should be checked. One way to ensure the security is if the website has https URL and other can be that is has a lock sign in its tab bar.

d) Watch your online activity:
   - Users should keep a track of their online activity as internet globally connects its every user so use good online practices.
   - Users should post content online carefully that does not aggravate any emotions or avoid comments that hurt someone's sentiments.
   - Users should share information or personal data with limited access as this data can put them in the vulnerable position.

e) Protection from Virus and Trojan
   - Use of Antivirus and regularly updating it with latest patches.
   - Execute prog that is from the secure source in presence of sensitive data.

f) Policy Creation and Compliances
   - To avoid privilege escalation policies should be created.
   - Regular audit is required to check that actual systems are working in compliance with the policies.

g) Data Backup and Storage
   - there are different backup types a) full b) Incremental c) Differential d) cloud back up

- The Recommendation should be provided to choose the right backup type that favors the conditions.

h) Social Engineering
   - A way to psychologically manipulate individuals into performing specific actions or giving out confidential info.
   - A number of social engineering techniques is used that are dependent on human decision making.

i) Disaster Recovery
   - Organizations usually have DRP in position in case of any environmental physical disaster.
   - The Contingency plan is the main part of DRP and it is well documented so it can easily be implemented in such situations.

j) Access Control
   - Access Control should be in place so after authentication every user has access to services that are designated for them.
   - ACL can be made on basis of organization policy so users are fully authorized and authenticated.

5.6.4 Cyber Awareness Week:

In a country like Pakistan where resources are so limited an initial step in promoting cyber security would be celebrating a whole week for cyber awareness as currently cyber defense day is being celebrated as mention in section 2.. A week should be dedicated on national level and the target audience should be wider in this regard. Currently any efforts for CCB in Pakistan are for targeted audience i.e. IS professionals and specialist.

Activities in the week:

a) Password protection day can be celebrated where the importance of a strong password can be taught.
b) Cyber competitions can be conducted among the young IT professionals to assess their potential and talent in cyber security.
c) Awareness seminars against cyber bullying and cyber security issue that target general audience can be held

d) A day for safer use of internet can be celebrated where the internet service providers can collaborate with social media to generate awareness.
e) Cyber literacy day can be celebrated where families as a whole can be given education on their rights and responsibilities as a secure cyber citizen.
f) Seminars can be held to encourage young students to consider cyber security as a career option.

5.7 Training:

In human resource development according to [54] training constitute of developing a particular skill set to a desirous level by practice and instruction. It is the perhaps the most useful tool that can equip an individual to act effectively in a crunch situation and prepare him for any unforeseen circumstances as in Infosec preventive measures prove to be highly effective in specific situations. The sole purpose of training can be to increase the knowledge and skill of an individual to perform any specified activity.

According to [55] Dale S.Beach defines training as "the structured procedure by which individuals learn and develop skills for a definite purpose." These training can be held in training centers or conducted at online platforms as they can be tailored to organizational need and resources.

5.7.1 Training Life Cycle:

A Cyber workforce is a continuous effort so the training is usually carried out in phases. The training methodology analyzed from the selected countries can be concluded as described below. An individual develops the proficient skill

Level and gained knowledge to perform its job duties in an effective manner after passing through these phases.

a. Phase 1: Knowledge Building

It is the first step where learners are equipped with fundamental concept and skills. Online deliveries can be the most cost-effective and time efficient.

b. Phase 2: Skill Building

The concepts learned in the previous phase are reinforced through tasks and hands-on experience. Individuals apply knowledge it into ability.

c. Phase 3: Experience Building

All the skills and knowledge are to be applied in the real world on job scenarios where a controlled environment is not present to increase the performance of individuals.

d. Phase 4: Evaluation

Assess skill proficiency and knowledge achieved by the learners in training phases. The results of the assessment can be beneficent in designing next cycle of training.

5.7.2 Training Course:

The essential training courses are listed below that are a prerequisite for cybersecurity training:

a. Low and high-level programming (C, Java, Javascript and assembly language)
b. Reverse engineering (malware analysis, software, techniques, and tools.)
c. Theory of operation systems(operations and internals)
d. Networking (traffic analysis, protocols, packet inspection)
e. Telecommunication (core network and infrastructure)
f. Cyber defense mechanisms
g. Security fundamental principles (policies, domain separation, and applied cryptography)
h. Vulnerabilities (buffer overflow, root cause, malware, privilege escalation attacks and rootkits)
i. Legal (regulations, Law, policies and cyber security directives)

5.7.3 Training Types:

Training can be divided into three types as mentioned and discussed below. Different factors need to be considered for choosing which training type will give best results. As the factors can be the environment, budget, level of expertise required, number of trainees and the purpose for which they are trained for so any given type can be selected on basis of these factors.

5.7.3.1 Video Training:

A video training where the instructor and the trainers can interact in a virtual environment. This training types will resonate with highly qualified professional as they are used to such training so it can be a familiar environment and they can learn fast and adapt easily to these conditions. If the training is promoted well then professionals will be

interested in investing in such activity as they could grow in the professional career. Without incentive, nobody is ready to invest so the training level should be equal to international standards and on local rates or packages can be given to growing the interest of the audience. ENISA or GSCC types organizations can be contracted or countries whose cyberspace can be threatened if Pakistan cyberspace is attacked can help out in this process

5.7.3.2 Web-Based Training :

In cyberspace and for the distributed environment this training type is probably the best option. The attendees of such training can study independently and learn at their own individual speed. For a country like Pakistan where economic crises are evident such training can generate fruitful and effective results. A national plan should opt for the option that is effective and less expensive giving maximum output. Awareness Month is celebrated by ENISA and such organization their online sessions are available regarding training of individuals on different level considering their background knowledge of infosec such materials can be helpful in designing training material. Research students can be motivated to design training material for the general audience and they can be hired for this job.

5.7.3.3 Instructor-Led Training :

This is one of the oldest end perhaps sometimes most effective training method. Interaction rate is probably the highest in this technique. This might not be the most suitable option where the large workforce is involved as it would be hard to schedule such activity on a gigantic scale. Information security training centers can be created where young students or professionals can be trained according to the latest trends in infosec. A cyber army should be created that is equipped with a skill set that will counteract infosec attacks and prevent any such activity.

5.7.3.4 Level Of Training According To User Type:

The Table 5.2 below provide the details of training on account of the user type provided as training for different users should be different as understanding level of users differ from each other in this respect.

Table 5.2 Level Of Training According To User Type

User type	**Level of Training**
Regular	Use of Antivirus Scanning softwares knowledge Basic protection mechanism
Professionals	Use of specific security softwares of the respective field CSCU certifications Device encryption Password protection Secure coding Email filtering
IS Specialist	CISSP certification CEH OWASP Reverse Engineering tools Malware Analysis

5.7.4 Training Outcomes (Cyber Scout)

a. The results of appropriate technical training will provide smooth cyber operations in cyberspace
b. The technically sound workforce will be developed that will provide cyber security solutions to the nation.
c. The cyber army is created that is tasked to fight against cyber crime and targeted cyber security attacks.
d. Cyber security ranking of Pakistan can be upgraded as its workforce in cyber security will be increased.

5.8 Education:

Critical Infrastructure of a nation can be protected by expanding and promoting cyber security education. In the 21st century every state should strive to build a newly educated

workforce and include additional skills in current workforce. Educators should try to comprehend critical knowledge, abilities, and skills from elementary school to postgraduate so that the future cyber security professionals are fully equipped with. Along with every other subject taught students should get knowledge about the ever evolving technologies and how to securely use them. Education is used as a medium to promote or develop a new fully equipped workforce. Training and awareness are the building blocks for cyber security capacity building and education plays a key role in resource development.

A dignity literate workforce is required if any nation wants to fight cyber attack and counteract with reactive measures. The State should offer educators with required resources to empower students with foundational skills to grow and built a career in cyber security. The educations ministry needs to have various resources for curriculum development and should have activities to discover the knowledge and skills that are required for being part of this growing community.

5.8.1 Middle School:

A three-course elective sequence for students of 6-8 that will be explore, discover and apply should be incorporated into the normal studies to broaden their horizon in cyber security field.

a) Explore:

Students should be encouraged to question about technology in the present time. The Class can be held to teach students of new growing trends in the industry so that they develop a habit of exploring techniques on their own that will be beneficial for them in the future

b) Discover:

The Education system of Pakistan lacks the quality where students are advised to discover new stuff. A general practice of discovering should be incorporated in students because children learn fast and develop habits for lifetime in their students to submit reports in discoveries in three months. This will generate their interest in different fields thus provoking a thought that is essential in professional development.

c) Apply:

When the students will explore and discover technologies then automatically they will try to apply such practices in real life. In the process, something fruitful might come out as a result of such strenuous activities. Our Education system lacks in the application so it is the duty of schools to encourage their students for applying art techniques that they have learned in the process.

5.8.2 High School (9-12)

STEM: Science, Technology, Engineering, and Math are usually incorporated in western schools for grades 9^{th} till 12. A blend of programming and science can be beneficial for students while they can get the education on threats, vulnerabilities, and legal constraint that are associated with how to operate in cyberspace.

a. Students can attend boot camps like cyber showcase for two months in summer where basic skills can be taught regarding cyber skills.
b. Computer science can have a stream of IS where a portion can be introduced as an introduction to information security and the course can be developed by cyber security professionals.
c. Colleges should have cyber security class where the cyber crime bill can be taught and just like the constitution students should be aware of our cyber crime bill and its punishments in case of any cyber crime.

5.8.3 Graduate:

At this stage, the students are mature enough to grasp knowledge about cyber security. At present universities are not offering four-year degree program in information security where NUST is offering is stream after completion of two-year degree program in computer science. Cyber security is a budding profession in Pakistan right now as it is evident from the stats that no professional college is present for cyber security. Different streams of cyber security are mentioned below in Table 5.3 that can be offered in graduate program along with it are the predicted skills that will be gained by students.

Table 5.3 List Of Graduate Courses With Their Description

Course	Course Description	Skill Gained
Fundamental Of	Provides an overview of networking technologies for	a. recognition of network design

Networking:	the wireless network, LAN, and WAN.	for any given scenario b. security protocols c. network protocol
Installing And Configuration Windows Server	it will cover how to install, configure and troubleshoot any operating system like windows, Linux or virtual machines.	a. configuration of server features and roles b. configuration of Hyper-V c. deployment and configuration of core network services d. creation and management of group policy
Ethical Hacking	Discover vulnerabilities in any information system and recommend solutions for data protection from potential hackers. it will focus on penetration testing and how its tool and techniques can be deployed to get desired results.	a. knowledge of safe world wide web techniques b. hands-on practice to defend a computer against security attack c. to defend a LAN against any security attacks because of hands-on technique

Security area with its description and tools required to counter are mentioned in the table below. Any student graduating in Cyber security should be familiar with these security domains and the required techniques and tools that are helpful in fighting against tailored cyber attack.

Table 5.4 List of Different Security Areas With Course Description

Security Area	**Course Description**
Access management	Tools need to be studied that will provide additional protection

	for active directory security gaps
Botnet protection	Threats that botnet can cause and related vulnerabilities that can be exploited. Study tool that provides protection against botnet without the need for individual detection and identification.
Data encryption	Data encryption techniques like are included thus aiding the audience with tools.
Next-generation firewall	In network security, next-generation firewall should be studied as it is very advanced as compared to the traditional firewall. It special features are to provide intrusion protection, application and identity awareness and stateful inspection.
Wireless Security	Provide knowledge on WEP/WPA/WPA2 all the protection protocols. It includes guidelines that need to be implemented in case of wireless security.
Malware /Virus Security.	Study the malware analysis as it will be aided with the tool that will reverse engineer the malware and prevents attacks that are specially targeted to harm both hardware and software of any information system.
Data Leak Prevention	DLP techniques and tool are used to ensure that the information of the system is secured from any intruder access in case of any security breach. Any Graduate in IS should have knowledge about these techniques as if is the most common security area.
Endpoint Protection	This deals with security issues of endpoints that are PC's, network connected printers, servers and mobile devices and others. Tool required for endpoint protection can be used to further understand the concept.

5.8.4 PostGraduate:

Masters and doctoral degree program of cyber security should teach student practices that will make them sophisticated practitioner in the digital industry as they secure vital digital networks electronic infrastructure from targeted cyber attacks.

Table 5.5 List of Postgraduate Courses With Their Description

Course	**Course description**	**Skill Gained**
national security technologies	discover the impact of technology on national level security and lesson learned that are documented should be studied explore the risk and advantages of technological innovations on the military.	a. national security policy b. intelligence gathering c. fight cyber terrorism
penetration testing	This course is effective when it is lab-based while providing students an understanding of the risks and threat factor analysis. Techniques used for exploitation and penetrate system and network is a major part of the course.	a. vulnerability assessment b. exploitation technique c. remediation technique
cyber risk management:	Examine the cyber risk management policies while addressing their issues and concerns. students can learn to identify high-level risks and counteract upon them while mapping their impact across any specific organization	a. mitigation strategies b. standards, legal issues and cyber ethics
applied cryptography	Cryptographic techniques, encryption algorithms along with integrity technique, steganography, and understanding of different	a. cryptography technique b. encryption algorithm

	ciphers and their detailed techniques.	
computer and database security	Basic concept and terminologies in the field of computer security and provide an understanding of its relationship with information technology. While database security presents the framework and student can learn how to secure a company's technology and information system.	a. hardening system b. defending against security attack c. understanding of database security model d. securing network

The Table contains courses along with their brief description of what that course should offer to its students and ultimately what are the skills that the students will acquire after studying those courses in detail.

5.9 Research And Development

a. Invest and participate in research project and activities that concern cyber security on National Level.

b. To designate any specific organization to act as the main point of contact in case of cyber security research. The main center that can have information of every research that is happening in cyber security.

c. Ministry of education should appoint cyber security experts and professional to design curriculum according to the different age group of students.

d. To prioritize research and development on national-level and hence actively stimulate investment for the purpose.

e. Cyber capacity center can be designated by providing the appropriate resources. On basis of incentives, these professionals will carry out research in different security streams of cyber security.

f. A research team on national level can be created that will perform need assessment of recent market and what are the latest trends and threats in cyber security. They can thus allocate team members on disseminating such information and guiding research analyst accordingly.

g. Computer science degree students who are in their final year and are selecting their research topics can contact this center and hence the research center have different security related topics so the research analyst can guide them they can develop practical applications. A database can be created that have the record of all the ongoing research on cyber security in the country.
h. Private sector needs to collaborate with academia and provide sponsorship to research product that can ultimately make a difference to the information technology industry.

5.10 Home Grown Industry

It was the idea presented in cyber security index document 2017 [56] under the section of capacity building in the framework where Ireland was mentioned because of its fast-growing cyber security industry. Pakistan should draw an existing incentive and aim to become a cyber security facility and some day in future to become a capital. The basic way to achieve this goal is to provide favorable environment for business, low taxes, and a talent pool of technically sound workers that have good knowledge base of the market. Below mentioned are some way forwards in attaining the above mentioned ambition in a country like Pakistan where basic necessities are hard to provide.

a. Youth is the main target whenever a new industry is growing or being set up [57] so students from the different educational background that is basically computer science and telecommunication disciplines can be involved in developed cyber security products that provide services needed according to the nations requirement and the current security posture of Pakistan.
b. Cyber security capacity can be established with the resources available and the professionals can be hired. They can collaborate with different private companies to develop indigenous products that suit best the requirements of the situation.

It is a long process and results can be achieved at least after five to ten years. As the dependency on technology is increasing, the dependency on security products is growing day by day as well. Hence, there is an urgent need to make an effort in this regard. If Pakistan will take a step today so we will be able to protect our critical infrastructure in future. It will open new avenues and job opportunities for cyber security students and professionals.

5.11 Implementation

The last stage of the strategy is perhaps how to implement and what are the required actions that need to be considered for effective implementation of the strategy. Another factor that is important is the cost of implementation along with the time required to complete any specific action. The costing is decided by the authorities and budget is decided on basis of the requirement of implementing any certain factor while considering how critical it is in the process. The ultimate goal is to keep the cost as realistic as possible so fruitful results are gained in an effective and efficient manner.

5.11.1 Immediate Actions- Phase A:

It is evident from the strategy that a number of actions mentioned in this chapter need to start immediately. The strategy is circling five main factors through which cyber capacity building of any state is increased so that the two actions that need to start early are mentioned below:

a. Designing a comprehensive national awareness program for cyber security capacity building, including all users of electronic system from private to government sector.
b. Human resource development that will have the required technical know-how and different certifications to implement the provision of strategy. All skills gained should be inculcated by every individual in their respective job description.

5.11.2 Mandatory Actions- Phase B:

Phase B is as important and critical as phase A but the only difference lies in the urgency of the situation in which they should be implemented. As every action needs to be implemented but it is not feasible for a country like Pakistan to start implementing all action at one time so the best option is to implement the strategy in phases. Mandatory actions are listed below:

a. Curriculum to grow cyber literacy should be designed by the information security professional incorporation with the individuals involved in education system.
b. Establishment of the research center and gaining resources from the international organization by presenting the country's current security scenario.

The document provides full synopsis of the strategy that Pakistan can deploy to safeguard its digital citizens. However for right implementation of strategy, each action should be analyzed and resources can be allocated for implementation accordingly.

5.12 Conclusion

The chapter provides the essence of the research that was to develop cyber security capacity building strategy which was a tedious task in the current cyber landscape of Pakistan. It provides the basic guidelines and the approach used to cater the cyber security capacity building issues. Personnel that will be required in case of smooth functioning of strategy are mentioned. A generic overview of the strategy is given at the start to give the reader a clear picture of the framework. Then every aspect is discussed in detail by providing solutions to the security issues faced by the cyber space. The chapter is concluded by providing the implementation approach that is required and that compliments the circumstances.

Chapter 6

CONCLUSION

6.1 Introduction

The cyber landscape is going through an evolutionary phase where new challenges are faced by technology as it is in evolving phase and adversaries are acting to exploit it. The strategy proposed in this research provides a range of capabilities, policies, and techniques that each new challenge arisen is responded flexibly and quickly. If a state fails to act effectively the threat might grow to outpace the ability to protect against these respective threats. The chapter shed light on the concluding statement of the research while providing what is achieved already and what is next in this research. At the end of the chapter future directions are discussed that what new avenues can be explored while keeping this research as a baseline.

6.2 Objective Achieved

Below mentioned are the research objectives that were specified at the start of this research. The main objectives of the thesis were to:

a) Assess the maturity level in accordance with cyber crime and security in Pakistan
b) Comparative analysis of capacity building regime of different countries
c) Formulate the national strategy for cyber security capacity building

Chapter 4 is catering the first research objective as all the results of the survey conducted are mentioned and elaborated where required. In the same manner chapter 3, is catering the second research objective as comparative analysis was done and depending on the comparison this research generated and specified recommendations that can be adopted by counties striving to construct their cyber capacity building culture in an advanced and adequate manner. Chapter 5 is catering the third research objective Figure 6.1 will provide a detailed demonstration of the cyber security capacity building strategy.

6.3 Limitation

The Cyber capacity building is a strenuous task as Pakistan is an underdeveloped country [11] so developing and implementing a national strategy is not an easy task. Standards of cyber security are usually included as a factor in capacity building framework of ITU. In

Pakistan even the PECA was passed in 2015and cyber security standards are not a priority or even in the talk at this time. It is a very gigantic domain that cannot be touched as professionals from information technology, cyber security, and legal advisor are required to develop standards.

The foremost issue faced will be while implementing and gathering investment for the strategy. The human resource requirements can be a limitation too as it is very difficult to find skilled professionals that are willing to play a part in national capacity building. In the start, the government might not have the funds to execute each plan so a number of professionals need to voluntarily help the government in achieving this goal.

6.4 Future Directions

The world is continuously transforming through digitalization. As digital network is entering in different aspects of society so cyber security capacity building is required to broaden its horizons and discover new ventures in order to stay updated and combat against cyber crime. As this research does not focus on the legalization and does not include cyber security standards in capacity building. This research can be taken forward in this regard as listed below are some recommendations for the future to strengthen the cyber security capacity building within a state.

a) Advice the formulated cyber security standards to government agencies
b) Promote international standards compliance on business activities
c) Adoption of international standards according to threat environment of our country
d) Devise local relevant standards for secure use of cyber space

Another recommendation is that cyber capacity for all should be the future direction in this respect as infrastructure is the common source for developing any new Industry.

Cyber capacities can range from national policy to daily local practice, from the rapid response to crises to the long-term development process and from international collaborations to local expertise. Building global cyber capacities in a state will strengthen the global resilience and it can enable the citizens and organization to get more advantage in cyberspace opportunities. As mentioned in Chapter 5 section 5.10 about growing industry in cyber security and developing local products that can compete against international products and are of same standards while serving the same purpose. To achieve such strenuous objective the state needs to take initiative and build an infrastructure that lay the foundation.

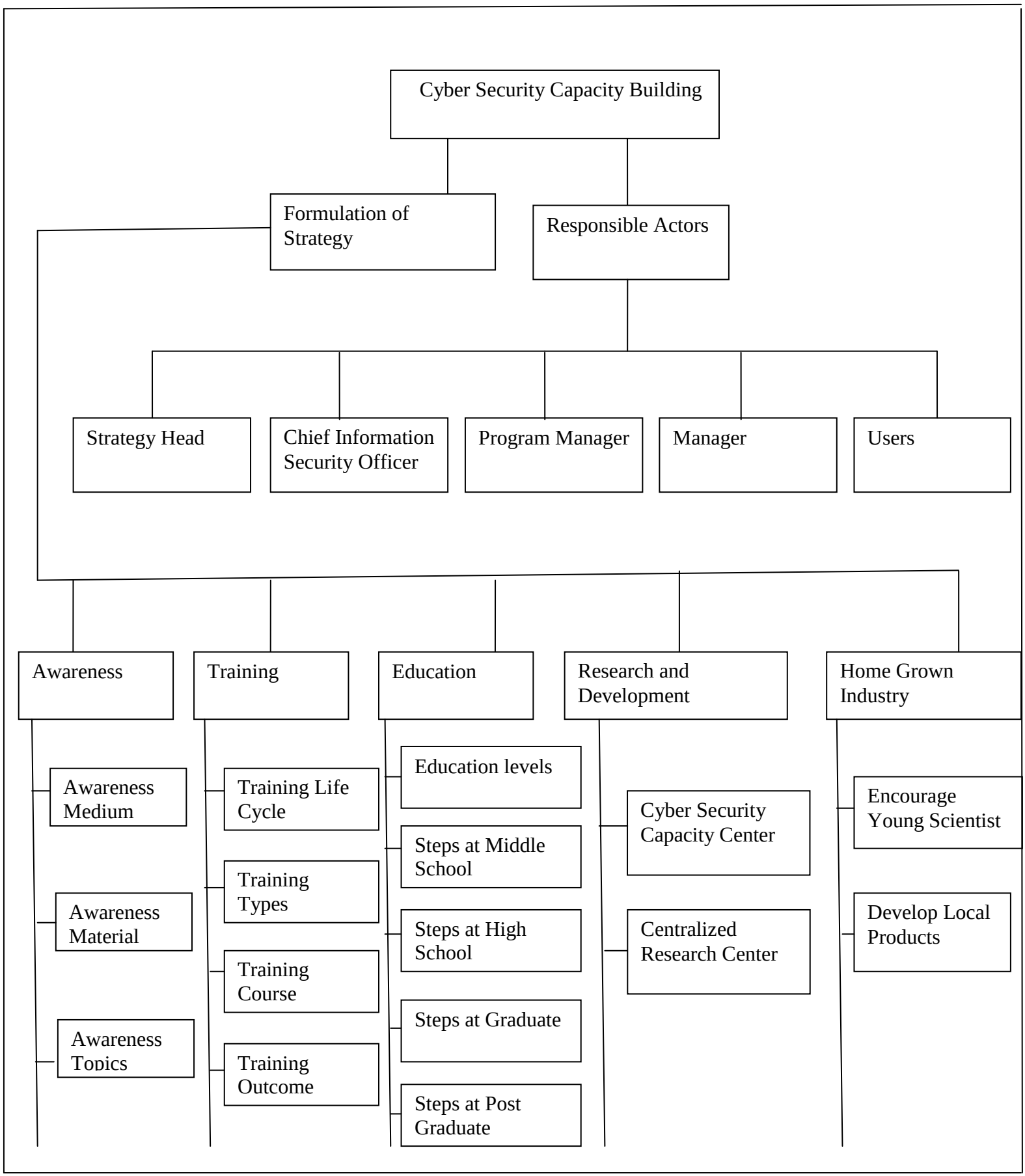

Figure 6.1 Cyber Security Capacity Building Strategy

6.5 Concluding Remarks

Cyber security is a vast domain and countries are spending billions to cater the threats it poses as mentioned in Chapter 3 section 3.5.10. Any progressing country should spends on cyber security in the same way as it spend on its defense in order to defend the national security. The latest trend today is cyber warfare and it is going on since the world became such digitilized and every operation became dependant on computer networks and internet. According to cyber security index document [4] it is concluded that some countries having large economies can be lower in ranking list than the countries having higher economy as Malaysia is on higher ranking than Canada [58] so technological advancement is not totally correlated with how advance that country is so in case of Pakistan there is hope that it can become a cyber security hub and it will have services that are digilent.

As Pakistan has no infrastructure or cyber security capacity building strategy acting at the moment or in development phase so guidance is taken from other countries that have the sophisticated infrastructure, standards and practices in place as done in this research. So because of difference in law, culture, governing system, the pace of cyber development and institutional structure efforts should be tailored according to the nation's cyber security capacity building needs. It is a long-term and continuous effort and process so in order to get fruitful results in future the seeds need to be sowed today. If Pakistan wants to compete with other developed nations in cyber security heterogenous initiatives in cyber security capacity building should be taken nationwide.

Security is a step that should be by default so it is inculcated in commodities and technologies then consumers and businesses can worry less about cyber security. In the most optimistic scenario and even in the best suitable conditions it would take time to develop cyber security posture. The strategy formulated in this research nonetheless provides means to transform the future security and safeguard prosperity of the nation in the digital era.

Appendix "A" –Cyber Maturity Assessment Questionnaire

Cyber Maturity Assessment

This survey is conducted by a student of NUST, Pakistan for research purpose in order to analyze the cyber maturity level in Pakistan.

Gender

- Male
- Female

Age

- 10 – 20
- 21 – 30
- 31 – 40
- 41 – 50
- 51 – 60
- above 60

What is your understanding of the term CYBER in "Cyber Security"?

- Umm, No idea
- Not sure, but i guess it has something to do with information security
- Other

Choose appropriate option	**Yes**	**No**
• Are you familiar with the Pakistan Electronic Crime Act (PECA 2016) enforced at the moment in Pakistan?		
• Do you share your pictures on social media e.g. Facebook, Instagram etc		
• Do you use bit locker or drive encryption		
• Is it safe to use public WI-Fi at shopping malls, airport etc		

Which URL would you use to open Facebook

- http://facebook.com
- https://faceboook.com
- none

Which of the given passwords is most secure?

- Apple26Mango
- Uweplk&1
- 5ea123

Which of the following circumstances would you treat as suspicious?

- Email/ phone call from your bank's representative asking for credit card information
- Email from government employee with email address pak.gov@gmail.com
- Both

Which national organization would you contact in case you find your Facebook profile hacked?

- No idea
- There is no such national organization in Pakistan that can deal with it
- other

BIBLIOGRAPHY

[1] "Global Commission on Internet Governance", *Centre for International Governance Innovation*, 2017. [Online]. Available: https://www.cigionline.org/initiatives/global-commission-internet-governance

[2] *Pakistan electronic crime act*, 1st ed. government, 2016 [Online]. Available: http://www.na.gov.pk/uploads/documents/1470910659_707.pdf. [Accessed: 08- Apr- 2018]

[3] z. iqbal, "Cyber security in Pakistan–myth or a reality", *pakistan observer*. 2018 [Online]. Available: https://pakobserver.net/cyber-security-Pakistan-myth-reality/. [Accessed: 08- Apr- 2018]

[4] G*lobal cyber security index*. international telecommunication union, 2017, pp. 71-75 [Online]. Available: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

[5] *Building Community Capacity*. Scottish Government, 2007, p. 6 [Online]. Available: http://www.scdc.org.uk/media/resources/what-we-do/building-comm-cap/building_community_capacity_resource_for_cld.pdf. [Accessed: 17- Apr- 2018]

[6] A. Klimburg and H. Zylberberg, *Cyber Security Capacity Building: Developing Access*. Norwegian Institute of International Affairs, 2015, pp. 8-9 [Online]. Available: https://www.files.ethz.ch/isn/195765/NUPI_Report_6_15.pdf. [Accessed: 17- Apr- 2018]

[7] Top 25 Developed and Developing Countries", *Investopedia*, 2017. [Online]. Available: http://www.investopedia.com/updates/top-developing-countries

[8] Enisa.europa.eu. (2015). *Good Practice Guide on National Cyber Security Strategies — ENISA*. Retrieved 16 December 2015, from https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/good-practice-guide-on-national-cyber-security-strategies

[9] B. Lee, "The Organization of American States", *council foreign relation*. 2018 [Online]. Available: https://www.cfr.org/backgrounder/organization-american-states. [Accessed: 19- Apr- 2018]

[10]"United Nations Millennium Development Goals", *Un.org*, 2018. [Online]. Available: http://www.un.org/millenniumgoals/. [Accessed: 17- Apr- 2018]

[11]. Avena and V. Grebennikov, *Microsoft Security Intelligence Report*, 22nd ed. micosoft, 2017 [Online]. Available: https://www.microsoft.com/en-us/security/Intelligence-report. [Accessed: 05- Dec- 2017]

[12] One in Four Computers in Pakistan are Attacked by Malware: Microsoft", *Propakistani.pk*, 2017. [Online]. Available: https://propakistani.pk/2017/09/19/one-four-computers-pakistan-attacked-malware-microsoft/. [Accessed: 05- Dec- 2017]

[13] "Cyber security and Pakistan - PakObserver", *PakObserver*, 2017. [Online]. Available: https://pakobserver.net/cyber-security-and-pakistan/. [Accessed: 11- Dec- 2017]

[14] [Online]. Available: https://www.quora.com/What-is-a-list-of-Pakistani-sites-hacked-by-Indian-hackers. [Accessed: 11- Dec- 2017]

[15] Pakistani Ministries websites hacked by Indian Hackers", *TechJuice*, 2017. [Online]. Available: https://www.techjuice.pk/pakistani-ministries-websites-hacked-by-indian-hackers/. [Accessed: 11- Dec- 2017]

[16] Cybercrime", *PwC*,2017.[Online].Available:https://www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey/cybercrime.html.

[17] Cyber Security Strategies Documents (Australia, Canada, Czech Republic, Estonia, France, Germany, India, Iran, Israel, Japan, Malaysia, Netherlands, New Zealand, Egypt, South Korea UK, and the USA). CCDOE.

[18] Capacitybuilding", *En.wikipedia.org*,2017.[Online].Available:https://en.wikipedia.org/wiki/Capacity_building

[19] "cybersmart.gov.au", *Amta.org.au*,2017.[Online].Available:http://www.amta.org.au/pages/Cybersmart

[20] Available: https://www.stopthinkconnect.org/.

[21] get cyber safe", 2017. [Online]. Available: https://www.getcybersafe.gc.ca/index-en.aspx

[22] "Mauritian National Computer Security Incident Response Team - Home", *Cert-mu.govmu.org*, 2018. [Online]. Available: http://cert-mu.govmu.org/English/Pages/default.aspx. [Accessed: 08- Apr- 2018]

[23] "JPCERT Coordination Center", *Jpcert.or.jp*. [Online]. Available: https://www.jpcert.or.jp/english/.

[24] Mcmc.gov.my [online] https://www.mcmc.gov.my/

[25] "Singapore master plan", 2016 [Online]. Available: https://www.sbs.ox.ac.uk/cybersecurity capacity/system/files/NationalCyberSecurityMasterplan%202018.pdf

[26] CNN, "Georgia Russia Conflict Fast Facts", 2018 [Online]. Available: https://edition.cnn.com/2014/03/13/world/europe/2008-georgia-russia-conflict/index.html. [Accessed: 08- Apr- 2018]/.

[27] "Information Security Human Resource Development Program", Information Security Policy Council, 2011 [Online]. Available: https://www.nisc.go.jp/eng/pdf/hrd_pg_eng.pdf.

[28] S. Baunfire.com, "National Cyber Security Alliance | StaySafeOnline.org", *Staysafeonline.org*. [Online]. Available: https://staysafeonline.org/.

[29] The National Cybersecurity Workforce Framework | Homeland Security", *Dhs.gov*, 2017. [Online]. Available: https://www.dhs.gov/national-cybersecurity-workforce-framework. [Accessed: 30- Aug- 2017]

[30] CyberSAFE", *Cybersafe.my*. [Online]. Available: http://www.cybersafe.my/en/

[31] W. Newhouse and S. Keith, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*. NIST, 2014 [Online]. Available: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-181.pdf. [Accessed: 08- Apr- 2018]

[32] "COMPUTER SECURITY RESOURCE CENTER", NIST, 2018 [Online]. Available: https://csrc.nist.gov/topics. [Accessed: 19- Apr- 2018]

[33] "Teacher Resources | NICERC", *Nicerc.org*, 2016. [Online]. Available: https://nicerc.org/pd/teacher-resources/

[34] C. University, "Homepage - CMU - Carnegie Mellon University", *Cmu.edu*, 2018. [Online]. Available: https://www.cmu.edu/. [Accessed: 08- Apr- 2018]

[35] T. Antonio, "Welcome to The University of Texas at San Antonio | UTSA", *Utsa.edu*, 2018. [Online]. Available: https://www.utsa.edu/. [Accessed: 08- Apr- 2018]

[36] "Norwich University", *Norwich University*, 2018. [Online]. Available: http://www.norwich.edu/. [Accessed: 08- Apr- 2018]

[37] "Ed. D. in Educational Leadership - School of Education - Syracuse University", *Soe.syr.edu*, 2018. [Online]. Available: http://soe.syr.edu/academic/teaching_and_leadership/graduate/PhD/educational_leadership/. [Accessed: 08- Apr- 2018]

[38] I. Team, "Mississippi State University", *Mississippi State University*, 2018. [Online]. Available: https://www.msstate.edu/. [Accessed: 08- Apr- 2018]

[39] "George Mason |", *Www2.gmu.edu*, 2018. [Online]. Available: https://www2.gmu.edu/. [Accessed: 08- Apr- 2018]

[40] "A comprehensive research university and experiential learning leader in Philadelphia, PA - Drexel University", *Drexel University*, 2018. [Online]. Available: http://drexel.edu/. [Accessed: 08- Apr- 2018

[41] "Rochester Institute of Technology (RIT)", *Rochester Institute of Technology (RIT)*, 2018. [Online]. Available: https://www.rit.edu/. [Accessed: 08- Apr- 2018]]

[42] E. Caroline Campbell, U. Center for Population Health Sciences | Seminar Series: Rayid Ghani, D. Series and W. Ellington, "Stanford University", *Stanford University*, 2018. [Online]. Available: https://www.stanford.edu/. [Accessed: 08- Apr- 2018]

[43] "Welcome to the University of South Florida | Tampa, FL", *Usf.edu*, 2018. [Online]. Available: http://www.usf.edu/. [Accessed: 08- Apr- 2018]

[44] *CYBERWELLNESS PROFILE REPUBLIC OF ESTONIA*. ITU, 2017, p. 2 [Online]. Available: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Estonia.pdf.

[45] *Homeland Security Advanced Research Projects Agency*. DHS Science and Technology Directorate, 2015 [Online]. Available: https://www.dhs.gov/sites/default/files/publications/HSARPA%20Fact%20Sheet-508.pdf

[46] *Executive Summary ofReview ofthe Unauthorized Disclosures ofFormer National Security Agency Contractor Edward Snowden*. us house of representatives, 2016, pp. 2-3 [Online]. Available: https://intelligence.house.gov/uploadedfiles/hpsci_snowden_review_-_unclass_summary_-_final.pdf. [Accessed: 08- Apr- 2018]

[47] "GLOBAL CYBER SECURITY CAPACITY CENTER The Global Cyber Security Capacity Centre", *Oxford Martin School*. [Online]. Available: http://www.oxfordmartin.ox.ac.uk/cybersecurity/.

[48] Why Israel dominates in cyber security", *Fortune.com*, 2017. [Online]. Available: http://fortune.com/2015/09/01/why-israel-dominates-in-cyber-security/.

[49] *CYBER SECURITY IN SINGAPORE*. RSIS, 2016, pp. 18-20 [Online]. Available: https://www.rsis.edu.sg/wp-content/uploads/2016/12/PR170217_Cybersecurity-in-Singapore.

[50] "How to Surf the Internet Safely - Protecting Your Kids on the Internet", *Safesurfingkids.com*, 2018. [Online]. Available: http://www.safesurfingkids.com/. [Accessed: 08- Apr- 2018]

[51] "Cyber Security Awareness Alliance", *Cyber Security Agency*, 2018. [Online]. Available: https://www.csa.gov.sg/gosafeonline. [Accessed: 08- Apr- 2018]

[52] P. Cléroux, "2018 economic outlook: Global growth brings good news for Canadian entrepreneurs", *bdc*. 2018 [Online]. Available: https://www.bdc.ca/en/blog/pages/2018-economic-outlook-global-growth-brings-good-news-canadian-entrepreneurs.aspx. [Accessed: 15- Apr- 2018]

[53] P. Bowen and J. Hash, *Information Security Handbook: A Guide for Managers*. us department of commerce,2006,pp.8-9[Online].Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf. [Accessed: 19- Apr- 2018]

[54] "Types of Training", libraries, Human Resource Management, 2018 [Online]. Available: http://open.lib.umn.edu/humanresourcemanagement/chapter/8-2-types-of-training-2/. [Accessed: 19- Apr- 2018]

[55] D. Phutela, "A Review on Human Resource Planning", *International Journal of Engineering and Techniques*, vol. 2, no. 1, pp. 1-2, 2016 [Online]. Available: http://www.ijetjournal.org/Volume2/Issue1/IJET-V2I1P15.pdf. [Accessed: 19- Apr- 2018]

[56] Global Cybersecurity Index (GCI) 2017. 2017, pp. 45-47 [Online]. Available: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf. [Accessed: 19- Apr- 2018]

[57] The Role of the Youth in Nation Building", *teen ink*. 2013 [Online]. Available: http://www.teenink.com/hot_topics/all/article/533316/The-Role-of-the-Youth-in-Nation-Building-/. [Accessed: 19- Apr- 2018

[58] "GDP Annual Growth Rate", trading economics, 2018 [Online]. Available: https://tradingeconomics.com/country-list/gdp-annual-growth-rate. [Accessed: 19- Apr- 2018]