Cyber Security Norms in South Asia: A Case Study of Pakistan Cyber Space Security and Analysis

By

Hanzala Jahangir

Thesis submitted to the faculty of Center of International Peace and Stability, National University of Sciences and Technology, Islamabad in partial fulfillment of the requirements for the degree of MS in Peace and Conflict

Aug 2018

CERTIFICATE

This is to certify that **Hanzala Jahangir** Student of **MSPCS-16** Course Reg.NO: **NUST201664807MCIPS79516F** has completed her MS Thesis title **"Cyber Security Norms in South Asia: A Case Study of Pakistan Cyber Space Security and Analysis"** under my supervision. I have reviewed her final thesis copy and I am satisfied with her work.

____

Thesis Supervisor

(Brig Tughral Yamin, PHD)

Dated: __________________

Plagiarism Certificate (Turnitin Report)

This thesis has been checked for Plagiarism. Turnitin report endorsed by Supervisor is attached.

Signature of Student

Registration Number

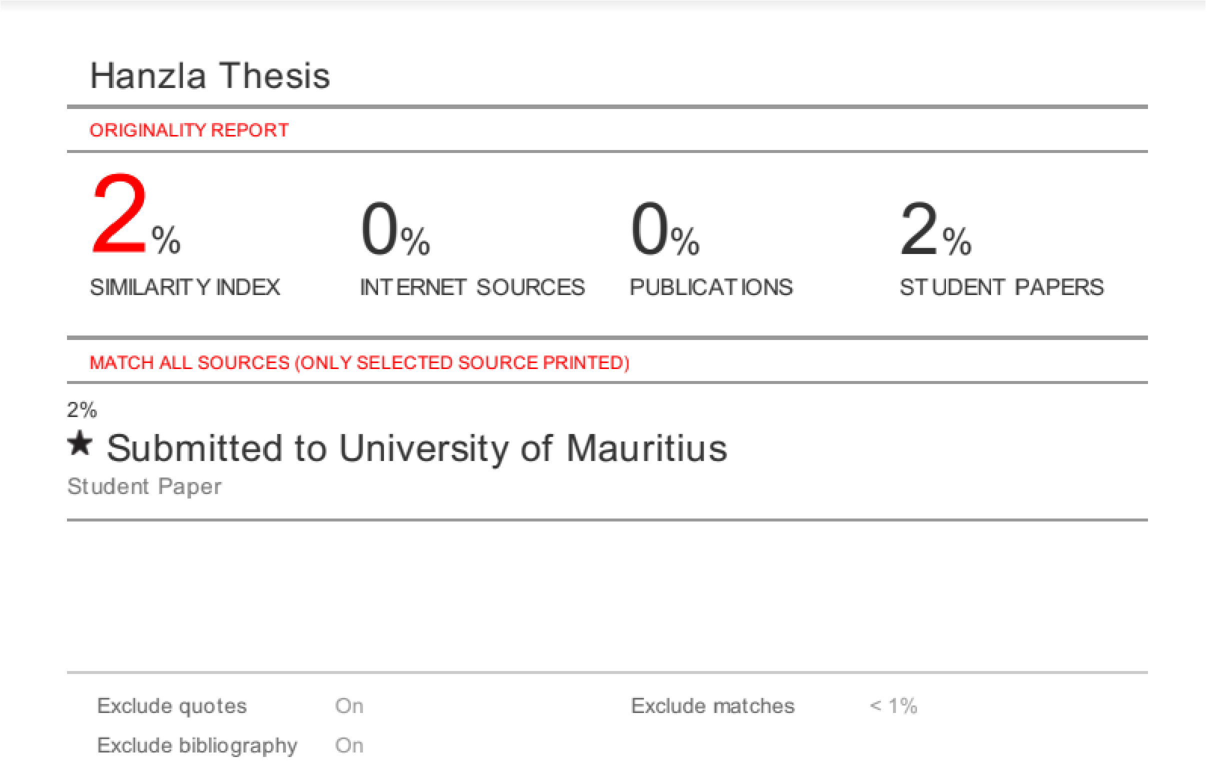
NUST201664807MCIPS79516F

Signature of Supervisor

Copyright Statement

contrary, and may not be made available for use by third parties without the written permission of the CIPS, which will prescribe the terms and conditions of any such agreement.

- **Further information on the conditions under which disclosures and exploitation may take place is available from the Library of Center for International Peace and Stability (CIPS), Islamabad.**



Hanzla Thesis

ORIGINALITY REPORT

2%	0%	0%	2%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

MATCH ALL SOURCES (ONLY SELECTED SOURCE PRINTED)

2%

★ Submitted to University of Mauritius

Student Paper

Exclude quotes	On	Exclude matches	< 1%
Exclude bibliography	On		

ABSTRACT

A strong cyber security is very important for any state to flourish and to develop economically, politically and socially. It forms the intrinsic part of progress and development of any country. The unparalleled challenges in the global world make it difficult to detect cyber-attack techniques, posing serious threats to the states confidentiality, national security, stability and economy. The mysterious challenges to the global and domestic computer networks can play havoc with the function of the government or the private organization. Almost all countries of the world are devising policies, cybersecurity laws and confidence building measure (CBM) with each other to protect the critical infrastructure resources and to protect all sort of digital information from getting lost. Every country endeavors to protect its cyberspace. Pakistan is a developing country and lags way behind developed countries in the domain of cybersecurity. This adds to its security dilemma, since it is a major victim of cyber terrorism, cyber-attcaks and cyberwarfare. Unfortunately it has no national policies to regulate and protect its information technology structure. There is no national cybersecurity strategy or governance framework to protect its national cybersecurity mechanism from cyber-attacks.

The aim of this research work is to provide a framework for cybersecurity policies in Pakistan and suggest proper regulation at national level. In order to compare different cyber security strategies of various countries I have consulted international best practices. I have also analyzed cyber threat landscape of Pakistan and examined the existing cyberlaws to find out technical and legal loopholes. I have surveyed the steps taken for the capacity building of the cyber security at the national level. My research highlights the vulnerabilities of the cyber infrastructure of Pakistan. The main delivery of the research is to suggest cybersecurity strategy policy document that explain national cyber vision and propose a high level cybersecurity plan in the best possible way to prevent, identify the cyber threat and to respond quickly in the effective way to cyberspace incidents.

ACKNOWLEDGEMENTS

All praises and glory to Allah Almighty, who gave me strength to accomplish this important task. I offer utmost gratitude to my thesis Supervisor, Dr Brig Tughral Yamin, for his excellent guidance and encouragement. This research wouldn’t have been possible without his expert advice, unfailing patience and invaluable efforts.

I am indebted to Narmeen Shafqat (lecturer Military College of Signals) and Usama Khilji (digital right activist) and Khawar Khokhar (Principal Sir Syed College) for taking out time through their busy schedules for lively discussions and insightful comments. I also owe a dept of gratitude to my mother, Mrs Abida Jahangir for her help with the referencing and proof reading and deeply appreciate my instructors Dr Waqas Ahmed and Dr Muhammad Makki for constant encouragement and practical advice.

Lastly, I am very grateful to my family and well-wishers for their admirable support.

TABLE OF CONTENTS

CHAPTER NO 1: ITNRODUCTION

CHAPTER NO 2: LITERATURE REVIEW

CHAPTER NO 3: COMPARATIVE ANALYSIS OF NATIONAL CYBER SECURITY STRATEGIES

CHAPTER NO 4: PAKISTAN'S CYBER THREAT LANDSCAPE

CHAPTER NO 5: DOMESTIC CYBER LAWS AND E-REGULATIONS IN PAKISTAN

CHAPTER NO 6: MEASURES TAKES FOR CYBER SECURITY CAPACITY BUILDING IN PAKISTAN

CHAPTER NO 8: CRITICAL ANALYSIS OF CYBER-SPACE SECURITY AND PROPOSED CYBER SECURITY STRATEGY FOR PAKISTAN

ACRONYMS

AES	Advance Electronics Signatures
APCERT	Asia Pacific Computer Emergency and Response Team
APNIC	Asia Pacific Network Information Centre
APSIRC	Asia-Pacific Security Incident Response coordination
APT	Advance Persistent Threat
ATM	Automated Teller Machine
BGP	Border Gateway Protocol
BYOD	Bring Your Own Device
C2S	Command and Control Server
CBC	Cipher Block Chaining

CCM	Computers Cleaned Per Mile
CCNA	Cisco Certified Network Associate Security
CCNP	Cisco Certified Network Professional Security
CEH	Certified Ethical Hacking
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CGEIT	Certified in the Governance of Enterprise IT
CHFI	Computer Hacking Forensic Investigation
CI	Critical Infrastructure
CIA	Central Intelligence Agency
C-I-A	Confidentiality, Integrity, Availability
CIIP	Critical Information Infrastructure Protection
CISA	Chief Information System Auditor
CISO	Chief Information Security Officer
CISSP	Certified Information System Security Officer
CNIC	Computerized National Identity Card
COD	Cash On Delivery
CRISC	Certified in Risk and Information System Control
CISM	Certified Information Security Manager
CSIRT	Computer Security Incident Response Team
CSP	Certified Service Providers
CSP	Cyber Secure Pakistan
CTF	Capture the Force
DC	Data Centre
DDOS	Distributed Denial of Service
DNCR	Do Not Call Registers
DNS	Domain Name System

DOS	Denial of Service
DRP	Disaster Recovery Plan
ECES	Ec-Council Certified Encryption Specialist
ECHI	Ec-Council Certified Incident Handling
ECP	Election Commission of Pakistan
ECSA	Ec-Council Certified Security Analyst
ECSO	Ec-Council Certified Security Officer
ECSP	Ec-Council Certified Secure Programmer
ECSS	Ec-Council Certified Security Specialist
EDRP	Ec-Council Disaster Recovery Professional
ENISA	European Union Agency for Network and Information Security
ER	Encounter Rate
ES	Electronic Signatures
ETO	Electronic Transaction Ordinance
EU	European Union
FBI	Federal Bureau of Investigation
FBR	Federal Board of Revenue
FIA	Federal Investigation Agency
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
GAC	Government Advisory Committee
GIAC	Global Information Assurance Certification
HEC	Higher Education Commission
HMAC	Hash Message Authentication Code
HTCN	High Tech Crime Network
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol

ICANN	Internet Corporation for Assigned Names and Numbers
ICMP	Internet Control Message Protocol
ICT	Information and Communication Technology
IDS	Intrusion Detection System
IE	Internet Explorer
IEEE	Institute of Electrical and Electronics Engineers
IMCEW	Inter-Ministerial Committee for the Evaluation of Websites
IP	Internet Protocol
IPOP	Internet Policy Observatory Pakistan
IPS	Intrusion Prevention System
IS	Information Security
ISACA	Information System Audit and Control Association
ISACS	Information Sharing and Analysis Center
ISC^2	International Information Systems Security
ISMS	Information Security Management System
ISO	Information Security Officer
ISP	Internet Service Provider
ISPA	Internet Service Providers Association of Pakistan
IT	Information Technology
ITU	Information Telecom Union
MNP	Mobile Number Probability
MOIT	Ministry of Information Technology
MSRT	Malicious Software Removal Tool
NAB	National Accountability Bureau
NADRA	National Database and Registration Authority
NATO	North Atlantic Treaty Organization
NCSS	National Cyber Security Strategies

NDU	National Defense University
NESCOM	National Engineering and Scientific Commission
NIMIS	National Institute of Management and Information Security
NISG	NUST ISACA Student Group
NIST	National Institute of Standards & Technology
NOC	Network Operation System
NR3C	National Response Centre for Cyber Crimes
NSA	National Security Agency
NSS	National Security Standards
NTC	National Telecommunication Cooperation
NTISB	National Telecom and Information Technology Security Board
NTN	National Tax Number
NUST	National University of Sciences and Technology
OGDCL	Oil and Gas Development Company Limited
OS	Operating Systems
P2P	Peer-To-Peer
PASHA	Pakistan Software Houses Association
PBX	Private Branch Exchange
PC	Personal Computer
PECO	Prevention of Electronic Crimes Act
PEMRA	Pakistan Electronic Media Regulatory Authority
PI	Privacy International
PIA	Pakistan International Airlines
PIE	Pakistan Internet Exchange
PIPS	Pakistan Institute of Parliamentary Services
PISA	Pakistan Information Security Association
PPP	Public Private Partnership

PTA	Pakistan Telecommunication Authority
PTCL	Pakistan Telecommunication Company Limited
R&D	Research and Development
RAW	Research and Analysis Wing
SAARC	South Asian Association for Regional Corporation
SAPT	Security Assessment & Penetration Testing
SCADA	Supervisory Control and Data Acquisition
SCP	Security Certified Program
SECP	Security and Exchange Commission of Pakistan
SOPS	Standard Operating Procedures
TCP	Transmission Control Protocol

CHAPTER 1

INTRODUCTION

1.1 Introduction

Internet world has converted the world into a global village and tools of information technology (IT) have become indispensable part of our lives. Digital components of our daily use and the associated IT tools /products and embedded processors that connect and control the network of computer or create, store, modify, use and exchange digital information collectively makes up the “Cyberspace”. It is referred to the fifth domain of the warfare as nation states, terrorists, nongovernment organizations, hacktivists, criminals attack the cyber space for their own benefits. It is very grave issue to consider for national security but Pakistan has made no policy for it while other countries have defined policy for it.

This chapter will specifically highlight the problem statement, objectives, significance, of the research and its scope with the aim to safeguard the national cyberspace of Pakistan. The definitions of the cyber terminologies have also been added, followed by the description of how the thesis has been organized.

1.2 **Problem Statement**

The Pakistani cyberspace is extremely susceptible to foreign espionage, cyber-attacks and cyber terrorism because domestic IT laws and regulations have been formulated without meaningful inputs of the industry stakeholders and lack deep research of national cyber threat landscape. The major drawback of this is that it has created an uncertain cyber environment that decreases the growth of e-commerce, increases grey traffic and inhibits foreign investment. It also poses threat to the critical cyber infrastructures, nuclear command control systems and the burgeoning IT industry. Every country has different cyber security framework and cyber threat landscape, therefore, their laws and policies cannot be adopted without suitable modifications. The problem is: Why is there no proper national cyber policy? What is the threat landscape of Pakistan? What can be the best possible strategy to increase the cyber security framework in Pakistan?

1.3 **Research Objective**

The only solution to the aforementioned problem is to develop and effectively implement a well-structured and well defined cyber security policy after a thorough analysis of Pakistan’s threat landscape and international best practices and adopt a multi-stakeholder approach in order to ameliorate the confidence of citizens and public sector organizations in the use of ICT devices/products. Hence the objectives of this research study are as follows:

a. Thoroughly review the cyber threat landscape of Pakistan in order to highlight the emerging cyber threats and technical mal-practices of the cyber community.
b. To detect the technical and legal loopholes of domestic cyber laws and regulations
c. Conduct a survey of the measures taken for cyber security capacity building at national level
d. Throw light on why the government is so unconcerned about this critical issue of cyber security when even the countries like Malaysia, Kenya and Bangladesh have formulated their cyber security strategies
e. Carry out comparison of various national strategies cyber security strategies and derived the best cyber security strategies.
f. Formulate the draft of the national cyber security strategy in accordance with the conducted critical analysis, national needs, international best security practices and cyber security strategy guidelines of international telecommunication union (ITU), European Network and Information Security Agency (ENISA), National Institutes of Standard and Technology (NIST), North Atlantic Treaty Organization (NATO).

1.4 Scope of Research

The research applies to the whole of the national cyber space with the exception of defense forces and nuclear installations, since they are already running in a highly secure environment and their confidential details cannot be disclosed in an academic thesis.

1.5 Significance of Research

The increasing dependence on ICT based products and services has brought along persistent threats that in the absence of any adequate cyber laws or strategy are critical to the thriving IT industry of Pakistan, National Information infrastructure, Nuclear programmed the citizen’s fundamental right of privacy. This research will provide considerable benefits within governmental department, ICT domain, academia and other sectors as listed below.

a. The critical analysis of cyberspace will help the cyber community, industry and the government to identify the persistent cyber threats faced by Pakistan, the identification of cyber security challenges will help to improve knowledge and decision-making capabilities.
b. The development of cybersecurity policy will help the government to devise a defense mechanism against cyber-attacks (e.g. cyber-warfare, international terrorist, foreign sabotage, intelligence activities, inside threats, espionage), thereby providing resilient and interoperable cyber space suitable for communication, e-governance and e-commerce.
c. In the long run, there will be following undisputed benefits to the Pakistani cyber community,

1. There will be increased transparency in the cyber security policy promoting anti-corruption in the government and industry.
2. There will be safe reliable ICT which will increase organizational performance both at private and public sector, boost up public's confidence in e-commerce leading to increase in more sustainable economic growth.
3. There will be increase in collaborations both at governmental and international level to improve Pakistan IT and provide with incentives to be the parts of the formation of international cyber security laws.

1.6 Research Methodology

I have used qualitative research methodology in the following manner:

1.6.1 Literature Review

This literature review will cover existing cyber laws and policies, the publically available executive-level cyber strategies of various countries, critical cyber landscape of Pakistan, NIST standard guidelines, the international strategy guidelines and pertinent journals and research papers.

1.6.2 Surveys

This research is based on following surveys.

a. Cyber Security Degree Programs currently offered in universities.
b. National initiatives taken for protecting cyberspace.
c. Organizations accreditation and compliance to latest security standards.
d. Comparison of various national cyber security strategies.
e. Information Security (IS) service providers.
f. Semi-structured interviews with Cyber Security Governmental Officials and Digital Activist.

1.6.3 Types of Data

The research contains both primary and secondary data. The primary data includes face to face interviews and surveys. The secondary data is mostly derived from the cyber security journals and research papers available on the Internet.

1.6.4 Study Area

The research study includes governments departments dealing with cyber security and law enforcement agencies, the parliament making cyber laws, the public sector cyber security departments, the digital civil organizations.

1.6.5 Critical Analysis of the Cyber Security

According to the literature review, surveys, interviews, a consolidated critical analysis of the cyber space landscape of Pakistan was carried out. This includes the critique of major legal loopholes in the domestic Cyber Laws, Analysis and formulation of threat landscape, and highlighting major cyber threats Pakistan facing these days.

1.6.6 Formulation of National Cyber Security Policy

This research includes proposed cyber security strategy derived from the results of the primary and secondary data including study of the best international practices in cyber security strategy and guidelines of NIST, ITU, and ENISA. The following diagram in literature review elaborately explains the research approach.

1.7 Key Terminologies

The major key terms used in this research i.e. cyber security, critical infrastructure, cyber security strategy, cyberspace and cyber laws have been defined below. These definitions apply to the complete research work.

1.7.1 Cyberspace

It is decentralized digital domain consisting of all the computer networks, computing devices, software, control devices, the internet, ICT resources, and the constituent information exchanged, processed, stored or modified within any of these.

1.7.2 Cyber Security

It is basically IT security taking protective, predictive, responsive and preventive measures to safeguard the cyber system from damage, modification and corruption, the resident information from unauthorized access and the soft wares and e-services from being disrupted.

1.7.3 Cyber Laws

They are basically referred as computer laws, legal issues related to the technologies, cyber system and the internet like information access, intellectual property, privacy of data, fundamental rights of netizens etc., thereby creating a secure cyber environment to reduce the damage of cyber-attacks.

1.7.4 Cybercrime

It is basically electronic crime referred as any computer offence and criminal activity whereby any ICT devices or the networks act as tool, source, target or place of the offense. Injections of malware, identity theft, denial-of-service attack, cyber terrorism, phishing, cyber stalking, cyber espionage, etc. are all examples of a cybercrimes.

1.7.5 Critical Cyber Infrastructure

An information system, whether virtual or physical, whose destruction, inoperability, or compromise can destructively affect the national security, public health, economy or the environment comes under the definition of Cortical Cyber Infrastructure.

1.7.6 National Cyber Security Strategy

It is the national cyber action plan at the high level that depicts the vision of the country pertaining to the cyber security and develops measures to improve the prevention, detection, recovery and response of the national cyber-attack.

Literature View

2.1 Introduction

Cyber security has become the topic of very important discussion in the contemporary era .Every developed country consider cyber space security more important than national security as this advanced technology modern world totally changed the tools of war, China, Russia, America etc. have the most advanced cyber security mechanism and they are also among those countries which have advanced tools for hacktivism, virus installations. This chapter will list down the latest advanced information t technology in Pakistan including internet statistics and current technology trends so far, describe the research papers, strategy guidelines, review articles, books, public global strategic documents, cyber laws that have been consulted for caring out the research work.

2.2 Pakistan Cyberspace

The national cyberspace is the area government controls, owns, operates, and encompasses the following:

a. Physical ICT infrastructure, devices and products.
b. Computer networks.
c. The internet.
d. Computing devices and the pertinent software and services.
e. Digital information processes, stored and transmitted in any of these.

The national cyberspace therefore stretches from the undersea cables that land into Pakistan to the ICT users and devices that make use of it .The rate of adoption and use of the digital information technology is quite low as Pakistan is a new member of the cyber world. (ITU, 2015) The broadband internet connections and the satellite internet etc. are used by only around 18.4 % of the Pakistani population.

In the cyber world, the international connectivity of Pakistan with other countries is very less through internet satellite while more through the undersea cables .Pakistan has an overall internet bandwidth of 360Gbps. The cyber citizen receives internet services through the channel depicted in figure 2.1 below.

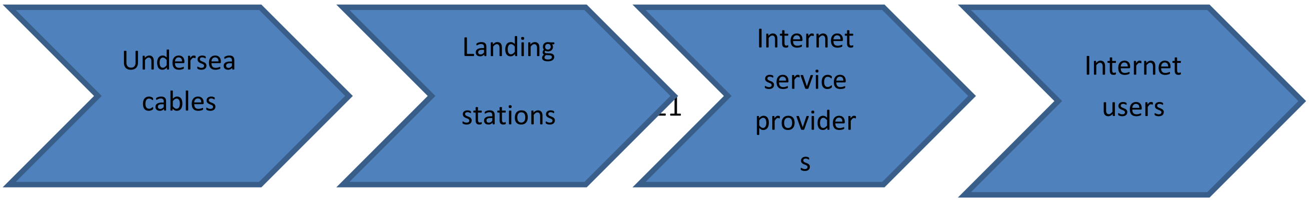


Figure 2.1 Internet connectivity through under sea cables

2.3 Undersea Cables:

Pakistan gets internet connectivity through the following cables.

a) SEA-ME-WE-3(South East Asia –Middle East and Western Europe -3)
b) SEA-ME-WE-4
c) I-ME-WE
d) Tran’s world associates (TWA-1)
e) The recently introduced first ever ground based Pak-China Optical Fiber as a result of China Pakistan Economic Corporation
f) There is also PakChina optical Fiber link between Khunjerab Pass on the China-Pakistan border and the city of Rawalpindi about 820 Km long it is land based.

2.3.1 Landing Stations

The landing stations i.e. PTCL control the internet connectivity through the undersea cables in Pakistan .It operate the Pakistan Internet Exchange (PIE) to provide peering points for ISPs to exchange internet traffic . (Attaa, 2016) There is also another landing station Trans world which is the sister concern of Mobil ink and has major operators like Wateen, World call, Wi_Tribe, Nayatel etc. on its network. (Internet | Pakistan Bee – Part 4, 2016)

2.3.2 Internet Service Providers (ISPs)

There are around 50 internet service Providers within Pakistan that regulates and monitors the internet. Amongst these PTCL,Wateen,Qubee,COMSATS,World Call,WiTribe etc are quite popular .

2.3.3 Internet Connectivity through satellite

Satellite internet is available in Pakistan but its usage is very low in Pakistan .It is only used in those remote areas in which the terrestrial internet connection accesses not in range or secure or reliable. (About Us – Go Wireless Pakistan | Wireless ISP Consultancy Firm, Wireless ISP Setup in Pakistan, 2016)

2.4 Pakistan internet usage statistics

The increase in telecommunication technology has leads to the production of cheap smartphones in the country and the easy connectivity to the mobile phone internet services ,have vigorously increased the usage of internet in Pakistan i.e., from 6.5 % population in 2006 to 18.4% population in 2015 .It clearly depicts how the usage of internet has increased in Pakistan . (Internet User's Growth Rate in Pakistan 2015 | Dosta Inc., 2015)

2.4.1 Internet Users in Pakistan

There are 35 million internet users in Pakistan that are penetrating with the rate of 15 % each year. Due to that Pakistan stands among the 2nd highest country with respect to the growth of internet users in the region, after the country Maldives. In the world ranking, However Pakistan position is 19th, with the china highest internet using population followed by India, US, Brazil, Japan, Russia etc. (Pakistan mobile internet stand at 21 percent of the population, 2018)

Latest research on the Pakistani netizens shows that 18 million users, out of 35million users of the Pakistani internet, browse internet through smartphone devices (2013 statistics of Pakistan telecom authority). As Pakistan is developing country so mostly 80 -84 % males comprises the cyber community of Pakistan, and the age group of mostly people using actively internet are of 20-24 years and among them more than 80% have spent an hour on the internet everyday. In most of the rural areas of Pakistan there is no internet access to the local people . (Telecom Coverage Maps, 2016)

2.4.2 Social Media users

The access to social media sites is very easy in Pakistan this is the reason the number of social media users are increasing in Pakistan. In the light of the recent statistics 35.5 are active social media users, 109.5 million are unique mobile users, 44.6 milllion are internet users, 32 million are active mobile social users. Among social media user facebook is 92%, youtube 0.4%, twiiter 0.1%, instagram 0.1%, pinterest 0.1%. (pakistan social media stats 2018, 2018)

2.4.3 E-Banking

Gradually the use of E-banking is increasing in Pakistan. While 3.1 million are the electronic channels users such as mobile phones, internet and ATMs machines out of 198 million populations. (ebanking in pakistan is on rise, 2017)

2.4.4 E-Commerce

The most famous e-commerce Pakistani websites are daraz.com, shophive.com, zameen.com, pakwheels.com, rozi.pk etc. The e-commerce market in Pakistan is making the huge money worth $80 million annually, and the most common transaction is the cash on delivery method while the other rare transactions methods are easy paisa, mobi cash. credit cards etc. This high growth in term of sales and consumer preference has encouraged branding system to introduce alternate ecommerce techniques with regard to conventional techniques. (pakistan ecommerce sale set to cross 1 billion by 2020, 2018)

2.5 Existing Technology Trends in Pakistan

However the department of information and technology is evolving with great speed but adoption to the new trends in technology does not run parallel with it .Mobile phones are very popular in Pakistan among the major computing devices ,followed by less usage of laptops/PCs but tablets ,however not managed to attract most of the users. Amongst the operating systems (OS) which are developed for computer/ laptops, window 7 largely used operating system in Pakistan and produces 54% of the share. 20.36% are the users of WinXP which is an obsolete operating system and is extremely vulnerable to cyber-attacks, although Microsoft has officially ended the support of this window but still there are users which use this window .Windows 8 and windows 8.1 are also in use but lower than the expected rate .The usage of Apple's OS X accounts 1.23% of the users. (Stat counter Global Stats ,2017)

Android operating systems are very common smart phones in Pakistan, because these are cheap as compared to apple products. There are 68 % android users in Pakistan and apple users are 24 % in Pakistan. The number of window users are very less in Pakistan just 8 %because this company is not fulfilling the required criteria of the privacy of the user. (E-commerce Trends Pakistan, 2018)

1. The most widely used desktop web browser's in Pakistan is Google chrome 87%, while 9.53% uses the fire fox, while 2% uses the internet explorer .The major drawback is that most of the Pakistani cyber community doesn't update its browser regularly or they don't know how to update these. There is twice the number of users of chrome 43 as compared to chrome 44. Some users have also using Chrome 2, Safari 4 ,Firefox 2. As most of the world is using Google for the research, Pakistan prefer Google (97.7% usage in Pakistan) over other search engines such as

Bing(0.81%) ,Yahoo(1.27), Web Crawler (0.01%), Baidu (0.05%) is used by the fraction of cyber community in Pakistan. (browser market share pakistan, 2018)

2. Cyber security has been made among the top security concerns after Edward Snowden's revelations regarding large scale surveillance operation by USA,s NSA (National Security Agency). All cyber information provided through American servers is accessed by American intelligence agencies .So this the reason most of the countries started a blanket ban on most of the American digital companies such as; Facebook ,Apple ,Yahoo, Google ,Microsoft etc. which provide data on surveillance request to NSA ,which lead to the increase in the usage and development of indigenous /local search engines , email services ,operating systems etc. .This section of research will throw a light on the local digital solutions used and developed by various countries to secure their national cyber space infrastructure. (The best replacements for privacy-invading services , 2017)

2.7.1 **Domestic Political literature**

There is the literature reviews of the publically available policies /Laws/Regulations, in this research, on the use of ICT and the use of Digital information technology in Pakistan, including but not limited to. (Comparison of webmail providers, 2014)

1. *Pakistan Telecommunication Act 1996* permits the government of Pakistan to Intercept/trace the calls and messages in, interest of National Security.
2. *Electronic Transaction Ordinance (ETO) 2002.*This law monitor, helps facilitate and legally can back up all day to day transactions and all forms of e-communication .
3. *The Defamation Amendment Act 2004 and the Defamation Ordinance 2002* deals with the online case of libel, blasphemy and slander.
4. *Pakistan Electronic Media Regulatory Authority (PEMRA) Ordinance (2002) and PEMRA Amendment Act 2007* passed for regulating electronic media.
5. *Payment System and Electronic Fund Transfer Act 2007* (State Bank Of Pakistan) provides the regulatory framework for fund transfer and e-payments (OS", 2016)
6. *Monitoring and Reconciliation of International Telephone Traffic Regulation 2008 and 2010 by PTA* attempted to blanket ban encryption for signaling information and Virtual Private Networks (VPN)
7. IT secretary and MO IT of Pakistan issued Draft National ICT policy 2012 (Revised)
8. *The Investigation of Fair Trail* Act (2013) gave the military right to online surveillances.
9. *7 Points Action Plan* to address issues regarding cyber security in the country given by the Senator Mushahid Hussain Sayed.
10. The National Cyber Security Bill of 2014, which is for the establishment of National Cyber Security Council, proposed by the Senator (Mushahid Hussain) in Senate. (Deepin, 2016)

All the drafts of Cyber- Crime legislations are put forward to prosecute cyber criminals and vandals ,it includes the Electronic Crime Act 2004, Prevention of Electronic Crime Ordnance 2009 ,Prevention Of Electronic Crimes Act (PECA),2007,Draft Electronic Documents and Prevention of Cybercrimes Act ,2014,Prevention of Electronic Crimes Act 2015 (awaiting approval of national assembly) .To draft the cyber policy of the country for research purpose , these all above mentioned legislation were consulted . (Kylinos.com.cn, 2016)

2.7.2 **Global Political Literature**

How to tackle the cyber menace , different cyber security strategy documents of various countries were accessed ,consulted and analyzed and to understand how these countries have postured themselves to minimize cyber threats .This include strategies of Australia, Austria, Bangladesh ,Canada, China ,Czech Republic ,Denmark, Estonia, Finland ,France, Germany ,India, Israel ,Iran ,Malaysia ,Korea ,Japan ,New Zealand ,Netherland, Russia ,Spain , Saudi Arab, south Africa , turkey ,USA UK and few others .The ENISA's document ,National Cyber Security Strategies : Setting the Course for national efforts to strengthen security in cyberspace. (China COS, 2016) provides the best updated analysis of the various cyber security strategies of the different countries.

Also the strategy guidelines were consulted which were given by relevant security global organizations such as The ENISA , ITU (international telecommunication unit), Common Wealth , NATO etc ,apart from the strategy documents .

The ITU's **National Cyber security Strategy Guidelines**, (Danchey, 2015) gives a reference framework to make the process of formulation of cyber security strategy easy, so therefore, pointing the stakeholders engaged in building cyber security resources and capacity.

The **National Cyber Security Framework Manual**, which is developed by the CCDOE, (comprehensive risk assessment guidance for federal information system published,2015) the guideline which provides strategy for the holistic cyber security frame work, regarding all aspects of cyber security i.e. strategic, political, technical and operational.

The **Commonwealth's approach for developing National Cyber Security Strategies** is Commonwealth's guide on to identify the best possible practices which can be adopted by a certain country in relevant with its cyber threat landscape, national priorities ,culture ,etc. It also provides good security practices from a security strategies which can be used by the various countries having plan to improve or devise their national cyber security policies and strategies .(Security and privacy controls for federal information systems and organizations, 2013)

The **Cyber security Guide for Developing Countries 2009** is very useful special guide book for the developing countries, by ITU. In order to form the cyber security strategies in accordance with the national needs such as technical ,legal ,operational and pertinent with economic issues ,it provides them best guidelines and also prepare country for the cyber-attacks attempts .(Guide for mapping types of information and information systems to security, 2014)

The **National Cyber Security Strategies: Practical Guide on Development and Execution**, provides most of the implementation and development guidelines .This guide book issued by ENISA (Security and privacy controls for federal information systems and organizations, 2015) basically emphasize the basic need of having the harmonized definition of key terms and basic tools of cyber security having unanimity in technical and legal approaches to increase the international cyber security collaboration.

The academic study **Tallinn Manual on International Law Applicable to Cyber Warfare**, (published in 2009) (ENISA.,2014**)** very elaborately explain how the international cyber Laws and regulations can be applied to cyber warfare /cyber conflicts. There are very interesting internationally books on the cybersecurity especially the Tallinn Manual on International Law Applicable to Cyber Warfare in which it very explicitly explains the association of international humanitarian law applying to the cyberwarfare such as authors in the manual are of the view that the damage to the digital information is same as the physical damage.

Dr Tughral Yamin's book on **Developing Information Space Confidence Building Measure (CBMs)** between India and Pakistan provided multidimensional ways of establishing Confidence Buliding Measures (CBMs) in the cyber space between India and Pakistan. CBMs preclude inadvertent wars and also control and monitor malicious cyber behavior. (Yamin, 2014)

Also, ENIAS's **National cyber security strategies an implementation guide** were accessed. It provides proper cyber security guidelines, cyber action plans and present some very important practical cyber security practices that help the developing countries in proper execution of comprehensive national cyber security strategy. (ENISA, 2014**)**

An Evaluation Framework for National Cyber Security Strategies, by ENISA ,was read ,present the various key performance indicators (KPIs) which are essential to evaluate NCSS's components . (Klimburg, 2015)

No doubt, Pakistan is the new member of the cyber world 18.4 % of the total population of Pakistan ,which is estimated about 35 million users of internet in Pakistan but the rate of internet penetration is increasing day by day at high rate and also the number of e-commerce users .It also increases the probability of cyber –attacks hitting the cyberspace infrastructure .These cyber-attacks and cyber threats will cause debilitating effects on the national security , economy and law and order .Therefore it is very necessary to protect the national cyber space infrastructure from the malicious threat agents ,the literature highlighted in the chapter is very helpful in the revision and formulation of a harmonized cyber security strategy ,which can effectively secure and defend the national cyber space.

CHAPTER 3

Comparative Analysis of Various Cyber Security Strategies

The information and telecommunication technology (ICT) has converted the world into a global village and provide efficacy to the government and convenience to people's life .The more development and advancement in technology ; the more sophisticated method of cyber-attacks which changed from financial breaches and small scale intrusion to highly organized state-sponsored attacks. According to the prominent business leaders and state officials Physical war can bring less harm as compared to the cyber war and cyber terrorism which can cause more financial and physical harm. The biggest threat which is caused by the cyber-attacks is that they can endanger the freedom of an individual and a state.

The ever-growing cyber-attacks and the Snowden's revelations of 2013 make many countries to accept the devastating fact of this digital age, that their cyber national information infrastructure is so vulnerable to the cyber-attacks and cyber thefts. It also stresses the need to establish cyber capacity building network at federal level and formulation of high level plan of actions such as NCSS (National cyber security strategy) (ITU, 2015). To address the grave issue of the national cyber security, almost 50 countries have formulated their national cyber security strategies. There is a varying cyber threat landscape, so the national cyber security strategies of the countries vary, and considerable types of variations can be seen in approaches adopted by different countries and also prominent variations in their defensive, preventive and offensive measure. (Common wealth, 2015)

So in order to compare and analyze different cyber security strategies of different countries, the top countries on the latest ITU Ranking was considered. ITU (International Telecommunication Union) has been forming the ranking the countries on the basis of their cyber commitment. In year 2017, ITU has formed the ITU ranking on the basis of 5 conceptual frameworks Technical, Legal, Organizations, Capacity building, Cooperation. This chapter analyze 14 different countries of different regions from the world, including developed countries such as UK,USA, Japan, Israel, Australia, Finland, Russia, Germany, Canada ,Estonia and the developing countries such as India, Oman, Malaysia, and Singapore based on legal documents ,technical ,operational and policy related measures .This study will surely of the great help ,therefore ,countries designing their cyber security strategy or updating their existing cyber security strategies .How we use the comparison methodology method is explain in the diagram below.(ITU. Cyber security guide for developing countries, 2015)

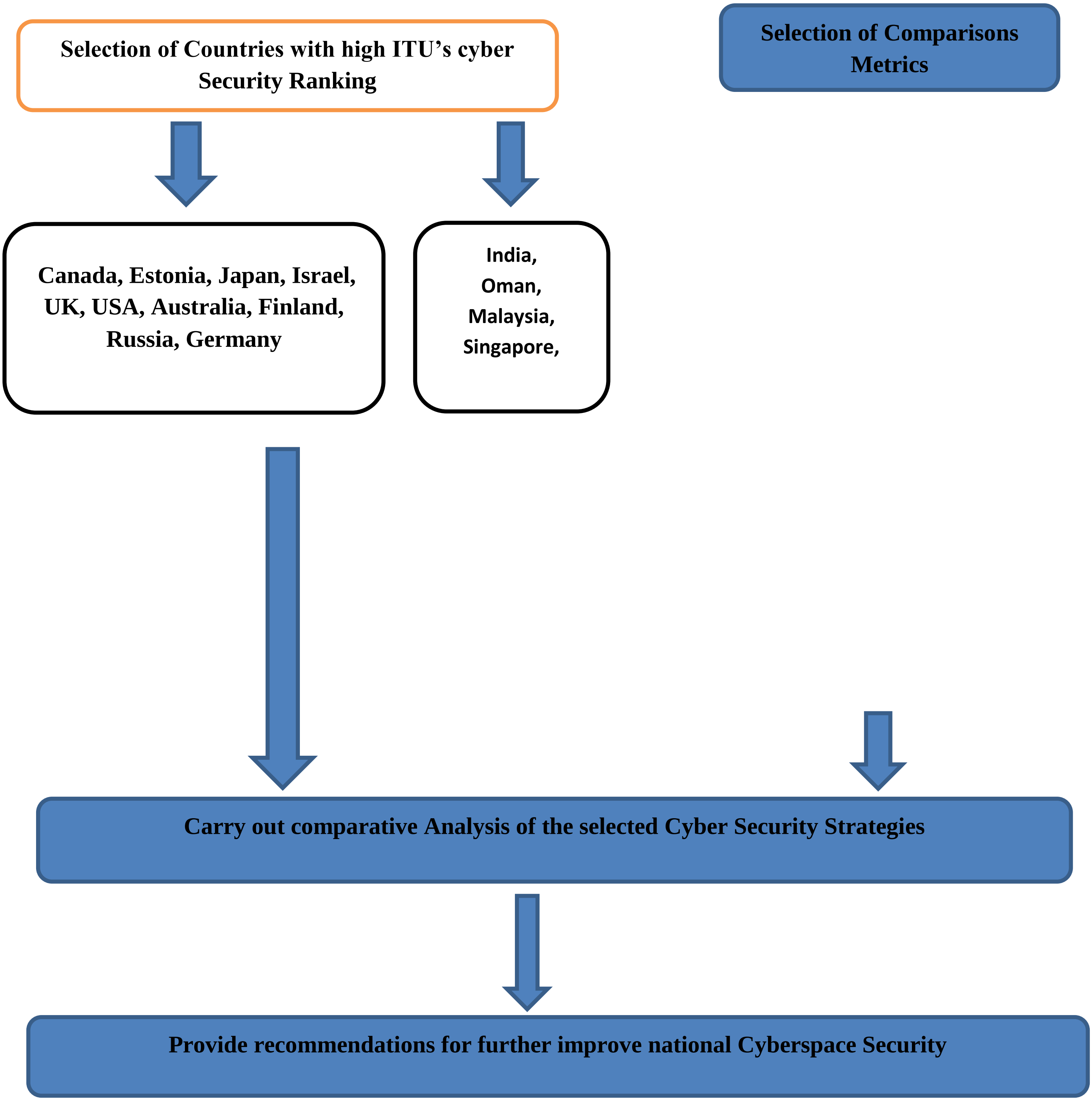

Selection of Countries with high ITU's cyber Security Ranking
Selection of Comparisons Metrics
Canada, Estonia, Japan, Israel, UK, USA, Australia, Finland, Russia, Germany
India,
Oman,
Malaysia,
Singapore,
Carry out comparative Analysis of the selected Cyber Security Strategies
Provide recommendations for further improve national Cyberspace Security

Figure 2.1 Comparative Methodology

(Image made from the source of information from the ENISA Europa Eu website related to cyber security strategies)

3.1 Selection of Countries

The countries that top the ITU‘s cyber security setting have the best cyber security practices, therefore this research have chosen those countries to highlight the best cyber security strategies. Developed /advanced countries with highest ranking in ITU with regard to cyber preparedness .The analysis of these countries strategies will provide a secure cyberspace practices which must be considered during the formulation of the cyber security strategy document.

The cyber security strategies of UK, USA, France, Estonia and Singapore are particularly acknowledged worldwide for having dual aspects of cyber security (Enisa.europa.eu., 2015) i.e. both offensive and defensive cyber security actions plan. The countries like Canada, Japan, Finland, UK and Australia have selected on the basis that, they have high usage of ICT technology and the highest cybercrime rate in the world after Germany and US, so the analysis of their strategies will give potentially secure approaches to decrease the rate of cybercrimes in the country. The countries like USA,UK and Estonia have updated their first cyber security strategy draft and ,hence, it is essential to look up to their updated drafts especially the amendments which they have done in their latest version .The reason Japan is being chosen because it has also formulated its two strategies ,one for civil cyber security and the second one for military cyber security .Malaysia and Oman is selected because among Muslim countries ,it has also establish its best cyber defense mechanism lately .On the other hand Israel is considered the best example of cyber excellence by many security researchers(“Tallinn Manual on the International Law Applicable to Cyber Warfare”, 2009).This is all the reason why these countries strategies have been selected for the research.

Developing countries according to ITU 2017 having high cyber security ranking are Singapore, Malaysia, and Oman. How these listed developing nations make such a quick progress in the cyber domain ,will be analyzed and there will be the cross comparison of these strategies that, how even they leave behind the developed countries .According to researchers Malaysia is the most cyber shrewd country of the Asia and, hence it is included among the set of countries for research .India and is selected because it have the highest cybercrime rate ,so therefore the analysis of the cyber security strategies of these countries will provide substantial directions to tackle diverse cyber threat landscape .(World Economic Outlook Database April2015 – WEO Groups and Aggregates Information, 2016)

3.2 Comparison Metrics

The one thing common in the all cyber strategies framework is that they have one identical aim to protect cyberspace against adversaries and to enhance the cyber resilience. The variations in the strategies of the country are, however, due to security trends, variable cyber threat landscape, level of cyber consciousness, socio-political condition etc., which result in the different approaches of the selected countries. Special set of metrics have been developed to do the comparison and analysis of the above mentioned selected countries strategies. (MOHAMED, 15)

a) Year of development

b) Objectives of strategies understanding of major security key terms
c) Lead responsible cyber security organizations
d) Review /evaluation mechanism for the strategy
e) Level of prioritization assigned to national cyber security
f) Country's perception of cyber threat
g) Capacity building measures
h) Critical cyber sectors and infrastructure listed in the cyber security strategy
i) Incident response capabilities
j) Collaboration for cyber security (inter-state, intra-state, international)

3.3 Comparison based on identified metrics

The cyber security strategies of the countries exist in various dispositions and length differs from nine pages (Finland Cyber Security strategy of 2011) to ninety pages of (Malaysia Cyber Security Strategy of 2013). Many countries have developed separate strategies for cyber security and national defense, whereas few countries have added a portion of strategies of "Cyber Security" in their national defense security strategy. (CYBER SECURITY FOR THE DEFENCE INDUSTRY | Cyber Security, 2015)

The cyber security strategies of most of the countries, in most Instances, published in the English language .Australia, Estonia, Finland, Germany which is non-native English-speaking countries also have a published draft simultaneously in English. Succeeding sub-sections will provide more results of the analysis and comparison based on the comparison metrics explained earlier.

3.3.1 Development of the Cyber Security Strategy

The trend of developing of cyber security strategy gained momentum after 2008, when the simple cyber-attacks converted to huge targeted state-sponsored attacks. Among the selected countries, all countries have published their cyber security strategies online with the few exceptions of Malaysia and Israel. The data of their cyber security strategy have been collected from the public documents attributed to cyber security approaches of the country. (Lehto, 2013)

USA had published the first strategy draft in 2003, when cyber-attacks weren't very common. And majority of the countries published cyber security strategy in 2011. However, the continuously variable spectrum of cyber threats has made it crucial to update the strategies to fringe new cyber threats and relevant counter measures. The UK, USA, Estonia have consequently published updated versions of their strategy as well, with USA updating and reviewing their strategy most frequently. (Luiijf, Besseling, Spoelstra, 2013)

3.3.2 Strategic Objectives outlines in NCSS

NCSS basically defines the theme of strategies, at national level, addressing the cyber security challenges. Most strategies share many common visions and concerns, so therefore, having the ultimate objective of safeguarding their countries cyberspace infra-structure, although Germany lists down some priority areas as their objectives. While all other countries explicitly explained their strategic objectives in the document. So the common objectives in all NCSS are: (Alliance,2015)

a. To create a resilient and secure cyber space
b. To safeguard critical national cyber assets and cyber infrastructures,
c. To define properly cyber security regulatory, assurance framework and legislative,
d. To raise cyber awareness among citizens, IT professionals and the government official's.
e. To develop cyber security national response center such as detecting incident and response capabilities e.g. Cyber Security Incident Response Team (CSIRT)etc,
f. To establish indigenous cyber security technology,
g. To respect the fundamental rights of netizens,
h. To develop strong relation and co-operation between public private sectors for enhancing the cyber security,
i. To inculcate international co-operation with the regional and neighboring countries

Many countries also have objectives for their national interests, specific to their country, beside the common ones .For example in future USA wants to become a global leader in cyber security domain. Japan also has some specific purpose of introducing global outreach programs for cyber security having active adaptation to emerging cyber threat. (Top 20 Countries found to have the most Cybercrime, 2015)

By thoroughly reviewing the selected cyber strategies brings forward the very fact, that with the change of time, the scope of cyber security strategies is switching from the objective of merely protecting government and citizens from cyber threats to protecting the whole information society generally. (Robinson, 2013)

3.3.3 Diverge Understanding of Key Terms

Cyber security is very broad domain. Almost every country has developed its own definition of cyber security strategy; therefore, there are no globally harmonized definitions and key terms of cyber security. The subsequent section will analyze and compare the different cyber security definitions in the respective strategies.

3.3.4 Cyberspace

The comparison of different strategies indicates that for many countries ,cyberspace discern to be a complete network consisting of all virtual and physical Information Communication Technology devices that can be targeted by cyber criminals .However, Germany ,Australia , Canada ,the term cyberspace allude to the internet and the relevant ICT devices (Enigma software,2015)

Furthermore, Estonia have only tacitly defined cyberspace without giving their complete definitions. Finland has used the key term ‘cyber domain’ instead of using cyber space in their strategy. (N. Gribbon, 2015)

3.3.5 Cyber Security

Most of the countries cyber security strategies have defined “cyber security” as combating against every cyber threat within the cyber landscape .However, Australia and Finland limit it to only secure the digital information .So multifaceted approaches of different strategies come into existence this way for alleviate and for addressing cyber-attacks., Canada, Finland, France, Germany, Saudi Arab are the countries which explicitly mentioned the definition of the cyber security while Canada and UK have descriptive texts to define cyber security .Moreover Japan ,the only country ,not clearly defined the term “ cyber security” (Global Defence Outlook, 2014)anywhere in the strategy . The following table contains the summarized results.

3.3.6 Level of Prioritization assigned to cyber security

Beside global terrorism, economic downturn, natural hazard, etc. cyber terrorism, cyber-attacks and cyber espionage have also emerged as global menace. The different cyber security strategies of countries shows, that cyber security has now become their top-tier national security issues .Countries that have highest rate of cybercrimes (Global Defence Outlook, 2016)have allocate consequential huge resources to cyber security community .The publically available date tells , that India spends $500 million ,UK $650m annually ,Australia $1.2 billion ,Canada $6 billion ,with the USA spending the highest annual cyber amount of $10 billion .(N. Gribbon, 2016) The is the variations in amount allocated to national cyber security initiatives of these countries, but they have the same common prioritization of cyber security .(Levin, Goodrick, Ilkina,2013)

3.3.7 Characterization of Cyber Security Threats

For most of the countries, the potential threats and risks poses to cyberspace orbit around state-sponsored attacks, mostly organized cybercrimes, unauthorized access, cyber terrorism, interception of digital information vandalism, extortion, forgery, identity theft etc. Sometime software/hardware failures are also considered as the cyber threat .For Germany and Netherlands, natural hazards too part of cyber threat.

The concept of cyber threat in Germany, such as attack on ICT system is regarded as attack on confidentiality and integrity of information systems, While USA consider cyber threat as attack on ICT devices ,digital networks and cyber networks .So where probing is considered as a cybercrime in Germany ,it is not considered crime in USA (Klimburg,2012)Therefore it is difficult to adopt a holistic global cyber approach to cyber-attacks and adversary because of the varying perception of cyber threat landscape and cyber security .

3.3.8 Critical Sectors Infrastructure

Critical infra-structure is considered any digital assets or physical landscape which if compromised can cause a deteriorating effect on national security, economy and prosperity. In the cyber domain its definition is presented as, the criticality of an infrastructure by the digital information that it transmits, processes and stores and the core values and services which digital assets provide.

Country geographical conditions, peculiarities, socio-political factors , specific traditions, culture ,cyber threat perception highly impacted the choice of critical infra-structure of any country .This is the reason that different countries physical or digital assets have been classified under different terms i.e. developed countries consider smart electricity grids a vulnerable assets but it is not true for developing countries.(EU-U.S Security Strategies-comparative scenarios and recommendations, 2012)

Following sectors are mentioned by most of the countries as a part of critical infrastructure.

a) ICT/Telecom,
b) Government,
c) Finance,
d) Public health,
e) National Security Forces,
f) Transportation (air, rail, road),
g) Rescue Services,
h) Electricity,
i) Water Supply,

The oil and gas, chemical sectors, food, dams, judiciary, critical manufacturing sectors and agriculture sectors also come in the critical infrastructure of few countries. The above mentioned list for the critical infrastructure is not conclusive for any country because the increasing sophistication of cyber-attacks, digitalization of crucial resources, inherent vulnerabilities etc., are always on the verge of introducing new infrastructure and sectors to the list.

3.3.9 Organizational Overview –Lead responsible Authority

The subsection analyze the responsible authorities of the country ,the officially recognized organization which are accountable for the executing the cyber security strategies

,safeguarding the critical assets and implementing the well maintained status of cyber security at national level. (Analyzing a New Generation of National Cyber security Strategies for the Internet Economy, 2013)

Majority of the countries have setup of inter-departmental response capabilities such as under the supervision of various governmental departments, they have a manageable task of cyber security distributing the task among multiple organizations. Defense traditions, cyber threat perception have and resource allocation have major implications, within the government on these organizations. (Khan, 2012)

3.3.10 Technical Measures

To efficaciously avert targeted cyber threats and incidents for a country ,it is very crucial that very actively the dissemination of threat information reach to the concerned organization by the qualified technical team, in order to equipped with resilience capabilities and cyber protection.(Min, Chai, Han, 2015) There are various forms of such teams in the countries such as Computer emergency Response Team (CERT) ,Information Sharing and Analysis Centers(ISAC) ,Computer Security Incident Response Team (CSIRT).All the countries have their own NCSS centers which can be the above mentioned CSIRT/ISAC/CERT to efficiently responding to cyber-attacks .However , all countries have different aim and purpose for these technical measure . There are few countries, which in addition to the CERT/ CSIRT/ISAC also established other co-coordinating bodies with them like Japan has cyber security strategy headquarter. (Commonwealth Approach for Developing national cyber security strategies, 2015)

3.3.11 Legal Measures

In order to evaluate the advancement of the proposed objectives of the cyber security strategy ,and to make sure that all the elected government and private entities can deal with cyber security challenges ,so therefore, it become very important to establish suitable cyber policy framework for the frequent check on and to revise the cyber security strategy. The review mechanism of these all cyber security policies is very necessary for the proper enforcement for the advancing required necessities. Many countries have established the appropriate review mechanisms and even most of the developed countries like UK, Germany , Austria ,Estonia have mentioned their specific factors for evaluation and reviewing mechanism .(Cyber wellness Profiles, 2015)There is a review cycle for example biannual for UK and Australia, UK,USA and Estonia are among those few countries which vey frequently update their cyber strategy ,and unlike there are many countries which even didn't revise their initial cyber security strategy once .

3.3.12 Cyber security Capacity Building

For all cyber security strategies it is always crucial to have the vital cyber defensive and preventive capabilities to defend the national cyber space landscape in effective most appropriate way .There are many capacity building initiatives which are as follows awareness’, training and R&D initiatives mentioned in the country cyber security strategy . (Benoliel, 2014)

3.3.13 Manpower Development and Cyber awareness’ program

The cyber awareness’ is also the goal of all the cyber strategies ,that their citizens especially IT professionals , policy makers ,government officials and businessman become aware of the cyber threats .Countries like UK Japan and Australia have the special programs for the training of children and parents too .There are many countries like India ,Malaysia ,UK which launches the campaign on social media about the cyber awareness .However , Singapore and Malaysia suggest that cyber security should be included in the academic curriculum.(AIIA,2015)

Mostly all countries have cyber security outreach programs to provide their citizens with basic cyber security tools and practical education .There are many most famous programs of few countries for example “Get Safe Online” program of UK ,stay safe online campaign by Australia , “Cyber Safe Program” by Malaysia , and “Cyber Security Month” annually by USA ,UK and Australia . Japan has a desire of becoming cyber world global leader by the establishment of various cyber security support services for the preventive and defensive capacity building .Moreover, many countries like UK, India Malaysia, Oman emphasize on the need of having the cyber security training for IT professionals to produce experts, and to also launch different commercial security programs by having proper certifications. (The Cyber Index International Security Trendand Realities, 2015)

3.3.14 Research and Development

To efficaciously deter cyber threat inherent cotemporary vulnerabilities of the Information Communication Technology devices and equipment’s from being corrupted by the adversaries, it is very important to safeguard the local ICT devices to enhance cyber security capacity building. All the countries, except UK, Finland, Australia, have entities for promoting R&D at national level which are officially recognized. The basic task of the divisions of the research and development is to sponsor academic and industrial projects related to cyber security as mentioned in various strategies. (Cybersecurity Ventures, 2014) It task include finding best security practices and standards; develop indigenous cyber security products at national level, etc.

3.3.15 Co-operation

Cyberspace has the global natures, it has inter-connected networks ,apart from having strong intra –nation co-operation ,it become essential to have inter –state and international collaborations .To increase cyber resilience and to effectively tackle cyber issues Cyber security always require multi- stakeholder approach**.**

3.3.16 Public Private Partnership (PPP)

Most of the internet infrastructure is owned by the private sectors, hence public-private collaboration is crucial and their co-operation can better defend cyberspace. There is a concept of Public-Private partnership in NCSS. It is a strategy to obtain cyber defense at national level.

3.3.17 Cooperating with ISP's

Many countries like USA, UK, Japan has mentioned in their strategy about partnership of the government with the private telecom and internet service providers from both internal and external cyber preparatory to defend national cyberspace .Others countries didn't mention about partnership explicitly . **(ENISA.europa.eu; cybersecurity strategies)**

(Actually there are two main documents on the comparison of cyber security strategies available online which said that they get the information from the main ITU website on which cybersecurity strategies of the countries are written. The chapter 3 of comparison of cyber security strategies of my thesis is actually derived from the below mentioned links) http://scholar.google.com.pk/scholar_url?url=https://securitymetrics.org/attachments/Metricon-3-Cybenko-Article.pdf&hl=en&sa=X&scisig=AAGBfm0aikPIyEEDsSJ6itFNNQSGF8Tt7A&nossl=1&oi=scholarr

https://www.researchgate.net/publication/261987241_Ten_National_Cyber_Security_Strategies_a_Comparison_Critical_Information_Infrastructure_Security

https://link.springer.com/content/pdf/10.1007/978-3-642-41476-3_1.pdf

https://www.tripwire.com/state-of-security/government/a-comparative-analysis-of-national-cyber-security-strategies-germany-and-the-u-s/

http://scholar.google.com.pk/scholar_url?url=https://inldigitallibrary.inl.gov/sites/sti/sti/3375141.pdf&hl=en&sa=X&scisig=AAGBfm1R3CXT0qaN3ishVmeqwyRhVh9eiw&nossl=1&oi=scholarr

3.1.18 International Collaboration

International collaborations are indispensible for any cyber security strategy to operate successfully in a country because of the global nature of cyber security especially with the neighboring and the regional countries. It is impossible to gain cyber security in an unsecure global environment without international co-operation .Many country strategies present global partnership as the part of their objective. (Yamin, 2014)

3.4 **Recommendations**

With the increasing inherent vulnerabilities cyber preparators are advancing day by day .No nation is immune to cyber-attacks .Following recommendation can help, while formulating or revising strategies to mitigate cyber risks of the national cyberspace. ((ENISA Threat Landscape 2014 __ ENISA, 2015)

a. To explicitly explain the aims, define the major key terms and its scope in the document, according to the country actual threat landscape.
b. To protect the fundamental rights of the internet users beside the protection of the critical digital assets in order to safeguard the whole national cyberspace
c. To redefine the word “critical infrastructure ’’ in the strategy because infrastructure when compromised threat national security and adversely effects the national economy.
d. Introduce new threat vectors to measure cyber threat e.g. cloud computing smart phone etc.
e. While formulating domestic cyber security strategy ,policymakers should take input from telecom providers, international stake holders ,military, judiciary , civil society, cyber security experts ,religious leaders ,financial institutions
f. The strategy should be subject to revision by the cyber industry to increase the sophistication of cyber security and also to keep pace with the new trends in the technological advances.
g. To reform the national legal cyber infrastructure framework to deal with cyber offenders and criminal efficiently.
h. To introduce the information sharing framework between the government and the private sectors regarding cyber security incidents
i. To prominently define the responsibilities and tasks of CERTs/CSIRTS such as instantly forensically responding to cyber incidents and to raise cyber awareness
j. To introduce certified educational training programs for netizens self-training and to spread cyber awareness.
k. To promote and develop the local products and indigenous security services
l. To ensure proper cyber resilience in the country reinforce private-public partnership
m. To introduce cyber norms in the strategy to prevent cyber warfare in the future

n. The countries ,that do not have the advance technology and the digital tools to develop own network engines, browsers can use any of the non-US based alternatives, but before that taking proper risk assessment that are neither vulnerability embedded by the developer nor backdoors installed.

Countries around the world are nowadays focusing on formulating cyber security strategies to address this viral issue, because in contemporary times digital security has gained more importance than physical security .The are many strategies common in the documents like raising cyber awareness in general public, develop cyber capacity building , establishing incident response and preventive capabilities at the national level etc. The dilemma is that, however, many countries tried so less to achieve their strategy objectives.

Despite the similarities, it is observed in the countries strategy drafts that there are many differences and variations such as the task of CERT vary from country to country, they have variable approaches for the cyber awareness programs in the country. From the above mentioned research it can be easily conclude that USA,UK, Singapore, Malaysia, Oman, Germany specifically have better strategies in terms of technology and enforcement of action plans .Despite defensive mechanism ,offensive mechanism is also seen in their strategy which give them the edge over other country strategies . (Robert, 2015)

Concluding Economics, Defense and Military are the major starting points which effect in forming the strategy of any country. Also the major difference is that cyber security is not just related to the internet connected device which most of the countries mistaken, it is the whole ICT system. Only Japan, UK, Malaysia, Singapore mention in their draft about the electromagnetic spectrum threats toward the cyberspace. Mostly all the countries selected for study didn’t focus much on cyber awareness, only the Australia has an outreach program in which public is given the knowledge of basic cyber security tools. (Deune, 2014)

The one major flaw in all the countries National Cyber Security Strategy is that they all are formed on the basis of departmental playing fields and political sensitivities , so they least have smart global approach. All activity lines and set of actions can change when there would be the change in the political infrastructure leading to very less progress in cyber security. The one very important point which they lack is that they have no policy regarding towards the manufacturing of the software. (Dealing with a changing threat landscape, 2015)

All the above mention Cyber security strategies recognized the global cyber threats and accepts the importance of international legal , technical and operation collaborations. But still they lack the true global guidance, leadership and aggressive approach. In 2011 America drafted international strategy for cyberspace, with reference to the Council of Europe Cybercrime convention, for harmonizing the legal policy of the countries approaches towards cyber security. This draft has both offensive and defensive approach such as to build military alliances and to enhance them confronting the potential international threat landscape.

For international collaboration first there should be the harmonization in the definitions of the cyber space, cyber security, cybercrime, cyber threat etc. Two out of fourteen countries mention the need of relating the cyber security strategy with the CIP (critical infrastructure protection), while all other countries explicitly in their NCSS discussed related to cyber critical infrastructure but very less explicitly explained the relation between NCSS and CIP. There should also be the cultural analysis to determine the pathway

There are five main global organizations which also form international global cyber strategy such as United Nations (UN), the Organization for Economic Cooperation Development (OECD, the International Telecommunication Union (ITU), North Atlantic Treaty Organization (NATO), the European Union (EU).

_ ***CHAPTER 4***

Pakistan Cyber Threat Landscape

4.1 Introduction

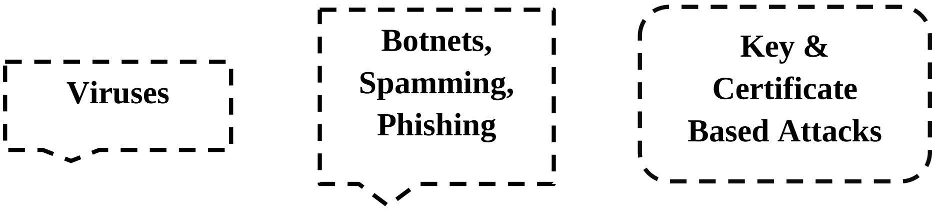
In the cyber world defender and attackers is playing relentless war. Attackers have edge over defenders due to sophisticated attack tools and complex attacking techniques. So in order to deal effectively with these cyber-attacks, the information security practitioners and professionals, such as defenders to first completely understand the cyber threat landscape and then find multiple dimensional ways to fight against cyber-attacks. Cyber threat landscape includes the list of threats having information new threat vectors and attacking agents .(Dealing with a changing threat landscape,2015) The main focus of this chapter is to analyze the Pakistan threat landscape such as which cyber threats Pakistan is facing ,the emerging cyber threats that can harm the cyberspace infrastructure .

4.2 Evolution of Cyber Threats

The frequent advancement of the capabilities, resources, tools and skills of the cyber threat agent’s escort to the evolution of cyber threat landscape in Pakistan. The advancement in the ICT technology both brings revolution in technology and threats to information technology such as cyber threats.

The cyber threats of the twentieth century in Pakistan, is limited to small-scale hacking, intruding attempts through malware and website defacements. But the sophistication in technology brings the sophistication in cyber attacking techniques leading to phishing, spamming and botnets in 2005, and suddenly to the most sophisticated Advanced Protection Threats (APT). (Yamin, 2014)

The attacks on authentication keys and certificates are the dreadful cyber-attacks, because they increase the risk in the man in the middle attacks, which make it easy for cyber criminals to legitimize the malware by signing the rouge certificates. This trend of man in the middle attacks is increasing day by day. Pakistan is an attractive target for cyber preparatory because of technical malpractices and cyber unawareness. In addition to the cyber-attacks on the critical sector and the existing infra-structure, the flourishing IT industry and the recently launched 3G and 4G are major in future hotbeds for the cyber threats in Pakistan. (Recorded Future, 2014). The below diagram summarizes the threat evolution of Pakistan.



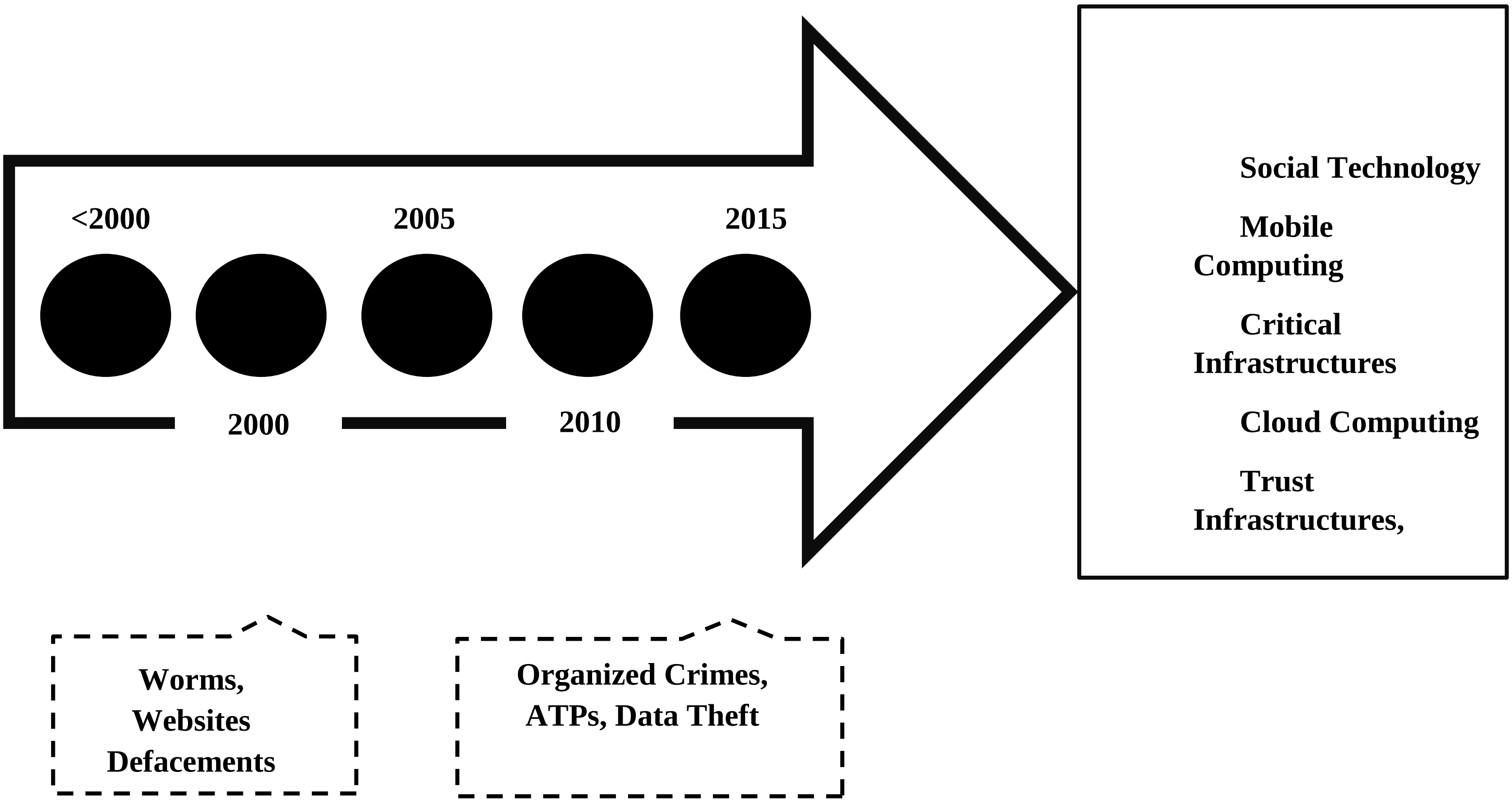


Diagram 4.1

(image source of information is from the site of eandt.theiet.org hacking through the years a brief history of cybercrime)

4.2.1 Social Technology

The internet social life is always the main target of the cyber criminals. They do data theft ,identity theft , abuse on social networks and misuse of the social media .Social bots have the likely chance of emergence in Pakistan .The cyber-attacks through Trojans ,phishing ,worms, drive-by exploits are on the verge of increase in Pakistan .

4.2.2 Mobile Computing

Recently the trend of money transaction through the usage of the mobile phone made smart phone the pretty target for cyber attackers, and also the frail BYOD policies of IT organizations of Pakistan. However, in future cross platform attacks using botnets, malware, drive-by exploits, phishing, exploit kits trend will increase than a normal rate.

4.2.3 Critical Infrastructures

In future, the main target of cyber-criminal in Pakistan will be on the critical information infrastructures specifically that of ISPs, Internet exchange point, cloud service providers etc. Pakistan critical infrastructure is very clearly defined in the PECA (Prevention of electronic crime act).

4.2.4 Cloud Computing

Cloud computing attacks may lead to the loss of important data or corruption or sensitive information which may lead to denial of service attacks directory traversal attack ,SQLi code injection etc., and there trends are increasing day by day.

4.2.5 Trust Infrastructures

Trust Infrastructure includes secure communication protocols, public key infrastructures, authentication infrastructures, etc. These are the part of ICT systems that provide authentication communication to make trusted connection between two points.

4.2.6 Big Data

Big Data is the latest trend evolving in Pakistan. Big data basically is a massive volumes of data, gained from multiple resources, which cannot be process using old traditional data processing techniques. Pakistan has a national center in Big data and cloud computing having 12 major laboratories in the top leading 11 universities of Pakistan. Recently at LUMS university Lahore Ahsan Iqbal inaugurates the 1st National Center in Big Data and Cloud Computing. (to boost big data analytics, Pakistan now has a national center with 12 affiliated laboratories; Technology review, 2018)

4.3 Greatest Cyber Threat to Pakistan

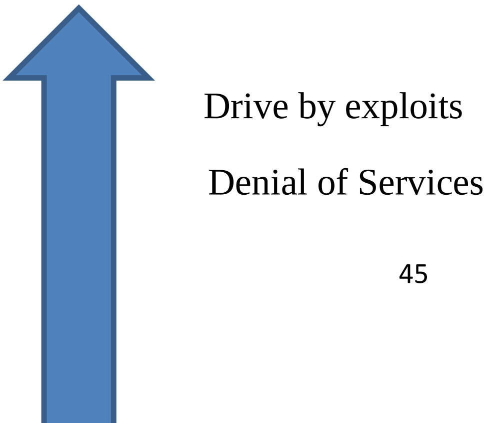
Pakistan has not fully identified its critical structure especially NADRA, E-government and capital markets of Pakistan. Skilled cyber terrorists may be able to create an integrity, availability or confidentiality attack on the network of these services therefore this type of cyber activities may damage or stop the essential ICT services including NADRA, E-Government websites, Stock exchanges, Mobile banking and money transfer services which will be having serious impact on the performance of government services and possibilities of hacking IDs from NADRA servers and also can be used for any other terrorist activities. In addition, it will create a collapse or crash the economics of Pakistan by hacking and after that controlling the stock exchange and financial services by adding their own fake figures. It is therefore very important for Pakistan to identify its critical infrastructure.

Microsoft's security intelligence report (Vol 18) rated Pakistan top among the countries with the highest malware encounter rate (ER) and infection rate (computer clean per mile CCpm). In 2015 as opposed to the global rate of malware infection 14.8%, Pakistan encounter 45.1% of malware infection rate .Similaraly,58.6% computer are scanned in Pakistan as compared to the world rate of 8.4 CCM. The line graph of different countries illustrating the countries having highest malware infection rates shows that the malware infection rates of Pakistan is tops the list.

A malware is actually harmful software which install unwanted unprotected programs on the computer, spy on personal information, create backdoors, crash the system, hijack a computer. Pakistan has the cyber illiterate community which cannot prevent the harmful malware attacks, in result the efficiency of the computer system decreases, affect business and other daily tasks. Except for the ransom ware virus, Pakistan has highest infection rates of all other malwares.

4.4 Common Cyber Threats to Pakistan

The below arrow flow shows the common cyber threats of Pakistan in ascending order. The following diagram explains cyber threat vectors facing Pakistan. Owing to the different targets of cyber attackers threats have been categorized into typical three groups i.e. targeting government, organization, and individual.



Drive by exploits

Denial of Services

Phishing

Data theft

Spam

Targeted attacks

Physical loss/theft

Identity theft

Search engine poisoning

Rogue certificate

4.5.1 Cyber Stalking

This is the most prevalent inconvenience in Pakistan. The cyber complaints reported to FIA, among them 80% are of cyber stalking, mostly made against the female community on face book and twitter. Harassment through emails and social networking apps is common in Pakistan. (I am more scared of harassment online than offline; theguardian, 2017)

Social harassment has become a major stigma of our society, because there is no check and balance on the cyber activities. It is the huge threat for the netizens, particularly the female community. (cyber stalking facts, 2016) which are continuously harassed and threatened through SMA, emails etc., for the sake of fun and mostly the revenge. The worst cases are to pay the money to the cyber criminals for keeping the secrecy.

4.5.2 Cyber Defamation

They are produce as a result if rivalry conspiracy, mostly by the competitors in Pakistan .In most of the cases they hacked the account and send some vulgar, blasphemous, racist, politically subversive messages and emails to someone else account from targeted side or posted something of negative material on social blogs and, other internet forums to personality defamation. (Nick, 2014)

4.5.3 Disseminating Offensive Material

The indecisive regulatory environment of Pakistan give freedom to the cyber terrorist, offenders, even the youngsters to promote racist propaganda, sexually explicit content etc., The recent example of Tehreek e Taliban on YouTube videos shows the frequent upload of the fabrication of explosive material on YouTube videos.

https://www.youtube.com/watch?v=GG9p1qibeW4

4.5.4 SMS Spoofing

The most serious and convenient way of spreading the information is messaging. But the cyber offenders extract all the confidential information of a person by claiming to be some authority or deliver a false message. In most frequent cases internet offenders sent messages from a designated number, which is very difficult to trace because having no account of the actual sender. Nearly 80,000 SMS Spoofing cases have been reported in the past year to be sent to Pakistan. https://tribune.com.pk/story/520548/evil-mobile-software-spoof-message-software-could-be-dangerous/

4.5.5 Spamming

When recipients open a spam email they become victim of a malware, this issue is mainly due to cyber unawareness. Very frequently netizens in Pakistan receive spam e-mails specifically Nigerian property scams and chain letters accompanied with harmful malware.

(Cybercrime: scam, bam, thankyou ma'am; Dawn, 2018)

4.5.6 Phishing

Phishing is very easy in Pakistan; a cyber-criminal can easily extract personal details of innocent individual by manipulating. This is the reason the finance departments and banking sectors of Pakistan asked customers to update their profile, and frequently update their passwords. (Social Media harassment in Pakistan: only 5% cases registered in 2015, 2015)

4.5.7 Child pornography

Child pornography is illegal in Pakistan and it is considered cybercrime in Pakistan but unfortunately the rate of this crime is very high. Cyber defaulters easily access e-content aimed to sexually exploit children, they also create and distribute such content. (Debunking

Dark Web and Child Pornography in Pakistan; thenation 2018) (Pakistan tops list of most porn-searching countries: Google – The Express Tribune, 2017)

4.5.8 Intellectual property rights

The crimes related to trademarks violations, infringements of copy rights, software piracies etc. are very common in Pakistan. They are illegal in Pakistan. The theft of student university assignment and projects are also considered these days emerging cyber threats, and also the stealing of application /software source codes. (Intellectual property rights in global trade; Dawn, 2018)

4.5.10 Internet Time Theft

Cyber literates easily hack the PTCL's DSL internet with default configuration, and use the internet free of cost. **(**New Leaks: NSA Hacked PTCL ITI, Multinet, Paknet and Micronet Servers; ProPakistani, 2016)

4.5.11 Financial Crimes

Credit card skimming, money laundering etc. are financial crimes very common in Pakistan. Despite the expensive advanced security technology of many leading banks e.g. askari bank, American bank, Muslim commercial bank, union bank, city bank etc., they still face the credit card frauds. The huge loss suffered by the National Bank of Punjab, the amount of Rs. 1.39 corers using fake debit and credit cards. (Mumbai Kars bewares! Your bank details are being stolen and sold, 2015)

4.5.12 Electronic Forgery

The business of forged mark sheets, revenue stamps, certificates, currency notes etc., is at a loud deep in Pakistan, by the use of sophisticated printers, computers, scanners, therefore presenting a dangerous threat. (Cheating forgery in Pakistan, lawsofPakistan 2018)

4.5.13 Web Jacking

It is mostly done by the cyber hackers belonging to India, Israel. They almost daily hack insecure Pakistani website for the sake of website defacing. http://www.supremecourt.gov.pk/ijc/articles/10/5.pdf

4.6 Cyber threats to Organization

4.6.1 Unauthorized Accessing of Computer

Mostly many organizations in Pakistan use old computers, which are vulnerable, easily accessed by unauthorized persons or posted ,posting on blog ,websites etc.

4.6.2 Illegal Usage and Interception of Telecommunications

The gaining of illegal access to the telephone switch board of an organization (PBX) for the sake of hackers own communication is quite ubiquitous in Pakistan. Also the cyber offenders for international calling services they install VoIP gateway exchanges. (FIA and PTA get aggressive against rising grey traffic in Pakistan, 2017)

4.6.3 Data Diddling

It is the change of data before or during infiltrating to computer systems .Data Diddling also target the electricity board of Pakistan by faking the documents during electricity board digitalization system by the third parties. (Cyber Crime in Pakistan Research Report, 2015)

4.7 Cyber Threats to National/Government

4.7.1 Electronic Vandalism and Extortion

This is the horrid threat; it requires money for it termination. This malware embeds cracked software installing ransom ware infecting websites on the victim computers. (http://www.nr3c.gov.pk/cybercrime.html)

4.7.2 Cyber Warfare and Terrorism

Cyber offenders especially the hackers from India, Russia, Israel, USA etc. almost on daily basis hack ICT systems, inject malware, send obnoxious emails, damage information system etc., to spread pervasive terror in Pakistan.

4.7.3 Hacking into Government’s or Military sites

Israel and India love to hack government military sites to defame the Pakistan army. Indian and Israeli hackers took down 36 governmental websites by Indian Cyber Army. These hackers for the sake of politics and socially motivated to promote a specific cause. Indian Hacktivist hack notable Pakistan government‘s website; Cabinet ministry, Ministry of Defense, National Portales. Many hackers also hack government website to in protest against government’s decision, load-shedding, high prices etc. (Websites of several key federal ministries hacked; THE NEWS, 2017)

4.7.4 Cyber Stalking

Pakistan is rated as the second highest country on the list of the nations, by the NSA, that spies upon for nuclear programs, sensitive data, domestic politics, through the internet, webcams, e-mails, websites, SMS etc.(US agency collected second-highest amount of digital data from Pakistan – The Express Tribune, 2013)

RAW has been reported to espionage and transfer funds to it elements in India by using Pakistan cyberspace. Black Water and CIA also intervene in Pakistan cyberspace landscape by using personal internet satellites. (Indo-Israeli Cyber Warfare against Pakistani nuclear program | Asian Tribune, 2014)

4.7.5 Cyber Threats Agents

A cyber threat refers to an entity which can cause, support, or spread a cyber-threat. The different type of cyber threat agents are mentioned below;

a) Stalkers

NSA, according to Edward Snowden daily stalks on the Pakistan cyber space to extract the content of their interest. Moreover, the activity of netizens is also stalked by our own government, intelligence agencies, rival countries especially the India. (http://www.currenthistory.com/Deibert_CurrentHistory.pdf)

b) **State-sponsored Attacks**

State-sponsor attacks on Pakistan are mostly done by Indian state-sponsor hackers by doing the intruding attempts to gain access to the government sensitive information. Since 2010, the India state-sponsored hackers are continuously Pakistan, government, military intelligence agencies. Small scale state-sponsor attacks are also done by Russia, US, Israel Iran from time to time. (https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity)

c) **Insiders/employees**

The insiders pose the most dreadful threat to the integrity of the cyberspace, as they are aware of the top secrets and confidential information and ICT devices' vulnerabilities, which are being used in the organization.

d) Competitors

The competitors of the enterprise and corporation used offensive tactics and human engineering intelligence to get the competitive edge.

e) Hackers, Script kiddies, Crackers

There are many powerful hacker's group in Pakistan e.g. Pak Cyber Lions, Team Pirate Pakistan (TPP), Pak Cyber Eagle, Pak Cyber Attackers, Pak Cyber Experts, CraXer Cyber Hackers, (CCH) and many more etc. (Top 10 Pakistani Hacker Team – TheTopTens.com. Retrieved 4 December 2015, 2015)

Some are good hackers too which warn Pakistan government about the cyber security loopholes by the cyber criminals while some are also famous for defaced sensitive websites government of Pakistan, banks and telecom companies.

f) Cyber Hacktivists

These hackers for the sake of politics and socially motivated to promote a specific cause. Indian Hacktivist notable Pakistan government 's website; Cabinet ministry, Ministry of Defense, National Portales. Many hackers also hack government website to in protest against government's decision, load-shedding, high prices etc. (Websites of several key federal ministries hacked; THE NEWS, 2017)

g) Terrorist groups (Cyber Jehadis)

Al Qaeda, a renowned terrorist group, is highly proficient to tap the national internet traffic to connect with their peer, while using Pakistan cyberspace. (https://link.springer.com/article/10.1007/s12115-017-0114-0)

4.7.6 Scammers and Phisher's

They manipulate the innocent Pakistani netizens to fulfill their mean desires

CHAPTER 5

DOMESTIC CYBER LAWS AND E-REGULATIONS IN PAKISTAN

All countries consider cyber security as an essential part of their national security strategy, but Pakistan's government taken this issue for granted .Pakistan is a developing country, it is fighting a dreadful war against terrorism along with a conundrum of illiteracy, corruption, incompetent government, poverty, provincialism etc.

As this is the digital world and Pakistan has taken the first step to enter into the race of digital world by the first digital policy of Pakistan after approval from the cabinet. This policy aims to build incubation centers facilitating IT startups in provincial capitals and major cities and introducing specialized innovation centers of artificial intelligence and robotics to increase digital ecosystem. Digitalization is the modern day mantra of all countries. No industry gets more developed than the digital industry. It has outpaced the growth of all other developments. Our records are computerized, data banks, personal documentation of identities are all digitalized and the average time Pakistanis spent on internet is one hour fifty minutes. Similarly cyber warfare is gaining more popularity than conventional warfare, and it has become more forceful factor in country politics, culture, and economics. Therefore it is very important to have cyber laws in the country for the proper digital governance.

Pakistan's legislation and law agencies tried many times to draft a national cyber security policy and other relevant laws, but all in vain due to disapproval of opposition parties and organizations of civil society. Therefore, the complete nonexistence of the dedicated cyber security strategy, the government is relying on the amplified version of the internet and ICT civil laws to regulate and govern the national cyber space landscape. The cyber initiative (laws, regulations, policies) to protect the national cyber security and their loopholes has been discussed in this chapter. (Tracking cyber Crime Legislation –Bolo Bhi , 2015)

5.1 Cyber Laws of Pakistan

5.1.1 Pakistan Telecommunications (Re-organization) Act 1996

It is the first national initiative by the Pakistan government for the reorganization of telecommunication infra-structure in the country, which provides the basic general legal framework. The very important section 54 is pertinent to cyber security states authorities are legitimize to trace/intercept calls and messages for the sake of interest of national security.

(XVII OF 1996 An Act to provide for re-organization of telecommunication system, 2013) `

"……**in the interest of national security or in the apprehension of any offence, the Federal government may authorize any person or persons to intercept calls and messages or to trace calls through any telecommunication system."**

Digital right activist fear that this clause can be misused for personal aims. This clause should be rephrased, by assigning the limit to this service such as mentioning the terms, conditions and under what circumstances they can intercept electronic information. The Babar, the opposition leader of senate belongs to PPP in 2017 presented the document o the senate in which he mentioned the state agencies continues to invade privacy and he said he feels that his phone had been intercepted. Also the Saleem Mandviwala, who belongs to PPP claimed that federal government intercepts his phone and personal data.

5.1.2 National IT policy and Action plan (2000)

It covers most of the cyber infrastructure making important security provisions i.e. setting minimum encryption standards, local map exchange, digital signatures, did classification of electronic information, sponsoring of symposium on internet security, local mail exchange etc. It is considered a guidance structure for the formulation of cyber security strategies and IT laws in Pakistan. (Pakistan IT Policy and Action 2000, 2015)

Best practices should be incorporate in IT laws for protecting the secrecy and privacy of data and transactions such as online child safety, more usage of electronic transaction method. The one very important point that has not defined adequately in the policy is the protection of fundamental right of netizens.

5.1.3 Electronic Transaction Ordinance ETO (2002)

This is the first Pakistani cyber law regulating ordinance aiming at organized use of IT. It assists to reorganize and facilitate the electronic communications, electronic documents, all sorts of electronic records of communications and transactions. Important points of the ETO (2002) pertaining to the security of digital information and environment are as under: (Electronic Transaction Ordinance (ETO) 2002, 2015)

Section 36: “Violation of Privacy of Information”,

To access the information illegally by the cyber violator will be imprisoned 7 years and get fined up to one million, or in the worst scenarios both. This is getting the common case in Pakistan, many state agencies instead of spying on terrorists are found of guilty of tracking their enemies’ personal communications online. Also the citizens of Pakistan are often accused of this, recently the cyberstalking has increased and resulting in blackmailing and ransom, mostly the girls are victim. There are many cases like they invade the privacy of girl on social media asking them for picture and afterward resulting blackmailing them for money or sexual benefits. The banks also leaked the information of the bank holders without proper allegations of wrongdoing.

(https://bytesforall.pk/sites/default/files/State-of-Privacy%20Pakistan.pdf)

Section 37: “Damage to Information System”,

Any person found guilty of editing, transmitting, modifying, using, or processing information without the permission of the author will get imprisoned for 7 years and fined rupees one million or both. NADRA the biggest data hub, the Turkish hacker claimed that he had hacked NADRA servers and also of FIA. The Punjab Information Technology Board was responsible for the leakage of the personal data of the thousands of citizens.

Section 38: Cyber Offences

All offences are non-bail able, under this act.

Section39: Prosecution and Trial of Offences

Only the Court of Session or other superior court would deal with the offence.

Other provisions in ETO 2002 are prevalent to

a. Advanced Electronic Signatures (AES) , ES (Electronic Signatures) and the pertinent offences
b. Certification Service Providers (CSP) accreditation
c. Protection against Denial of Services (DOS), spyware, hacking, etc.
d. Network Service Providers limitation etc.

Despite contained best practices for the national cyber security laws for the cybercrimes, it has many flaws such as not defined the integrity of electronic data systems and networks, compromised confidentiality. ETO covers 21 different cybercrimes. Therefore, ETO 2002 must be revised and extended to cover parameters like non-repudiation, authentication, privacy, trustworthiness, etc. to deal with the cyber issues of cloud computing risks, mobile data leaks, cyber extortion etc.

The ETO 2002 also lacks the e-commerce transaction section, e-banking, employment directives in ICT, outsourcing of digital assets etc. ETO 2002 is also blamed for giving pervasive rights to FIA which has resulted in the unnecessary seizure of innocent people properties and their imprisonment.

5.1.4 The Defamation Ordinance 2002 and Defamation Bill 2004

According to the ordinance, defamation can be harming someone’s reputation unjustly by a false written statement (libel), or a false oral statement. The defamation ordinance 2002 mostly deals with the online cases libel, slander, blasphemy. The modified bill of 2004 supported the defamation ordinance of 2002, with few additions and amendments. But it was not strictly enforced by the government. (The Defamation Ordinance, 2002) The severe allegations of ARY media group on the Jang and Geo media group is also a major case of defamation.(UK judge orders ARY to air summary of judgment in defamation case; DAWN, 2016)

5.1.5 PEMRA Ordinance (2002, 2007)

The Ordinance 2002 of Pakistan Electronic Media Regulatory Authority (PEMRA) (PEMRA Ordinance 2002, 2011) is supported by the PEMRA Amendment Act 2007; PEMRA assists the proper organized regulation of electronic media and issue certificate, license to both national broadcast media and international broadcast media and distribution of media operators. In reality PEMRA misuses its power and the authority to abuse the freedom of electronic media under the cover of national security and stability, hence constricting the fundamental rights of citizens restricting their views and limiting their freedom of expression. Recently the PEMRA bans the reenactment of crimes such as rape, murder, suicide and also said legal notice to the producer of drama uddari for the unethical scenes in the drama. PEMRA should direct its energies where they are required.

5.1.6 Payment System and Electronic Fund Transfer Act 2007.

This fund transfer act is presented and prepared by the State Bank of Pakistan providing e-regulatory framework for fund transfer and e-payments. It also had the electronic security provisions for payment instruments, the liability of consumer, financial institutions, and real-time gross settlement. It covers many aspects of e-commerce ignoring few like micro-payment systems etc. (Payment Systems and Electronics Fund Transfer Act, 2007) There are a lot of digital fraudulent online cases in Pakistan like the person preparing the international debit card having stolen credit card information in the name of his father or mother and used them for online shopping.

5.1.7 Monitoring and Reconciliation of Internet Telephone Regulations (2008, 2010)

This regulation is for to prevent the secret communication of terrorists in the Pakistan cyberspace. It imposed ban on the VPN and signaling encryption, thereby allowed the state to do obscure indirect internet surveillance .But this ordnance didn’t work out for the e-commerce market such as for banks and financial institutions ,which have to make use of VPN’s and encryption which provide their service worldwide.

5.1.8 Net Café Regulation Act (Punjab Cyber and Gaming Cafe Regulation Act, Jan 2012)

This act was made to prevent the cases of online harassment and identity thefts .This act made it mandatory for the owners of internet café to have a detailed data of their customers especially their names, CNIC, contact details etc. (Rehman, 2015). In case the offenders couldn’t be located, the café owner’s to held responsible for the cybercrimes committed from the internet café, being run by him/her.

5.1.9 Draft National ICT policy 2012 (revised)

The ministry of Information and Technology, the Secretary IT issued the draft national ICT policy in 2012 (revised). This policy basically focused on the national security such as integrity and confidentiality of the information and communications, preservation of national security but it didn't mention security aspects considering the wide use of IT. (Draft National ICT Policy, 2012)

5.1.10 Draft Cyber Security Strategy for Pakistan 2012

The cyber task force (CTF) formed the first ever draft cyber security strategy for Pakistan. It was established by Pakistan senate defense committee in 2012.The following key components of the draft strategy are as follows

1. Need for cybercrime legislation
2. Establishment of a Joint Inter services Cyber Defense Command
3. Creation of computer emergency response team
4. Formulation of Cyber (rules of the Game) within SAARC framework especially between Pakistan and India, therefore each country ensure each other that they will not violate the cyber rules, and neither side engages in cyber warfare or hacks each other websites.

5.1.11 Surveillance 101/Fair Trail Act 2013

This act permitted the military and state to intercept the private communication of any netizens without their consent, to do online surveillance for preventing the acts of terrorism. According to this law investigation in terrorism activities can be done by Intelligence bureau, Director General of Inter-Services Intelligence, police and three services intelligence .This act in many instances failed to provide certain data of the activity under surveillance and mostly officials used it for their personal motives too. (Investigation for Fair Trial Act, 2013)

5.1.12 Mushahid Hussain's 7 Points Action Plan

The Chairman of Senate committee, Mushahid Hussain Sayed gave 7-point Action Plan to address the defense and defense production in 2012. These points are summarized as under (Khan,2012)

1. To formulate cyber security legislation
2. Creation of National Computer Emergency Response Team "PKCERT"

3. To establish cyber security Task Force for combating cyber threats and formulation of National Cyber security Strategy.
4. To build Confidence Building measures between the eight members of SAARC especially with India that these members will not get engage in any cyber warfare with any country.
5. To arrange special media workshops in collaboration with media to promote the cyber awareness among local community and among the people related to IT department, in collaboration with PISA.
6. This is the basic agenda of that seven points action plan for the senate defense committee to secure national cyber security.

5.1.13 National Cyber Security Bill 2014

In 2014 to establish the cyber security council in Pakistan, Mushahid Hussain proposed a bill in Senate. The bill describe the authorities and responsibilities of the council for formulating the policy and outline the proper guidelines, governance models, strategic plans as per international best practices.(7-Point Action Plan to make Pakistan secure from Cybercrimes and attack Senate Committee, 2015)

But however the IT ministry rejecting this bill declared that to be against national security and anti-state. Some shortcomings of the act are as follows.

a) It does not address sufficiently all the issue related to cyber security i.e. unauthorized interceptions, personal data protection etc.
b) It does not provide adequate guidelines on which the council can draft a cyber-security bill
c) It doesn't bind the critical infrastructure operator to equip them with cyber rist assessment.
d) This bill totally counters the trichotomy of the state organs as given in the constitution of 1973.

5.1.14 Laws for Child Online Protection

Cyber law protects the children from the cyber criminals and to keep them away from the pornographic material. It is indispensible to have child online protection legislation. Thereby Pakistan also endorses the following laws with few reservations.

Articles 2 and 3, of the Optional Protocol to the Convention on the Rights of the child on the sale of children, Child prostitution and Child Pornography (Bill for the establishment of a National Cyber Security Council, 2014). Article 3 makes certain that government has taken measures both operational and legal to prosecute the evil offenders.

Articles 16, 17e and 34(c), to the **Convention on the Rights of the Child** (Curbing cybercrimes: Ministry rejects cyber Security Council bill The Express Tribune, 2014) the state provide guidelines to safeguard children from the content of harassment, sexual abuse or exploitation.

The cases of child pornography are very common in Pakistan despite this adherence.

5.1.15 Blasphemy Laws

In Pakistan, the blasphemy laws come under the sections of 295-B, 295-C, 295-A, 298 and 298-A of the Pakistan Penal Code (Convention of the Rights of the Child., 2014)Insult of religious beliefs or passing humiliating statements about holy personalities and deliberate defiling of the place of worship all are regarded as the blasphemous acts. In the cyberspace there is no as such law to block online anti-Islamic content or punishing the offender. The case of Mashaal khan murder as discussed in the last chapter.

5.2 Cyber Crime Legislations

Almost all the developed countries have cybercrime legislations which have laws and corresponding punishments for the cyber offenders found guilty of unauthorized access, interference, or interception of data and the ICT devices systems. Unfortunately, there is no dedicated cybercrime legislation in Pakistan in place yet. However there are some extended laws from some past acts related to computer and internet to penalize cyber-crime. (The Electronic Crimes Act, 2004)

5.2.1 The Electronic Crimes Act 2004

Electronic crime act 2004 was introduced on the basis of the Electronic Transaction Order 2002, to punish cyber criminals and offenders. This law has provisions for the followings (The Electronic Crimes Act, 2004)

- Electronic Fraud
- Electronic Forgery
- Spoofing
- Spamming
- Cyber Terrorisms
- Wagging Cyber War
- Powers of investigating officers
- Illegal access to Electronic Systems
- Criminal access to Electronic Data

According to the Electronic Crime Act of 2004, above mentioned cyber offences can be penalized for 2-3 years imprisonment with a fine of few thousand rupees. However, this law doesn’t address adequately the cyber security threat challenges faced by Pakistan. The definitions provided in the draft mostly are unclear or practically incorrect. Many sections need to be redrafted in this Act. (Rizvi, 2015)

5.2.2 Prevention of Electronic Crimes Act (PECA), 2007

This ordinance took the form of law, when General Pervez Musharraf signed. It remained applicable for a time period of only two years on Dec 31, 2007. This law was meant to control 17 types of cyber-crimes including: (Prevention of Electronic Crimes Ordinance, 2007)

a) Criminal access
b) Criminal data access
c) Data damage
d) System damage
e) Electronic fraud
f) Electronic forgery
g) Misuse of electronic device/system
h) Unauthorized access to code
i) Misuse of encryption
j) Malicious code
k) Cyber stalking
l) Spamming
m) Spoofing
n) Unauthorized interception
o) Cyber terrorism
p) Offences by corporate body

It was the first ever applicable law formulated in Pakistan pertinent to cyber security. But, there were many policy loopholes in PECA. For instance:

- It paid no attention to many international practices, disregarded civil liberties, took no account of business continuity and, therefore, dealt with heavy criticism from industrial groups and civil advocacy.
- There is no adequate strict implementations of the law, therefore, the cybercrimes like Ransom, fraudulent messages and calls of winning prize money and extortion were transmitted unchecked.
- This law offered no safeguards against victims of fabricated electronic evidence. This cybercrime was non-bail able leading to punishment of innocent victims.
- These policy loopholes forced it to pause in 2009. Therefore, in the absence of any cyber security law, under the section 36 (violation of privacy information) FIA registered cases of internet abuse and misuse, under the section 37 of the Electronic

Transaction Ordnance (damage to information system), and the Pakistan Penal Code section 419 (Punishment for cheating by impersonation) of the Pakistan Penal Code.

5.2.4 Prevention of Electronic Crime Ordinance 2009

President Asif Ali Zardari in July 2009 promulgated Prevention of Electronic Crime Ordinance. However, again the combined pressure from the civil society and netizens and various policy loopholes, the legislation got withdrawal from the National Assembly. (Prevention of Electronic Crimes Ordinance, 2009)

5.2.5 Cyber Crime Act 2009

This cybercrime act also rejected due to other parties political motive, although very negligible shortcoming of it. It was suggested by Marvi Memon and Anusha Rehman , as an alternative legislation in place of PECO 2009 . The Cyber Crime Act was presented to the National Assemble as a private member bill. (Mir, 2015)

5.2.6 Misuse of Electronic Equipment Bill

Misuse of Electronic Equipment Bill was formed due to the anti-state messages hovering over the internet media on emails, mobile-phones, etc. It was drafted in December 2011by Ministry of Interior Rehman Malik. This bill restrict the multiple usage of sims and their illegal usage, banned mobile number partiality (MNP), and introduced SMS filtering policy. This bill was very helpful especially in the countries like Pakistan, but unfortunately, it was not enforced strictly.

5.2.7 Draft of Prevention of Electronic Crimes Act (2012, 2013, 2014)

The law firm “Jamil & Jamil” in collaboration with the Pakistan Software Houses Association (PASHA) and the Internet Service Provider Association of Pakistan (ISPAK) revised the nonfunctional PECO. This new draft primarily focused on forgery, financial crimes, electronic fraud, cyber stalking, cyber terrorism, data corruption, defamation, e-mail spoofing, malware infection, unauthorized access to cyber network, information theft, password cracking, intellectual property crimes etc.[116]. The technical assistance of International Telecom Union (ITU) and Council of Europe’s Budapest Convention on Cybercrime was also taken into consideration for the preparation of the draft, so that it has all the crucial clauses to prevent cybercrime in all ways possible. The draft for further consideration was put forward to National Assembly in November 2012. .(ACT To make provision of prevention of the electronic crimes, 2012)This redraft demanded FIA , which got rights under the PECO 2007 provisions to seize data and electronic equipment and conduct searches, to follow all the necessary procedural guidelines given by the act to avoid all kind of power misuse. FIA was reluctant to compromise, which delayed the process.

With little amendment in 2013, Zahid Jamil redrafted the PECO 2012. However after deadlock of a year between intelligence agencies and private sector, finally in 2014 the stakeholders reached to the mutual final terms over PEC Bill 2014 .And then bill was sent to the cabinet. (Legislative bungling: In a bill about cybercrime, MoIT inserts clauses legalizing censorship, 2015)

5.2.8 Draft Electronic Documents and Prevention of Cyber Crimes Act, 2014.

This draft also covers the most of cybercrimes; the one important thing of this draft is that it laid down the establishment of Cyber Emergency Response Team and Cyber Authority Court. (Sheikh,2014) The electronic crimes which it covers are cyber terrorism, electronic forgery, electronic fraud, illegal unauthorized access to the online documents and protection of women's right on the internet. The Act addressed strict punishments for the cyber prosecutors from the minor offence (junk mail) to the massive well organized cyber-attack (country defaming). On top of this, the intelligence agencies have to abdicate the power of snooping on the domestic cyber space, under section 51 of the act. This act declared all offences as bail able making easy for the rich peoples to be exempted from the blame.

In short, this bill gave more control to the government over the cyber space having internet surveillance and censorship, thereby violating the privacy, fundamental rights of speech and open access to the information. This draft has the following shortcomings;

a) Lack of definition: after the enactment of law, this can lead to the practical problems for the netizens.
b) Establishment of state-controlled Cyber Authority Court: It will increase the government power so much that it can intervene in the electronic communication, also encryption and electronic signature.
c) Minor offences like junk mailing and cybersquatting are non-bailable with regard to the act, also the imprisonment up to 3 years.
d) Internet activities like hacking and spoofing are referred as strict legal offences, without taking effect into account- a problem for pen testers and ethical hackers.

5.2.9 Prevention of Electronic Crimes Act 2015

The major drawback of the PECO of 2014 was that, although got approval from the Ministry of Law, the Ministry of IT rejected on the act for being non0pertnent to the National Action Plan. Civil society Activists voice their concerns against the draft before the draft was presented to the National Assembly Standing Committee on Telecommunications and IT for approval. (Prevention of Electronic Crimes Act, 2015)

The parliamentary sub-committee consisting of four members was set to amend, review and finalize the PECO 2014 draft, in Feb 2015 .The Jamil's PECO 2014 draft (industry stakeholder draft) emerged from the Cabinet Division with certain modifications. The Ministry didn't invite anyone from the IT's sectors especially PASHA or ISPAK. The Jamil, original architect of the PECO 2014, wasn't even invited who has been advising many countries on cyber security legislations for Cyber Crime treaty and the European Union. The main points of the PECO 2015 are as follows:

a) Sending e-mails and SMS to anyone without their accord is a crime.
b) Police, FIA and other agencies must have a warrant to arrest or to before investigation or seize someone's personal property etc.
c) All ways of political criticism even the memes, cartoons etc., are come under cyber-crimes.
d) Government can block any online website if it was consider inadequate. All places, under the section of 26, equipped with the internet facility especially ISP's, hotels, airports, shopping malls, offices must have data record of 3 months.

The new draft was sent to the Cabinet Division, after the approval from the IT ministry, for consideration in 2015. The civil society also presents their reservations after the acceptance from the Cabinet. Considering unprofessionalism attitude of FIA officers, the state government withdraws the cybercrime investigation from purview of FIA and created a new department to deal with cybercrime cases. Also the new cybercrime agency recommends giving authority to PTA to block any objectionable website. (Independent agency proposed in final draft, 2015)

This bill draft was an attempt to convince Google for creating YouTube local version. Nevertheless, this draft faced huge criticism from the IT industry, human rights organization and the netizens, who consider the bill as stringent, punitive and unreasonable. Civil disagreement main reasons are:

- **Vague definitions:**

There are uncertain definitions of unauthorized access, illegal access to ICT system, unauthorized interception, electronic fraud, electronic forgery, identity crime, spamming, identity information, cyber stalking etc. Many are legally and technically flawed. (Opennet.net, 2015)

- **Undefined Words:**

Many words are not defined and; they are left to open interpretation such as injury, crime, damage etc.

- **Unlimited Blocking of Internet Content:**

Under section 31, Pakistan government got right to block any website.

Ignored legal protections and rights of netizens:

Electronic communications including caricatures and cartoons, which are intended to harm the reputation or defaming of any individual can subject to the punishment of several years. (Sindh govt to block WhatsApp, Viber & other services for 3 months, 2013)

- **Unclear delegation of responsibilities of Cyber Authority:**

The responsibilities of the authority are very vaguely defined; especially the non-transparent and non-accountability of power and thus lead to abuse of power.

- **Private entities little presentation in the Cyber Authority:** This act leads to the direction of government authorities, while giving little presentation to private entities in cyber authority .This will allow government to handpick candidates. (Policy for Internet, Intranet, Websites, and E-Mail in Federal Government Organizations, 2014)
- **Uncertainty of certificate accreditation:** There is no credibility of the system work.
- **Removal of safeguards:** The initial versions of the safeguards have been removed/ amended to give the government free hand, so cyber-criminal can be defined by their choice.

Non proportional punishments:

The punishments are not in accordance with the crimes. The draft also missed details considering data/system access, phishing, website censorship by the state etc.

- **Undefined description:**

Undetailed and undefined processes to determine a crime, leading legislation liable to abuse and misuse and, consequently cause innocents to be charged

- **Replication:**

Many portions of the act have been replicated from the India Information Technology Act 2000 like, PEC Act section 44 and 45 are a replica of India IT Act Section 43 and 45. Also, the sections 54 and 55 are offsets of India Act Section 67 which itself was highly objected for transgression into Indian citizen personal liberties and also for not considering the latest IT technologies. (PTA, Protection from Spam, Unsolicited fraudulent and obnoxious communication Regulations, 2009)

5.3 E-Regulation

For E-Regulation the government of Pakistan has taken many measures for social and electronic media. Such as;

5.3.1 Net Café Regulation

In 2002, PTA directed net cyber café to keep the record of their all customers. When cyber café become hub of cybercrimes then again in in 2012, “Net Café Regulation Act” was drafted.

5.3.2 Formulation of Inter-Ministerial Committee for the evaluation of websites (IMCEW)

This does evaluation of the websites and restricts online offensive material in the cyberspace. It was formed under 2006, under the Ministry of Information Technology.

5.3.3 Monitoring VoIP content

PTA asked ISPs to do surveillance of the misuse of VOIP, in 2009. These applications are found to be used by the terrorists.

5.3.4 Policy for Internet, Intranet, Websites and E-Mail in Federal Government Organizations:

Government designed a special policy for internet, in 2009, for email, Web-Sites etc. to secure the government's computer. Multi-layered security solutions were established, according to Data Center (DC), for internet and intranet across 42 federal government divisions.

5.3.5 Protection from Spam, Unsolicited fraudulent and obnoxious communication Regulations, 2009:

This regulation was passed to control spams. The regulators had to create Standard Operating Procedure (SOP's), black list, Do not Call Registers (DNCR) to control spams. (PTA, Protection from Spam, Unsolicited fraudulent and obnoxious communication Regulations, 2009)

5.3.6 Retention of Internet log:

It increased the retention time for internet logs from 45 days to 90 days.

5.3.7 SMS Filtering:

In 2011, PTA issued the list of 1000 words which were meant to be blocked, to effectively filter offensive messages. But unfortunately the decision was regressed due to huge objection.

5.3.8 Ban on Encryption

PTA ordered ISPs to give the report of all the customers using Virtual Private Network (VPN)

5.3.9 Internet & E-mail Policy for Government Departments 2011

This policy mainly describe rules for acquisition of internet connection, hosting of government web pages/portal, exchange of official emails, monitoring of network traffic, mail servers, security trainings and strict implementation of the policy to make it practical and that the government departments are safe from hacking and intruding attempts. (Pakdocs.com Internet & E-Mail Policy for Government Departments, 2011)This policy was given by NTISB to regulate the use of online communications and internet in state departments.

5.3.10 Blocking of offensive content

a) Blasphemous site: Government of Pakistan is on the mission of blocking the blasphemous sites since 2003. Most of the proxy websites which are used to access the blocked content were also got blocked. In 2008, when YouTube didn't block the videos showing Holy Prophet (PBUP), then all the URL's and IP addresses got blocked from Pakistan. The Facebook, YouTube, Wikipedia, Flickr pages having the caricatures of the Holy Prophet (PBUH) were blocked, it remained blocked until they removed them. However, the trailer of the movie "innocence of Muslims" containing blasphemous content, resulted in a world-wide ban on YouTube for almost 3 years, until removal from internet in January 2016. ("YouTube Ban Finally Official Removed In Pakistan" , 2016)

b) Pornographic material

With the passage of time government take instant and frequently measure to block the website containing indecent material. In 2003, government blocked 1800 websites containing pornographic material. In 2017, 17,000 pornographic website got blocked due to massive crackdown lodged against online pornographic sites. **(Pakistan to block over 400,000 websites; The Express Tribune, 2016)**

c) Anti-state content

There is a massive block of the websites containing anti-state content in 2006. Also on frequently basis ISP's have a check on internet blocking website containing anti-state content. (PTA to deploy "national firewall" to block sensitive content in Pakistan; Techjuice, 2017)

d) **National URL Filtering and Blocking System**

PTA under the supervision of Ministry of Information Technology proposed the idea of National URL Filtering and Blocking System, which function is same as the Great Firewall of China to review millions of webpages containing objectionable content in less than one second. The objectionable content includes all the above mentioned three contents. (E-regulations Timeline Bolo Bhi, 2015).

e) Website Monitoring Assigned to PTA

This website monitoring task was formed after the dissolution of the IMCEW (Inter-Ministerial Committee for the Evaluation of website). In 2015, the Ministry of Information and Technology, on the basis of the petition, dissolve IMCEW because it is prone to political hijacking and gave the task of website monitoring to the PTA. (Website monitoring assigned to PTA, 2014)

f) Viber banned for government officials

NTISB banned the application of the famous instant messaging smartphone app “Viber” for all government officials, because of weak encryption and for security purposes. Also Israel Defense Forces spying on the monitoring and handling of user’s online communication. (Use of web applications Viber, 2015)

5.4 Conclusion

From the above mentioned discussion it was concluded that Pakistan has no cyber security policy. Cyberspace is regulating through the Electronic Transaction Ordinance of 2002 with many shortcoming. There is no criminal legislation and also there is no roadmap for governance. All the policies discussed above are never been impressive , government always wanted to have the major centralized control over the internet, therefore snatching the netizen’s liberties and freedom of expression for under the name of national interest. When the federal government decentralized their control over internet and the law makers acquired the policy of multi-stakeholder approach over political power show and equipped the IT department with the latest technology trends, only then cyber security regulation start being effective in the country.

Chapter 6

MEASURE TAKEN FOR CYBER SECURITY CAPACITY BUILDING IN PAKISTAN

Cyber security capacity building is intended to enhance cyber security through the cyber awareness programs, strengthening the internet rights in cyberspace, development of the skilled workforce, threat information sharing, building international computer emergency response teams, making international agreement etc. This chapter discusses the role of government, public and other private sector national initiatives for cyber security capacity development in Pakistan. The facts have been collected through different sources including; interviews, surveys and relevant websites.

6.1 Responsible Agency

Pakistan has officially no central recognized department, agency, advisory council, working group, committee, cross-disciplinary center for implementation of a national cyber security strategy/policy, organizational structure for development of incidence response etc., unlike most of the countries. There are individual institutions under the ministry of Information and Technology to perform the task of cyber security building.

6.1.1 National Response Center NR3C 2009

In 2009, FIA established a national crime unit called NR3C (National Response Center) especially aimed to deal with the issues related to cyber-crimes. NR3C functions are: (National Response Centre for Cyber Crime, 2015)

a) Effective investigation and prevention of increasing cyber offences in the cyberspace,
b) Digital, responder and forensic services On-demand,
c) Apprehension of cyber criminals
d) To coordinate with international Law Enforcement Agencies

NR3C can only function most effectively and adequately if it has cyber expert and more funds, unfortunately which it lacks.

6.1.2 National Telecom and Information Technology Security Board (NTISB)

The former name of NTISB is NCSB (National Communication Security Board), this NTISB is the main factors for cabinet division to serve as secretariat. NTISB perform following functions with regard to cyber security

a) Formulate national security standards (NSS).
b) Administer the Department of Communication security.
c) Revise technical manuals and cryptographic guidelines.
d) Organize seminars and conduct trainings on cyber security for public awareness
e) Validate and certify Information Technology products with embedded encryption module.
f) Conduct from the different departments of government IT security audit.
g) Regularly inspect public communication centers.

h) Regulate the selection of the secure ICT devices.
i) Assist implementation of “Federal Government E-mail & Internet Policy” to federal organizations
j) Assistance to federal government on ICT policies related to cyber security issue. (http://www.cabinet.gov.pk/cabinet/userfiles1/file/Cabinet/wings/ntisb-wing.pdf)

6.2 Incident Management Capabilities

Incident management approaches such as National Computer Security Incident Response Teams (CSIRT), early warning systems, Information Sharing and Analysis Center (ISAC) etc. are adequate means of securing, identifying and responding to cyber threats. There are many measures taken by government and private sectors of Pakistan to form such incident management capabilities.

6.2.1 Establishment of National Cert “PakCERT”

PakCERT is officially recognized incident response team establishes in January 2001(Azam,2015) It was formed with the central aim of preventing, detecting and responding to national cyber threats, along with the distribution of the pertinent security advisories amid the national cyber community but unfortunately there is no PakCERT now. Various functions of Pak CERT performed are:

a) Cyber Risk Assessment
b) Forensic investigation
c) Penetration testing
d) Creation of a security policy framework and its implementation
e) Encourage compliance to ISO 17799 and to BS 7799
f) Train technical workforce of private and public organizations regarding Assurance and Information Security.

It has the honor of successfully founding two serious threat vulnerabilities in Microsoft.Net Passport services, which if exploited can cause harm to the 200 million Microsoft user worldwide but unfortunately it remained operational since 2011. It also discovered the YAHA Virus, injected in Pakistani computers. In spite of this, PakCERT was also a member of Asia Pacific Security Incident Response Coordination Working Group (APSIRC-WG). The major shortcoming of PakCERT is that at national level it cannot response to computer emergencies

6.2.2 Establishment of Public CERT “PISA-CERT”

It was established with aim to diminish the misconducts of the computer but it didn't get success in his goals, and is not operational anymore. It is merely theoretical CERT with practical limitations by Ammar Jaffari.

6.2.3 Establishment of National Response Center NR3C under FIA (2009)

It was established in 2009 by FIA to eradicate the misuse and abuse of internet in the country. It informs all the victim organizations about the cyber threats timely, the most common cyber threat of which is DOS attack. To address cybercrime emergences, it established the cybercrime Hotline. It also launched SMS Alert System to update about trending cybercrimes to the people, including fake advertisements, fake price money and other privacy matters but limited to it.

6.2.4 Establishment of Digital Forensics Laboratories at provincial level (2012)

To trace the offenders committing e-crimes the government established Digital Forensic Laboratories**.** Punjab Forensic Science Agency has a computer forensic (Pakistan Forensic Science Agency (PFSA), 2015) Sindh Police Forensics division has Digital Forensic Science Laboratory (Digital forensic lab to probe heinous crimes, 2015)

6.2.5 Cyber Net's Specialized Cyber Security Team. (2010)

Cyber Net established a specialized joint team with authority and capability to manage all sorts of network misuse and abuse in joint collaborations with APNIC in 2010. At present on monthly basis Cyber Net manges100 cases of internet misuse. (A. Siddique, 2016)

6.2.6 Establishment of Academic CERT "NUST CSIRT" (2013)

It is the Pakistan's first academic CERT established by NUST University in 2013 called "Computer Security Incident Response Team". NUST CERT frequently responds to the cyber security complaints and timely spread security information and advisories regarding dereliction attacking the national cyberspace, but it targets limited selected audience basically students. It doesn't address any major national computer emergency issue but on university level they address many small privacy issues related to app developing. They basically keep the university update about the latest cyber-attacks. NUST CERT frequently responds to the cyber security complaints and timely spread security information and advisories regarding dereliction attacking the national cyberspace, but it targets limited selected audience basically students. It doesn't address any major national computer emergency issue but on university level they address many small privacy issues related to app developing. They basically keep the university update about the latest cyber-attacks. (NUST official website)

6.3 National Cyber Security Awareness Initiatives

In Pakistan there is a lack of the general awareness of the cyber security among the decision makers, professionals and particularly among the common masses. To help disseminate cyber awareness, the general public and private sectors often organize conferences, campaigns, seminars and security guidelines on the hot cybercrime issues too Pakistan (Institute for Parliamentary Services (PIPS), 2015) However, they are still not effective with the general public who must needs to first understand that cyber security is the mutual responsibility and they should play their part. Some of these are:

6.3.1 Awareness Seminars

Agencies and alliances that have struggled to organize cyber security awareness seminar for the local masses include the following.

a. Pakistan Information Security Association

PISA is actively and effectively spreading cyber awareness in Pakistan and is non-profit organization. PISA conduct most successful seminars are as under:

1) **Defending Pakistan through Cyber Security Strategy:** It was very successful seminar deliberations developed 7-point Action Plan on cyber security. It was organized at Pakistan Institute of Parliamentary Services (PIPS) by the joint efforts of PISA and Ripah International University. (Institute for Parliamentary Services (PIPS), 2015)
2) **Cyber Security Awareness Seminar:** It was held at LUMS in 2013 by the joint collaboration of PISA and Cyber Security Task Force for creating awareness among industry professionals and students regarding increasing cybercrimes, cyber terrorism and cyber threat.
3) **International Chapter programs:** They are international non-profit chapter programs of ISC2, Cloud Security Alliance, ISACA, Internet Society (ISOC), ISACA etc. have established in Islamabad, Lahore and Karachi. These programs assist in increasing the level of cyber consciousness by building a focal network of peers to spread cyber security knowledge, expertise and resources etc.

a. PakCERT

It organize information security seminar at national level and deliberate valuable presentations in different IT events; conferences, campaigns, workshops, etc. but it is not operational now.

b. National Response Center for Cyber Crimes (NR3C)

NR3C is the very active organization with regard to arranging workshops and conferences on cyber awareness and educate people about the general knowledge of Cyber Security. It has conducted more than 40 workshops/seminars to deliver the knowledge of cyber security to more than thousand industrialist and government personnel in many cities of Pakistan. Major seminar conducted are listed down. (Federal Investigation Agency, 2015)

1. “Cyber Security Challenges and Solutions” up to middle and senior level management from the period of 2002 to 2004. More than thousand professionals attended that seminar.
2. “Coordination Efforts to Combat Banking Related Cyber Crimes and Money Laundering”. Forty senior bank executives attended this seminar in 2003.
3. “Processing of first Cyber Crime Case” by NR3C in 2003.
4. “Coordination efforts to combat ISP’s related Cyber Crimes” in 2003.
5. “Cyber Crimes for SIG” conducted in 2004 by FIA Academy.
6. Lecture on “Information Security” in NAB from the period of 2007-2008
7. Seminar on “Cyber Threats to Critical Cyber Infrastructure” in April 2008
8. Lecture on “Cyber terrorism and Eminent Threat of Cyber Crimes” delivered to professionals in April 2008, etc.

c. Sustainable development Policy Institute

Sustainable development Policy Institute conducted a conference on “Cyber Security and Emerging Threats” in Jan 2016. Like other conference it scope was also limited.

6.3.2 Cyber Security Conferences and Journals

The famous Cyber Security Conference that has been conducted in Pakistan till now are:

a) The first security convention of Pakistan was held by Pakcon, from 2005 to 2007
b) National Conference on Information Assurance at MCS (NUST2010, 2013)
c) “Privacy Rights and digital surveillance” national Conference in Pakistan conducted by Digital Rights Foundation in 2014. (National Conference on Privacy Rights, 2015)
d) Ripah International University and Pakistan Naval Engineering College, NUST (2014) organized “National Information Security Conference” (NISC)
e) Cyberspace Conference held in Islamabad in February 2015.
f) Bahauddin Zakariya University conducted Cyber Security Conference (CSC) in Multan May 2015
g) Conference on Information Assurance and Cyber Security (CIACS) from 2014 to 2015

h) Annual Conference International Bhurban Conference on Applied Science and Technology (IBCAST) also has semi focus on cyber security.(Cyber Defense Day to be celebrated by PISA…, 2015)
i) Pakistan Internet Summit held in April 2016.
j) "International Journal of Communication Networks and Information Security" (IJCNIS) by far is the only international journal from Pakistan related to information security, which publish research journals thrice a year. Kohat University of Sciences and Technology (KUST) manage this Journal. (H. Malik, 2014)

6.3.3 Cyber Security events

6.3.3.1 Cyber Secure Pakistan

PISA start an initiative named as "Cyber Secure Pakistan", in 2013 it is the leading cyber security event of Pakistan which is bringing together specialists, experts, professionals and executives on the platform of cyber security. But it just happened once. (Cyber Secure Pakistan; The News, 2013)

6.3.3.2 Cyber Defense Day

In the history of Pakistan on september6, 2015 first time ever Cyber Defense Day was celebrated. Number of digital security professionals and students attended this to discuss and share their views about the emerging cyber security challenges and threats caused to Pakistan. Also the participants had the free certified training of hacking countermeasures. (H. Malik, 2014)

6.3.3.3 Participation in PACERT's Cyber Drill

Asia Pacific Computer Emergency Response Team (APCERT) organized an International Cyber Drill where professional from PISA-CERT, CASE, and CARE participate annually as a team called Pakistan Research Center for Cyber Security (PRCCS) in 2012. Pakistan team got leading position over teams from china, Vietnam, OIC CERT, Australia and Taiwan. (H. Malik, 2014)

6.3.4 Cyber Security Scouts

NR3C FIA has taken an initiative at grass root level named as "Cyber Scout". These Cyber Scouts are actually students from various universities and colleges, to whom cyber security defensive and preventive training is given to assist them to raise cyber awareness amongst their friend, class fellows and parents. (National Response Centre for Cyber Crime- Cyber Scouts, 2015)

6.3.5 Civil Protection Agencies Cyber Security Awareness Campaigns

For spreading cyber security awareness amongst the general public, there are few non-profit domestic civil protection agencies. They also fight for the fundamental rights of the netizens.

Many times these civil domestic agencies stand against infringement of digital rights in Pakistan. Famous amongst them are:

a. Bytes for All, Pakistan,
b. Media Matters For democracy,
c. Digital Rights Foundation (Digital Rights Foundation, 2015),
d. Internet Policy Observatory Pakistan (IPOP), Quetta
e. Peace Niche,
f. Bolo Bhi,
g. Pakistan for All. (Pakistan for All, 2015)

They initiated many campaigns against misuse of the internet, inhuman crime bill, mass surveillance by the government, etc. includes:

6.3.5.1 Writing on the Wall: Poster Advocacy Campaign

This campaign was started by Bolo Bhi against the Cyber Crime bill 2015 before it got approved by the National Assembly. It also recognized the changes the government made in industry stakeholder draft of 2014 of the Cyber Crime Bill, they have been partially successful in coercing the government to amend those changes and pass the draft in the original form. (The Story So Far – Bolo Bhi, 2015)

6.3.5.2 Jasoosi Band Karo

Digital Foundation Rights launched this campaign in collaboration with Bolo Bhi, Electronic Frontier Foundation (EFF) and Privacy International (PI) in 2014, to raise voice against unrestrained e-surveillance by the intelligence agencies and the state government. (https://jasoosibandkaro.pk/)

6.3.5.3 Hamara Internet

Digital Foundation Rights started this pioneer campaign against internet technology related abuse for promoting a secure and free cyberspace where women can participate freely. (Digital Rights Foundation, Hamara Internet, 2015)

6.3.6 Cyber Security Manuals, Books and Guidelines

Some of the famous guidelines, manuals, books and Action Plans issued regarding cyber security of Pakistan, are Guidelines by State Bank of Pakistan, Internet Training Guidelines, Telecom Security Guidelines, Guidelines by NTISB, A Beginners guide to Ethical Hacking. They are discussed as below,

6.3.6.1 Guidelines by State Bank of Pakistan,

There are many several guidelines issued by the state bank of Pakistan related to information security.

a) Business Continuity Guidelines to protect IT based banking systems from terrorism and natural disaster. (September 2004)

b) Guidelines for the user using Credit/ Debit and Smart Cards. (Dec 2005)

c) Regulations for the protection of Internet Banking(2015): To alleviate security risks pertaining to internet banking this calls for regular security risk assessment of ICT systems and data, controls monitoring, implementation of security controls , launching a customer awareness program, etc. (Internet Trading Guidelines, 2005)

6.3.6.2 Internet Training Guidelines, 2005

Security and Exchange Commission of Pakistan (SECP) in March 2005, issued trading guidelines for the Internet Service Providers having compliance to international standards and keeping CIA of processed, stored or transmitted data. (Securities and Exchange Commission of Pakistan, 2005)

6.3.6.3 Telecom Security Guidelines, 2005

PTA issued network related security guidelines and general telecommunication for all telecom stakeholders in 2010. This document also contains relevant guidelines for recovery and physical security, security standards and international best practices. (Telecommunication Security Guidelines, 2010)

6.3.6.4 Telecom Security Guidelines

Senate Standing Committee on Defense and Defense production issued first ever manual related to online, print and electronic media in collaboration with German Foundation Konard-Adenauer-Stifung (KAS). (Telecommunication Security Guideline, 2010)

6.3.6.5 Guidelines by NTISB

NTISB for all the state officials of Pakistan issued certain cyber security guidelines in Sept 2013, and made its implementation mandatory for all of them. The guideline called for (Attaa, 2013)

a) Avoid coping official sensitive data on personal laptops, computers and USB,
b) Abstain from downloading software's from the internet,
c) To isolate computers connected to internet from the internal network,
d) To properly scan the official content on websites,
e) To use the internet connection of National Telecommunication Corporation (NTC)
f) Government department's internet usage regulations.
g) For official correspondence avoid the usage of private/free email services.
h) Abstain from uploading the official information or photos/ videos of official gatherings on social media.
i) But government official blatantly ignored these guidelines.

6.3.6.6 A Beginners guide to Ethical Hacking

Pakistan has the youngest hacker Rafay Baloch, who has written three very informative books on cyber security. In 2010, he wrote "A beginner guide to Ethical Hacking, in 2011, An Introduction to Keylogggers, RATS and Malware" and "Ethical Hacking and Penetration Testing Guide" in 2014.These book can give the reader a great insight of ethical hacking for security systems. (Mansab, 2015)

6.3.6.7 Online Cyber Security news

There is an unofficial advisory group of Facebook created by few Pakistani students and professionals to keep the audience update about the latest cyber threats, hacking news, cyber security breaches and cybercrime regarding Pakistan. The cyber news website "**Who Got Hacked**" is the most renowned online cyber news website.

6.4 Information Security Manpower Development

Academic institutions, the research community, training centers and NGO's etc. can lead to development of trained competent work force. It can instill essential security skills to perform effectively to as many individuals as possible. Several institutions in Pakistan offer degree programs in security training, information security, and international security certification and have form research collaborations for cyber security manpower development.

6.4.1 Information Security Degree Programs

Many institutions in Pakistan currently offer Information security degree programs in Masters and PhD students. While in Bachelor's degree students are just taught two or one subjects regarding information security such as Forensics, Network Security and Computer Security. In schools and colleges there is no concept of cyber security education.

To find out the educational institutions offering degree in Information Security a survey was conducted, results are shown below.

a) **Military College of Signals, NUST.**

MCS is the first ever institute in Pakistan to offer the degree in Information Security both at graduate and postgraduate level since 2001.

Degree Programs: Master's students (145) and PhD's student (9) have graduated so far.

Student groups: Pakistan first Information Security Group NUST ISACA Student Group (NISG) is 22nd in the world.

Trainings: It trained more than 400 Information Security professionals and organize dozens of trainings (CSCU, CISA, CHFI, CEH, CISM, CISSP etc.)

Conferences conducted: Conference on Information Assurance and Cyber Security (2014, 2015), National Conference on Information Assurance (2010-2013).

Other initiatives: MCS has the honor of establishing Pakistani's first academic CERT named as NUST CSIRT (NUST computer security incident response team). Its focal aim is to raise the cyber security awareness and increase security emergency preparedness.

b) **School of Electrical Engineering and Computer Scineces(SEECS), NUST.**

Degree: It offers the degree in MS Security Information, until now 44 students have been graduated so far. (Applied Information Security: Ais.seecs.nust.edu.pk, 2016)

Lab: It has Advanced Information Security (AIS) Lab in collaboration with Royal Institute of Technology, Sweden.

Conference Conducted: Cyber Secure Pakistan (2015)

c) **Ripah International University, Islamabad** (MS Information Security, 2015)

Degree programs: Master in Information and Security

Faculty: 1 PhD from Australia, 1 from Japan and 2 from UK

Students groups: Offensive, Security, Network Security,

Trainings: it has conducted 30 training (CEH, CSCU, ECSA, CHFI, LPT, CISA, CISM, CISSP, CRICS) across Pakistan and trained more than 350 Information Security Professionals.

Conferences Conducted: National Information Security Conference (2014)

Other initiatives: formation of Information Security Team

d) **COMSATS Institute of Information Technology, Islamabad**

Degree programs: Master in Information and Security

Conferences Conducted: International Training Workshop On internet Security for 5 days in 2012

Center for Advanced Studies in Engineering Case University, Islamabad (MS Information Security, 2016**)** (CASE: Center for Advanced Studies in Engineering, 2015)

Degree: Master and PhD in Information and Security

Student group: “Communication, Network and Security Group”

e) **Air University, Islamabad (MS in Avionics Engineering-Air University. 2016) a center for cybersecurity excellence has been established in Air university offering the BS and MS programs in cybersecurity.**

Degree: Master in Information and Security

Research Center: Security and Cryptology Cell

Institute of Space Technology, Islamabad

Degree: Master in Information and Security and Cyber security (Master of Information and Cyber Security. 2016)

Conference conducted: international Conference on Aerospace Science and Engineering having cyber security as main theme.

f) **NED University of Engineering and Technology, Karachi** ([NEDUET] – ACADEMIC PROGRAMMES, 2016)

Degree: Master in Information and Security

g) **Punjab College Of Technology and Management Sciences Lahore**

Degree: Master in Information and Security (Punjab College of Technology And Management Sciences Lahore Admission announcement for Bachelor Master PCTMS admissions, 2014)

h) **Szabist University, Islamabad, Karachi (SZABIST Islamabad, 2015) and Suffa University, Karachi** they offered some special program in MS Computer science curriculum related to Network and Information security.

Lahore Leads University (Faculty of Computer Science,2015), Allama Iqbal Open University (Department of Computer Science, Allama Iqbal Open University Islamabad Pakistan, 2016) Minhaj University Lahore (Minhaj University Lahore, 2015)and etc. they also offered some special program in MS Computer science curriculum related to Network and Information security. Moreover, National Defense University (NDU) also offered the strategic studies (National Defence University, Islamabad, 2015), and International Relations (National Defence University, Islamabad, 2015) programs focusing on cyber security.

6.4.2 Training Programs:

Apart from educational institutes offering Information Security degree programs, there are some institutes which offer short courses cyber security programs for professionals and students. They are trained according to their nature of job/tasks with regard to best international security practices and basic cyber investigations and cyber security in the following cyber security training institutions etc.

a) **National Institute Of Management and Information Security (NIMIS)**

It gives consultancy and training sessions to industry professional regarding Information and Cyber security.

b) **Academic institutions**

Ripah University and Military College of NUST (MCS) provide training sessions on cyber security to IT and IS professionals and to the students also.

c) **NR3C, FIA**

It also gives couple of training sessions to the followings,

a) Judicial Community
b) Techniques and method of cyber investigations to the Officers of National Accountability Bureau.
c) Training on “Collection of Digital Evidence from Scene of Crimes” in NR3C’s First Responder course to all police officers and ASP’s of all the four provinces.
d) Online Cyber security Training in Urdu such as C-Atrax conducted a 2-day online course in Urdu about cyber security training in 2015.

6.4.3 Research Centers

These are many following research centers in Pakistan established with the focal aim of advancing indigenous information and communication (ICT) and new research on cyber security and development at the national level. They are listed down below;

6.4.3.1 Center for Network Centric Technologies (CENTech)

CENTech provide cutting edge solutions to ICT developers and also provides technical IS consultancy to the defense strategic organizations at national level. They also developed "Tahir Pak Crypto Library" (TPCL) and got it certified from the Federal Information Processing Standards (FIPS, NIST).

6.4.3.2 Pakistan Research Center for Cyber Security (PRCCS)

It was established by Cyber Security Task Force for national research on cyber security, for promoting national research on cyberspace security to help the private and public department to prevent the emerging cyber-attacks.

6.4.3.3 LUMS Research Initiative on Internet and Society (RIIS)

It is an inter-university initiative for research on cyber security launched by LUMS and how to utilize the national cyber space in best possible way.

6.4.3.4 Internet Policy Observatory Pakistan

iPOP it is also cyber security research institute which do the analysis and scrutinize the national ICT policies and e-regulations to help researchers, governments, development agencies, multilateral institutions and regulators. It also launched a repository of ICT data for further development on e-regulations, digital surveillance, Net Neutrality and rights of the internet users. (Internet Policy Observatory Pakistan, 2015)

6.4.3.5 Pakistan Honey net Project

This project is an active research member of the well renowned project Honey Net Research Alliance. It is non-profit, volunteer organization, which promote research on Honey net and investigate the motives and tactics of cyber preparatory and hackers hacking Pakistan's critical assets. (Pakistan HoneyNet Project – Honeypots, 2015)

6.4.4 Hacking Competitions

Pakistan hosted many hacking competitions with the basic aim of hunting the best hackers of the country. Many competitions have been organized till now;

- **a. PAKCON Game Hack and Capture the Flag** events. (2004 to 2007)
- **b. Capture the flag CTF** hacking competition**, Lahore**
- c. **Procam.net** hacking competition organized by Fast NU annually.
- **d. Capture the flag** CTF hacking contest organized by Cyber Secure Pakistan annually.

http://cyberttacks.blogspot.com/2015/02/ctf-hacking-competition-will-be-held-in.html

https://tribune.com.pk/story/1378011/13-year-old-pakistani-hacker-helping-worlds-top-tech-companies/

https://propakistani.pk/tag/hacking-competition/

https://propakistani.pk/2013/04/03/tranchulas-brings-competition-for-hackers-in-pakistan/

6.5 Professional Security Certifications

Unfortunately in Pakistan, there is no approved government cyber security framework for providing professional security certifications and accreditation of any organization or cyber workforce. However, there are some recognized international certification programs. (A+ (Plus) Certification | CompTIA IT Certifications, 2015)

6.5.1 Security Certifications for Regular Computer users

- a) Comptia Certifications

6.5.2 Security Certifications for IT Specialists

- a) Cisco Certifications
- b) Microsoft Certifications
- c) Huawei Certifications
- d) EC-Council Certifications
- e) GIAC Certifications
- f) Certified Internet Web (CIW) certifications:
- g) ISC2 Certifications:
- h) CompTIA Certifications

6.5.3 Security Certifications for IS Experts

a) EC-Council Certifications
b) ISACA Certifications
c) ISC2 Certifications
d) CompTIA Certifications
e) Global Information Assurance Certification GIAC
f) CISCO Certifications
g) Cloud Security Alliance Certifications
h) Offensive Security Certifications
i) Red Hat Certification

6.6 Compliance to ISO 270001 standard

Pakistan does not have any organizational or national framework, unlike many countries, for the implementation of internationally certified cyber security standards (e.g ISO, IEEE, IETF, ITU) within the public agencies and the government sectors. (Certification Services Pakistan (CeSP), 2015)There are many security service providers in Pakistan which provide Information Security Management Systems (ISMS) (Quality Management Systems.9000, 2015) under the internationally recognized ISO 270001 standards. This ISO 270001 certification makes them able to implement technical, physical and legal controls for the might security of the cyber infrastructure. (ISO 27001 (Information Security Management System) | DAS Pakistan)

6.7 Information Security Service Providers in Pakistan

Any international security company give the following information security services sucha as (IT Consulting | Software Services | Information Security Assurance| e-governance – Information Security Services Information Risk Assessment | Risk Mitigation | Information Security Management, 2015)

a) **Risk Assessment:** It includes Physical Security Review, Application Penetration Testing, Network Risk Assessment, Information Asset Profiling, Gap Analysis, Network Penetration testing, Vulnerability Assessment etc. (IT Consulting | Software Services | Information Security Assurance| e-Governance – Information Security Services Information Risk Assessment | Risk Mitigation | Information Security Management, 2015)
b) **Risk Mitigation:** it includes Disaster Recovery Plan (DRP), Information Security Polices, and Contingency Planning etc.
c) **Risk Implementation/ Management services**

6.9 Collaboration for Cyber Security

Cyber security is not only the responsibility of country, government, organization or a citizen. It need responsive measures and collaborative proactive role to be perform amongst public and private organizations to effectively and adequately address the issues of national cyber security infrastructure.

6.9.1 National Collaboration

There should be the framework for the exchange of cyber security assets (people, processes, tools) within the government or private sectors or government approved ventures for national collaboration in Pakistan. However, there is some national collaborative project, PISA R3C promoting public private partnerships (PPP) for enhancing national cyber resources. It also has collaborations with police departments and investigation agencies in tracing digital evidence.

6.9.2 International Cooperation

International cooperation tells us state participation in the global cyber security forums/platforms to promote cyber security. Pakistan also collaborates internationally in the field of cyber security. But it does not have any bilateral agreements and official framework to exchange cyber security resources with the other countries.

a) Relation with Global CERT

However, Pakistan participates in some global CERTs.

a) Pak CERT represents Pakistan in APSIRC-WG.
b) NR3C represent Pakistan in Organization of Islamic Cooperation CERT (CERT OIC)
c) NUST CSIRT has many international collaborations with MyCERT (Malaysia)

a) Relation with Global Organizations

1. **ITU_IMPACT**

Pakistan is the member of ITU_IMPACT and therefore have full access to services of ITU's cybersecurity.

2. **G8 24/7 High Tech Crime Network (HTCN)**

HTCN is unofficial network of 45 countries providing online platform 24/7 for the exchange of information regarding online cyber investigation of cybercrimes and cyber criminals. Ammar Jafri is the focal part from Pakistan in HTCN. (Tranchulas | Cyber Security Company, 2015)

3. **ICANN**

ICANN is the international global organization which assists Pakistan in framing the national cyber security policy, with regard to the Pakistan active participation in legislation forming process of ICANN.

4. **Subsidiary of International Cyber Security Organizations**

First regional forensic company in Turkey, “Forensic people” has a subsidiary in Pakistan. It provides Pakistan many services related to cyber security such as malware detection, steganography, and forensics (mobile, laptop, computer, GPS, video, audio, memory, wireless, network etc.) (Pakistan’s best network security solution provider, 2015)

5. **Security Trainings**

US FBI (federal Bureau of investigation) often give training to official of FIA (Federal Investigation Agency), Pakistan to fight against cybercrimes particularly financial frauds.

6. **International Cyber Security Competitions**

Asia Pacific Computer Emergency and Response Team (APCERT), since 2012, have organizing International Cyber Security Drills. The Pakistan team participated in drills successfully. (Malik, 2014)

6.10 Conclusions

There is no dedicated cyber security responsible agency in Pakistan. Only at national level there is one CERT known as PakCERT which is not operational now. There are very few cyber security initiatives. Few universities offer MSIS and PhD programs in Information Security but no education related to Information Security is given at school, college, bachelor’s level. There is no National Framework for professional certifications; Information Security professionals acquire international certifications from accredited training partners. There is no national framework for the accreditation of agencies. There is no national framework for inter-agency Cooperation only PISA R3C is initiative for public private partnership. There is no national framework for intra state-cooperation. It is a member of few international cyber security collaborations such as member of ITU impact, APSIRC-WG. Pakistan should adopt the multi-stakeholder approach to protect the national cyber space. Cyber security is a shared responsibility therefore there should be the exchange of cyber security expertise and resources both at national and international level for developing skilled workforce for cyber security but it seems Pakistan government is least concerned about this sensitive issue. There is no government collaboration to the public and private agencies working for cyber security such as there are no funds and no support. The government of Pakistan on urgent base needs to frame policies for accreditation, certification and for public-private and international collaboration etc. to build cyber security capacity building in Pakistan.

CHAPTER 7

Critical Analysis of Cyber Space Security and Proposed Cyber Security Recommendations

7.1 Introduction

Cyber security is a matter of prime concern globally. Pakistan has no proper regulation of cyber security policies and although there is a Cyber Crime Act of 2016 but it is insufficient to address all the cyber security issues especially the state sponsor cyber-attacks and Cyber Warfare terrorism. There is no regulatory framework or dedicated cyber security governmental wing being responsible for the task of cyber security. Proceeding chapters of this research which discusses elaborately cyber security laws , national capacity building measures, formulation of cyber threat landscape of Pakistan, this chapter will have the critical analysis of various aspects of cyber security at government, private and public sector for the safeguard of Pakistan national cyber space.

As there are a lot of cases of cybercrimes residing in Pakistan. NADRA the Pakistan first ever digital data hub containing all the information of citizens is easily vulnerable to hackers having not even the basic security. Every organization or institute easily access NADRA information without any permission of government officials responsible for this. Last American elections where Cambridge Analytica was able to harvest a trove of data from Facebook to influence the results cannot be ruled out. The recent case of Cambridge Analytica in America, the electronic election fraud of Facebook data breaching is the case of cyber security, where you can easily access the data of your voters and start influencing them with electronic campaigns of any kind like blogs, apps etc. The cammbridge analytica made Donald Trump won the American elections of 2017. Similarly, there are worries that the data collected for the upcoming elections of 2018 in Pakistan may be manipulated by the political parties of Pakistan using the social media, which is the greatest threat to cyber security. So the government needs to secure the digital information of their citizens and to protect the micro targeting by the e-commerce industries government should devise the proper guidelines that how to use social networks and to protect their data. (Cambridge Analytica, 2017). The Pakistan election commission results of 2018 got delay due to the anomalies in RTS system an android application introduced by NADRA, the incident of the Result Transmission System (RTS) failing in the aftermath of the recent national elections indicates a serious technical glitch that couldn't be addressed in time. There could have been possible intrusion with malicious intent. An inquiry has been ordered and we will have to wait for its findings. But most probably it is due to the untrained and unprofessional ICT app developers or they may import that app from some foreign android experts therefore don't know how to deal with the errors. There is no cyber security check on even the important government sites of the country including military and defense and many times the Pakistani governmental and military sites were hacked by Indian and Russians. And we know the consequences like if someone post false news on the website like India will launch a missile in Pakistan then it will shake the whole country.

Recently a senior officer of the FIA deposed before the Chief Justice of Pakistan that he has only 10 experts to investigate over 2600 cases of cybercrime. (FIA has only 10 experts to investigate cybercrime; Dawn News, 2018) This is the worst condition of the Pakistan cyber investigation center. They don't have enough workforce of people to deal with all the issues related to cybercrime similarly and there are only two investigation centers in the Pakistan one is in the capital Islamabad and the other one in Karachi. During my interview with deputy director of the national response center for cybercrime (NR3C) he said they have plan of opening cybercrime investigation center in the main police station of the city but it doesn't seem practical as far as they don't devise some practical policy for it. Also for the further investigation of cybercrime they want the proper FIR against the criminal which takes a lot of time further they don't have the proper procedure for the investigation of the crime.

The very recent case of the Careem company which is an online car ride service company, its data was stolen online by the hackers having unauthorized access which is a major cyber theft such as 14 million usesr data has been stolen from the Careem app.(Careem Hacked, User Data Stolen!; Pakistan Today, 2018) There are data protection laws made by the countries due to which the government can challenge Careem company, but in Pakistan there is no data protection law, ultimately users have to suffer the consequences. PECA have data protection laws for the privacy of its citizen's personal data in Pakistan but no MOUs signed with the middle east car riding company careem due to which the citizens have to face the consequences, but Careem said there was no misuse of data or the extent of damaged is not known because there are no sources which confirms the data breaching of the users. There are a number of cyber harassment and blackmailing cases in Pakistan among women's, and the government of Pakistan is taking actions against it, there are few cases in which the cybercriminal is behind jails. But it is on a very small scale while the cyber harassment and blackmailing in Pakistan is on mega scale. The blasphemous case of Mashaal khan in Pakistan pertinent to Facebook is the instance of major cyber issues in Pakistan, where the country lacks the proper laws regulation and vague policies. And also Pakistan has no mutual legal corporation pacts signed with the foreign countries to track the information on facebook. Pakistan is also importing undersea optical fibers from the Indian two biggest companies, on which there are chances of Indian surveillance according to experts. There are also the chances of the leakage of the information of the CPEC. But recently Pak China optical fiber line project introduced by CPEC has reduced the dependence on the undersea cable and the Indian intrusion.

Cyber security is the top priority of the government and corporations, but Pakistan is lagging way behind cyber security international trends. Sophistication of cyber-attacks is deleterious to the information communication technology and why the government is still insensitiveness to the cyber security despite many national stakeholders' efforts this research figure out the following points such as,

a. Pakistan is intertwined with so many issues with the consequential issues of national security from Taliban's, cross-border neighbors and its own citizens. It has many issues to handle despite terrorism such as elimination of poverty; illiteracy etc. that's it never treated the grave issue of cyber security with seriousness.
b. Most of the countries include cyber domain under the ministry of Information and Technology, but Pakistan Ministry of Information and Technology argues that cyber security is not their absolute duty as it has not been defined in their duty.
c. Pakistan government is oblivious towards impacts of large-scale security breaches such as protecting the national ICT resources and assets which can lead to the heavy uncompromised economic loss to the state. It is attacked by mild cyber-attacks every now and then which also mildly affected Pakistan cyber infrastructure this is also the reason government of Pakistan is insensitive about this grave issue. (Iran hackers penetrate key networks in Pakistan: Researchers - The Express Tribune, 2014)
d. The Pakistan government believes fewer ICT products and resources means less exposure to cyber threats and vulnerabilities. Therefore they do not redeem the national information infrastructure and didn't consider it vital enough to spend to spend billions of money on it.
e. The Pakistan government is so much confident about the existing security controls which have already implemented to secure the cyber infrastructures.
f. There is weak enforcement of cyber laws in Pakistan owing to very short age of Presidential ordinance acceptance.
g. Bureaucratic red-tape and politicking.no doubt, is the main hurdle in the proper implementation of the cyber legislation. (Desk, 2014)
h. The NR3C (National Response Center for Cyber-crimes) under FIA claims that they have less rate of reported crimes because most of the victims due to fear of closing personal secrets, blackmailing and the fear of police don't register their cases. Therefore very less attention of government towards the issue of cyber security.
i. To combat cyber terrorism in the country, the government has introduced the term URL and SMS filtering on electronic data traffic but the civil society organizations vehement online campaigns and massive criticism and street agitation is the main cause of their non-implementation. When in 2013 the Sindh government outlaw Whatsapp, Viber, Tango,Skype (encrypted communication applications) met heavy criticism from media and civil society.
j. The biggest problem of the Pakistani citizens and the government is that they are resistant to adopt to the changes especially the new technologies, laws etc. (Cybercrimes: Pakistan lacks facilities to trace hackers - The Express Tribune, 2015)

k. Pakistan usually bans the websites containing offensive or religiously disturbing content especially the case of banning of you tube. To circumvent the block, majority citizens use proxy and hotspot shields to open these sites but these proxy sites are equipped with malware, viruses posing big threat to national landscape.

l. The existing cyber regulations cannot ensure full cyber security of electronic information and IT assets. Even the ISPs cannot ensure basic netizens rights.

7.2 Analysis of Domestic Cyber Laws and Regulations

Cyber laws hold all aspects of security of cyber space and therefore, before formulating them there should be through research of country cyber threat landscape. The major flaw is that most of the policy makers are the technology-illiterate people who even don't have the basic knowledge of internet, technology and its inherent flaws, safeguard measures and exploitation techniques. The following points will discuss the major loopholes in these domestic cyber laws, their regulations and the policy framework making strategy.

a. Laws like Fair Trial Act, Telecommunication Reorganization Act 1996 etc. have not defined limitations in interception of digital information. (Cybercrimes: Pakistan lacks facilities to trace hackers - The Express Tribune, 2015)

b. There are vague definitions (unauthorized access, electronic fraud, forgery) and unclear undefined words such as the crime etc. in Electronic Crime Act 2004, Electronic Crime Bill 2015 etc., which can lead to the misuse of the term by the authority.

c. There is state controlled lead agency in the crime Bill of 2015 and 2016, giving the state uncontrolled power to amend the laws and regulations in their favor. Although the cybercrime bill of 2014 was formed with the assistance of ITU to incorporate best security practices, but it was revised by the government in its own favor in 2015, violating the digital rights of people.

d. Most of the cyber laws ignore major cyber security issues like privacy, authentication, non-repudiation etc. and mainly concerns with the matter of CIA user's data.

e. These laws do not address advanced threats and cyber-crimes such as cloud computing, trust infrastructure, bid data, 3G and 4G and social networks.

f. There are no security provisions for micro-payment systems, e-commerce etc.

g. The reconciliation of International Telephone Traffic Regulations in 2008, 2010 ban VPN and encryption services which can affect the secure functionality of financial institutions.

h. The laws formulation process lacks the technical body which lead to the huge loss of money to the government on the purchase of grey traffic filtering system.

i. The stakeholder responsibilities are unclear.

j. There is no strict implementation of the laws and no periodical update of the cyber laws.

k. The crimes and their corresponding punishments given in proposed crime bill are inappropriate like there is three year punishment even for the minor offences like cybersquatting, junk mailing etc.

l. There is no proper procedure to suspect the label as innocent or cyber offender therefore no mechanism to challenge the government and most cyber offences are unbillable leading to imprisonment of innocent people.

m. Most of the laws are replica of existing IT international laws or other country laws without considering Pakistan cyber threat landscape such as IT Act of India 2000.

n. FIA and Intelligence agencies were given unrestricted power for investigation without warrant. (Cyber-crime bill: FIA may be excluded from investigation process – The Express Tribune, 2016)

7.3 **Analysis of National Cyber Security Capacity Building Measures**

Few private sector and public organizations especially NR3C, PISA, Bytes for All have often tried to hold cyber security conferences, workshops, training sessions and seminars in major cities of Pakistan. But there is a lack of funds, and negligence of the law enforcement agencies that these initiatives don’t have much impact. The analysis of national cyber security capacity building measures aspects are given in the following point.

a. There is no responsible national body encompass with the task of cyber security in Pakistan. However, NR3C and NTISB endeavors individually to build national cyber security capacity wing. There should be central responsible cyber task agency, state-independent, official wing should be created not like existing bodies which either work as coordinating bodies or merged with any of government department.

b. The incident management capabilities of the existing national cyber institutions have been exacerbated by the cyber unawareness, lack of budget, accountability .FIA for instance do not have the enough capacity and required manpower to deal with cases of cybercrimes such as recently a senior officer of the FIA disposed before the Senate that he has only 10 experts to investigate over 2600 cases of cybercrime. Also the Pakistan ISP’s, call centers, banks don’t even have the capacity to deal with small 5Gbps DDoS attack. The PakCERT(National CERT) and the PISACERT (Private CERT) are specifically established with the aim of enhancing and building incident management capabilities, but sadly they are not operational now.(Press Release Don’t block the blog, 2015)

c. The seminars conducted by PISA, NR3C, and the chapter programs ISC2, ISACA, and cloud security associations are not enough to increase the awareness of cyber security among citizens. They should conduct them on the huge scale in both languages English and Urdu so the voice gets heard. There are annually cyber security conferences which are not enough, only the biggest cyber conference in Pakistan history the conference organized by the Cybex "Cyber Security and Technology Summit 2018" where more than 1000 people attended it.

d. International OIC drill held annually, where team of Pakistan usually give tough competitions to other countries. It shows that we have the required incident management skills but basically lacks in good incentives to implement those skills practically. (Nasir, 2013)

e. To increase the cyber security capacity building in Pakistan, there is a dire need to establish a cyber-security governance framework with national and international collaborations. It should have operational division with different responsible centers to stimulate the process of cyber capacity building in Pakistan. They should have awareness raising center, research and development educations centers pertaining to cyber security, training, standardization, collaboration etc. (Aziz, 2010)

7.4 Analysis of Pakistan's Cyber Threat Landscape

Due to the lack of proper policy, technical malpractices and cyber unawareness, Pakistan has been a very easy target for cyber preparatory. The greatest cyber threat Pakistan facing these days according to research is the malware infection which hijacks a system/ computer and even can make changes to the data and the settings. Due to cyber unawareness the illiterate people of Pakistan cyber community is incapable of thwarting these cyber-attacks. Due to is this in Pakistan malware infection rates always on the verge of increase level with the world. The most common malpractices of Pakistan cyber community and it critical analysis is as under.

a. In Pakistan there is usage of obsolete Operating Systems and have outdate windows and software which should be on immediate basis uninstalled from the operating systems. There is no basic awareness of updating the software on daily basis, and even how to update and from where. (Omer, 2015)

b. Most of the cyber community evens the employees of the sensitive organization keep an easy password which can be brute forced easily within no time.

c. Netizen should be taught about the secure ways of using the soft wares such as their downloading, installing and updating. The usage of proxies such as using Hotspot Shield, Spot flux etc., have the major Viruses, Trojans, Malware infections, the Pakistan government should develop a policy on it and define the punishments and repercussions for bypassing the electronic content website blocked by the Pakistan government.

d. Most of the people also the literate one are unaware of the privacy policies of the websites either install the software or submitting credentials on website without reading the privacy policy end up compromising their Data/system.
e. Owing to cyber security unawareness, many people are victims of phishing mails and Spams like the messages or mails promising prizes or money, so the most of the people get allured to the offers and become the victim. The Pakistan mostly import hardware technology and anti-virus software from the foreign countries which is the reason for most of the cyber threats in Pakistan.

(Yamin, 2014)

The increasing reliance on information and communication technology (ICT), ease of Internet access and uncertain cyber regulatory environment, have made the Pakistan's cyberspace an ideal arena for various cyber offence, cyber terrorism, cyber warfare etc., thereby posing pernicious threat to the national security, stability, economic vitality, public health and the normal functioning of the society and digital infrastructure. Today, these threats have escalated to the point that cyber security should be widely accepted as a top national security that and development of defensive cyber capabilities should be fostered to cope up with this growing cyber peril.

7.5 Vision

To improve national cyber consciousness and hygiene in order to make the national cyberspace secure, robust and profitable for the Pakistani citizens, government and business to conduct daily activities smoothly, help burgeon e-commerce and IT sector and guarantee basic digital rights and liberties.

7.6 Guiding Principles

The national cyber security strategy of Pakistan will be based on the following guiding four guiding principles.

a. **Policy**: To make proper workable policy to protect the national values, abide by the rule law, and guarantee basic rights to netizens.
b. **Awareness:** There should be the element of awareness in every point of policy because all we lack is proper cyber awareness to address cyber threats systematically to avoid the duplication of resources and efforts,
c. **Will:** There is dearth of will both at governmental and private level to work on the premise of shared responsibility, thus every individual should assume his/her responsibility.

d. **Wherewithal:** An implementation of cyber security policy requires a lot of financial wherewithal for practical cyber wing to adopt a multi-stakeholder approach in devising the national cyber security strategy.

7.7 Objectives

The primary objective of this research is to recommend a cyber-security strategy which direct and prioritize the cyber security efforts made at national and organizational levels to create safe, trusted and resilient cyberspace. However, to achieve the aforementioned vision, the energy sets forward the following objectives too:

a. To propose a Cyber Security Governance Framework in order to identify key stakeholders and processes required to manage the national cyberspace.
b. To ensure digital continuity by safeguarding the digital infrastructure, national critical information elements and digital information.
c. To encourage creation and enhancement of cyber incident recognition, preparedness, response and recovery capabilities at national and organization levels, thereby, minimizing cyber-attacks and coping with cyber delinquency.
d. To propose an appropriate Cyber Security Legislative Framework which can help create effective cyber deterrence.
e. To foster a strong and sound national cyber security culture by intensifying cyber consciousness, training and education.
f. To stimulate Research & Development on Cyber Security in order to attain real national self-sufficiency in Cyber Security.
g. To promote Information Security Standardization, Accreditation and Certification.
h. To encourage national and international strategic collaboration to effectively manage cyber risks and secure national cyberspace.
i. To suggest bounds to the legal internet surveillance and censorship thereby protecting the fundamental rights of netizens and intermediaries particularly right to privacy, freedom of expression and access of digital information.

7.8 Strategic Cyber Security Guidelines:

7.8.1 Proposed "cyber security governance framework" under challenging timelines with clearly defined role, responsibility, authority and accountability for each concerned national, legal and organizational stakeholder.

The Cyber Security Governance Framework will help direct, prioritize and coordinate cyber activities at national and organizational level, thereby addressing national cyber security challenges. First and foremost there is a need to establish a supervisory body, a **National Cyber Security Council (NCSC)** that will adopt a coordinated and focused approach to strengthen the country's cyber security arena. This can be established as per the 2014's Act for the establishment of a National Cyber Security Council.

The National Cyber Security Council will comprise of one member from each; Ministry of Information Technology, Ministry of Interior, Ministry of Education and Research, Ministry of Defence, Ministry of Justice and Ministry of Finance. The business and academic representatives will also be included as associated members. The Council will:

a. Discuss the major national cyber security issues and threats posed to cyber space in meetings conducted every month,
b. Provide oversight regarding planning, revision and implementation of cyber security initiatives and structures,
c. Evaluate progress of the Cyber Security Action Plans.
d. Prepare and publish an annual report outlining the performance of the entities in the current year and appreciated plans for the year ahead.
e. Create and manage a secure national **Cyber Security Repository** for storing all accreditation certificates, balance sheets, cyber performance reports, etc. The uncritical data and content of national interest e.g. List of accredited organizations, standards being compiled to, best security practices etc., will be shared with the public on the **Cyber Security Resource Portal.**

A member of the National Cyber Security Council will be appointed as the **National Cyber Security Advisor,** who will be responsible for communicating the national cyber security key decisions of the National Cyber Security Council to the President/Prime Minister.

The Council will be assisted by a **National Cyber Security Advisory Body,** that will have separate technical, operational, policy as well as industry groups who will put forward their consolidated recommendations on the task and performance of the various divisions of the National Cyber Security Council. The groups will comprise of one member from each of the listed organizations.

a. Operations Advisory Group:

Pakistan Telecommunication Authority, Federal Investigation Agency, Inter-Services Intelligence, Intelligence Bureau, Capital and provincial Inspector, Internet Service Providers, National Finance Commission members;

b. Technical Advisory Group:

Research institutes, Engineering Universities, Technical Laboratories, Cryptographers , Cryptologist, Encryption Experts, Cyber Security Professionals, White-Hat Hackers, Researchers and Academics, Technical Experts, Chief Security Officers, Chief Information Officers and Chief Information Security Officers of Financial Institutions;

c. Policy Advisory Group:

Policy Institutes, Thinks Tanks, Legal Experts and Consultants, Policy Expects and Consultants, Strategists, Defence Experts, War Study Experts, National Security Experts, Law Enforcement Experts;

d. Industry Advisory Group:

Industry Associations, Management Consultants, Industry Chief Executive Officers, particularly Financial Institutions, Federation of Pakistan Chamber of Commerce and Industry and Provisional Branches.

There will also be a Cyber Fund Center in order to meet the costs and charges incurred for carrying out cyber security tasks. The authorities will

a. Collect aid, grants and donations from the national or international agencies for carrying out cyber security task.
b. Provide incentives to major organizations for adopting best information management practices
c. Prepare a financial report and balance sheet for the cyber security spending of each entity, and an audited statement of income and expenditures.

6.8.2 National Cyber security Council

The National Cyber security Council into four divisions; National Cyber Security Policy Division, National Cyber Security Capacity Building Division, National Cyber Incident Management Division and the Cyber Crime Division.

a. National Cyber Security Policy Division

It will be under the purview of Ministry of IT, and overseen by the Pakistan's Council for Science and Technology/ NTISB for policy directions. Apart from the policy makers, the division must have information security expert too. The policy division will entrusted to

1. Develop a legal Cyber Security Framework and oversee implementation.
2. Design a common mechanism for regular assessment of the cyber security action plans after every two years.
3. Review domestic cyber security laws and legislations and recommend improvements,
4. Regularly evaluate and assess international regulations, legislations, trends and solutions to cyber security issues and advise National Cyber Security Council to apply appropriate recommendations.
5. Formulate Cyber Security Policies/ regulations and crime bill when needed.
6. Prepare a national dictionary of cyber security key terms to prevent potential conceptual confusions
7. Ensure that the cyber laws and legislations are harmonious with the international laws and agreements.

8. Revise Cyber Security Strategy after every two years.

b. National Cyber Security Capacity Building Division

This division will be responsible for determining national needs, promoting and monitoring cyber developments in the global cyberspace, and establish progressive capacity development programs. The National Cyber Security Capacity Building Division will support the compliance of the legal cyber security framework through the establishment of:

1. **Cyber Training and Education Centre: this will be aimed** at promoting cyber security culture, raising cyber consciousness, and preparation and implementation of various educations and training programs. This will help improve the competency of cyber workforce, and the ordinary citizens.
2. **National Center for Information Security Standardization.**

This will promote and facilitate accreditation and certificates of ICT products, users and organizations, monitor and ensure compliance by the accredited certification service providers and revoke or suspend accreditation if required. The body will also establish cyber security standers and best practices for the consideration of the National Cyber Security Council. It will also prescribe the procedures for formation, verification, disposal and renewal of electronic signatures.

3. **Research Center of Excellence:** it will carry out research in the area of cyber security and facilitate the development, implementation, promotion and commercialization of indigenous cyber security products.
4. **Centre of the Cyber Security Partnerships:** this entitle will promote public-private partnerships and closely coordinate national security programs, in collaborations with Mol, at national level. It will also stimulate international coordination and collaboration in the field of information security, investigations, training and capacity building, together with MoFA.

c. National Cyber Security Incident Management Division

This division will be responsible for carrying out technical and operational tasks in order to assess the security of the national cyber space and defend it from evil actors. The National Cyber Security Incident Management Division will also support the compliance of the legal cyber security framework through the establishment of:

1. **Cyber Eye (Incident Monitoring Centre):** This will carry out real-time tracking of the national cyberspace and rings an alarm to alert the PakCERT.
2. **Pak CERT (Cyber Emergency Readiness Team):** This will be the focal team that would respond to cyber crises/ cyber incidents hitting the national cyberspace.
3. **Critical Infrastructure Protection Centre:** This center will work in close collaboration with the CERT, but it will be more focused on identifying,

responding and preventing cyber threats and attacks targeting the critical national infrastructure.

4. **Cyber Forensic Investigation Centre:** This will investigate the cases involving digital crimes. The forensic team will also help CERT in responding national attacks effectively and the police in investigations.
5. **Threat Information Sharing Centre:** This will be responsible for disseminating the cyber threat information to all the concerned stake-holders.
6. **Cyber Exercise Centre:** it will help assess the credibility of national cyber security plans and enhance cyber preparedness and responsiveness.

d. Cyber Crime Division:

To ensure that cybercrimes are effectively prevented, suppressed, investigated and prosecuted, the Cyber Crime Division will

- Bring police, law enforcement, judicial and prosecution authorities of Pakistan on one platform for enhanced celebration and provision of specialized training.
- Create harmonized set of rules and appropriate tools to facilitate the collection, admissibility and analysis of electronic evidence.
- Analyze the trends and patterns of cyber offences
- Advice and assist the National Policy Division in making holistic cybercrime laws.
- Encourage cross-border cyber investigations and judicial cooperation with regional and international countries.

7.8.3 Ensure digital continuity through protection of information and information infrastructure to ensure digital continuity

Digital continuity can only be ensured in the national cyberspace if the entire national ICT infrastructure, devices, services, applications, etc., operating within the cyberspace are safe and secure. For the secure working of ICT resources and residing information, following needs to be done. Create an appropriate **"Cyber Security Technology Framework"** to ensure existing ICT networks, systems, critical national information infrastructure and digital information. For this, there is need to

1. Specify the set of minimum cyber security controls that each organization should mandatory comply with.
2. Formulate and enforce uniform standard for the protection of crucial cyber assets, data repositories and e-services in order to harmonize the diverse security practices being followed nationwide.
3. Publish fundamental rules on development of secure hardware and software
4. Develop clones and test beds to verify the security updates and patches.

5. Design and implement a security assessment and certification program for all ICT resources.
6. Discourage Bring Your Own Device (BYOD) policies, use of removable media, and downloading the usage of cracked software in al critical organizations.
7. Define rules of security and penetration testing of all websites.

7.9 Propose an appropriate Cyber Security Legislative Framework to create effective cyber deterrence.

To ensure national cyberspace security for netizens, repress cyber offences and impose sanctions on offenders, there is a need to create a well-defined cyber security legislative framework. The Cyber Security Policy Division should therefore

a. Analyze and update existing domestic cyber laws to address dynamic cyber risks and threats.
b. Review global cyber strategic legislations, adapt relevant good measures ratify international treaties where required.
c. Enact the prevention of Electronic Crimes Act, 2014, after amending it in light of public feedback, till another cyber law is devised.
d. Develop and enact national cyber-crime legislation against cyber criminals, whether local or foreign, especially spy agencies, wire-tappers and the defaulters for deliberate non-compliance to mandatory information security controls. The legislation should encompass all major offences including cyber-bullying, illegal interception and access, spamming, sabotage, identity theft, child pornography Intellectual Property crimes, aiding and abetting as well as, emerging cyber threats due to cloud computing, big data, social technology etc.
e. Encourage other policy makers to embed cyber security widely while formulating terrestrial laws.

7.9.1 Encourage national and international strategic collaboration to effectively manage cyber risks and secure national cyberspace

As cyber are not confined to organizational boundaries and state borders, it is imperative to establish cohesion at the intrastate and interstate level in technical, legal and operational aspects to secure the ICT environment.

7.9.1.1 National Collaboration

Effective incessant cooperation between the government, private sector, public sector, industry and other national key stakeholders is required at both strategic and operational level to secure the cyber space since they support daily activities and hold extremely sensitive information in the cyber assets. The National Centre of the Cyber Security Partnerships, should thus,

Clearly state responsibilities and work methodology for the collaborating organizations or entities to achieve shared goals.

a) Promote exchange of cyber security expertise within ministries and organizations to address common cyber security challenges
b) Collaborate with the civil society and lay-users for execution of cyber awareness programs.
c) Collaborate with all major stakeholders i.e. government departments, telecom regulators, data protection service providers, critical infrastructure operators etc., to get input and feedback on the cyber laws devised by the Cyber Security Policy Division and pertinent security development.
d) Encourage national and local CERTs and Information Sharing Centre to effectively share threat information at the national level.

7.9.1.2 Foster International Collaboration

For promoting international collaboration consolidating all national efforts for international cooperation on cyber security, the National Centre of the Cyber Security Partnerships, in collaboration with the Ministry of Foreign Affairs, will;

Collaborate with strategic and regional partners e.g. China, Iran, Turkey etc., to develop joint cyber security capabilities, recognition of digital signatures, information security standardization in the region, etc. Explore avenues for developing bilateral and multilateral relations with emerging cyber powers, notably the USA, UK, Germany, France, Estonia etc. Sign MLAT (Mutual Legal Assistance Treaty) for effectively exchanging cyber security workforce, organizing international training, research and education programs and enforcing public and criminal laws

a. Create a multinational Information Sharing and Analysis Centre (ISACs) for sharing cyber treat information, technological knowledge, vulnerabilities of major ICT products etc., with partner countries.
b. Provide mutual legal assistance to international police, judiciary and law enforcement agency in coordinating investigations of high-tech crimes, apprehend cyber perpetrators and facilitate intelligence-gathering
c. Facilitate Training and Education Department in organizing annual international cyber security conference in the country, and invite foreign speakers.
d. Provide intermediary liability protection (legal protection from unlawful exploitation by third parties e.g. users),
e. Coordinate with international bodies, strategic alliances and multi-national agencies subject to safeguard of global cyberspace (UN, OSCE, Council of Europe, NATO, EU, SAARC, SCO, OIC, ISO, OECD, ENISA) by

1. Preparing an external cyber security policy to coordinate interests of Pakistan in these international organizations,
2. Supporting mandate and whenever possible appointing qualified cyber experts to represent Pakistan in these-bodies
3. Developing Confidence Building Measures with the SAARC members particularly India to establish cyber rules of game and prevent inadvertent cyber was in the future**.** (Yamin, 2014)
4. Signing bilateral, multilateral or international treaties and conventions related to information security, preferably Council of Europe's Convention on Cyber-crime, International Code of Conduct for Information Security etc., if they do not run counter to the national security interests.
5. Actively support and participate in the international efforts for drafting international norms and legal acts concerning cyber intelligence sharing and cyber defense.
6. Supporting Common wealth in promoting model legislation on Cybercrime
7. Supporting ITU in training on technical standards.

In order to do the survey and to check the general awareness of the students of Pakistan I devised a form given below. I distributed that form in 12 engineering universities which include 8 universities from Islamabad/Rawalpindi and 4 universities from Lahore. All these universities are well reputed but out of them all only few universities students have the general knowledge about cyber security. But target audience is all the educated once but we can infer from that if the educated people don't have the much knowledge about the cyber security than what about the rest of the common people. Obviously they will have the least knowledge of it. So the cyber capacity building measures and the cyber policies must make cyber awareness in the general public their first priority.

7.9.1.3 Questionnaire-Cyber Security Education in Pakistan

Cyber Security Education in Pakistan

This Cyber Security Questionnaire is a part of Graduate Thesis of a student of Center for International Peace and Stability (NUST). The questionnaire seeks to determine whether the local students of Pakistan universities have the general awareness about Cyber Security and issues related to it, what cyber security facilities are provided to them in building capacity for Cyber Security in Pakistan.

This questionnaire consists of 12 questions on 2 pages. Your participation in filling this questionnaire will be greatly appreciated. In case of any query, please contact hanzngir90@yahoo.com .

Student Name: ______________________ **Signature:** ________________

Institution: ______________________________ **Date:** ______________________

Questions

1. You are a student of which program?
    - Undergraduate
    - Graduate
    - Post-graduate
    - No program

2. Do you think there are risks associated with public Wi-Fi?
    - Yes
    - No

3. Have you installed anti –virus on your computers?
    - Yes
    - No

4. Do you know how to protect yourself against identity thefts?
    - Yes
    - No

5. Do you have the general idea about cyber security?
    - Yes
    - No

6. Do you know what are cyber-crimes and cyber threats?
    - Yes
    - No

7. Is there any governmental organization dealing with cyber-crimes in Pakistan?
    - Yes
    - No

8. Is there any governmental Computer Security Incident Response Team (CSIRT/ CERT) in Pakistan?
    - Yes
    - No

9. Do you know about the online privacy?
    - Yes
    - No

10. Did you attend any cyber security conference and seminars in any university or organization?
    - Yes
    - No

11. Do you know what is cyber warfare and that it is more dangerous than conventional warfare?
    - Yes
    - No

12. Do you have the general idea regarding recent cyber laws in Pakistan?
    - Yes
    - No

Result of the Survey

The result of the survey conducted in different universities is quiet similar. Most of the students have least concern with the cybersecurity of their softwares and online apps. They don’t even have the general concept of the cybersecurity and its importance. According to them cybersecurity is just about identity thefts and hacking. Many knows about the NR3C (National Response Center for Cyber Crime) but only few students knows what is the actual function of the NR3C in Islamabad. Mostly respond that they have no idea about cyber laws. Few students said that they wanted to attend the cyber security short courses but they are expensive that they can’t afford. Many said they attended the cybersecurity conferences in their university but most of the time these conferences don’t focus on the main theme of the title of the conference. With the exception of the students related to computer and technology only few knows about the online privacy. They don’t have idea about the digital organization and the organizations working for the cyber laws. They are unaware about the punishment of cybercrime most of the time they think they are legal. That’s the major dilemma of the country facing so far concerning cybersecurity.

Inferences

I have drawn the following inferences from the data collected above that firstly all the government and the public organization should make people aware of the general idea of cybersecurity, cyber laws and the cybercrimes. They should install the antivirus in the public computers and software and make the antivirus software cheap and easy available to the general public. Rather importing anti-software from the foreign countries they should make their own. The public conferences and the university based conferences should offer basic cybersecurity workshops free to the students and the conferences should held monthly rather than yearly. The public awareness should be the first and foremost objective of all the organizations related to cybersecurity. As today the global village world so they should offer cyberawarness programs online and on public social platforms.

References

ITU, “Percentage of Individuals Using the Internet”, International Telecommunications Union (Geneva), 2015.

Attaa, A, (2015) Internet Speed in Pakistan Plunges Due To Fault in Submarine Cable. Propakistani.Pk. Retrieved 01 January 2018, from https://propakistani.pk/2015/06/25/intenet-speeds-in-pakistan-plunges-due-to-fault-in-submarine-cable/

Pakbee.Com, “Internet | Pakistan Bee – Part 4”, 2010. [Online]. Available: https://pakbee.com/tag/internet/page/4/- [Accessed: 01-Jan-2018].

Ugowireless.Biz, “About Us – Go Wireless Pakistan | Wireless ISP Consultancy Firm, Wireless ISP Setup in Pakistan”, 2016. [Online]. Available: https://www.ugowireless.biz/about.html. [Accessed: 07- Jan- 2018].

Odosta.Com, “Internet User’s Growth Rate in Pakistan 2015 | Dosta Inc.”, 2015. [Online]. Available: https://odosta.com/internet-users-in-pakistan-2015/. [Accessed: 01- Jan- 2018].

Pta.gov.pk, “Telecom Coverage Maps” , 2016 [Online]. Available Https://Www.Pta.Gov.Pk/En/Digitalmaps/Digitalmaps.Php. [Accessed: 02- Jan- 2018].

Odosta.Com, (2015). Internet User’s Growth Rate In Pakistan 2015 | Odosta Inc. Retrieved 28th June 2018, from https://odosta.com/internet-users-in-pakistan-2015/

Release, P. (2014). Internet Banking Regulations to Be Issued in Weeks: SBP. Propakistani.Pk Retrieved , from 28th June 2018 https://propakistani.pk/2014/12/15/intenet-banking-regulations-to-be-used-in-weeks-sbp/

Dawood, A. (2014). Tech Week in Pakistan (Issue 27: 29th September) – Dyl Ventures, Dyl Ventures. Retrieved , from https: 28th June 2018 //dylventures.com/tech-week-pakistan-issue-27-29th-september/

Gs.Statcounter.Com, (2015). Statcounter Global Stats – Browser, OS, Search Engine Including Mobile Usage Share, Retrieved 28th June 2018 , from https://gs.statcounter.com/#

Kaymu.Pk, (2015), Ecommerce Trends Pakistan / Report By Kaymu.pk Retrieved 25th June 2018 , From https://www.kaymu.pk/researh/

Rains, t. (2013). The threat landscape in Pakistan: one of the most active in the world. Cyber trust blog. Retrieved 28th June 2018 , from https://blogs.microsoft.com/cybertrust/2013/01/23/the-threat-landscape-in-pakistan-one-of-the-most-active-in-the-world/

Lifehacker.com, (2015). The best replacements for privacy-invading services. Retrieved 25th June 2018 , from https://lifehacker.com/5965462/the-best-replacements-for-privacy-invading services/

Readwrite.com, (2011). Where in the world people do not use facebook? Retrieved 25th June 2018 , from http://readwrite.com2011/11/01/where_in_the_world_people_do_not_use_facebook

The webcertain search and social report 2011. (2011). Retrieved 25th June 2018 , from http://webcertain.com/webcertain-search-and-social-report-2011,pdf

Search engine marketing, inc -- the book, (2015). Country search engines, search engine marketing, inc - the book. Retrieved 25th June 2018, from http://seminbook.com/country-search-engines/

Page, T. (2015). 2013 search engine market share by country – resources / return on now. Return on now. Retrieved 25th June 2018 , from http://returnonnow.com/intenet-marketing-resources/2013-search-engine-market-share-by-country/

Technology personalized, (2013). The best non US based providers you can trust your privacy on. Retrieved 25th June 2018 , from http://techpp.com/2013/08/28/non-us-encrypted-email-service-privacy/

Wikipedia, (2015). Comparison of webmail providers. Retrieved 25th June 2018 , from https://en.wikipedia.org/wiki/comparisonofwebmailproviders

Startos.org, “OS”, 2016. [Online]. Available: http://www.stratos.org/

[Accessed: 19- Jan- 2018].

Deepin.org, “Deepin”, 2016. [Online]. Available: http://www.deepin.org/-

[Accessed: 05- Jan- 2018].

Kylinos.com.cn, 2016. [Online]. Available: http:/www.kylinos.com.cn/- [accessed: 05-Jan- 2018].

Bosslinux.in, (2015). About us | boss Linux. Retrieved 14 December 2018, from http://www.bosslinux.in/about-us

COS. [Online]. Available: http://www.china.cos.com/. [Accessed: 05- Jan- 2018].

Danchev, D. (2012). The cyber security publications of Iran’s government-backed antivirus software/ ZDNet. Retrieved 25th June 2018 , from http://www.zdnet.com/article/the-cyber-security-publications-of-Iran’s-government-backed-antivirus-software/

Nist.gov, (2011) comprehensive risk assessment guidance for federal information system published. Retrieved 25th June 2018 , from http://www.nist.gov/itl/csd/risk-092011.cfm

NIST, (2010). Guide for applying the risk management framework federal information systems: a security life cycle approach. Retrieved 25th June 2018 , from http://www.nist.gov.publicatiob/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

NIST special publication 800-53 revision 4. (2013). Security and privacy controls for federal information systems and organizations. Retrieved 25th June 2018 , from http://csrc.nist.gov/publications.drafts/800-53-rev4/sp800-53-rev4-ipd.pdf

NIST, (2008). Guide for mapping types of information and information systems to security categories. Retrieved 25th June 2018 , from http://csrc.nist.gov/publications/nistbups/800-60-rev1/sp800-60_Voll-Rev1.pdf

ENISA. (2014). Setting the course for national efforts to strengthen security in cyberspace.

Klimburg, A. (2012). National cyber security framework manual. [Tallinn, Estonia]: NATO Cooperative Cyber Defense Center of Excellence.

ITU. (2015). National Cybersecurity strategy guideline. Retrieved 25th June 2018 , from http://www.itu.int/ITU-D/cyb/cybersecurity.docs/itu-national-cyber-security-strategy-guide.pdf

Common wealth. (2015). COMMONWEALTH APPROACH FOR DEVELOPING NATIONAL CYBERSECURITY STRATEIGIES. Retrieved 25th June 2018 , from http://www.cto.int/media/fo-th/cyb-sec/Commonwealth%20Approach%20for%20National%20Cybersecurity%20strategies.pdf

ITU. (2015). Cyber security guide for developing countries. Retrieved 16 December 2015, from http://www.itu.int/ITU-D/cyb/publications/2009/cgdc-2009-e.pdf

Enisa.europa.eu. (2015). Good Practice Guide on National Cyber Security Strategies --- ENISA. Retrieved 25th June 2018 , form https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-startegies-ncsss/good-practice-guide-on-national-cyber-security-strategies

NATO CCDCOE, “Tallinn Manual on the International Law Applicable to Cyber Warfare”, 2009. [Online]. Available: http://www.peaseplacelibrary.nl/ebooks/files/356296245.pdf. [Accessed: 02- Jan- 2018].

Yamin, T. (2014). Developing Information-Space Confidence Building Measures (CBMs) between India and Pakistan. Sandia. Retrieved 25th June 2018 , from https://prod.sandia.gov/techlib/access-control.cgi/2014/144934.pdf

Enisa.europa.eu. (2015). National Cyber Security Strategies: An Implementation Guide --- ENISA. Retrieved 25th June 2018 , from https://www.enisa.europa.eu/activities/Rsilience-and-CIIP/national-cyber-security-strategies-an-implimentation-guide

Enisa.europa.eu (2015). An evaluation framework for Cyber Security Strategies --- ENISA. Retrieved 25th June 2018 , from https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncss/an-evalution-framework-for-cyber-security-strategies-1

World Economic Forum, (2013). Global Risk Report Eighth Edition. Retrieved 25th June 2018 , from http://www3.weforum.org/docs/WEF_GlobalRisk_Report_2013.pdf

World Economic Forum, (2013). Global Risk Report Eighth Edition. Retrieved 25th June 2018 ,from http://www3.weforum.org/docs/WEF_GlobalRisk_Report_2013.pdf

Tatar, U. Calik, O. Celik, M. Karabacak, B. (2014). A comparative analysis of the National Cyber Security Strategies of landing nations. 9th International Conference on Cyber Warfare & Security,

CCDCOE, (2014). Cyber Security Strategy Documents. (Australia, Austria, Canada, Czech Republic, Estonia, Finland, France, Germany, India, Iran, Israel, Japan, Malaysia, Netherlands, New Zealand, Spain, Saudi Arab, Turkey, UK and the USA) Retrieved 25th June 2018 , from https://ccdcoe.org/strategies-policies.html

ITU, (2015). A COMPARATIVE ANALYSIS OF CYBERSECURITY INITIATIVES WORLDWIDE. Retrieved 25th June 2018 , from https://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_Cybersecurity_initiatives_worldwide.pdf, Hdr.undp.org, “Human Development Report 2014 | “Human Development Reports”, 2014. [Online]. Available: http://hdr.undp.org/en/content/human-development-report-2014. [Accessed: 06- Jan- 2018].

European Parliament,. (2014). Cyber defence in the EU Preparing for cyber warfare?. Retrieved 25th June 2018 , from http://europart.europa.eu/EPRS/EPRS-Briefing-542143-Cyber-defence-in-the-EU-FINAL.pdf

Enigmasoftware.com,. (2015). Top 20 Countries Found to Have the Most Cybercrime. Retrieved 25th June 2018 , from http://www.enigmasoftware.com.top-20-countries-the-most-cybercrime/

Phoenix TS,. (2013). The Best and Worst of Cyber Security | Phoenix TS Blog. Retrieved 25th June 2018 , from http://phoneix.com/blog/best-and-worst-cyber-security /

Imfo.org, “World Economic Outlook Database April2015 – WEO Groups and Aggregates Information”, 2016. [Online], Available:

http://www.imf.org/external/pubs/ft/weo/2015/01/weodata/groups.htm. [Accessed: 05-Jan-2018].

MOHAMED, N. Malaysians are the most cyber-savvy among Asians. Retrieved 25th June 2018 , from htpp://www.therakyatpost.com/life/trends-life/2015/08/25/malaysians-are-the-most-cyber-savvy-among-asians/

Cybersecurit-review.com, (2015). CYBER SECURITY FOR THE DEFENCE INDUSTRY | Cyber Security Review. Retrieved 25th June 2018 , from http://www.cybersecurity-review.com/industry-perspective/cyber-security-for-the-defence-industry

Lehto, M. (2013). The Ways means and ends in cyber security Strategies. Proceedings of the 12th European conference on Information Warfare and Security.

Luiijf, H., Besseling, K., Graaf, P., & Spoelstra, M. (2013). Ten National Cyber Security Strategies: A Comparison. Critical Information Infrastructure Security. Lecture Notes in Computer Science Volume, 6983, 1-17.

Alliance, B. (2015). 2015 Asia Pacific Cyber Security Dashboard. 2015 BSA APAC Cyber Security Dashboard. Retrieved 25th June 2018 , from http://cybersecurity.bsa.org/2015/apac/index.html

Enigma software.com,. (2015). Top 20 Countries found to have the most Cybercrime. Retrieved 25th June 2018 , from http://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/

Robinson, N. Gribbon, l,. Horvath, V. and Robertson, K. (2013), Cyber-security threat characterization – A rapid comparative analysis.

Global Defence Outlook, (2014). Retrieved 25th June 2018 , from http://www2.deloitte.com/content/dam/Deloitte/global/Documents/Public-Sector/gx-ps-global-defense-outlook-2014.df

Levin, A. Goodrick,P. and Ilkina,D.(2013).Securing Cyberspace: A Comparative Review of Strategies Worldwide. Ryerson University.

Klimburg, A.(2012). National Cyber security framework manual. [Tallinn, Estonia]: NATO Cooperative Cyber Defense Centre of Excellence.

EU-U.S Security Strategies-comparative scenarios and recommendations, (2010). Retrieved 25th June 2018 , from http://csis.org/flies/publication/110614_conley_EUUSSecurity_WEB.pdf

Cyber security policy making at a Turning Point: Analyzing a New Generation of National Cyber security Strategies for the Internet Economy,(2012). Retrieved from http://dx.doi.org/10.1787/5kg8zq92vdgtl-en

Min, K., Chai, s., & Han, M. (2015). An international comparative study on cyber security strategy, IJSAI, 9(2), 13-20. http://dx.doi.org/10.14257/ijsia.2015.9.2.02

CTO, Commonwealth Approach for Developing national cyber security strategies. Retrieved 25th June 2018 ,from http://www.cto.int/media/fo-th/cyb-sec/

ITU., (2015), Cyber wellness Profiles. Retrieved 25th June 2018 , from http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Country_Profile.aspx

Benoliel, D. Towards a Cyber Security Policy Model- Israel National Cyber Bureau (INCB) Case Study. Retrieved 25th June 2018 , from http://Towards a Cyber Security Policy Model—Israel National Cyber Bureau (INCB) Case Study

AIIA,. (2015). Review of Australian Government Cyber Security Strategy. Retrieved 25th June 2018 , from http://www.aiia.com.au/documents/policy-submissions/policies-and-Submissions/2015/150417_AA_Cyber_Security_Submission_Final.pdf

The Cyber Index International Security Trendand Realities, (2013). Retrieved 25th June 2018 , from http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf

Cybersecurity Ventures, (2014). The Cyber security Market Report Covers the business of cyber security, including market sizing and industry forecasts, spending, notable M&A and IPO activity and more. . Retrieved 25th June 2018 , from http://cybersecurityventures.com/cybersecurity-market-report/

Enisa.europa.eu, (2014). ENISA Threat Landscape 2014 __ ENISA. Retrieved 25th June 2018 , from http://www.enisa.europa.eu/activities/risk-manaement/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014

Computer Weekly.(2015). Opinion: Dealing with a changing threat landscape. Retrieved 3rd June 2018, from http://www.computerweekly.com/opinion-Dealing-with-a-changing-threat-landscape

Recorded Future, (2014). Cyber threat Landscape: Forecast, Retrieved 25th June 2018 , from http://www.recordedfuture.com/cyber-threat-landscape-forecast/

Microsoft, (2014). Microsoft Security Intelligence Report- Regional Threat Assessment. Volume 18. Retrieved from http://www.microsoft.com/en-us/download/details.aspx?id=46929

Microsoft, (2014). Microsoft Security Intelligence Report – Worldwide Threat Assessment. Volume 18. Retrieved from http://www.microsoft.com/en-us/download/details.aspx?id=46928

Singh, H. (2013). Cyber Crime - A Threat to persons, Property, Government and Societies. International Journal of Advance research in computer Science and software engineering. 3(5). Retrieved 25th June 2018 from http://www.ijarcsse.com

Mali, P. (2015). Cyber case consultant, Filing Cyber Crime Case against Individuals, Property, Organization and society. Retrieved 25th June 2018 , from http://www.cyberlawconsulting.com/cyber-case.html

Shahid, J. (2014). Cyber stalking: New Challenges. Dawn.com. Retrieved 25th June 2018 , from http://www.dawn.com/news/1078417

M. Magazine, “Social Media harassment in Pakistan: only 5% cases registered in 2015”, Moremag.pk, 2015. [Online]. Available: http://www.moremag.pk/2015/12/18/social-media-harassment-in-pakistan-only-5-cases-registered-in-2015/[Accessed: 04-Jan-2018].

The Express Tribune, “Pakistan tops list of most porn-searching countries: Google – The Express Tribune”, 2015. [Online]. Available: http://tribune.com.pk/story/823696/pakistan-tops-list-of-most-porn-searching-countries-google/. [Accessed: 03-Jan-2018]

Mid-day, “Mumbai Kars beware! Your bank details are being stolen and sold!”, 2015. [Online]. Available: http://www.mid-day.com/articles/mumbaikars-beware-your-bank-details-are-being-stolen-and-sold/16218163/. [Accessed:01-Jan-2016]

M. Desk, “FIA and PTA get aggressive against rising grey traffic in Pakistan”, Moremag.pk, 2014. [Online]. Available: http://www.moremag.pk/2014/12/11/fia-pta-grey-traffic/ [Accessed: 02-Jan-2018]

Scribd, “Cyber Crime in Pakistan Research Report”, [Online]. Available: http://www.scribd.com/doc/24986331/Cyber-Crime-in-Pakistan-Research-Report. [Accessed: 03-Jan-2018].

The Express Tribune, “US agency collected second-highest amount of digital data from Pakistan – The Express Tribune”, 2013, [Online]. Available: http://tribune.com.pk/story/560949/us-agency-collected-second-highest-amount-of-digital-data-from-pakistan/. [Accessed: 07- Jan-2018].

Asiantribune.com, (2015). Indo-Israeli Cyber Warfare against Pakistani nuclear program | Asian Tribune Retrieved 25th June 2018 ,. from http://www.asiantribune.com/news/2009/09/08/indo-israeli-cyber-warfare-against-pakistani-nuclear-program

Dunyanews.tv, “Dunya News: Technology:-Indian cyber attacks targeted Pak military sites…,” 2013. [Online] Available: http://dunyanews.tv/en/Technology/174784-indian-cyber-attacks-targeted-Pak-military-sites. [Accessed: 03-Jan-2018]

Thetoptens.com, (2015). Top 10 Pakistani Hacker Team – TheTopTens.com. Retrieved 25th June 2018 , from http://www.theytoptens.com/pakistani-hacker-teams/

Bolobhi.org, (2015).Tracking cyber Crime Legislation –Bolo Bhi. Retrieved 14 December 2015, from http://bolobhi.org/resources/timelines/tracking-cyber-crime-legislation/

Act No. XVII OF 1996 An Act to provide for re-organization of telecommunication system. Retrieved 14 December 2015, from http://serl.pk/lawfile/12/PTRA-1996.pdf

Pakistan IT Policy and Action 2000. Retrieved 17 December 2015, from http://www.unapcict.org/ecohub/resources/pakistan-information-technology-policy

Pakistan IT Policy and Action 2000. Retrieved 17 December 2015, from http://www.unapcict.org/ecohub/resources/pakistan-information-technology-policy

Electronic Transaction Ordinance (ETO) 2002. Retrieved 4 December 2015, from http://www.pakistanlaw.com/eto.pdf

Punjablaws.gov.pk, (2002). The Defamation Ordinance, 2002. Retrieved 6 December 2015, from http://punjablaws.gov.pk/laws/2219a.html

Pakistanpressfoundation.org, (2011). PEMRA Ordinance 2002 | Pakistan Press Foundation (PPF) Pakistan Press Foundation (PPF). Retrieved 2 December 2015, from http://www.pakistanpressfoundation.org/freedom-of-expression/380/pemra-ordinance-2002/

Pakistan Electronic Media Regulatory Authority (PEMRA) Amendment Act 2001, Retrieved 14 December 2015, from http://www.na.gov.pk/uploads/documents/1321341849_903.pdf

Payment Systems and Electronic Fund Transfer Act 2007. Retrieved 25th June 2018 , from http://www.sbp.org.pk/psd/2007/EFT_ACT_2007.pdf

Rehman, K. Cyber Laws in Pakistan. Retrieved 25th June 2018 , from http://www.supremecourt.gov.pk/ijc/articles/101.pdf

Pta.gov.pk Monitoring & Reconciliation of International Telephone Traffic Regulations 3010. Retrieved 25th June 2018 , from http://www.pta.gov.pk/media/monitoring_telephony_traffic_reg_070510.pdf

K, F. (2012). Act for Monitoring Internet Cafes in Punjab to be imposed soon. Propakistani.pk. Retrieved 25th June 2018 , from http://propakistani.pk/2012/04/13/act-for-monitoring-internet-cafes-in-punjab-to-be-imposed-soon/

Draft National ICT Policy 2012. Retrieved 25th June 2018 , from http://pasha.org.pk/wp-content/uploads/2011/10/draft-IT-Policy-revised-July-3-2012.pdf

Investigation for Fair Trial Act 2013. Retrieved 25th June 2018 , from http://www.na.gov.pk/uploads/documents/1361943916_947.pdf

Khan, M. (2012). NA Passes Fair Trial Bill to Allow Agencies to Monitor Calls, Emails and More. Propakistani.pk. Retrieved 25th June 2018 , from http://propakistani.pk/2012/12/21/na-passes-fair-trial-bill-to-allow-agencies-to-monitoer-calls-emails-and-more/

Smspunch.net, (2015). 7-Point Action Plan to make Pakistan secure from Cybercrimes and attack Senate Committee on. Retrieved 25th June 2018 , from http://smspunch.net/single-article-forum-post-7304.

Bill for the establishment of a National Cyber Security Council (2014). Retrieved 25th June 2018 , from http://www.senate.gov.pk/uploads/documents/1397624997_197.pdf

The Express Tribune, (2014). Curbing cybercrimes: Ministry rejects cyber Security Council bill - The Express Tribune. Retrieved 25th June 2018 , from http://tribune.com.pk/story/789626/curbing-cybercrimes-ministry-rejects-cyber-security-council-bill/

Ohchr.org, (2015). Convention of the Rights of the Child. Retrieved 25th June 2018 , from http://www.ohchr.org/en/professionalinterest/pags/crc.aspx

Ohchr.org,(2015). Optional Protocol to the convention on Rights of the Child. Retrieved, 25th June 2018 from http://www.ohchr.org/en/professionalinterest/pags/OPSCCRC.aspx

Pakistan Penal Code (XLV OF1860). Retrieved 25th June 2018 , from http://www.oecd.org/site/adboecdanti-corruptioninitiative/46816797.pdf

The Wireless Telegraphy Act, 1993 Act Xvii of 1933. Retrieved 25th June 2018 , from http://pklegal.org/pdf/Wireless-Telegrphy-Act-1993.pdf

Federal Investigation Agency Act, 1974 (Act No. VIII OF 1975). Retrieved 25th June 2018 , from http://pklegal.org/pdf/FIA-ACT-1974.pdf

The Telegraph Act, 1885 (Act No. XIII of 1885). Retrieved 25th June 2018 , from http://pklegal.org/pdf/Telegrph-Act-1885.pdf

The Electronic Crimes Act 2004. Retrieved 25th June 2018 , from http://www.pakcon.org/post-pc-2004/pc-khi-02-jawad-electornic-crimes-bill-2003.pdf:

Rizvi, T, Cyber Laws. Retrieved 25th June 2018 , from http://www.superemecourt.gov.pk/ijc/articles/10/4.pdf

Prevention of Electronic Crimes Ordinance 2007. Retrieved 25th June 2018 , from http://serl.pk/lawfile/36/PECO-2007.pdf

Prevention of Electronic Crimes Ordinance 2009. Retrieved 25th June 2018 , from http://unpan1.un.org/intrdoc/groups/public/documnets/apcity/unpan037738.pdf

Mir, A. (2015). Electronic Communication Misuse Proposed To Be Booked Under Anti-Terrorism Act – TelecomPK. Telecompk.net. Retrieved 25th June 2018 , from http://telecompk.net/2011/12/20/electronic-communication-misuse-proposes-to-be-booked-under-anti-terrorism-act/

ACT to make provision of prevention of the electronic crimes 2012. Retrieved 25th June 2018 , from http://pasha.org.pk/wp-content/uploads/2012/12/E-Crime-Bill-Draft-v15.5.pdf

The Express Tribune, (2015). Legislative bungling: In a bill about cybercrime, MoIT inserts clauses legalizing censorship – The Express tribune. Retrieved 25th June 2018 , from http://tribune.com.pk/story/867824/legislative-bungling-in-a-bill-about-cybercrime-moit-inserts-clauses-legalising-censorship/

Sheikh, A. (2014). Draft Electronic Documents and Prevention of Cybercrimes Act, 2014. Retrieved 25th June 2018 , from http://bolobhi.org/wp-content/uploads/2014/01/Draft-Law-by-Akram-Sheikh-2014.pdf

Thenews.com.pk, (2015). The News International-Latest-News-Breaking-Pakistan-News. Retrieved 25th June 2018 , from http://www.thenews.com.pk/Todays-News-13-28608-New-cyber-crimes-law-proposes-heavy-fines-jail-but-exempts-intel-agencies/

Prevention of Electronic Crimes Act 2015. (2015). Retrieved 25th June 2018 , from http://na.gov.pk/uploads/documents/1421399434_340.pdf

The Express Tribune, (2015). Cybercrime legislation: Independent agency proposed in final draft – The Express Tribune. Retrieved 25th June 2018 , from http://tribune.com.pk/story/854949/cyber-crime-legislation-independent-agency-proposed-in-final-draft/

Opennet.net, (2015). Pakistan | OpenNet Initiative. Retrieved 25th June 2018 , from https://opennet.net/research/profiles/pakistan

Dawn.com, (2013). Sindh govt to block WhatsApp, Viber & other services for 3 months. Retrieved 25th June 2018, from http://www.dawn.com/news/1047209/sindh-govt-to-block-whatsapp-viber-other-services-for-3-months

Policy for Internet, Intranet, Websites, and E-Mail in Federal Government Organizations. Retrieved 25th June 2018 , from http://ntc.net.pk/policies/Email-Policy-by-Ccabinet-Division-%28NTISB%29.pdf

PTA, Protection from Spam, Unsolicited fraudulent and obnoxious communication Regulations, 2009. Retrieved 25th June 2018 , from http://www.pta.gov.pk/media/pro_spam_reg_09.pdf

The Express Tribune, (2011). Filtering SMS: PTA may ban over 1,500 English, Urdu words - The Express Tribune. Retrieved 25th June 2018 , from http://tribune.com.pk/story/292774/filtering-sms-pta-may-ban-over-1500-english-urdu-words/

The Express Tribune, (2011). Virtual watchdog: Internet users banned from browsing privately for security reasons' – The Express Tribune. Retrieved 25th June 2018 , from http://tribune.com.pk/story/virtual-watchdog-interneet-users-banned-from-browsing-privately-for-security-reasons/

Pakdocs.com Internet & E-Mail Policy for Government Departments 2011. Retrieved 25th June 2018 , from http://www.pakdocs.com/wp-content.uploads/2012/08/INTERNET-E0MAIL-POLICY-FOR-GOVERNMENT-DEPARTMENTS-2011.pdf?b50277

Infopakistan.pk, "YouTube Ban Finally Official Removed In Pakistan" , 2016. [Online]. Available: http://www.infopakistan.pk/20160/01/youtube-ban-finally-official-removed-in-pakistan/. [Accessed: 18- Jan- 2018].

Bolobhi.org, (2015). E-regulations Timeline – Bolo Bhi. Retrieved 25th June 2018 , from http://bolobhi.org/resources/timlines/state-of-internet-in-pakistan-e-regulations-timeline/

Saleem, Sana, (2012). #Stopcensoringpk: What is the National URL Filtering & Blocking System & Why Should You Care – Bolo Bhi. Bolobhi.og. Retrieved 25th June 2018 , from http://bolobhi.org/stopcensoringpk-what-is-the-national-url-filtering-blocking-system-why-should-you-care/

Dawn.com, (2015). Website monitoring assigned to PTA. Retrieved 25th June 2018 , from http://www.dawn.com/news/1172974/website-monitoring-assigned-to-pta

Use of web applications – Viber. (2015) Retrieved 25th June 2018 , from http://www.parc.gov.pk/files/parc_pk/January-15/viber-2015.pdf

Nr3c.gov.pk, National Response Centre for Cyber Crime. Retrieved25th June 2018 , from http://www.nr3c.gov.pk/

Azam, M. (2011). Cyber Security Regime in Pakistan, Still a Lot to be done! Propakistani.pk, Retrieved 25th June 2018 , from http://propakistani.pk./2011/0117/cyber-security-regime-in-pakistan-still-a-lot-to-be-done/

Pakistan's Perspective and Experience With Reference To Cert in Combating Cyber Terrorism. Retrieved 14 December 2015, from http://www.asean.org/archive/arf/13ARF/2nd-Cyber-Terrorism/Doc-12.pdf

Pakcert.org, (2015). PakCERT: Pakistan Computer Emergency Response Team. Retrieved 14 December 2015, from http://www.pakcert.org/

Pakistan Information Security Association (PISA). Retrieved 14 December 2015, from http://pisa.org.pk/

Pakistan Forensic Science Agency (PFSA). Retrieved 14 July 2015, from http://pfsa.gop.pk/cumputer-forensic

Pakistantoday.com.pk, (2012). Digital forensic lab to probe heinous crimes. Retrieved 14 December 2015, from http://www.pakistantoday.com.pk/2012/11/city/karachi/digital-forensic-lab-to-probe-heinous-crimes/

A. Siddique, "CERT Status in Pakistan: Authenticity of IRT –Objects" , APNIC, 2016. [Online]. Available: https://conference.apnic.net/data/37/apnic37-cert-status-in-pakistan_1393386654.pdf. [Accessed: 06- Jan- 2016].

Pips.gov.pk, (2015). Pakistan Institute for Parliamentary Services (PIPS). Retrieved 14 December 2015, from http://www.pips.gov.pk/

Fia.gov.pk, (2015). Federal Investigation Agency Retrieved 14 December 2015, from http://www.fia.gov.pk/en/NR3C.php

Sdpi.org, "Seminar", 2016. [Online]. Available: https://sdpi.org/policy_outreach/event_details588-2016.html. [Accessed: 09- Jan- 2016].

Jasoosibandkaro.pk, (2015). National Conference on Privacy Rights | Jasoosi Band Karo. Retrieved 14 December 2015, from http://jasoosibandkaro.pk/conference/

Pakistan Defence, (2015). Cyber Defense Day to be celebrated by PISA… Retrieved 14 December 2015, from http://defence.pk/threads/cyber-defense-day-to-be-celebrated-by-pisa.395573/

H. Malik, “Pakistan Gets Leading Position in International Cyber Drill”, Propakistani.pk, 2014. [Online]. Available: http://propakistani.pk/2014/02/24/pakistan-gets-leading-position-in-international-cyber-drill/. [Accessed: 04- Jan- 2016].

Nr3c.gov.pk, (2015). National Response Centre for Cyber Crime- Cyber Scouts. Retrieved 14 December 2015, from http://www.nr3c.gov.pk/scouts.html

Digital Rights Foundation, Digital Rights Foundation, About Retrieved 14 December 2015, from http://digital-rights-foundation.pk/about/

Pakistanforall.blogspot.com, (2015). Pakistan for All. Retrieved 14 December 2015, from http://pakistanforall.blogspot.com

P. Bhi, “PECB2015; The Story So Far – Bolo Bhi Bolo Bhi” , Bolobhi.org, 2015. [Online]. Available: http://bolobhi.org/resources/press-kit/pecb2015-the-story-so-far/, [Accessed: 03- Jan- 2016].

Digital Rights Foundation, (2015). Digital Rights Foundation, Hamara Internet. Retrieved 25th June 2018, from http://digital-rights-foundation.pk/work/hmara-internet/

Hamarainternet.org, (2015). Hamara Internet, Retrieved 25th June 2018 , from http://hamarainternet.org.pk/

State Bank of Pakistan, REGULATIONS FOR THE SECURITY OF ITNERNET BANKING. Retrieved 25th June 2018 , from http://www.sbp.org.pk/psd/2015/C3-Annexure-A.pdf

Securities and Exchange Commission of Pakistan, (2005). Internet Trading Guidelines. Retrieved 25th June 2018 , from http://www.secp.gov.pk/SECGuidSeries/PDF/Guidlines_InternetTrading.pdf

PTA, (2010). Telecommunication Security Guidelines Retrieved 25th June 2018 , from http://propakistani.pk/wp-content/uploads/2010/01/PTA_ict_ssecurity_guidlines_270110.pdf

Senate Defence Committee, (2013). Cyber Security Manual for Journalists, Retrieved 25th June 2018 , from

http://senate-defence-committee.com.pk/download/cyber-security-manual.pdf

Attaa, A. (2013). Pakistan, Among Top 5 NSA Targets, Takes Steps to Secure its Cyber Space. Propakistani.pk. Retrieved 25th June 2018 , from http://propakistani.pk/2013/09/27/among-top-5-nsa-targets-takes-steps-to-secure-its-cyber-space/

Mansab, C. Who Got Hacked-Hacking News and Cyber Attack Updates. Whogothacked.org. Retrieved 25th June 2018 , from http://www.whogothacked.org/

Lab, K. (2015). Applied Information Security: Ais.seecs.nust.edu.pk. Retrieved 25th June 2018 , from http://ais.seecs.nust.edu.pk/Achievements.php

Ripha.edu.pk, (2015). MS Information Security. Retrieved 25th June 2018 from https://www.ripha.edu.pk/facilities/information-security/ms-information-security

Ww3.comsats.edu.pk, (2015). MS Information Security. Retrieved 25th June 2018 , from https://ww3.comsats.edu.pk/cs/MSIS.aspx

Case.edu.pk, (2015). CASE: Center for Advanced Studies in Engineering. Retrieved 25th June 2018 , from http://www.case.edu.pk/DECE/ProgramMSIS.aspx

Au.edu.pk, (2015). MS in Avionics Engineering-Air University. Retrieved 25th June 2018 , from http://www.au.edu.pk/ms_ins.aspx

Ist.edu.pk, (2015). Master of Information and Cyber Security. Retrieved 25th June 2018 , from http://www.ist.edu.pk/ee/graduate/ms-information-cyber-security

Neduet.edu.pk, (2015). [NEDUET] – ACADEMIC PROGRAMMES. Retrieved 25th June 2018 , from http://www.neduet.edu.pk/academic/acad_programs.html

Eduvision.edu.pk, (2015). Punjab College of Technology And Management Sciences Lahore Admission announcement for Bachelor Master (ma MSc) PCTMS admissions 2014. Retrieved 25th June 2018 , from http://www.eduvision.edu.pk/admissions/index.php?ad=PPTC_8_8_14.jpg&ins=1407518136_PUNJAB-COLLEGE-OF-TECHNOLOGY-AND-MANAGEMENT-SCIENCES-LAHORE

Szabist.isb.edu.pk, (2015). SZABIST Islamabad. Retrieved 25th June 2018 , from http://www.szabist.isb.edu.pk/MSCS_Program.asp

User, S. (2015). DHA Suffa University - MS (Computer Science). Dsu.edu.pk. Retrieved 25th June 2018, from http://www.dsu.edu.pk/index.php/en/ms-computer-science

Csit.leads.edu.pk, (2015). Faculty of Computer Science. Retrieved 25th June 2018 , from http://csit.leads.edu.pk/PR%20MSIT.aspx

Mul.edu.pk, (2015). Minhaj University Lahore | Welcome….. Retrieved25th June 2018 , from http://www.mul.edu.pk/education/72/School-of-Information-Technology.html

cs.asif@yahoo.com, A. (2015). Department of Computer Science, Allama Iqbal Open University Islamabad Pakistan. Dcs.aiou.edu.pk. http://dcs.aiou.edu.pk/mscs.php

Ndu.edu.pk, (2015). National Defence University, Islamabad. Retrieved 25th June 2018 , from http://ndu.edu.pk/fcs/fs_sns_mphil.php

Ndu.edu.pk, (2015). National Defence University, Islamabad. Retrieved 25th June 2018 , from http://www.ndu.edu.pk/fcs/fsc_ir_mscc.php

lpop.org.pk, (2015). Internet Policy Observatory Pakistan. Retrieved 25th June 2018 , from http://ipop.org.pk/

Honeynet.pk, (2015). Pakistan HoneyNet Project – Honeypots. Retrieved 25th June 2018 , from http://www.honeynet.pk/honeypots.html

Certification.comptia.org, (2015). A+ (Plus) Certification | CompTIA IT Certifications. Retrieved 25th June 2018 , from http://Certification.comptia.org/getCertified/certifications/a.aspx

Eccouncil.org, (2015). Retrieved 25th June 2018 , from http://www.eccouncil.org/Certification/Professional-series/network5-course-outline

Eccouncil.org, (2015). Retrieved 25th June 2018 , from http://www.eccouncil.org/Certification/certified-secure-computer-user

Cisco, (2015). CCNA Security. Retrieved 25th June 2018 , from http://www.cisco.com/web/;earning/certifications/association/ccna_security/index.html?mdfd=2805638_5

Learningnetwork.cisco.com, (2015). CCNP Security – Cisco Certified Network Professional (CCNP) – The Cisco Learning Network. Retrieved 25th June 2018 , from https://learningnetwork.cisco.com/community/certifications/ccnpsecurity.

Csmd.edu, (2015). Microsoft Certifies System Administrator (MCSA) Security. Retrieved 25th June 2018, from http://www.csmd.edu/itcertification/courses/classes/mcsa.html

Eccouncil.org, (2015). EC-Council's Network Security Administrator ENSA. Retrieved 25th June 2018 , from http://eccouncil.org/Certification/eccouncil-network-security-administrator

Eccouncil.org, (2015). EC-Council Certified Secure Programmer ECSP. Retrieved 25th June 2018 , from http://www.ccouncil.org/Certified/ec-council-cerified-secure-progrmmer

Eccouncil.org, (2015). EC-Council Certified VOIP Professional. Retrieved 25th June 2018 , from http://www.eccouncil.org/Certified/ec-council-certified-voip-professional

Giac.org, (2015). GIAC GCWN Certification | Certified Windows Security Administrator. Retrieved 25th June 2018, from http://www.giac.org/certification/certified-windows-security-administrator-gcwn

Giac.org, (2015). GIAC GCUX Certification | Certified UNIX Security Administrator. Retrieved 25th June 2018 from http://www.giac.org/certification/certified-unix-security-administrator-gcux

Partners, C. (2015). CIW | Security Analyst Exam Guide (Retired) Ciwcertified.com. Retrieved 25th June 2018 , from http://www.ciwcertified.com/certifications/security_analyst.php

Isc2.org, (2015). System Security Certified Practitioner certification. Retrieved 25th June 2018 , from https://www.isc2.org/sscp/default.aspx

Certification.comptia.org, (2015). CompTIA Security+ Certification. Retrieved 25th June 2018 , from http://certification.comptia.org/getCertified/certifications/security.aspx

Certification.comptia.org, (2015). Cloud+ (Plus) Certification | CompTIA IT Certifications. Retrieved , 25th June 2018 from http://certification.comptia.org/getCertified/certifications/cloudplus.aspx

Certification.comptia.org, (2015). Server+ (Plus) Certification | CompTIA IT Certifications. Retrieved 25th June 2018 , from http://certification.comptia.org/getCertified/certifications/server.aspx

Csmd.edu, (2015). SCP's Security Certified Network Specialist. Retrieved 14 May 2018, from http://www.csmd.edu/itcertification/courses/classes/scnp.html

Checkingtricks.blogspot.com, (2013). Security Learners Blog. Retrieved 25th June 2018 , from http://checkingtricks.blogspot.com/2013/12/majjor-it-security-certifications-list.html#3kOdXYWtc

Isc2.org, (2015). Member Count. Retrieved 14 December 2015 , from https://www.isc2.org/memeber-counts.aspx

Isc2.org, (2015). CISSP – Certified Information Systems Security Professional | (ICS)^2. Retrieved 25th June 2018, from https://www.isc2.org/cissp/defalut.aspx

Certification.comptia.org, (2015). Social Media Security Certification. Retrieved, 25th June 2018 from http://certification.comptia.org/getCertified.certifications/smsp.aspx

Certification.comptia.org, (CASP) Advanced Security Practitioner Certification | CompTIA IT Certifications. Retrieved 25th June 2018 , from http://certification.comptia.org/getCertified/certifications/comptia-advanced-security-practitioner-(casp)

Giac.org, (2015). GIAC Security Certification | Security Administration Certifications. Retrieved 25th June 2018 , from http://www.giac.org/certifications/security-administration

Cisco, (2015). Cisco Cybersecurity Specialist. Retrieved 25th June 2018 , from http://www.cisco.com/web/;earning/certifications/specialist/security/sec_cyberSec.html

Alliance, T. (2015). Technologies Net Alliance. Tna.edu.pk. Retrieved 25th June 2018 , from http://tna.edu.pk/aboutus.php

Nhpakistan.com.pk, (2015). New Horizon Computer Learning Center Pakistan, IT Training, Microsoft Training, Cisco Training, Computer Training, Certifications, Computer Learning Centers. Retrieved 25th June 2018 , from http://www.nhpakistan.com.pk

Stscomps.com, (2015). Student Shelter in Computer | Pearson VUE Center. Retrieved 25th June 2018 , from http://www.stscomps.com/

Techno-ed.com, (2015). Techno-Ed. Retrieved 25th June 2018 , from http://www.techno-ed.com/

Das.com.pk, (2015). DAS Pakistan (Pvt) LtdTM | World Wide Certification Training & Inspection. Retrieved 25th June 2018 , from http://www.das.com.pk/

Amiapex.com, (2015). Ami Apex. Retrieved , 25th June 2018 from http://amiapex.com/s2/w/index.php

3deducators.com, (2015). PROFESSIONAL TRAINING COURSES IN KARACHI AND PAKISTAN - 3D EDUCATORS. 25th June 2018, from http://www.3deducators.com/

Limited, e. (2015). eVentureSolutions (EVS) – Center of excellence for NET, Java, PMP, PHP, Web Designing, MCTS, MCPD, SCJP, SCWCD training in Pakistan(Lahore, Rawalpindi / Islamabad). Evslearning.com. Retrieved 25th June 2018 , from http://www.evslearning.com/

Moon International, (2015). Retrieved 25th June 2018 , from http://mooninternational.com.pk/

Cesp.com.pk, (2015). Certification Services Pakistan (CeSP). Retrieved 25th June 2018 , from http://www.cesp.com.pk/

Qmsiso.com, (2015). Quality Management Systems.9000. Retrieved 25th June 2018, from http://qmsiso.com/about.aspx

Das.com.pk, (2015). ISO 27001 (Information Security Management System) | DAS Pakistan™ . Retrieved 25th June 2018 , from http://www.das.com.pk/iso-27001.php

Cyberqindia.com, (2015). IT Consulting | Software Services | Information Security Assurance| eGovernance – Information Security Services Information Risk Assessment | Risk Mitigation | Information Security Management. Retrieved 25th June 2018 , from http://www.cyberqindia.com/information_security

Trillium-Pakistan.com, (2015). Trillium-Pakistan (Pvt) Ltd. Retrieved 25th June 2018 , from http://www.trillium-pakistan.com/index.php

Tranchulas.com, (2015). Tranchulas | Cyber Security Company. Retrieved 25th June 2018 , from http://tranchulas.com/

Deltatechglobal.com, (2015). Pakistan's best network security solution provider. Retrieved 25th June 2018 , from http://deltatechglobal.com/

Securityexperts.com.pk, (2015). SECURITY EXPERTS. Retrieved 25th June 2018 , from http://www.securityexperts.com.pk

Quality Management Systems. 9000 Client List. Retrieved 25th June 2018 , from http://www.qmsiso.com/UserFile/File/Client%20List.pdf

Sidathyder.com.pk, (2015). Information Technology Risk Management Pakistan | Sidat Hyder Morshed Associates. Retrieved 25th June 2018, from http://sidathyder.com.pk/trm.html

Questconsultants.com.pk, (2015). Quest Consultant | Pakistan N0. 1 ISO Consultant | ISO Consultant | ISO Consultants in Pakistan | ISO Consultants in Karachi. Retrieved, 25th June 2018 from http://questconsultants.com.pk/

Isoexpert.com, (2015). Online Training, Auditing, Consulting & Certification Services | ISO Xpert Management & IT Consultants. Retrieved , 25th June 2018 from http://www.isoxpert.com/

Nimis.org, (2015). NIMIS | an Information Security Services Company. Retrieved 25th June 2018, from http://www.nimis.org/

Securebeats.com, (2015). Company. Retrieved , 25th June 2018 from http://securebeats.com/

C-ATRAX. (2015). Retrieved 25th June 2018, from http://www.c-artax.com/

Trats3CT, (2015). Trats3CT. Retrieved 25th June 2018 , from http://www.trats3ct.com

Oic-cert.org, (2015). OIC Cert | the Organization of Islamic Corporation Computer Emergency Response Teams. Retrieved , 25th June 2018 from http://oic-cert.org/en/fullmembers.html#.VeBTg_mqqko

Daily Times, (2005). FBI training FIA officers on cybercrime. Retrieved , 25th June 2018 from http://archives.dailytimes.com.pk/national/11-Jul-2003/fbi-training-fia-officers-on-cyber-crime

Malik, H. (2014). Pakistan Gets Leading Position in International Cyber Drill. Propakistani.pk. Retrieved 25th June 2018 , from http://propakistani.pk/2014/02/24/pakistan-gets-leading-position-in-international-cyber-drill/

Khandelwal, S., & Khandelwal, S. (2015). Pakistani Hacker Arrested for Hacking Telecom Company Database. The Hacker News. Retrieved 25th June 2018 , from http://thehackernews.com/2014/04/pakistani-hacker-arrested-forhacking_5.html

The News Tribe, (2015). PIA hits worst cybercrime in history of aviation, no record maintained for tickets worth $7 million. Retrieved 25th June 2018 , from http://www.thenewstribe.com/2013/08/20/pia-hits-worst-cybercrime-in-history-of-aviation-no-record-maintained-for-tickets-worth-7-million/

Attaa, A. (2013). Aaj TV Gets Hacked, Entire Website Data Leaked Online. Propakistani.pk. Retrieved 25th June 2018 from http://propakistani.pk/2013/07/15/aaj-tv-hacked-entire-website-data-leaked-online/

NIST Special Publication 800-53 Revision 4, (2015). Security and Privacy Controls for Federal Information Systems and Organizations. Retrieved 25th June 2018, from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Critical Infrastructures: What Makes an Infrastructure Critical? (2003). Retrieved 25th June 2018, from http://fas.org/irp/crs/RL31556.pdf

The Express Tribune, “Iran hackers penetrate key networks in Pakistan: Researchers - The Express Tribune” , 2014. [Online]. Available: http://tribune.com.pk/story/801657/iran-hackers-penetrate-key-networks-in-pakistan-researchers/ [Accessed: 04- Jan- 2018]

Desk, M. (2014). Cyber security still not a priority for government. Mormag.pk. Retrieved 25th June 2018, from http://www.moremag.pk/2014/10/01/cyber-security-still-not-a-priority-for-government/

The Express Tribune. (2015). Cybercrimes: Pakistan lacks facilities to trace hackers - The Express Tribune. Retrieved 25th June 2018 , from http://tribune.com.pk/story/831178/cybercrimes-pakistan-lacks-facilities-to-trace-hackers/

The Express Tribune,. (2015). Cyber crime bill: FIA may be excluded from investigation process – The Express Tribune. Retrieved 25th June 2018 , from http://tribune.com.pk/story/844137/cyber-crime-bill-fia-may-be-excluded-from-investigation-process/

Press Release Don't block the blog. (2015) (Ist Ed.). Retrieved from https://docs.google.com/viewerng/viewer?url=http://help-pakistan.com/main/wp-content/uploads/2006/05/Press+Release+Dont+Block+the+Blogs.pdf

Nasir, S. (2013). Pakistan bottom of the barrel on net freedom: Report – The Express Tribune. Retrieved 25th June 2018 , from http://tribune.com.pk/story/612958/pakistan-bottom-of-barrel-on-net-freedom-report/

Aziz, f. (2010). The Dangers of a Content Filtration System – Bolo Bhi. Bolobhi.org. Retrieved 14 December 2015, from http://bolobhi.org/the-dangers-of-a-content-filtration-system/

Haque, J. (2013). Pakistan's Threat Landscape – A Report by Bytes for All. Retrieved 4 January 2018, from https://content.bytesforall.pk/sites/default/files/MappingReportFinal%20-%20published.pdf

Aziz, f. (2010). In the Name of the Law. Retrieved 25th June 2018 http://www.newslinemagazine.com/2010/06/in-the-name-of-law/

The Express Tribune. (2012). Video controversy: YouTube likely to remain blocked in Pakistan indefinitely – The Express Tribune. Retrieved 25th June 2018 , from http://tribune.com.pk/story/446121/video-controversy-youtube-likely-to-remain-blocked-in-pakistan-indefinitely/

Paktimes.com. (2015). ISP (Internet Service Provider) List of Pakistan – PakTimes. Retrieved 25th June 2018 , from http://www.paktimes.com/index.php?pln=isp_index