TALLINN UNIVERSITY OF TECHNOLOGY
Faculty of Information Technology
Department of Computer Science
TUT Center for Digital Forensics and Cyber Security

Taimur Tufail IVCM156329

COMPARING THE NATIONAL CYBER SECURITY FRAMEWORK OF PAKISTAN WITH INDIA AND UNITED KINGDOM

Master thesis

Supervisor: Hayretdin Bahsi (PhD)

Senior Research
Scientist

Tallinn 2018

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond
Arvutisüsteemide instituut
TTÜ küberkriminalistika ja küberjulgeoleku keskus

Taimur Tufail IVCM156329

PAKISTANI RIIKLIKU KÜBERTURVALISUSE RAAMISTIKU VÕRDLUS INDIA JA ÜHENDKUNINGRIIKIDEGA

Magistritöö

Juhendaja: Hayretdin Bahsi (PhD)
Vanemteadur

Tallinn 2018

Author's declaration of originality

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

Author: Taimur Tufail

01.05.2018

Abstract

These days the most critical challenges faced by the governments is cybersecurity. It is no longer just an IT issue and should be dealt on a National Level. This research paper compares and analyses Cyber Security Legislation, National Cyber Security Strategies, National CERT, CIIP, Education and Awareness based on documented Technical, Operational, Legal and Policy-Related measures of Pakistan with India and the United Kingdom.

These countries share the similar legal structure because Pakistani law is based on the legal system of British India which was ultimately derived from the "Common law of England and Wales". India is relatively similar to Pakistan as they both are under-developed countries. The UK, on the other hand, is a much more developed and advanced society.

Based on the comparison, this research recommends and specifies the guidelines for improving the national cybersecurity in Pakistan. Pakistan can use this research to develop and enhance its cybersecurity strategy and laws accordingly.

It is identified that Pakistan does not have a National Cyber Security strategy, and other essential institutions in this field. In this study, we also give recommendations to policymakers to improve the Pakistan situation.

This thesis is written in English and is 77 pages long, including 7 chapters, 5 figures.

Annotatsioon

Pakistani riikliku küberturvalisuse raamistiku võrdlus India ja Ühendkuningriikidega

Tänapäeval on valitsuste kõige olulisemaks väljakutseks küberturvalisus. Tegemist ei ole enam ainult IT probleemiga, vaid küsimusega, millega tuleks tegeleda riiklikul tasandil. Käesolev magistritöö võrdleb ja analüüsib küberturvalisuse seadusandlust, riiklikke küberturvalisuse strateegiaid, kohalikke CERT-e, CIIP-i, akadeemilisi võimalusi ja teadlikkust, mis põhineb dokumenteeritud tehnilistel-, operatiivsetel-, legaalsetel- ja strateegilistel näitajatel kolme riigi – Pakistani, India ja Ühendkuningriigi vahel.

Need kolm riiki omavad sarnast õiguslikku struktuuri tuginedes faktile, et Pakistani seadusandlus põhineb Briti-India õigussüsteemil, mis omakorda on algselt tuletatud Inglismaa ja Wales'i tavaõigusest. India on sarnane ja võrreldav Pakistaniga, sest mõlemad on vähearenenud riigid. Ühendkuningriigid on samas kõrgemalt arenenud ja edasijõudnud ühiskond.

Baseerudes eeltoodud võrdlusele toob käesolev uurimustöö välja soovitused ja täpsustavad juhised parandamaks riiklikku küberturvalisust Pakistanis. Pakistan võib kasutada käesolevat uurimust vastavalt edendamaks ja/või tugevdamaks oma küberstrateegiaid ja seadusandlust.

Pakistan ei oma töötavat küberturvalisuse strateegiat riiklikul tasemel ning selle implementeerimiseks vajaminevaid institutsioone. Antud uurimuses antakse soovitusi Pakistani poliitikaarendajatele olukorra parendamiseks.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 77 leheküljel, 7 peatükki, 5 joonist.

List of abbreviations and terms

CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
CISP	CISP - Cyber Security Information Sharing Partnership
CPNI	Centre for the Protection of National Infrastructure
ENISA	European Union Agency for Network and Information Security
ETO	Electronic Transactions Ordinance
FIA	Federal Investigation Agency
GCHQ	Government Communications Headquarters
GDPR	General Data Protection Regulation
ICT	Information & Communications Technology
IPC	Indian Penal Code
IRO	International Rights Organization
MeitY	Ministry of Electronics and Information Technology
MoU	Memorandum of Understanding
NADRA	National Database and Registration Authority
NCI-IPC	National Critical Information Infrastructure Protection Center
NCIIPC	National Critical Information Infrastructure Protection Centre
NCRB	National Crimes Records Bureau
NCSC	National Cyber Security Centre
NCSP	National Cyber Security Programme
NIC	National Informatics Center
NISCC	National Infrastructure Security Co-ordination Centre
NTC	National Telecommunication Corporation
NTRO	National Technical Research Organisation
NUST	National University of Sciences and Technology
OECD	Organisation for Economic Co-operation and Development
OIC-CERT	Organization of Islamic Cooperation- Computer Emergency Response Team
PISA	Pakistan Information Security Association
SCO	Shanghai Cooperation Organisation

Table of contents

List of figures

1 Introduction

Every nation is trying to boost its economy by expediting the economic benefits of ICT. These significant challenges are faced by every country due to the geographical hurdles, land laws and cultural patterns [1]. The cyberspace is so easily accessible and that it is the main reason why there has been a growth in internet related crimes [1] and hazard to the National Security of the country. The whole world is proliferating in cyberspace. According to the Global Cyber Security Index (2017) [2] Singapore, United States, Malaysia and Oman are busy securing their cyberspace and are in the top ten most committed countries list. Also, GCI 2017 states that some of these countries have developed laws and strategies to protect themselves from any imminent threat in the cyber world but other under-developed nations are still struggling to cope with the advancement of the technology and protecting its critical infrastructure.

India is relatively similar to Pakistan as both are under-developed countries which started at the same time in 1947. They share a similar culture, and population number is relatively high, but on the other hand, the UK is a much more developed and advanced society. Pakistan became an independent nation when it separated from British India on 14th August 1947. Since then Pakistan and India never had good relations with each other. The reason behind this was issues related to Siachen, disputed land of Kashmir and border. Once they became nuclear power nations, the threat model has been further enhanced to include both kinetic and non-kinetic [3].

Pakistan will be compared with the United Kingdom and India. These three countries are chosen because they share the same legal structure because Pakistani law is based on the legal system of British India which was ultimately derived from “Common law of England and Wales”. They all have the English language is spoken which is either first or second primary language in these countries.

Pakistan from the very start got way led in its democratic experiment as opposed to India. Very early the Army become involved in politics in Pakistan, and this followed brief

periods of a civilian rule which lasted for long periods of control by Martial Law Administrations. The constant political disturbance led to inconsistencies in policy shaping institutions and lack of setting up stable institutions which are essential for a country. So the IT sector had a late start and even the few laws and regulations which drafted eventually, failed to improve the core deficiencies in efforts related to regulation and protection of the cyberspace. Unprotected cyberspace can pose a threat to the economy and safety of a nation. As the political environment matures and becomes more stable there is a need for strict legislation to be introduced otherwise managing Cyber Crime and other significant Cyber threats would be impossible. It may be mentioned that Pakistan has no lacking a large potentially intelligent and capable workforce but ways must be developed to encourage and develop this pool, so they are lead into proper institutes and then employed in dedicated Government Departments focused solely on Cyber Security.

On every Independence day of Pakistan and India, the underground cyber teams in both countries try to deface as much government websites as possible and place their countries flag with the message that their country is great [4]. It is going on since quite a while in both countries, and many websites government and educational institutions websites compromised because of this.

The massive increase in cyber attacks was a wakeup call for each nation and some of them finally started to think about the security. This comparative analysis will discuss these further in detail.

1.1 Motivation

Many of the published comparative analysis regarding cyber security I have read are mostly focusing on other countries, but I could not find any research which compares Pakistan with its similar countries such as India and a developed country such as the United Kingdom.

The global rank in the Cyber Security Index 2017 for Pakistan is 67 [2]. If we compare this with its neighbouring country, it is 23 for India [2]. It is almost three times difference

in the ranking. The United Kingdom which is a developed nation has a global rank of 12 [2].

The main question is why two countries which share similar culture, languages and got independence from the United Kingdom at the same time have such a steep difference in the Global Cyber Security rank. That is the reason I wanted to write this research report to show what India did right, and Pakistan can learn from these mistakes for securing its cyberspace and creating stricter laws to protect the country against any cybercrime.

There is a rapid increase in online attacks and a constant fear that next major war will be the information war between nations [5]. We had already seen signs of information warfare when US Elections 2016 were manipulated [6] by transmitting false information on the social media against Hilary Clinton. Pakistan is a nuclear power country with almost 200 million people, and it cannot afford any negligence toward cybersecurity just because of its political policies. Even now Pakistan does not have a working Cyber Security Strategy on a national level.

There are only a few similar studies, but none of them gives a detailed analysis between these three countries. This research gives an insight into how effectively Pakistan is protecting its cyberspace and what it can learn from other countries such as India and the United Kingdom.

1.2 Scope

This report covers the indicators from the four pillars of the Global Cyber Security Index 2017 [2]. These indicators are Cyber Security Legislation, National Cyber Security Strategies, National CERT, Critical Information Infrastructure Protection, Cyber Security Education and Awareness based on the technical, operational, legal and capacity building Pillars of the GCI 2017 [2]. The Cyber Security Legislation includes Cybercrime and Data Protection laws. These indicators are used to compare Pakistan with India and the United Kingdom.

Another reason of choosing these indicators was that not every country is implementing all of the GCI 2017 indicators and if one of the indicators are not applied in a country,

then it cannot be compared with another. Also, these indicators are chosen for comparison because they cover each aspect of cyber security and what at least the country needs to secure its cyberspace.

1.3 Contribution

This research paper can be used to understand the different approach on Cyber Security in each of these countries and how government policies on early or later technology adoption can set back a country compared to others.

This research is analysing what India and the United Kingdom is doing to protect its cyberspace and what Pakistan can learn from them. Then, in the end, it provides a recommendation which Pakistan can follow and its cyber security in the country.

1.4 Limitations and Challenges

There are several limitations due to unavailability of the data mostly for Pakistan and India. I did the best to maximise the resources I found and tried to compare with most of the GCI pillars in the Global Cyber Security Index [2]. I have taken into account all the resources which are available publicly.

It is hard to compare if the government does not share information such as cybersecurity practices followed by the military or army divisions. Due to the scope of this report, this research is limited to the information which was made public and available to everyone. For example, especially for Pakistan, most of the information such as official laws Acts or statistic of the cybercrime arrest made in each year are not made public by these relevant departments. This information is collected from secondary sources such are news articles or blogs.

The United Kingdom has a well structured and detailed policy regarding cyber security which is available online to the public. It was tough to find resources for India and especially Pakistan as some of the information can only be derived from other similar article, news reports, and studies.

1.5 Thesis Structure

This thesis report is organised as follows. Chapter 2 gives a brief review of other similar reports and explains what reports were missing and how this thesis research report has covered those main points. Chapter 3 gives a general comparison between Pakistan, India and the United Kingdom. It compares the history, internet user's statistics over the years, population, corruption rate, cyber crime statistics between these countries. From the chapter 4, the comparative analysis starts, and it compares Cyber Security legislation (which includes Cybercrime and Data Protection laws), National Cyber Security Strategies, National CERT, CIIP, National Educational Programs and Awareness. In Chapter 5 recommendations have been made for Pakistan, and Chapter 6 gives the Conclusion.

2 Literature Review

There are only a few similar studies which compare and provide guidance for Pakistan. In some studies, the Cyber Security Strategies or Cyber Crime are compared but not in detail between India and Pakistan or between India and the United Kingdom. None of these reports is as much in detail as this one, and they do not cover most of the indicators of the Global Cyber Security Index [2]. There is no report which covers all three of these countries.

The report by Mr. Baqir [3] gives only a brief overview of the Cyber Security Strategy between Pakistan and India and does not cover cybercrime, data protection policy, CIIP and awareness of cybersecurity. In another report by Mr. Zibber [7] shows analysis of cyber crime laws in Pakistan but until 2006 only. There is another report by Miss. Sadia [8] explains the cyber threats faced by Pakistan but its main focus is on the cyber threats and its types only. It does not cover the institutions and laws.

3 General comparison

The number of users using the internet in Pakistan as displayed in Figure 1 has increased to 34 Million in 2016, but in the year 2006, it was only 10 million, that is 273% increase in 10 years only. Even though the increase looks positive, when we compare this with India the percentage increase is 1317%, which is a massive increase compared to Pakistan. The population increase in the same period is 25% in Pakistan compared to India who only had 16% only.

The United Kingdom, on the other hand, has 44% increase in the number of internet users from 2006 to 2016 as displayed in Figure 1, even though the total population increase is just 10%. A technologically advanced nation such as the United Kingdom does not have a massive increase in the number of internet users as they already adopted the technology at a very early stage. 70% of the population in the UK was already using the internet in 2006 as seen in Figure 2, but in India, it was 3% and 6% in Pakistan.

The results of Global Cybersecurity Index 2014 [9] shows that the global rank of Pakistan was 23, India and the United Kingdome both had 5. The global ranking in the Global Cybersecurity Index 2017 [2] for Pakistan was 67. If we compare this with its neighbouring country, it is 23 for India. The difference is three times in the ranking. The United Kingdom which is a developed nation has a global rank of 12 in GCI 2017. We cannot directly compare GCI 2014 with GCI 2017 as the methodology changed in both. In 2014, they used the “simple average method”, but in 2017 each pillar had a weighting factor.

If we compare the level of corruption in the countries, the Corruption Perceptions Index 2014 shows the perceived levels of corruption and gives a ranking for each country [10]. Pakistan’s ranking was 126/174, but in the Corruption Perceptions Index 2017, the ranking decreased to 117/180 [11]. Pakistan’s ranking in 2017 was still much lower than India and the United Kingdom. In 2014 India had a ranking of 85/174 [10], but in 2017 it was 81/180 [11]. The United Kingdom is the most corruption free country compared with India and Pakistan, with a massive difference in ranking of 14/174 [10] in 2014 and 8/180 [11] in 2017.

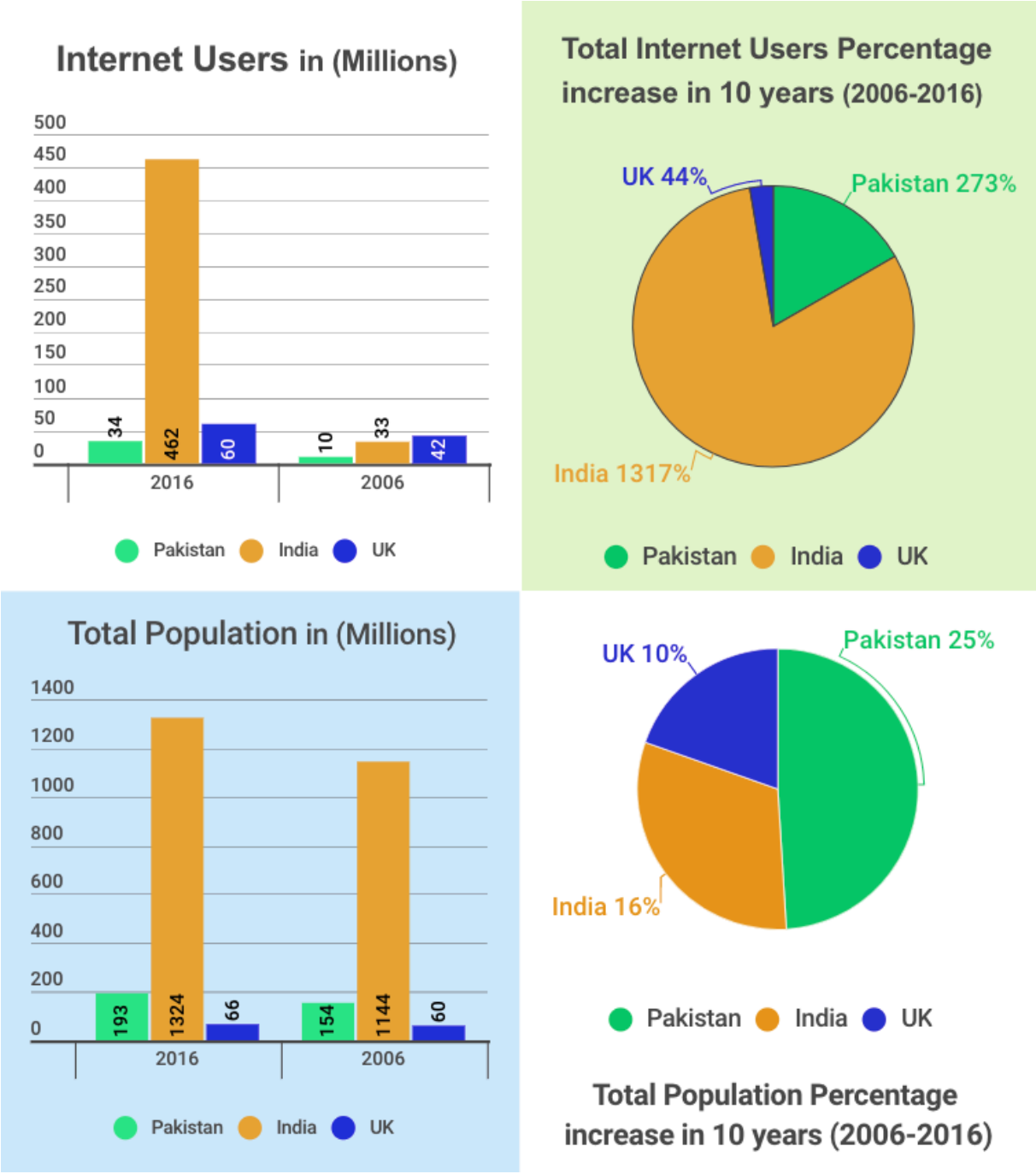

Figure 1 Adapted from [12] [13]

Global State of Mobile Networks reports shows that in 2016, Pakistan had 63.47% availability of 3G or 4G internet in the country [14]. India had 56.10%, and the United Kingdom had 84.20% availability. In 2016 the users spend 34.12% percent of their time connected to wifi in Pakistan, while in India it was 29.82% and in the UK it was 60.13% [14]. It shows even though India and Pakistan have similar availability of 3g and 4g

networks, in Pakistan users, are spending more time on the internet then India. The United Kingdom, on the other hand, is a developed country with 91% percent of the population in 2016 already using the internet explains why the users spend 60.13% of their time [14].

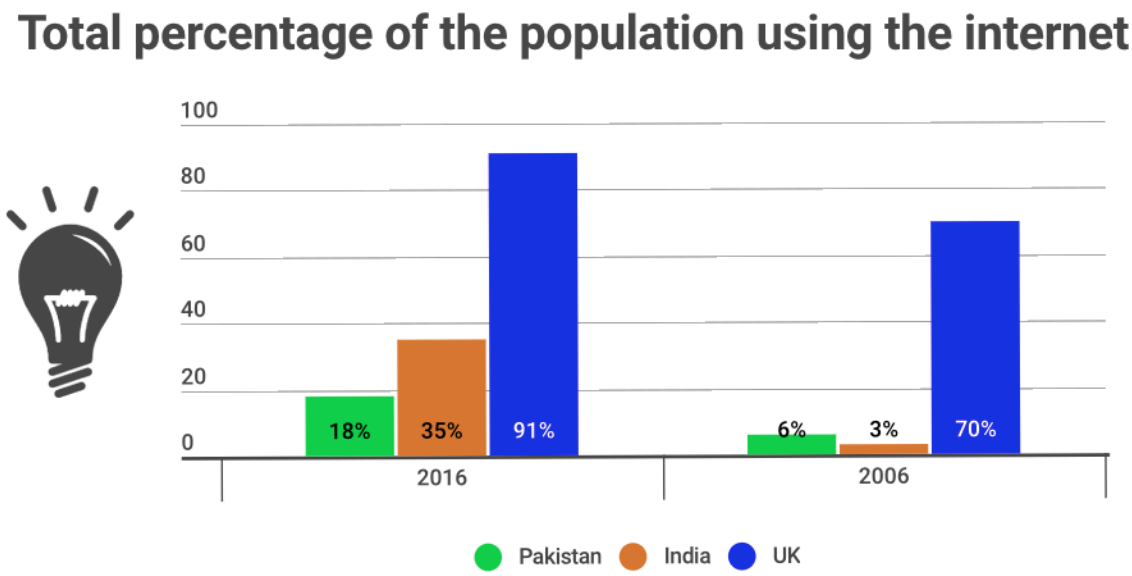

Figure 2 Adapted from [12] [13]

The amount of internet users in a country has a direct relation to the number of cyber attacks because if the number of internet users will increase the cybercriminals will get more opportunities to attack them. The figures in Figure 2 shows a trend in India's economy and how they adopted technology in their daily life in these years. Pakistan is far behind India if we only base on these statistics in Figure 2. There are some reasons why Pakistan was left behind in this year. These factors can be related to:

- **Changes in Income Brackets:**

  The middle class in India has increased almost three times [15] higher compared to Pakistan where it only increased two times [16]. The increase in the number of middle class means that as the income of the poor people increased, they could afford to buy and adopt the new technology.

- **Government Policies towards internet infrastructure development:**

  The Indian government introduced the new ISP policy in 2000 to invite private players in the market. By doing this, they created competition and lowered down the internet rates for an end user. Then the government also introduced its first broadband policy, and the aim was to connect every part of the country. Then after

2009, the mobile data users entered the market, and the user base increased rapidly after the launch of 3G and 4G services [17].

The UK has very early adoption of the Internet. According to the Figure 2, almost 70 percent of the population was using the internet in 2006. It also has well established legal structure, and one category falls into various numbers of Acts which shows that in 2006 alone 3,237,500 cyber crime related cases were reported [18].

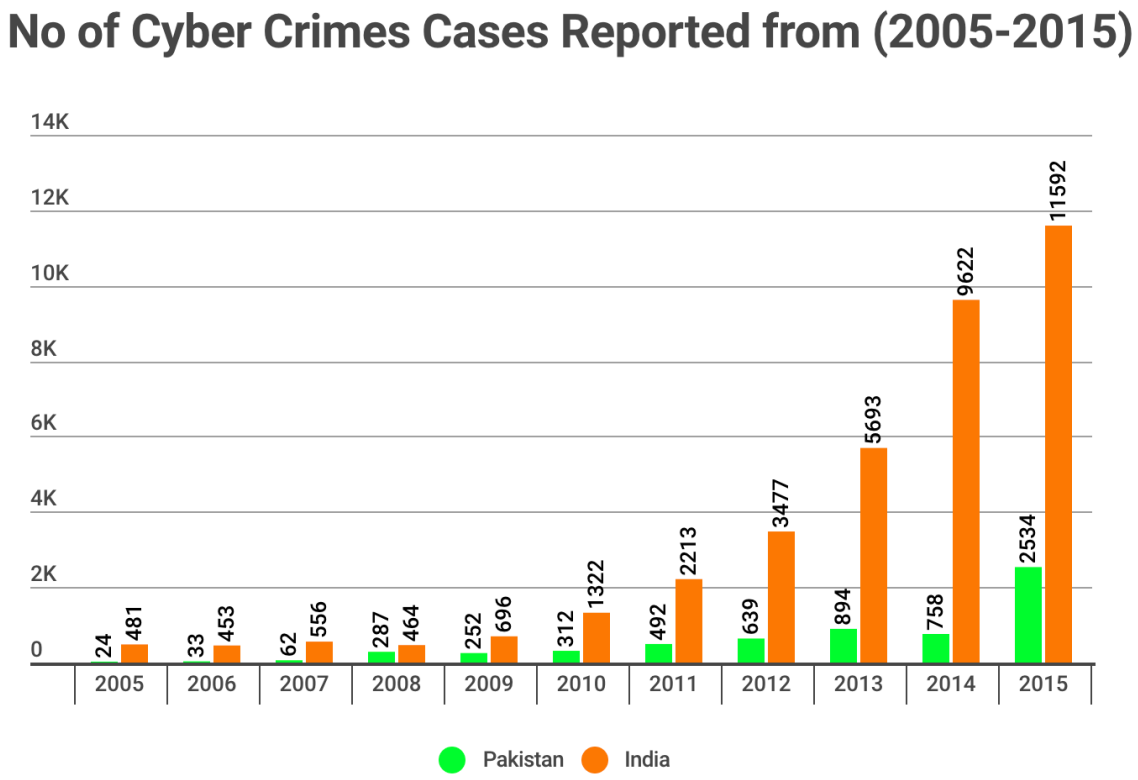

Figure 3 Adapted from [19] [20] [21] [22] [23] [24]

Pakistan's cybercrime reported cases are not publically available and the government does not appropriately handle the official documents. Most of the data for India is available, but for Pakistan, it is gathered from the secondary sources such as news websites. The UK, on the other hand, creates and publishes a cybersecurity report each year [25]. These reports show the detailed official statistics such as for the cybercrime reported cases. These reports show that the UK is much more transparent when it comes to cybersecurity-related incidents compared to India or Pakistan.

The cybercrime rate is gradually increasing in Pakistan as displayed in Figure 3, and there was a big gap between 2014 to 2015 because conviction rate is low. The NR3C in Pakistan convicted 44 offenders in total out of 2534 in 2015. Among these 44 individuals, 40 individuals still could not be arrested [26]. In India, the statistics show in Figure 3 that by 2013, 1600 people arrested out of 5693 [21] crimes reported. Among these 1600 arrested individuals, only seven convicted. "*In the year 2007, the arrests made were 154 while in the following year there was 178. In the years 2009 and 2010, the numbers of persons arrested were 288 and 799, and in 2011, it was 1,184*" [1]. The conviction rate is tremendously low, because of this the crime rate increased rapidly [1]

4 Comparative Analysis

In this report, online desk research was conducted by taking publicly available documents and using that information to do comparative analysis. This analysis shows the comparison of Cybersecurity Legislations, Cyber Security Strategies, National CERT, CIIP, Education and Awareness on Cyber Security in Pakistan compared with India and the United Kingdom.

4.1 Cyber Security Legislation

Cyber Security Legislation is comprised of different laws which help protect each aspect of cybersecurity in a country. In this research, only two will be discussed which are Cyber Crime and Data Protection Laws. Different Ordinances, Bills and Acts are discussed in this part, and the following is the brief description of each.

- An ordinance is a temporary local level law which is passed by municipalities. The municipalities can be cities, town and village. They have the same power as the "ACTs", but it is limited within that city or town [27].
- A Bill is the first stage of an Act; it is a proposal to create a new law [28].
- An Act is a law or statue that records a fact. In simple terms, it is a rule which is written on a piece of paper, and once it gets passed, it becomes law [29].

4.1.1 Cyber Crime Laws

The legislation is essential in every sector as it sets standards and controls to manage the actions of the people in both public and private sector [30]. The Cyber Crime Legislation deals with criminal offences which are committed using an electronic device such as computer [31]. These types of crimes are increasing rapidly with the adoption of technology, and the criminals are exploiting this anonymity, speed, and convenience of the internet to commit all sorts of unlawful activities anywhere in the world. There are two main types of Internet-related crimes according to INTERPOL, which is the "International Criminal Police Organization" [32]. The first one is "Cyber-enabled crime" which are the same as traditional crimes, but now they are committed over the internet. These could be financial crime or terrorism. An example would be sexual assault crime

which even happened before the internet age, but now this can happen over the internet. The second type is “Advanced Cybercrime” which is highly sophisticated, and the target is the computer software or hardware. This second type of crimes is more complicated such as unauthorised access to download data from someone’s computer. Before the internet age, this kind of hacking-related crimes did not exist, and that is why they are called Advanced Cybercrime.

4.1.1.1 Pakistan’s Cyber Crime Laws

In Pakistan, the first legal framework to address cyber crimes was passed by the government in 2002, named as Electronic Transactions Ordinance 2002 (ETO) [33]. The primary objective of this ordinance was to facilitate and identify information, documents, communications, electronic transactions, and records. This ordinance gave protection from any misuse of the electronic transactions such as bank payments, purchasing products online but there are not many details mentioned on how misuse case has could be identified. It helped to recognise the authenticity of these online transactions.

With this specific ETO 2002 ordinance, Pakistan was added to the number of other countries which now have legal backing for any electronic communication or information [33]. This ordinance leads to the birth of e-commerce industry and a significant decision for the information technology development in the country [7]. Although it did provide some punishments for various kinds of cyber crimes, there were many loopholes such as the ordinance failed to criminalise most of the crimes as compared to other international countries [34]. That is why there was a need for a quick update [33].

Later in 2004, the Ministry of Information Technology prepared Electronic Crime Act 2004 which is based on the ETO 2002 but with improvements [7]. This act included many legislative terms such as Cyber Terrorism, Criminal Access, Electronic Fraud and Data or System Damage [35]. Although these terms introduced in this Act, they were much in detailed and also it did not mention to establish a cybercrime unit [36]. This Acts primary objective was to give legal cover to any anti-cybercrime efforts [37].

In 2007 the government passed an updated Electronic Crimes Ordinance [38]. The ordinance covered the regulation of the internet sector but the main changes were that it

defined the punishments for 17 types of cyber crimes and the penalties were six months in prison to a death penalty. It also included a new type which was Cyber Stalking, which is a criminal acts "*with intent to coerce, intimidate, or harass any person uses the computer, computer network, internet, network site, electronic mail or any other similar means of communication*" [39]. Other changes in crime types were Spamming and Cyber Terrorism. This ordinance also required retention of traffic data by the ISP for at least 90 days.

In Pakistan, the latest cybercrime bill was passed by the National Assembly in 2016. The bill was named Prevention of Electronic Crimes Bill (PECB) [40]. This bill included the provisions which allowed surveillance, censorship and can be directly used to penalise online speech. It did contain some safeguards for cybercrime investigations by the government and law enforcement agencies [41].

It came under some intense criticisms from inside Pakistan, the United Nations (UN) and the International Rights Organization (IRO) [41]. It was said to be, too harsh and the punishments did not correctly fit with the crimes. It restricted the freedom of expression and any access to information. It did not differentiate cyber warfare and terrorism from cybercrime. Journalists sources could be exploited with this bill [42].

An example of exploitation on this Bill was in 2016 when a teenage boy was taken into custody for liking the Facebook post of a blasphemous content [43], and he is facing a prison sentence up to 10 years [44]. This example was the first time when a blasphemy taking place on a social media platform leads to a conviction of death penalty. There was another case in 2017 when a 30-year-old man given a death sentence for making comments against religion on Facebook [45]. There are other examples as well which shows that this bill directly restricts the freedom of speech.

Pakistan established National Response Centre for Cyber Crimes (NR3C) in 2007, to resolve all computer-related crimes and gather intelligence for these cases [46]. This centre provides the government with the highly technical expertise in Information Systems Security Audits, Digital Forensics, and Penetration Testing. It directly receives the relevant complaints about cybercrime incidents and also assists the other government based agencies in their cases.

Pakistan is not a member of the convention on cybercrime which is also known as the Budapest Convention [47]. The primary focus of this convention was to develop cybercrime analysis capabilities in its member's states and only coordinate in case of an incident.

4.1.1.2 Indian Cyber Crime Laws

The Information Technology Act first introduced in the country in 2000, where the House of Indian Parliament passed the bill, and it contained cyber laws as well [48]. The primary aim of this bill was to set up a legal framework for e-commerce in the country which helps and protect the customer and seller from cyber crimes related incidents. This Bill did try to change the outdated laws and laid out in detail how to deal with cybercrime, but it still lacks some areas of cybercrimes such as privacy, identity theft and so on. These areas eventually were amended in the Act of 2008 [48].

The Information Technology (Amendment) Act 2008 is the only regulation that administers cybercrime in India [49]. This Act was used to promote e-commerce, IT industries and help reduce the cyber crimes. To do that it is mentioned that the owner of the specific IP address will be held responsible any misuse done through it.

There are many changes made in that legislation with time. The significant changes were identity theft, piracy violations, cyber terrorism, and cheating are punishable under this Act [50]. The penalty can go to jail time for up to three years and impose hefty fines [1]. It also shows that IT Act is not the only one who is covering the Cybercrime. At some point, the India Penal Code (IPC) can be used to prosecute against the cybercrimes. *"For instance, offenses like hacking, data theft, virus attacks, denial of service attacks, illegal tampering with source codes including ransomware attacks could be prosecuted under S.66 r/w S.43 of the IT Act. Cases of forging a credit or debit card or even cloning a mobile SIM with dishonest or fraudulent intent to cause wrongful loss or wrongful gain could be prosecuted under IPC provisions (S.463 to S.471 IPC, as applicable)*" [51]. This Act was criticised because they decreased some of the cybercrime penalties and there were not enough safeguards to protect individuals civil rights [52]. According to various reports, this Act has given the power of monitoring, blocking and doing surveillance on

the internet traffic [53]. This way there are not enough checks and balances to prevent the misuse of information.

Indian home ministry announced in 2018 that they plan to create "Indian Cyber Crime Coordination Centre" (I4C) to deal with the financial frauds and to restrict circulation of pornographic content [54]. This centre will work with the government, and it will monitor the social media and other parts of the cyberspace. Its main aim is to block all those websites which break the law by circulating racially sensitive content. It will maintain a list of suspects and gather all the leads generated during the investigation and then shared with the law enforcement agencies. India has also established a CERT just for the financial sector and is named CERT-FIN. This CERT analyses the financial sector cyber incidents and reports every all the cybersecurity incidents to its national CERT (CERT-IN) [55].

Currently, India is not a member of the Budapest Convention [47], but The India Express news website reported in January 2018 that the home ministry of India has pitched the idea to sign and become a member of this convention [56].

4.1.1.3 United Kingdom Cyber Crime Law

In the United Kingdom, there are many laws which protect the cybercrime in each category. Some of these are "Computer Misuse Act, the Serious Crime Act, the EU Directive 2013/40/EU, Police and Justice Act, the Terrorism Act, Human Rights Act, Digital Economy Act, Extradition Act, Interception of Communications Act, Regulation of Investigatory Powers Act, Lawful Business Practice Regulation and more" [57]. Most of these laws have been introduced long time ago and amended with time.

The Computer Misuse Act 1990, first introduced with three significant offences in mind. These were "Unauthorized access to computer material, Unauthorized access with intent to commit or facilitate the commission of further offenses and Unauthorized acts with intent to impair, or with recklessness as to impairing, the operation of the computer, etc" [57]. This Act was further amended twice. First, amended by the Police and Justice Act in 2006 and then by Serious Crime Act in 2015 [57]. The significant changes were that

any unauthorised act which is creating or causing any severe damage and obtaining, building or supplying any articles for the use in the offence under section 1 and 3 [57].

The United Kingdom has a list of laws which relates to one kind of action such as hacking. If there is a case registered regarding malicious computer hacking, then there are many laws [57] which will be related to it. Such as "Terrorism Act 2000", "Human Rights Act 1998", "Serious Crime Act 2015", "Crime & Courts Act 2013", "Computer Misuse Act 1990" and many more. These Acts shows how the United Kingdom has incorporated cybercrime in different types of laws with various aspects.
The UK has established a "National Fraud & Cyber Crime Reporting Center" in 2009 which is name Action Fraud [58]. All the cyber crimes and frauds in the country are reported to this centre. This centre also deals with the financial or corporate related frauds.

The United Kingdom has signed the Convention on Cybercrime which is also known as the Budapest Convention with 56 other countries [47]. Being a member of this convention is an excellent step for the country to fight the cybercrime together.

4.1.1.4 Comparison

The public, in general, is still not fully aware of the actual use of technology. The lack of awareness brings in a gap which is exploited by the cybercriminals. The developing countries such as Pakistan and India are struggling to develop and implement proper cybercrime legislation where the laws are strong, and they cover each aspect of the cyber crimes.

In comparison to India and the UK's cybercrime bills, the Prevention of Electronic Crimes Bill in Pakistan gives stricter penalties for the similar crimes committed, and it also defines some crimes which not considered as unlawful in these other countries. With this Bill, the Pakistani authorities have full control to restrict and eliminate any online material without having a court order. It restricts freedom of speech, right to privacy and access to information. We have seen in many cases that the Pakistani government is corrupted [59] and the official authorities are misusing the law for their means [60].

India and Pakistan both are huge countries with an enormous population and the government Identity Card systems are still not strong enough. A large part of the population does not even register for the Identity Card which means they are not registered in the government systems and do not have a bank account [61]. These people are usually from the small towns and rural areas, who never needed to register for an Identity Card. This way it is very tough to track down these individuals if they are a suspect in a crime. There is also a huge problem for these countries to arrest a foreign national. The statistics by National Crimes Records Bureau (NCRB) in India shows that in 2015 while 9,960 arrests were of Indian Nationals, only eight arrests were made of foreign nationals [62]. There is no agreement of detention between Pakistan and India. There was a case in 2017 when the Indian cybercrime division traced the hacker who hacked 60 women's Facebook accounts in Pakistan [63]. Nothing could happen because India does not have any treaty on which they can make arrests in Pakistan. All of the above factors explains why the conviction rate is low in India and Pakistan.

In the UK recent general crime conviction rate is 95% [64] which also includes cybercrime. It still has a high number of cybercrime rate, and it is working continually on its legal system to make it more secure. According to Independent News in the UK, someone falls victim to a cyber attack or fraud every four seconds [65].

Pakistan does have a National Response Center for Cyber Crime (NR3C), but there is still no law or authority to deal with the financial frauds in the cyberspace. India has announced their plans to establish "Indian Cyber Crime Coordination Centre" (I4C) which will deal with online financial frauds as well. The United Kingdom has a well-established centre named Action Fraud, which also deals with the online financial frauds.

The United Kingdom is a part of the Budapest Convention on cybercrime with other countries, but Pakistan and India are not a member of this convention. India does have plans to become a member, but Pakistan is now shown any interest so far.

In Pakistan, the national level cybersecurity policy and its proper implementation are still incomplete. There is no National Cyber Security Policy yet, and the prevention of electronic crime bills is present, but it does not seem to be working effectively as the reported crime rate is still increasing in the last few years.

Sometimes even if the country is aware of the attack, due to internet anonymity and other factors, it is still challenging to enforce the law against the attacker. It could be one person, an organisation or even a country behind the cyber attacks. An excellent example of this was last year in Ukraine where multiple large companies, professional services firms, banking sector, government organisations, ATM's and supermarkets were affected as the cyber attack took down the power grid of the country [66]. The malware used in the attack was named "Crash Override". The motive of the attack was not to get ransom but to cause disruption. The main point here is that nobody knows who was behind this attack. There are some speculations but there is no hard proof, and this is a massive example of how sophisticated cyber warfare is and how it has changed the traditional dynamics of war between states [66]. There could be one nation, one organisation or multiple agencies behind this attack but it is tough to prove it. If it cannot be proven, the injured country cannot retaliate back.

4.1.2 Data Protection Laws

Data protection legislation deals with the security measures for the transmission and sharing of the data. It defines how the personal information can be used by the businesses, corporations and the government [67]. Everyone who is in charge of dealing with the data has to follow these rules stated in the law in each country. Figure 4 shows the primary points of the data protection laws in each country, and then each country's data protection laws will be discussed in detail followed by a comparison with Pakistan.

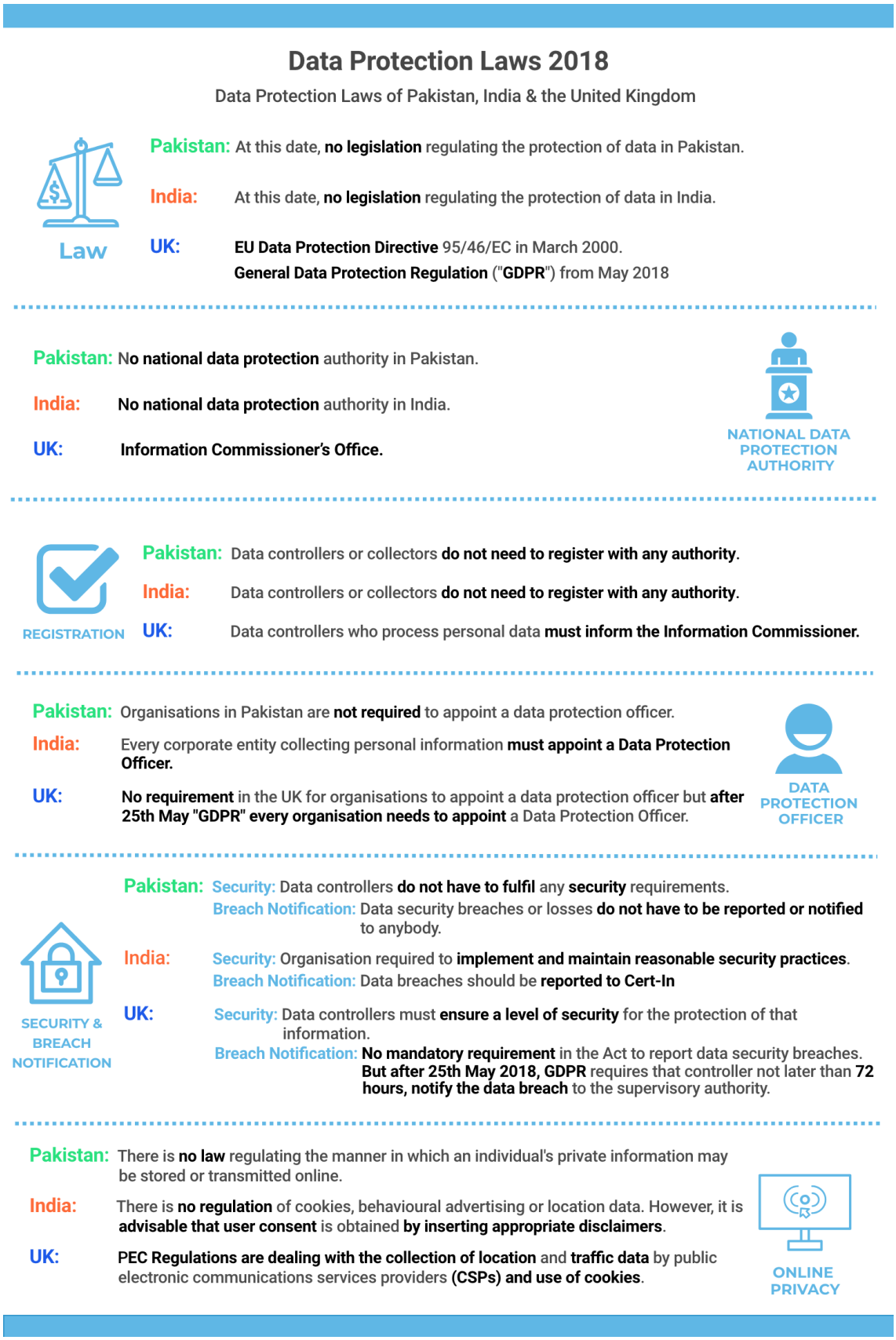

Figure 4 Adapted from [68]

4.1.2.1 Pakistan's Data Protection Laws

In Pakistan, at the moment there is no proper legislation on protection of data [69] and also no data protection authority. The Constitution of Pakistan [70] does focus on the right to privacy and says that it is the fundamental right of every individual. This right to privacy takes priority over any other law. Given that there are still many exceptions in Pakistan's constitution regarding the importance of fundamental rights. Such as the article 8 of Fundamental Rights of the Constitution does not apply to "*any law relating to members of the Armed Forces, or of the police or of such other forces as are charged with the maintenance of public order, for the purpose of ensuring the proper discharge of their duties or the maintenance of discipline among them*" [70].

As there are no data protection laws in Pakistan, the protection and privacy of the information are managed by the following parts of other legislation.

1. Even though the Data Protection is not regulated by the "Electronic Transactions Ordinance 2002" [25], but it states in its Section 36 that it is a punishable offence to access any unauthorised information. In the same ordinance, it was stated that government would establish an entity which will verify electronic documents and also should make regulations for the privacy of its users. There has not been any entity established by the government for this purpose yet.
2. Freedom of Information Ordinance 2002 [71] states under Article 17 that any disclosure of information is exempt if that would lead to invasion of privacy of a person.
3. The "Prevention of Electronic Crimes Act 2016" [40] has some parts related to data privacy and which are used to give private individuals data access to government departments and law enforcement agencies. It is also stated that regular citizens of the country cannot access the confidential government information as it would be considered as a criminal offence and which is punishable by law. The government law enforcement officers also cannot share this confidential information with anyone as stated in this Act and if they do it is also punishable by law. However, this Act states that government has full control to share its intelligence information with any foreign agency which also contains the private data of those individuals.

4. The “National Database and Registration Authority Ordinance” 2000 [72] is in charge of establishing NADRA which is the countries most significant citizen’s identity and biometric database. This ordinance states that NADRA is responsible for ensuring the protection of citizen’s data and make secure.

4.1.2.2 India’s Data Protection Laws

India does have a direct data protection legislation or agency. The Constitution of India does assure the right to privacy [73].

As there are no data protection laws in India, the protection and privacy of information are managed by the following parts of other legislation.

1. The Information Technology Act and Rules in 2011 [74] provides reliable legal protection for any individual personal information. It is stated that the corporations should provide privacy policy to each and require written consent before using or publishing their information. If for any lawful purpose the personal information needs to collect, then this Act states that individual should be informed with proper details such as the purpose of this data collection and name of the agency or department which requires it. Every citizen should have an option to opt-out or opt-of the services before collection of the information according to this Act. It also states that these agencies should only keep this information until completion of the required task.
2. The “Consumer Protection Act 2015” [75] emphasise that the misuse of personal data by corporations and other commercial agencies can be unlawful.

A report was presented by the group of experts on privacy [76] in 2012, on the request of the Planning omission of the government of India. This report contained some recommendations on the creation of the data protection laws. This report suggested that the law should contain the Principle of Choice and Consent, Notice, Collection and Purpose limitation, Access and Correction, Security, Accountability, Disclosure of Information and Openness.

India has also been creating many drafts on Right to Privacy in 2010 [77], 2011 [78] and 2014, which is still in consideration. On this draft on 2014 [79] which was leaked, it was stated to establish the Data Protection Authority within the country.

The government created a committee [80] in June 2017 to discuss the data protection framework of India and suggest a possible draft of the Data Protection Act. After few months in November, the committee presents a detailed white paper [81] on data protection, and the aim was to get feedback from the public on how to improve the data privacy in the country. So far there is no Data Protection law passed, but it seems like India is much closer now to passing this law.

4.1.2.3 The United Kingdom's Data Protection Laws

The United Kingdom is part of European Union, and as a member state, it has to follow the rules and regulations directed by EU. Therefore, the country has implemented the "EU Data Protection Directive 95/46/EC" [82] in March 2000 through its own Data Protection Act 1998 [83]. This directive which is based on the recommendations of the OECD is founded on seven principles. Their principles are that 1) A notification should be given to the individual whose data is being collected. 2) Data should only be used for the purpose which is appropriately stated. 3) Collected data should be kept secure. 4) Personal data stored can be amended by the subject. 5) If the data collector breaches these seven principles, they can be held accountable. 6) Data collecting party information should be passed along to the subject. 7) Data cannot be shared without consent of the subject with any other agency.

In April 2016 the EU adopted the General Data Protection Regulation (GDPR) [84] which will come into effect from 25th May 2018. This new regulation gives more power to the individuals and shows how their data will is managed. Now they have more control over their data. They gave companies and governments almost two years to make changes in their departments for GDPR as this changes how they can control user's data from now on. Any time a website or form needs to process individual's personal information, it will have to take a consent first, and without this consent, the marketing people cannot contact that information for any promotions or business development. GDPR states [84] that every public authority needs to appoint a Data protection officer who will be the point of

contact at the time of any security breach. GDPR also states that once the data protection officer is aware of the breach, it is his responsibility to inform the appropriate supervisory authority within 72 hours. According to GDPR, every company which is dealing with the customer's data has to have appropriate security measures in place to secure that data.

In Sep 2017, the UK government presented a new data protection bill to implement most parts of the GDPR in UK's Law [85]. There were some exceptions to providing some extra protection to scientific researchers, journalists and some other agencies which deal with the personal information of individuals. This bill is still yet to be approved by House of Lords and House of Commons before this bill can become an Act and replace the previous Act of 1998.

The UK voted for withdrawal from the EU in a referendum on 23rd June 2016 [86] and is called Brexit. This withdrawal means that it does not have to be part of any law created by EU once the withdrawal is complete. Then the UK government will decide if they still want to EU laws such a GDPR on the privacy or create its own.

4.1.2.4 Comparison

India and Pakistan do not have a separate data protection law. India has the more comprehensive law on the privacy policy in its IT act and rule of 2011 than Pakistan. India has created a draft which was presented by a committee, and even the leaked "Right to Privacy Act" draft stated that government has a plan to establish the Data Protection Authority, but Pakistan does not even have a suitable draft for the Data Protection Legislation.

The United Kingdom has a new Data Protection Act in the process which will bring the changes of GDPR in the country. After GDPR is in place, it means that the individual in the UK has far more rights to privacy and data protection then India and Pakistan. After the GDPR is in effect by 25th May 2018, any person in the UK, whether a citizen or a tourist can request the company or authority to remove its personal information from their system, and they have to comply with this request within 30 days. This show level of freedom an individual has while living in the UK compared with India and Pakistan.

In Pakistan, the "Prevention of Electronic Crimes Act 2016" give much more freedom to the government authorities to share any individual's personal information with any foreign government, but in India or the UK, the government cannot do this with the consent of that individual.

4.2 National Cyber Security Strategy

Protection of digital information is a very complicated issue. It is present in some different places, and multiple numbers of checks are required [3]. These kinds of checks usually are handled by the government which is managed by the ministries and its departments.

According to ENISA, the Cyber Security Strategy on a national level is a set of actions which are planned to enhance the security of the countries infrastructures and services [87]. These strategies are needed to be flexible enough to meet the new threats globally. ENISA also states that these strategies built on cooperation. To improving this cooperation between the stakeholders, it is essential to create partnerships between the private-public sector and sharing information with each other.

Any cyber attack could be a threat to National Security of a country, which includes Critical Information Infrastructures (CII), Government networks, Business systems. With the advancement in the technology and communication, new actors have joined the game and now internet, media and information are the new tools to be used in warfare side by side with the traditional ones. To deal with these cyber threats on a national level every country requires a National Cyber Security Strategy.

4.2.1 Pakistan Cyber Security Strategy

According to this report and by reading the news articles the government of Pakistan is more focused on the military prospects of cybersecurity rather than the cybercrime. Cyber Security strategy should have a much broader approach, and intelligence agencies should not be involved in the creation process.

Pakistan's national security used to be only focused on the Kinetic threats until now the policymakers are starting to think about the non-kinetic issues as well. There are two

significant actions taken by the government towards the creation of a cybersecurity strategy. The first one is the establishment of the National Response Center for Cyber Crime (NR3C) in the country and the second main one is the role of the "Pakistan's Senate Defense Committee" [3].

4.2.1.1 National Cyber Crime center established

Pakistan's first National Response Centre for Cyber Crimes (NR3C) established in 2007, and it was a department of the Federal Investigation Agency (FIA) [46]. The reasons why this centre established was that the public and private sector organisations were starting to depend more on the internet and there was a need for such department to investigate and resolve all computer-related crimes, at the same time gather intelligence to resolve these cases [3]. Another reason was that the terrorists were starting to use the internet to commit cyber-related attacks and India was progressing rapidly to develop its cyber army.

4.2.1.2 The Senate Defense Committee's role in developing the Cyber Security Strategy

According to reports submitted by Edward Snowden, the Ex CIA contractor in the United States, Pakistan was being spied through the internet by the National Security Agency (NSA) of United States. Pakistan was the second biggest target of the U.S according to Snowden [88]. They targeted the VIP Division of the National Telecommunication Corporation (NTC), which was the main communication channel which was used by military and civilian authorities. The NSA used a tool called SECONDDATE to make direct attacks on Pakistan's FOXACID server and then infecting the target computers and obtaining information [88]. Its believed that they intercepted more than 13.5 billion parts of emails, phone calls, and fax data [89].

The chairman of the Senate committee Senator Mushahid Hussain Syed met with the delegation from Pakistan Information Security Association (PISA) in Parliament House to debate on the Cyber Security Strategy [90]. In this crucial meeting, they presented a budget proposal which mentioned that separate funds should be allocated in the National Budget for Cyber Security Strategy as Pakistan was a part of this cyber attack.

The committee announced a seven-point action plan which was as follow [91]. 1) Draft of legislation which is currently in progress will secure, preserve and promote cybersecurity in Pakistan. They will present this bill in the Parliament. 2) Cyber Security threat should be taken seriously by the government and be considered same way as a terrorist threat. 3) National CERT should be established and named as PKCERT. 4) A new task force will be formed with affiliation with different ministries, security organisations and private security experts, whose primary focus would be to protect Pakistan from any Cyber threats and help create Cyber Security Strategy. 5) Establishing an "Inter-Services Cyber Command Center" to manage cyber defence and cybersecurity for Pakistan Army. 6) Pakistan should discuss cybersecurity within the framework or SAARC and its eight members including India, so these countries do not get involved in cyber warfare with each other. 7) PISA will conduct a cybersecurity workshop to educate the policymakers and spread awareness on this issue to the public.

Everyone accepted these proposals made by the Senator, and the meeting concluded with the outcome that a private Bill would be presented in the Senate & National Assembly on 14th Aug 2013 and PISA will be in charge to present the draft for the Cyber Security Policy Strategy [92]. They also concluded that economy, defence, and citizens would work together regarding the Cyber Security and the National Response of Computer Crimes Center and PISA will work together on the cybersecurity policy report. They all agreed that various departments in the Government and other private organisations require highly professional IT experts. Also, they agreed that the government should take an active part in making policies according to the international standards for protecting its cyberspace.

Given these proposals were sent to the National Assembly, there has been no progress so far regarding the Cyber Security Strategy on the National Level [93]. There have been several meetings, roundtable conferences on this issue which were conducted by IT professionals, government officials and researchers recently [93] but the country is still unable to produce a decent Cyber Security Strategy.

Pakistan has recently joined Information Security code of conduct treaty at Shanghai Cooperation Organization (SCO) [94]. The primary purpose of SCO is to identify the

responsibilities and tasks of the members and to develop cooperation for tackling the common challenges and threats in the information space [95].

4.2.2 India's Cyber Security Strategy

If we see India's economy, it is growing day by day. India is continuously working to improve its cyber strategy and protect its critical government infrastructure. The first step towards this was to establish the National Informatics Center (NIC) [96]. NIC's primary task was to provide information technology solutions to both private and government sector. The Indian government had to change its policies in 1998 when the Bhaba Atomic Research facility was attacked by some unknown hackers [97]. This attack on the Atomic Research facility was a wakeup call for the government, and they knew they had to take cybersecurity seriously. At this time Indian military was also very much dependent on the internet, and their space program was making significant improvements, they could not afford to lose this information to an unknown party [3].

In 1998 the government introduced the "New Internet Policy", to regulate the different internet service providers (ISPs) in the country [98]. If we see the Indian Railways online sales, there was a 132% increase from 2010 to 2013 only [99]. The Indian government is still trying to figure out the meaning and scope of securing the cyberspace. The government still need to work with private companies to promote cybersecurity and teaching best practices [3].

4.2.2.1 India's Cyber Security Strategy in making

India started regulating its IT sector in 1998 [98], it has made many further improvements until now. It is trying to catch up with other nations by introducing rigid cybersecurity policies, and the country is also meeting up with the cyber experts all around the world to acquire guidance and to learn how to improve their current policies [3].

As the economy is adopting the new technologies very quickly, they need to have a proper structure to safeguard them in case of an attack. The security experts are working with the government policymakers to create a strategy on how to deal with cyber threats. Later

in July 2010, they created a draft, and they also decided to hire IT experts and developers [3]. These individuals were given full authority to be in attack mode and start pre-emptive strikes on any computer network they can find. The reports submitted by these individuals and other research which conducted for four years helped the government to introduce the "National Cyber Security" Policy on 2nd July 2013 [100].

This National Cyber Security policy document showed the importance of Information Technology for India. It gave plans on how to protect the critical infrastructure of the country [101]. The plans include creating a system for a secure channel of information flow, creating crisis management plans, creating standards and providing proactive security assessment. The plan also stated to create a 24 hours open "National Critical Information Infrastructure Protection Centre" (NCIIPC) to provide CIIP [101]. The policy separated into different parts. It displayed how unsafe are the economic IT practices and how it can be improved [100]. This policy's primary objective is to protect the Indian cyberspace from both inside and outside state actors, resolve the cyber threats and eliminate the vulnerabilities in the systems [100]. The policy provided guidelines on how to respond in case of an incident as well as it helps to reduce the damage caused by an attack with the blend of institutions, government officials, technology, processes and collaboration [100].

India has to build protected cyberspace and improve its controlling body to accomplish the objectives of this policy. That is the reason India introduced "*National Critical Information Infrastructure Protection Center*" (NCI-IPS) [102]. Then the government created the National CERT which was called CERT-In. Followed by another two certs which were CERT-FIN for Finance Sector and NIC-CERT for Government Infrastructure [103].

The government is also working on a system to deal with cyber threats prevention, response and recovery activities. They are trying to build a stronger relationship between private and public institutions to deal with cyber threats together and quickly. Finally, they also made a plan to hire five hundred thousand IT experts in different parts of the institutions both in public and price sector [3].

India has signed MoU's between many countries such as Japan, Malaysia, and Singapore, South Korea, Canada, Australia and Uzbekistan. These MoU's will help these countries share information with each other and protect their cyberspace. India has also joined with Pakistan the Shanghai Cooperation Organisation (SCO) [94] treaty to ensure international information security.

The government decided to create a cyber division in their military departments in Aug 2010 [104]. The sole purpose of this department was to protect the country from any cyber attacks from all over the world. This military cyber division was protecting the critical infrastructure of the country as well as also planning to spy on its neighbouring countries for critical information.

This National Cyber Security policy was a significant development for the country and in South Asia. It also declares that a new kind of war which is cyber warfare entering this part of the world. India also showed in an army exercise named "Divine Matrix" in 2009 which revealed how serious is this country regarding the cybersecurity [105].

4.2.3 United Kingdom's Cyber Security Strategy

Cyber Security is considered to be a "Tier 1" level of threat to the national security of the country [106]. The United Kingdom has been busy dealing with cyber attacks since 2010. The country was dealing with the cyber attacked based on its "National Security Strategy". Later in November 2011, the National Cyber Security Strategy was implemented by the government. It was named the "National Cyber Security Programme" (NCSP) and is controlled by the Information Assurance and Cyber Security office in the Cabinet Office [107]. These are the four primary goals of this strategy [107]. The first goal is that it will help make the countries cyberspace more open, steady and alive. The public can use it securely, and it will support all kinds of open societies. The second goal is that the United Kingdom will protect its cyberspace from all kinds of cybercrimes and to make its cyberspace one of the most secure places for any business. The third goal is that the country will be more resistant to cyber attacks and protect everyone's interest in the cyberspace. The fourth goal is that the country needs skilled IT security experts and up to date knowledge to achieve these security objectives.

These departments and agencies are supporting the countries National Cyber Security Strategy *"Intelligence agencies and Ministry of Defence, The Government Communications Headquarters (GCHQ), The Defence Cyber Operations Group, The Global Operations and Security Control Centre, The Centre for the Protection of National Infrastructure, The Government Office for Science, The Serious Organised Crime Agency (SOCA), The Ministry of Justice, The Home Office, The National Crime Agency (NCA), The Child Exploitation and Online Protection (CEOP), The Metropolitan Police's Police Central E-crime Unit, The National Fraud Intelligence Bureau, UK Computer Emergency Response Team, The Public Services Network (PSN) and The Defence Cyber Protection Partnership (DCPP)"* [107].

In 2012 the UK government introduced the 10-step to cybersecurity. It was an infographic to be used by the companies especially the critical information infrastructures to review and protect themselves in the cyberspace [108]. Their steps included secure configuration, user privileges management, organisation's risk management, Working from home or remotely, Education and awareness of the user, Security of the Networks, Protection from Malware, Monitoring, Incident control and removable storage devices.

In 2013 the government implemented "Military Cyber Reserves" [109] which was also named "Join Cyber Reserves". It was not just meant for the military professionals only, and they targeted regular people, military people who are leaving, and current or former people in the military. These exercises helped a lot to grow the team of Cyber Security experts in the country [110]. In 2014 United Kingdom Government allocated £860 million pounds for the cybersecurity of the country [111].

The United Kingdom also signed cybercrime treaties with 30 countries in a Council of Europe (CoE) convention. These treaties will help these countries to assist and prosecute online crimes [112].

The government of the United Kingdom has already published its second Cyber Security Strategy in 2016, which is a five-year plan until 2021 and allocated 1.9 billion pounds for this purpose only [113]. The primary objective of this new strategy is to defend the country from any cyber attacks, create an industry for cybersecurity and priority given for the security of Critical National Infrastructures. This new strategy assures better

intelligence of the law enforcement agencies to identify and capture cybercriminals. Further investments in cybersecurity research, innovation and education are also mentioned in the new strategy [113].

The government is also working on the awareness and education in cyber security which will be discussed later in this report.

4.2.4 Comparison

Pakistan does not have a working Cyber Security Strategy on a national level. In 2013 PISA was supposed to present a draft of cybersecurity strategy, but nothing presented so far. There have been many meetings, conferences but there is no outcome which shows that Pakistan will soon publish its Cyber Security Strategy. India published its first National Cyber Security Strategy in 2013, and the United Kingdom has already published its second strategy in 2016.

It seems like Pakistan's policymakers are more focused on the cybersecurity from the intelligence perspective. They established a cybercrime unit NR3C but not a National CERT. NR3C had more forensic capabilities rather than incident handing. Pakistan has also not shown any interest in signing the Budapest Convention on Cybercrime. There is no legislation to protect the financial sector with cyber-related incidents such as fraud. All of these factors show the mindset of the policymakers, and they want to focus on intelligence intel gathering and to see the cybersecurity from one side only.

While comparing with India, Pakistan has not conducted vulnerability assessment on its CII. Pakistan needs to do more research and conduct different assessments in the system like India and then only come up with a strategy to protect their CII's and other infrastructure from the cyber attacks.

India has been conducting Cyber Army Exercises such as "Divine Matrix" which helps display the capabilities of their army and as well as show other countries their potential. The United Kingdom in 2013 implemented "Military Cyber Reserves" [109]. These exercises helped to grow the team of Cyber Security experts in the country. Pakistan has not conducted any such activities, or at least they are not known to general public.

The underground cyber hackers of India and Pakistan are trying to deface as much government websites as possible on important national holidays, and this has been going on since quite a while. Even though the impact is meagre, the government should still take notice of this and should not have basic vulnerabilities on their websites as these sites are representing the whole country.

Pakistan is a nuclear power country with almost 200 million people, and it cannot afford any negligence toward cybersecurity just because of its political policies. If these CII such as Nuclear arsenals get in the hands of terrorists, then the impact is huge on the country.

Pakistan did pass a Bill for "Prevention of Electronic Crimes Bill" [40] and established a cybercrime unit NR3C which is the right step towards cybersecurity, but it has a long way to go. The country should focus on the development of National CERT which is not just focused on the intelligence side but should protect the CII and in future a National Cyber Security Strategy. The way things are progressing in the world right now regarding cyber security the time is now to focus on this otherwise it will be too late.

Pakistan's dependence on cyberspace has been proliferating, but most of these users do not understand the security side of the internet. Government is still not working on as many awareness programs compared to the United Kingdom and India [8].

India and Pakistan are a part of information security treaty of Shanghai Cooperation Organisation (SCO), but India has signed more treaties and MoUs then Pakistan. Compared with the United Kingdom, as it is a part of European Union, it has signed treaties like COE and it a part of Budapest convention.

If we compare the cyber expertise between countries then the United Kingdom is on first, then on the second is India and the third one is Pakistan.

4.3 Computer Emergency Response Team (CERT)

A Computer Emergency Response Team is a government based National CERT and is equipped with the highly technical personnel who are responsible for handling computer-

related incidents such as theft, loss of essential data, corruption, cyber attack and so on. Their personnel have technical capabilities to deal with cyber incidents.
According to the ENISA [114], a National CERT is a team that assists the government by handling cybersecurity-related incidents and also assisting in protecting the critical information infrastructure of the country against any cyber-related attacks. It provides the incident management at a countrywide level. Sometimes due to some circumstances, a CERT can help to cooperate with other foreign countries.

This emergency response unit gets involved if an organisation in the country is subject to a cyber attack, then the nationals CERT will provide help and guidance to recover from that attack.

4.3.1 Pakistan's CERT

In Pakistan, there is no National CERT, but there is a National Response Centre for Cyber Crimes (NR3C) department which deals with few features of a National CERT [46]. NR3C deals with issues related to cyber crime-related incidents. It is the government agency which established in 2007, and it is a branch of the Federal Investigation Agency (FIA) [46]. FIA is border control, counter-intelligence, and security agency and it comes directly under Ministry of Interior of Pakistan [115].

The main aim of is to provide the government with the highly technical expertise in Information Systems Security Audits, Digital Forensics, and Penetration Testing NR3C [46]. It directly receives the relevant complaints about cybercrime incidents and also assists the other government based agencies in their cases. According to their website, the NR3C provides the services for Computer Forensics, Mobile Forensics, Technical Training, Video Forensics and Network Forensics [46]. Its capabilities are restricted to forensics issues only, but it does not provide training on how to secure system or deal with incident handling.

The Federal Investigation Authority in Pakistan is already combating the electronic crimes; it has suggested a Phase-III for NR3C which includes hiring new experienced and highly technical people in the ministry [116]. They also suggested to creating new

cybercrime divisions in the police stations which will be equipped with digital forensics laboratories in various cities on Pakistan.

Even though the NR3C has some features of a National CERT, but it is not the National CERT of Pakistan. It is also not a member of the global "Forums of incident Response of Security Teams (FIRST), where every country official CERT is registered)" [117]. Due to the lack of a National CERT in the country, a private company named "PakCERT" started as a group of cybersecurity experts in the year 2000, and they provided some services of a CERT to fill in the gap [118].

The National Cyber Security Council Act 2014 [119] was a draft which was presented to the Senate of Pakistan on 14th April 2014. It explicitly stated that a National CERT should be established under the private and public partnership which will include the sector-specific and different industry CERTs. The Ministry of Information Technology rejected this Bill, and it was said to be impractical. The ministry panel which rejected the bill issued a statement in which they stated that this bill did not address the critical issues related to the cybersecurity such as unauthorised interceptions and personal data protection. It shows how the decision makers think about cybersecurity and even if there were some flaws, instead of making amendments they just rejected it.

The Pakistan Information Security Association (PISA) recently announced that they had launched the (PISA-CERT) [120]. The capabilities of this CERT are not known because there is no information on their website or the internet available. They say that it is Pakistan first public CERT [120]. We also do not know if this CERT is a National CERT or not.

Pakistan has not signed any MoUs with any country, and it has also not signed the cybercrime convention which was also known as "the Budapest Convention" [121]. However, Pakistan is a member of APCERT which is "Asia Pacific Computer Emergency Response Unit" [122]. Pakistan's NR3C and PISA-CERT are also members of OIC-CERT [123], which is a group of Islamic countries joined together to focus on cybersecurity-related issues and share knowledge with each other. OIC stands for Organization of the Islamic Cooperation. There are 19 Islamic countries [123] which are members of the OIC-CERT, in which Pakistan is just a General Member, including

Bangladesh, Iran, and Turkey. The general member means that these countries do not have an authority to represent their countries interest. In OIC-CERT all the other countries are represented by its National CERT's, but Pakistan is represented by its national crime unit NR3C and PISA-CERT.

4.3.2 India's CERT

The National CERT of India which is called Indian Computer Emergency Response Team (CERT-In) was established in 2004 [124]. In the Information Technology Amendment Act 2008, the CERT-In was assigned as the national agency in India to perform these several functions in Cyber Security [124]. The primary functions are to analyse, collect the incidents information and to forecast incidents and alerts for the relevant parties. It prepares emergency procedures on how to handle the situation regarding a cyber attack. Issuing guidelines regarding the cyber incidents and much more.

India then created another CERT for the Financial sector on 24th May 2017, which is called CERT-Fin [55]. This CERT analyses the financial sector cyber incidents explicitly. It understands the patterns and any significant changes, then reports every cybersecurity incident to the CERT-In. It offers policy suggestions to improve the cybersecurity of the financial sector. It also conducts various training workshops, and above all, it has laid down the security checklist which every financial institution in the country has to follow.

By the end of 2017, the Indian policymakers established another CERT and this time for the Government itself. This is the third CERT which is called NIC-CERT, and the NIC stands for National Informatics Centre [103]. This CERT's primary role is to protect the digital services and infrastructure of the government such as India's e-business and e-governance originations. As India has a Biometric National ID, which is called Adhaar Biometric identity system, this CERT will focus on just protecting this kind of information. Even though India created the NIC-CERT which is focusing on the government internal IT infrastructure, in January 2018, there were reports that an online researcher hacked into Aadhaar's Android application, to show how insecure it is [125]. There have been many security issues before, and there were also reports that the Aadhaar's data can be downloaded from the black market for just INR 500 [125]. According to Elliot Alderson in this report which discovered this vulnerability said that

this app was saving the biometric information in the local database and for generating the password it used a random number as the seed which was "12345678" and a static string as "db_password_123". This was not at all a good development practice for an organisation which is protecting the biggest biometric database in the world [125]. It seemed that the Indian government knew that infrastructure of the Aadhar system was not that strong and that is why only one month before this breach they established the NIC-CERT to focus only on these platforms.

The CERT-In has even signed Memorandum of Understanding (MoU) with three of the Asian countries to share information when there is a cyber threat, this way they can tackle the threats far better and help each other at the time of crises. Those three countries are Japan, Malaysia, and Singapore [126]. Later it signed more MoUs with South Korea, Canada, Australia and Uzbekistan. It is also a member of the global "Forums of incident Response of Security Teams (FIRST)" [117].

In 2016 CERT-In signed another MoU with Ministry of Cabinet Office of UK which is represented by CERT-UK [126] and is also another National CERT we will compare in this report. The essential facts which were covered in this MoU were that it was intended to bring these two countries together and work to detect, resolve and prevent any incidents related to cybersecurity. They will exchange information of the security policies and its best practices. It will help both countries in improving relationships and capacity building.

4.3.3 United Kingdom's CERT

The United Kingdom's first National CERT was established in 2013, and it is called CERT-UK [127]. Before this, the CPNI was in charge of providing advice and information on cybersecurity to the Critical Information Infrastructures of the country.

The CERT-UK is the National Computer Emergency Response Team which will focus on the cybersecurity-related incidents [127]. It is located in London with a team of 55 [111] individuals. "*CERT-UK would issue an alert and appropriate guidance in the exceptional event of a critical national cybersecurity incident*" [111]. CERT-UK is a member of the global "Forums of incident Response of Security Teams (FIRST)" [117].

According to the Government's official website, this National CERT will work together with the government, corporations and educational institutions to improve the countries cyber capabilities [127]. The website also states the primary responsibilities of the CERT-UK, which are to manage national cyber-related incidents, providing cybersecurity support to the critical information infrastructure organisations, will be coordinating directly with other foreign countries CERT and will be involved in promoting cybersecurity through awareness and encouraging the educational institutions to offer more courses in this field.

As CERT-UK is involved in sharing information of cyber-related threats, for this reason, it manages the "Cyber Security Information Sharing Partnership" (CiSP) which started in 2013. CISP is sharing Cyber Security threats and guidance related information with industry, government and the lawmakers [128]. CiSP is a free resource which has 5000 individual members and 1750 companies in the UK [128].

Even though the CERT-UK works closely with the critical national infrastructures but it does not have responsibility for it [127]. CERT-UK is responsible for keeping a record of all cyber incidents happening at the national level. However, there is still no effective regulation which makes sure that all the incidents reported to CERT-UK [129].

4.3.4 Comparison

Pakistan's NR3C is not an actual National CERT and is focused on the cyber crime-related incidents; it lacks the essential duties of a National CERT such as incident coordination and response. We do not know about the PISA-CERT if it is a national cert or not because there is basically no information available on the internet. It more seems like a CERT for PISA's purposes only. The rejected "National Cyber Security Council Act 2014" did, in fact, stated that National CERT should be established but it was rejected by the Ministry of IT and no further developments have been made so far for establishing a National CERT. The Pakistani government only considers the cybersecurity related issues seriously which are mostly the "Whistleblowing" related incidents against their political parties [119].

India has advanced and fully functional National CERT as it has been almost 14 years since its establishment. India has also learned with time on how to make its CERT capabilities better and signed many MoU's with other countries to manage these cyber incidents better. Even India has three types of CERTs which are CERT-FIN, CERT-IN and NIC-CERT which are focusing on the National level, Financial sector and Government's digital services. The UK launched its first National CERT in 2014, and since then they have a national approach to cyber incident management. The CERT-UK is much more advanced and funded heavily by the government [130]. CERT-UK is also managing CiSP, which is just sharing critical incidents information between different entities. This show how India and the UK have improved their National CERTs and even further developed it by establishing other departments for one specific task, such as CERT-FIN in India for financial sector only or CiSP in the UK to share real-time critical information. Pakistan, on the other hand, remains behind far behind these countries when it comes to cyber incidents handling capabilities as both have a working National CERT, but it does not.

Pakistan has not signed any MoUs with any country, and it has also not signed the cybercrime convention which was also known as "the Budapest Convention" [121]. India and the UK have signed many MoU's with other countries and even with each other. National CERTs of India and the United Kingdom are both members of "Forums of incident Response of Security Teams" (FIRST), but as Pakistan does not have a National CERT, it is not a part of it.

Pakistan's NR3C and PISA-CERT are members of OIC-CERT and APCERT, which is a good thing as they can share the incidents information with each other and make their network stronger. Though NR3C does not have an incident coordination functions, it is still a part of it and seems like it is not a functional agreement with OIC-CERT.

4.4 Critical Information Infrastructure Protection

Critical Information Infrastructure (CII) has a huge part to play in an economy and society to function properly [131]. If any cyber attacks compromise these infrastructures, then it will have a massive impact on the country.

Critical infrastructure can be the supply of energy, emergency services, financial services, government services, telecommunications, healthcare, drinking water and networks which are essentials [132] for a country to function. These types of critical infrastructures depend highly on the Critical Information Infrastructures.

The antivirus software McAfee presented in their report of CIP in March 2011 that almost two-thirds of CI companies find highly sophisticated malware in their systems which are explicitly designed to compromise their systems [127]. This report shows how important is to protect CII in a country.

Many different countries consider different sectors [133] among there critical infrastructure, but the most common ones remain the same. Usually, the government assessment regarding critical infrastructure is different from everyone else. A good example was seen in US Elections in 2016 when different strategies deployed by Russian organisation to interfere [6] with the elections. Since then the Elections in the United States is classified [134] as critical infrastructure.

The Critical Information Infrastructure (CIIP) analysis is based on the model mentioned in the research [135] of Dan Assaf. These models are of the critical information infrastructure protection (CIIP). Figure 5 shows how a degree of government intervention can change the classification of government control.

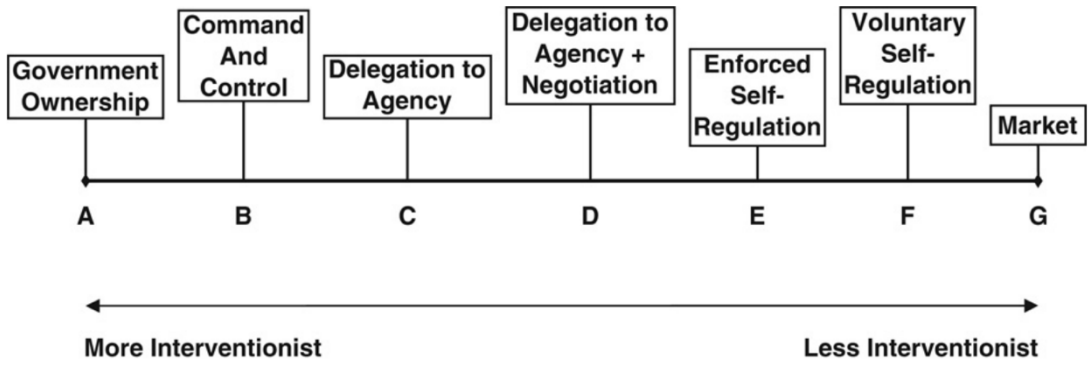

Figure 5 [135]

The CIIP is controlled and wholly owned by the government in the level A (Government Ownership) on Figure 5 and is the most interventionist option. In the first three levels A,

B, and C the government intervention is more, but in the level D, the public institution consults with the private institutions before setting any standards regarding CIIP. More it goes towards the G level (Market), it is partially controlled by the government and by the private sector. At level G, the CIIP's is controlled by the private sector only, and every enterprise has their CIIP policies. There are few limitations in this model as it only measures how much influence does the private or public sector has but it does not show if the country has executed a cybersecurity strategy or not. The government of each country has their own choice of regulatory arrangement s regarding the CIIP's.

4.4.1 Pakistan's CIIP

Pakistan does not have a government department for protecting its Critical Information Infrastructures. There is no defined list explaining which infrastructures are the official critical information infrastructures of the country.

The only thing which is related to this is under the National Cyber Crime Law which was called Prevention of Electronic Crimes Act, 2016 [40]. In this Act under the "Crimes Against Information and Data Systems, and Cyber-Terrorism" section it is mentioned that there are set of penalties if the crime is related to unauthorised access or modification with the data or information system. It also stated that this data or information is connected to the critical infrastructure of the country; then harsher penalties will be applied [136]. It shows us that even though there is no separate department but the country still considers its critical infrastructures as an essential entity and there is definition to protect them.

The Act also focusses on the crime related to cyber-terrorism. It stated that if any crime is connected to the critical infrastructure of the country, then it will be considered as a cyber-terrorism. The punishment can be a fine up to 5 Million Pakistani Rupees or up to 14 years in prison or both [136].

Pakistan is a nuclear state, and due to its significant geographical position, there are constant attempts of cyber attacks on the critical information infrastructure of the country [137]. There is no department such as CIIP, which will have direct communication with the CII's and then regulate the security checks on them.

In 2016 one of the Indian cyber security organisation claimed [138] to have hacked into Pakistan's military infrastructure, which is part of CII. They publically announced that they could destroy the military infrastructure of Pakistan if Indian government gives them a green signal [137].

According to Pakistan's Infrastructure report, almost 40 percent [139] of the CII's are controlled by the private sector which means the majority is under Public sector and the government has more intervention in Figure 5. It shows that Pakistan will fall into Level C which is "Delegation to Agency". On this level, there is a strong influence of the government on the regulation and monitoring of these infrastructures. Even though there is no such department but the government is still keen to protect its CII after finding out that NSA was spying on Pakistan's communication networks both civilian and military in various leaks by Edward Snowden [137].

4.4.2 India's CIIP

India has a proper protection centre for CII, and it is called "National Critical Information Infrastructure Protection Centre" (NCIIPC). It came under the "Information Technology Act" 2008 and was created in 16th Jan 2014 [140]. It was placed under the National Technical Research Organisation (NTRO) to initiate countermeasures and coordinate with other security agencies at the same time [141]. It started with many sectors but now reduced to 5 main areas [142] of the CIIP. These include Transportation, Energy sector, E-governance, Banking and all the financial institutions such as Insurance.

The primary objective of this centre is to identify and protect the national critical information infrastructure of the country. It gives early warnings of a threat and shares information with the specific departments. It is also involved in creating policies, vulnerability assessment, undertaking research, organising training and awareness programs and much more [140].

In Figure 5 India falls under level D "Delegation to Agency plus negotiations" because its CII's are almost the same number in public and private sector. It means that both sectors have an equal say in making and enforcing policies.

In the Information Technology Act India defined its CII as "computer resource, the incapacitation or destruction of which, shall have a debilitating impact on national security, economy, public health or safety" [143]

India believes that its NCIIPC department will involve private and public organisations and work together to secure its infrastructures. This department requires active cooperation between the government and the industry, and it should not be just NCIIPC task to protect the CIIs but it should be a shared collaboration, and all the stakeholders should be involved in this.

4.4.3 The United Kingdom's CIIP

The United Kingdom has 13 national infrastructure sectors, but not all are considered to be critical infrastructure [144]. According to the government, only those sectors are critical, the loss of which will result in severe consequences on social or economic, or even loss of life [144].

The UK's primary department to protect all the computer systems infrastructure is National Infrastructure Security Co-ordination Centre (NISCC) which was merged into departments to create a country's dedicated CIIP. It was named "Centre for the Protection of National Infrastructure" (CPNI) and is formed on 1st February 2007 [145]. It has partnerships with Security Services and CESG [146].

The primary objective [147] of the CPNI is to reduce the vulnerabilities and protect the critical organisations so they will not fall quickly in the hand of a terrorist or be part of espionage. It has substantial agreements with the critical infrastructures which are controlled by the private sector. It created an environment where both parties can trust each other and share information for their benefit. It has direct relations will all kind of professional service organisations and government departments.

The significant part of the UK's CIIs are owned privately [148], which means according to Dan Assaf's method in Figure 5, it falls into the level E "Enforced Self Regulation". Enforced Self Regulation means that government does not have direct control, but it still

plays a part in coordinating with the private sectors to achieve better policies. The private entities first develop the policies and then send it to the public sector for its approval and then it is implemented. The CPNI is actively consulting with the academia and the private sector to work together actively and advice on how to secure its CII [149].

Some reports suggest that the public and the private sector in CI have different priorities regarding cybersecurity because the government wants to invest more into security and restore the services as soon as possible after an incident, but private sector thinks differently [148]. As the government wants the private CI organisations to invest more and follow the proper services restoration guideline in the event of an attack [148] but mostly the private organisations are focused on maximising profits, and they will cut cost where ever they think it is feasible.

4.4.4 Comparison

Pakistan does not have an official description, and a list of critical information infrastructures as the CIIP authority usually creates these and Pakistan has not established it yet. The United Kingdom (CPNI) and India (NCIIPC) both have a separate department which is focused on protecting its critical information infrastructures, but in Pakistan, there is no such department which makes it more difficult to tell how effectively the CII's are secured.

We saw an example of how vulnerable Pakistani critical infrastructure as Indian Cyber Security Company quickly got access to their military infrastructure. If Pakistan does not think clearly about this issue, it could end up losing sensitive information. So far it only has a critical infrastructures definition of cybercrime.

The UK's CPNI is actively consulting with the academia and the private sector to work together actively and advice on how to secure its CII. It shows that the government is not just dictating but is interested in listening from the private sector and then designing the policies to protect these CII's.

Dan Assaf's model shows how to classify a country between its public and private partnership. Government intervention is necessary because government's goal is to

protect the whole country and if one cyber attack on a CII can disrupt the countries daily function, then it will do anything in its power to avoid that. The private sector is more focused on profit-making. If any extra security measure has a high cost of expenditures which reduces profit, then they might try to avoid it. That is why the government should work with the private sectors and then set the guidelines to protect these CII. We can see from the analysis that according to this model in Pakistan, the government has more influence on the CI compared to India which has both same influences in making and implementing security policies. The UK's majority of CIIs are controlled by the private sector which means the government has less influence in making and implementing policies.

4.5 Cyber Security Education and Awareness

Cyber Security is the most critical areas of studies these days. It focuses on dealing with threats analysis, detection and mitigation of the systems which protects from the hackers who use these inter-connected networks to conduct several attacks. To deal with these incidents the government and industry require professional security experts in this field. There are many cybersecurity awareness training programs offered by the government. The cybersecurity awareness programs, certifications and academic programs offered by the institutions or universities in Pakistan will be compared with the United Kingdom and India.

4.5.1 Pakistan's Education & Awareness on Cyber Security

Pakistan has only one university which is offering a post-graduate level program in Cyber Security which was also recently introduced [150]. Otherwise, there was no university in Pakistan offering a fully detailed program in Cyber Security. It only has been offering programs in Information Security in hand full of universities. Information security is a much more general degree, and it only has some fundamental parts of cyber security such as Cryptography, Reverse Engineering, Malware, and Forensics. There are no comprehensive courses offered by Universities in Pakistan which will focus just on Cyber Security. Few universities offer "Cyber Warfare" courses, but this is more related to military [151].

The top 5 universities in Pakistan do not offer any cybersecurity programs in post-graduate or PhD level. There is only one university named National University of Sciences and Technology (NUST) which offers MS and PhD in Information security [152]. This program does look good as it has subjects like computer, network security, and cryptography but this is only available in their Military College of Signals, and the whole focus is at the advance military level. Some lower-ranking universities also offer either some subjects of computer security degree, but a country, with a population of 200 million people, this is still very low. Overall to conclude only one lower ranking university is offering Masters in Cybersecurity, another one is offering a degree in Information Security but which is limited to military students only.

There are only a few professional training institutions in Pakistan which are providing certifications in information security such as CISSP [153]. CISSP stands for "*Certified Information System Security Professional*". Some of the training initiations offer Professional Ethical Hacking Courses [154]. PakCERT, a private security experts team, offers training for corporates customer on Ethical Hacking, Penetration Testing, CISSP, Digital Forensics, "Information Security Management Systems" implementation and Security Risk Management [118]. SKANS School of Accountancy is offering "Certified Information Systems Auditor" (CISA) certification [155].

From the year 2014 to 2017 the NR3C conducted basic cybersecurity awareness training in Pakistan for almost 12,458 individuals which included candidates from all sorts of backgrounds [156]. "Information Security Association Pakistan" (PISA) in Pakistan is also conducting some Cyber Security Awareness seminars. PISA is a non-profit organisation which improves the professional expertise of its members by providing publications, educational forums and other training or seminars.

In Pakistan, there was an initiative taken place "Cyber Secure Pakistan" in end of March 2018, which was a conference to talk about issues in cybersecurity [157]. The primary objective of this conference was to establish a coordination centre, and it aimed to train and educate both public and private sector so they can eventually protect themselves from cyber threats. Also in this conference, the girls and women in Pakistan were introduced to the cyber laws, which explained what their rights are and how they can report cybercrime to the law agencies.

4.5.2 India's Education & Awareness on Cyber Security

Even a developing country such as India is trying to catch pace with these developed countries and has quite many universities which are offering some specialisations and programs in Cyber Security. These programs are available from undergraduate level to PhD. According to India's university programs search website, there are 40 Masters degrees, nine undergraduate degrees and offered in cybersecurity or subjects related to cyber security in India [158]. Masters in Information Security offered in some universities including "Indraprastha Institute of Information Technology" which is one of the good universities who have their institutes in different parts of India [159] There is also one university named Amrita which is offering PhD in Cyber Security Systems and Networks [160].

There are a vast number of certifications offered in India for professional people. These certifications are CompTIA Security+ offered by CompTIA [161], CISM and CISA offered by ISACA [162], CISSP and SSCP offered by ISC [163], Certified Ethical Hacker (CEH) offered by EC-Council [164] and GIAC Security Essentials" GSEC offered by GIAC certifications [165].

India has a separate government department for which is called Information Security Education and Awareness (ISEA) [166]. The government approved to develop ISEA in 2005 and completed in 2014. Now, this is in the phase 2 stage already. ISEA focuses on Cyber Security Training, Awareness and Education and according to its website almost 11831 candidates have been educated, they have conducted awareness campaigns among 62043 individuals and trained almost 4567 candidates so far. These candidates include people from all kinds of backgrounds and cultures. India even has very cybersecurity information and awareness website for all kinds of people which is called "www.infosecawareness.in" which is established by "Ministry of Electronics and Information Technology" [167].

It recently joined Israel to improve its research regarding cybersecurity by working together. According to Israel, India's market on cybersecurity will reach up to 1 Billion US Dollars by 2020. India has also made such agreements with Singapore and Malaysia

for creating awareness regarding cybersecurity and doing research and development together [151].

India also conducts a Cyber Security Summit (SECURE) every year, which started in 2014 and in March 2018 it was its 5th time [168]. This summit is the most significant networking event in India, and here they talk about different issues on cyber security and how to solve them. There is also a cybersecurity conference held every year since 2016 [169]. It is another networking even where private, and public sector can sit together and talk about different issues.

4.5.3 The United Kingdom's Education & Awareness on Cyber Security

In the United Kingdom, the National Cyber Security Center which is a part of GCHQ has a brand named "CyberFirst". It is responsible for supporting the development of the countries new generation of cyber experts. They have courses for 11 to 17 years old, and competitions are held to develop the interest of the students from an early age [170]. According to the NCSC website, there are 25 Masters degrees and multiple certifications offered at various universities in the UK, which are certified by the government and this department. These NCSC certified degrees help the educational institutions to attract hard-working students from all over the world. The employers are benefited by this to hire talented people as well as improve the skills of their existing employees [171]. There are almost 23 PhD opportunities for students to have four years Doctoral Training programs [172]. Some of these programs offered by top universities are such as University of Oxford or University College London.

Apart from the certified programs the government is also offering scholarships to attract those high-quality students which could not afford to study otherwise. One of the prestigious scholarships is "The Arkwright Scholarships" [173].

In the United Kingdom, there are multiple certifications one can do in cybersecurity. There are various training centres present in the UK for these professional certifications, and these certifications are security training for HR, CISA, CRISC, CISM, CompTIA+, SSCP, CISSP and some more [174].

The best of all is the NCSC has developed a "Cyber Discovery" platform which is an interactive and fun learning program designed for the young generation to learn necessary skills and then enter into the cyber security profession [175]. They only target the student from age 10 to 13 years who have access to the internet, and there are no prerequisites required such as knowledge about computer sciences. The program divided into four phases which are CyberStart Assess, Game, Essentials and Elite. Only the top students can enter the final stage which is CyberStart Elite, and it provides direct mentoring, future training and opportunity to participate in competitions [175].
The NCSC also introduced the CyberUK Event, which is held every year since 2017 [176]. These events are *"Government's biggest and most influential IA and Cyber Security event to date"* [176]. The first one was hosted only five months after the NCSC was established. The CyberUK "*include the Government's IA and Cyber Security Flagship event, which for the past decade has been the principal vehicle for engaging with IA and Cyber Security leaders*" [176]. It has various kinds of workshops, Streams to share information, Spotlight talks, engagement for an audience and much more.

For awareness purposes regarding the Cyber Security, the UK government launched Cyber Streetwise and Cyber Essentials Programs [110]. These programs helped the small to medium size businesses and organisations to be fully aware of the cybersecurity. The government also started working with the Internet Service providers (ISP's) to educate the citizens on cybersecurity.

4.5.4 Comparison

Pakistan has not made any effort to build a capable team of Cyber Security professionals, and the result is that there are not enough technical people who actually understand the importance of the cyber threats and deal with them correctly [119].

PISA in Pakistan is also conducting some Cyber Security Awareness seminars. Even though this is a good step forward, but they do not focus on younger generation by giving them fun training and incentives to join this profession. PISA held the first cybersecurity conference in Pakistan in 2018, but in India, there has been cybersecurity summit and conferences happening for many years. The United Kingdom also has CyberUK networking event every year.

In the United Kingdom, there are many workshops and seminars where it is attracting students from the very early stage by offering activities, incentives and scholarships to build their interest and train them at the same time regarding cybersecurity. Even if these students do not want to pursue this as a profession, they will still be able to protect themselves from phishing or other kinds of social engineering attacks. The UK government is aware that if the general population is educated enough, there is less chance of someone making a mistake and accidentally give access to hackers or fall for some money schemes which will later end up giving his or her access to all the sensitive information. In India and Pakistan, their focus is mainly on the professional people, and they do not concentrate on the young generation at all.

India is offering 40 Masters and 1 PhD level programs in Cyber Security, but in Pakistan, only one university is offering a post-graduate level program in Cyber Security which introduced recently. Otherwise, there was no university in Pakistan offering a fully detailed program in Cyber Security. In the UK there are 25 Masters and 23 PhD level programs offered by the universities and which are backed by the National Cyber Security Center. Even though India has many Masters level programs offered in cybersecurity, there is no official body like in the UK which certifies that these programs are authentic. A student will never know the quality of education in India and Pakistan, but in the UK if it is certified by the NCSC, that means this program is authentic.

India and the United Kingdom has a vast number of training institutions which are offering many professional cyber security certifications in their country and compared to Pakistan there are only few training institutions which are offering these certifications, and from their website, they do not look very professional. Pakistan also does not have any separate entity which is responsible for undertaking the Cyber Security training, awareness campaigns and education like ISEA in India.

5 Recommendations

There are three kinds of countries. The first one has published its National Cyber Security Strategy twice already such as the United Kingdom. The second one has published its National Cyber Security Strategy only once such as India, and the third one is which has not yet published anything yet such as Pakistan.

Pakistan does not have a National Cyber Security Policy so far; there is no National CERT established, it does not have a CIIP authority or a Data protection policy. The only thing it has is cybercrime legislation and a cybercrime centre which deals with cybercrime related incidents only. Also, only a few universities are offering education both on a professional and academic level in the country.

Pakistan should establish a National Cyber Security Strategy as soon as possible and then establish the primary institutions and determine the national level role and responsibilities.

Pakistan did pass a Prevention of Electronic Crimes Act (PECA) 2016 and established a cybercrime unit (NR3C) which is the right step towards cybersecurity, but the PECA has had many criticisms both local and international forums. Policy makers in Pakistan should focus on improving the privacy of the citizens by this cybercrime law and also introduce data protection laws. It should consider joining the Budapest Convention and other multilateral or bilateral treaties on cybersecurity as they can share latest's technologies and information for making systems more secure against cyber attacks. The NR3C and PISA-CERT are also performing some parts of a National CERT, but a National CERT should separate from the cybercrime units, and all the objectives and capabilities should be made public. The country should focus on the development of National CERT like in India and the United Kingdom, which not just focused on the intelligence side but should improve its capabilities in incidence handling and response to protect the CII and in future a National Cyber Security Strategy. The way things are progressing in the world right now regarding cyber security the time is now to focus on this otherwise it will be too late.

Pakistan should create a security expert group. This group will conduct a security analysis on the Critical Infrastructures and come up with the definition, potential critical sectors and then identify the common security problems. This report will be a guide for the decision makers to make decisions and regulating the framework. As compared to other countries it should establish a CERT in Finance which will focus on protecting the financial sector from the cyber threats like India has CERT-FIN and the UK has ActionFraud. Later it should focus on the energy sector and other CIIs.

Pakistan's government should focus on the academic level and should work with the institution systems to offer more programs in cybersecurity. The Higher education commission (HEC) should certify the best cybersecurity programs offered in these universities and set up a system that if someone graduate with these certified degrees, they will be given a specific job position in the government. Focusing on younger generation luring them into this profession by giving them incentives and scholarships. The government should also focus on inviting more professional training institutions in the country, which will offer better quality certifications in the country.

Pakistan should have a separate cybersecurity training and awareness entity which focuses on awareness and set up training workshops like India has Information Security Education and Awareness (ISEA) department.

6 Conclusion

Pakistan has not taken cyber security very seriously all these years and that it is because of its political situation in the country and late adoption of technology. There is massive corruption in the government departments. While finding information about these three countries, it was hard to find much relevant information for Pakistan. It shows how serious the country is regarding cybersecurity.

Pakistan has the lowest ranking in Corruption Perceptions Index 2017 as well as in Global Cybersecurity Index 2017 compared with the United Kingdom and India.
India had a 1217% increase in internet users in only ten years from 2006 to 2016. Compared with Pakistan it was only 273%, and the UK had 44% increase. 70% of the population in the UK was already using the internet in 2006, but in India, it was 3% and 6% in Pakistan.

The National Cyber Security Policy and its proper implementation is still incomplete in Pakistan. It also does not have a National CERT which mainly deals with incident handling and response and is not under the intelligence agencies. The Senate defence committee in 2013 announced that they would publish a National Cyber Security strategy and establish a National CERT named PKCERT, but there has been no progress on that so far.

The country is still at the very early stages when it comes to the issues related to cybersecurity when compared with India and the United Kingdom. If the country is facing massive attacks on its critical national infrastructure, there is no authority assigned for the protection of these CIIs.

The definition of personal or sensitive data does not exist in the country because there are no defined data protection laws in Pakistan. The Electronic crime bills are introduced, but it does not seem to be working effectively as the reported crime rate is still going higher in the last few years. Cyberlaw agencies should actively fight the problem with cyber-crime. In Pakistan's Electronic Transactions ordinance 2002, it was stated that the government would establish a data protection authority and legislation for the privacy of

its users, but so far even after 17 years, there has been no data protection authority established or regulation for the data privacy improved.

Cyber warfare is the most critical issue in the world right now. It is a new kind of innovative war. Countries are investing in it heavily to make a steady force for the protection of their cyberspace. India and Pakistan should work on a policy to access, share and protect their information. Every country is still trying to understand the underlying attack and defence strategies of cyberwar. The reasons why this is difficult to understand is because there have not been any significant cyber wars between nations. It is still complicated to trace back where the attack originated and who was behind it. The dynamics of the cyber war are so technical and complex that they cannot be related to the conventional methods of the warfare. Like the cyber attack in Ukraine mentioned before, the government has some speculation on who was behind it, but nobody can say for sure as there is no proof.

All the developed nations are planning for the future and investing in education on cyber security such as the USA has various scholarships programs for all sorts of people and UK for Artwright Scholarships. The reason behind this is to fill those gaps in every sector where these cybersecurity graduates will work and make the infrastructure stronger.

We have also seen from the Aadhar's system data break as an example in India, a simple mistake or carelessness can make huge systems vulnerable. This example is notable because it teaches us that even if India developed a CERT just for this platform, they could not do anything if the developers are not aware of the security risks. Developers are usually focused on making things work. Before any new feature is introduced, it should go through the security check during the quality assurance process and only then it should be released to the public.

Both underdeveloped countries, India and Pakistan are working to improve their cybersecurity policies and compared to the developed nation which is the United Kingdom; they are still far behind. India is still far better than Pakistan and is heading in the right direction. Pakistan should follow India's footsteps in publishing National Cyber Security Strategy and setting up essential institutions.

To conclude, needs to sign related treaties with other countries and implement a nationwide cybersecurity strategy. If Pakistan and India will not coordinate and due to their political situation, it is expected that the new arms race will originate in the cyberspace, that is why it is essential for both countries to leave their differences behind and help each other to fight the cyber threats together.

7 Bibliography

[1] R. Wagh, “Comparative Analysis of Trends of Cyber Crime Laws in USA and India,” 09 Dec 2013. [Online]. Available: http://technical.cloud-journals.com/index.php/IJACSIT/article/view/Tech-160.

[2] ITU Cybersecurity Team, “Global Cybersecurity Index (GCI) 2017,” 01 Dec 2017. [Online]. Available: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Global%20Cybersecurity%20Index%202017%20Report%20version%202.pdf.

[3] M. B. Malik, “Pakistan & India Cyber Secuirty Strategy,” 2 June 2016. [Online]. Available: https://www.academia.edu/7935735/Pakistan_and_India_Cyber_Security_Strategy.

[4] S. Shekhar, “India and Pakistan at war in cyber space ahead of Independence Day,” 04 Nov 2017. [Online]. Available: https://www.businesstoday.in/current/economy-politics/india-and-pakistan-at-war-on-cyber-space-ahead-of-independence-day/story/257753.html. [Accessed 03 Feb 2018].

[5] A. Ansarov, “The Next War Will Be An Information War, And We’re Not Ready For It,” 29 Aug 2017. [Online]. Available: http://www.iflscience.com/technology/next-war-will-be-information-war-and-we-re-not-ready-it/.

[6] D. Clark, “Information warfare': How Russians interfered in 2016 election,” 17 Feb 2018. [Online]. Available: https://www.nbcnews.com/politics/politics-news/information-warfare-how-russians-interfered-2016-election-n848746.

[7] Z. Mohiuddin, “CYBER LAWS IN PAKISTAN,” 24 June 2006. [Online]. Available: http://www.supremecourt.gov.pk/ijc/articles/10/5.pdf.

[8] S. Rasool, “Cyber security threat in Pakistan: causes Challenges and way forward,” 12 Aug 2015. [Online]. Available: http://sociobrains.com/website/w1465/file/repository/21_34_Sadia_Rasool_Cyber_security_threat_in_Pakistan_causes_challenges_and_way_forward.pdf.

[9] GCI 2014, “GLOBAL CYBERSECURITY 2014,” 09 Dec 2014. [Online]. Available: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/WP-GCI-101.pdf.

[10] CPI 2014, “CORRUPTION PERCEPTIONS INDEX 2014,” 02 Jan 2015. [Online]. Available: https://www.transparency.org/cpi2014/results.

[11] CPI 2017, “CORRUPTION PERCEPTIONS INDEX 2017,” 21 Feb 2018. [Online]. Available: https://www.transparency.org/news/feature/corruption_perceptions_index_2017.

[12] Internet Live Stats, “Internet Users Statistics,” 1 July 2016. [Online]. Available: http://www.internetlivestats.com/internet-users/.

[13] Worldometers, “World Population,” 18 04 2018. [Online]. Available: http://www.worldometers.info/world-population/.

[14] OpenSignal, “Global State of Mobile Networks (August 2016),” [Online]. Available: https://opensignal.com/reports/2016/08/global-state-of-the-mobile-network. [Accessed 20 Mar 2018].

[15] H. H. MCVEY, “India: Shifting Landscape,” 15 Nov 2012. [Online]. Available: http://www.kkr.com/global-perspectives/publications/india-shifting-landscape.

[16] R. Kochhar, “A Global Middle Class Is More Promise than Reality,” 13 Aug 2015. [Online]. Available: http://www.pewglobal.org/2015/07/08/a-global-middle-class-is-more-promise-than-reality/.

[17] McKinsey&Company, “https://www.mckinsey.com/~/media/mckinsey/dotcom/client_service/high%20tech/pdfs/online_and_upcoming_the_internets_impact_on_india.ashx,” 01 Dec 2012. [Online]. Available: https://www.mckinsey.com/~/media/mckinsey/dotcom/client_service/high%20tech/pdfs/online_and_upcoming_the_internets_impact_on_india.ashx.

[18] S. Fafinski and N. Minassian, “UK CYBERCRIME REPORT 2009,” 01 Sep 2009. [Online]. Available: https://www.garlik.com/file/cybercrime_report_attachement.

[19] C. Mallapur, “As Internet Use Spreads, Cyber Crimes Up 19 Times Over 10 Years: Report,” 06 June 2016. [Online]. Available: https://www.youthkiawaaz.com/2016/06/cyber-crime-rate-in-india/.

[20] V. Munir, “The Debate on Cybercrimes Law,” [Online]. Available: http://www.technologyreview.pk/the-debate-on-cybercrimes-law/.

[21] A. Sharma and A. A. A. Tauheed, “India's digital war,” 20 Dec 2017. [Online]. Available: https://www.firstpost.com/india/indias-digital-war-surge-in-cyber-crime-rate-highlights-need-for-deeper-scrutiny-of-mediums-social-psychological-threats-4267385.html.

[22] S. FH, “Home Pakistan News 179 cyber crime cases decided, of 894 total registered in four years: FIA 179 Cyber Crime Cases Decided, Of 894 Total Registered In Four Years: FIA,” 19 May 2017. [Online]. Available: https://www.urdupoint.com/en/pakistan/179-cyber-crime-cases-decided-of-894-total-r-140426.html.

[23] Daily Times, “Cyber crimes in Pakistan,” 26 Oct 2014. [Online]. Available: https://dailytimes.com.pk/102728/cyber-crimes-in-pakistan/.

[24] T. Mehmood, “Cyber Laws In Pakistan,” 17 Apr 2008. [Online]. Available: https://www.slideshare.net/mehmood_taha/cyber-laws-in-pakistan.

[25] NCSC, “The 2017 Annual Review,” 03 Oct 2017. [Online]. Available: https://www.ncsc.gov.uk/news/2017-annual-review.

[26] A. Khan, “FIA fails to combat cyber crimes,” 23 Feb 2016. [Online]. Available: https://nation.com.pk/23-Feb-2016/fia-fails-to-combat-cyber-crimes.

[27] M. Eyaa, “Difference between Act and Ordinance,” 08 Jan 2017. [Online]. Available: https://accountantexplains.wordpress.com/2017/01/08/difference-between-act-and-ordinance/.

[28] K. S. Kumar, “DIFFERENCES BETWEEN ORDINANCE, BILL, LAW AND ACT,” 3 June 2017. [Online]. Available: https://www.linkedin.com/pulse/differences-between-ordinance-bill-law-act-k-satish-kumar-llb-cma/.

[29] “Difference between Act and Ordinance,” 10 Jan 2018. [Online]. Available: http://www.differencebetween.info/difference-between-act-and-ordinance.

[30] M. A. M. Swaby, “The Importance of Effective Cyber Crime Legislation,” 12 Dec 2016. [Online]. Available: https://www.oas.org/juridico/PDFs/cyb9_jmc_pres_mp_oea.pdf.

[31] HG.org, “Legal Resources,” 18 Mar 2018. [Online]. Available: https://www.hg.org/computer-crime.html.

[32] INTERPOL, “CyberCrime,” 29 Mar 2018. [Online]. Available: https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime.

[33] LawsOfPakistan, “Electronic Transaction Ordinance 2002,” 27 May 2015. [Online]. Available: http://www.lawsofpakistan.com/electronic-transaction-ordinance-2002-free-pdf-download/.

[34] S. A. Ahsan, “CURRENT SITUATION AND ISSUES OF ILLEGAL AND HARMFUL ACTIVITIES IN THE FIELD OF INFORMATION AND COMMUNICATION TECHNOLOGY IN PAKISTAN,” 01 Nov 2002. [Online]. Available: http://www.unafei.or.jp/english/pdf/RS_No79/No79_11PA_Ahsan.pdf.

[35] T. “Cyber Law And Cyber Crime Ordinance In Pakistan,” 16 Feb 2016. [Online]. Available: https://ilm.com.pk/pakistan/pakistan-information/cyber-law-and-cyber-crime-ordinance-in-pakistan/.

[36] M. A. Munir, “Draft Pakistan Electronic Crimes Act, 2004: The Proposed E-Law in a Judge’s Perspective,” 19 Aug 2005. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1912938.

[37] J. A. Sarwana, “http://www.pakcon.org/post-pakcon/pc-khi-04-jawad-electronic-commerceand-cyber-crime.pdf,” 01 Dec 2004. [Online]. Available: http://www.pakcon.org/post-pakcon/pc-khi-04-jawad-electronic-commerceand-cyber-crime.pdf.

[38] “Pakistan Law,” Government Of Pakistan, 31 Dec 2007. [Online]. Available: http://www.pakistanlaw.com/electronic_prevention_ord.pdf.

[39] K. O'connell, “INTERNET LAW - Pakistan's Prevention of Electronic Crimes Ordinance, 2007,” [Online]. Available: http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=2030.

[40] T. Ahmed, “Pakistan: National Assembly Passes New Cybercrime Law,” 21 Sep 2016. [Online]. Available: http://www.loc.gov/law/foreign-news/article/pakistan-national-assembly-passes-new-cybercrime-law/.

[41] Freedom House, “Freedom on the Net 2017,” 01 Jan 2017. [Online]. Available: https://freedomhouse.org/report/freedom-net/2017/pakistan.

[42] R. Khan, “DAWN News,” 11 Aug 2016. [Online]. Available: https://www.dawn.com/news/1276662.

[43] L. Dearden, “Teenage Christian boy arrested for sharing 'blasphemous' Facebook post in Pakistan,” 21 Sep 2016. [Online]. Available: https://www.independent.co.uk/news/world/asia/teenage-boy-christian-arrested-sharing-blasphemous-facebook-post-in-pakistan-nabeel-chohan-kaaba-a7321156.html.

[44] S. Ziamov, “16-Y-O Christian Boy in Pakistan Facing 10 Years in Prison for 'Insulting Islam' by Liking Facebook Post,” 28 Sep 2016. [Online]. Available:

https://www.christianpost.com/news/christian-boy-in-pakistan-facing-10-years-prison-insulting-islam-liking-facebook-post-170171/.

[45] T. Greene, "Facebook comment leads to death sentence for man, death of discourse for mankind," 01 Aug 2017. [Online]. Available: https://thenextweb.com/facebook/2017/06/12/facebook-blasphemy-death-sentence-affects-us-all/.

[46] NR3C, "NATIONAL RESPONSE CENTRE FOR CYBER CRIME," [Online]. Available: http://www.nr3c.gov.pk/.

[47] Council Of Europe, "Convention on Cybercrime," 24 April 2018. [Online]. Available: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures.

[48] "Cyber Laws India," 1 May 2001. [Online]. Available: http://www.cyberlawsindia.net/Information-technology-act-of-india.html.

[49] Government of India, "The Information Technology (Amendment) Act 2008," 01 Dec 2008. [Online]. Available: http://www.eprocurement.gov.in/news/Act2008.pdf. [Accessed 25 Feb 2018].

[50] Republic of India, "INFORMATION TECHNOLOGY ACT, 2000," 09 June 2008. [Online]. Available: http://ijlt.in/wp-content/uploads/2015/09/Information-Technology-Act-as-amended-in-2008.pdf.

[51] N. Nappinai, "Cyber Laws Part II: A guide for victims of cyber crime," 03 Nov 2017. [Online]. Available: https://economictimes.indiatimes.com/tech/internet/do-you-know-how-to-report-a-cyber-crime-heres-a-guide-for-victims/articleshow/61464084.cms.

[52] M. Rouse, "Information Technology Amendment Act 2008 (IT Act 2008)," 01 Jan 2010. [Online]. Available: https://whatis.techtarget.com/definition/Information-Technology-Amendment-Act-2008-IT-Act-2008.

[53] D. Pandya, "IT (Amendment) Act 2008 and its effect on the Indian enterprise," 23 Oct 2009. [Online]. Available: https://www.computerweekly.com/news/1372824/IT-Amendment-Act-2008-and-its-effect-on-the-Indian-enterprise.

[54] PTI, "Government to set up apex cyber crime coordination centre," 28 Jan 2018. [Online]. Available: https://economictimes.indiatimes.com/news/politics-and-nation/government-to-set-up-apex-cyber-crime-coordination-centre/articleshow/62679762.cms.

[55] FSDC Secretariat, "REPORT OF THE WORKING GROUP FOR SETTING UP OF COMPUTER EMERGENCY RESPONSE TEAM IN THE FINANCIAL SECTOR (CERT-Fin)," 24 May 2017. [Online]. Available: https://dea.gov.in/sites/default/files/Press-CERT-Fin%20Report.pdf.

[56] R. Tripathi, "Home Ministry pitches for Budapest Convention on cyber security," 18 Jan 2018. [Online]. Available: http://indianexpress.com/article/india/home-ministry-pitches-for-budapest-convention-on-cyber-security-rajnath-singh-5029314/.

[57] H. Graceful, "UK Cyber Crime Law," 15 June 2016. [Online]. Available: https://www.gracefulsecurity.com/uk-cyber-crime-law/.

[58] Action Fraud, “Action Fraud celebrates fifth birthday,” 30 Oct 2014. [Online]. Available: https://www.actionfraud.police.uk/news/action-fraud-celebrates-fifth-birthday-oct14.

[59] T. Rogan, “Pakistan has a huge corruption problem, from its prime minister on down,” 28 July 2017. [Online]. Available: https://www.washingtonexaminer.com/pakistan-has-a-huge-corruption-problem-from-its-prime-minister-on-down.

[60] I. Rehman, “Misuse of blasphemy law,” 28 Dec 2017. [Online]. Available: https://www.dawn.com/news/1379203.

[61] A. Agha, “Social Capital in Village Organization SadaatHackra, Miani, Bahawalpur, Punjab,” 01 April 2015. [Online]. Available: http://www.rspn.org/wp-content/uploads/2015/05/Case-study-Sadaat-Hackra.pdf.

[62] FirstPost, “With only 250 convictions, India’s cybercrime conviction rate remains abysmally low,” 22 Nov 2016. [Online]. Available: https://www.firstpost.com/tech/news-analysis/with-only-250-convictions-indias-cybercrime-conviction-rate-remains-abysmally-low-3692665.html.

[63] S. Mistry, “COPS TRACE HACKER TO PAK, BUT CANNOT MAKE ANY ARRESTS,” 18 May 2017. [Online]. Available: https://punemirror.indiatimes.com/pune/crime/cops-trace-hacker-to-pak-but-cannot-make-any-arrests/articleshow/58724511.cms.

[64] National Crime Agency, “NCA report and accounts 2016-17,” 20 July 2017. [Online]. Available: http://www.nationalcrimeagency.gov.uk/news/1151-nca-report-and-accounts-2016-17.

[65] N. Morris and P. Peachey, “Millions of cyber crimes recorded last year as banks' secrecy hampers police efforts,” 15 Oct 2015. [Online]. Available: https://www.independent.co.uk/news/uk/crime/millions-of-cyber-crimes-recorded-last-year-as-banks-secrecy-hampers-police-efforts-a6696076.html.

[66] A. GREENBERG, “CRASH OVERRIDE: THE MALWARE THAT TOOK DOWN A POWER GRID,” 06 Dec 2017. [Online]. Available: https://www.wired.com/story/crash-override-malware/.

[67] GOV.UK, “Data protection,” [Online]. Available: https://www.gov.uk/data-protection.

[68] DLA Piper, “DATA PROTECTION LAWS OF THE WORLD,” 29 April 2018. [Online]. Available: https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw.data_protection/functions/handbook.pdf?country=all.

[69] Privacy International, “State of Privacy Pakistan,” 01 Jan 2018. [Online]. Available: https://privacyinternational.org/state-privacy/1008/state-privacy-pakistan.

[70] Constitution of Pakistan, “Part II: Fundamental Rights and Principles of Policy,” [Online]. Available: http://www.pakistani.org/pakistan/constitution/part2.ch1.html.

[71] Government of Pakistan, “Freedom of Information Ordinance 2002,” 26 Oct 2002. [Online]. Available: http://www.cpdi-pakistan.org/wp-content/uploads/2017/04/Freedom-of-Information-Ordinance-2002-.pdf.

[72] Government of Pakistan, “The National Database and Registration Authority Ordinance, 2000,” 01 Mar 2000. [Online]. Available: http://nasirlawsite.com/laws/nadra.htm.

[73] A. Sinha, “CIS Statement on Right to Privacy Judgment,” 28 Aug 2017. [Online]. Available: https://cis-india.org/internet-governance/blog/cis-statement-on-right-to-privacy-judgment.

[74] Department of Information Technology, “MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY,” 11 April 2011. [Online]. Available: http://www.wipo.int/edocs/lexdocs/laws/en/in/in098en.pdf.

[75] Government of India, “THE CONSUMER PROTECTION BILL,” 23 Mar 2015. [Online]. Available: http://www.prsindia.org/uploads/media/Consumer/Consumer%20Protection%20bill,%202015.pdf.

[76] J. A. Shah, “Report of the Group of Experts on Privacy,” 12 Oct 2012. [Online]. Available: http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf.

[77] E. Hickok, “C.I.S Responds to Privacy Approach Paper,” 22 Nov 2010. [Online]. Available: http://cis-india.org/internet-governance/blog/privacy/c.i.s-responds-to-privacy-approach-paper.

[78] P. Iyengar, “The New Right to Privacy Bill 2011 — A Blind Man's View of the Elephunt,” 09 Jun 2011. [Online]. Available: https://cis-india.org/internet-governance/blog/privacy/new-right-to-privacy-bill.

[79] E. Hickok, “Leaked Privacy Bill: 2014 vs. 2011,” 31 Mar 2014. [Online]. Available: https://cis-india.org/internet-governance/blog/leaked-privacy-bill-2014-v-2011.

[80] Government of India, “Press Information Bureau,” 01 Aug 2017. [Online]. Available: http://pib.nic.in/newsite/PrintRelease.aspx?relid=169420.

[81] S. R. Maheshwari, “WHITE PAPER OF THE COMMITTEE OF EXPERTS ON A DATA PROTECTION FRAMEWORK FOR INDIA,” 05 Nov 2017. [Online]. Available: http://www.meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf.

[82] EUR-LEX, “Directive 95/46/EC of the European Parliament,” [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:31995L0046.

[83] Information Commissioner’s Office, “Data Protection Act 1998,” 01 June 1998. [Online]. Available: https://www.legislation.gov.uk/ukpga/1998/29/contents.

[84] P. Galdies and D. , “A Summary of the EU General Data Protection Regulation,” 12 Oct 2017. [Online]. Available: https://www.dataiq.co.uk/blog/summary-eu-general-data-protection-regulation.

[85] M. BURGESS, “What is GDPR? The summary guide to GDPR compliance in the UK,” 19 April 2018. [Online]. Available: http://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018.

[86] A. Hunt and B. Wheeler, “Brexit: All you need to know about the UK leaving the EU,” 12 April 2018. [Online]. Available: http://www.bbc.com/news/uk-politics-32810887.

[87] ENISA, “National Cyber Security Strategies,” [Online]. Available: https://www.enisa.europa.eu/topics/national-cyber-security-strategies.

[88] Dawn.com, “NSA used malware to spy on Pakistani civilian, military leadership: report,” 21 Aug 2016. [Online]. Available: https://www.dawn.com/news/1279013.

[89] M. P. Omtzigt, “Committee on Legal Affairs and Human Rights,” 26 Jan 2015. [Online]. Available: http://website-pace.net/documents/19838/1085720/20150126-MassSurveillance-EN.pdf.

[90] Asianet-Pakistan, “Senate body on Defence holds meeting with PISA on US agencies' interception,” 26 June 2013. [Online]. Available: https://www.thefreelibrary.com/Senate+body+on+Defence+holds+meeting+with+PISA+on+US+agencies%27+...-a0334994751.

[91] Senate of Pakistan, “REPORT OF THE SENATE COMMITTEE ON DEFENCE AND DEFENCE PRODUCTION,” 01 Sep 2013. [Online]. Available: http://www.mushahidhussain.com/publication-detail.php?pageid=publication&rid=MTQ=.

[92] Z. Khalid, “Need for a National Cyber Security Strategy in Pakistan,” 27 May 2015. [Online]. Available: http://insider.pk/opinion/need-for-a-national-cyber-security-strategy-in-pakistan/.

[93] M. Baloch, “Speakers call for national cybersecurity strategy,” 01 Mar 2018. [Online]. Available: https://www.dawn.com/news/1392379.

[94] NATO, “India and Pakistan Are the Newest Members of the Shanghai Cooperation Organisation,” 12 Dec 2017. [Online]. Available: https://ccdcoe.org/india-and-pakistan-are-newest-members-shanghai-cooperation-organisation.html.

[95] United Nations, “General Assembly,” 14 Sep 2011. [Online]. Available: http://www.ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf.

[96] NIC, “National Informatics Centre,” [Online]. Available: https://www.nic.in/.

[97] B. Meeks, “India has scary nuke hack,” 06 June 1998. [Online]. Available: https://www.zdnet.com/article/india-has-scary-nuke-hack/.

[98] P. WOLCOTT and S. GOODMAN, “GLOBAL DIFFUSION OF THE INTERNET I: INDIA: IS THE ELEPHANT LEARNING TO DANCE?,” 01 Jan 2003. [Online]. Available: https://pdfs.semanticscholar.org/145f/0fbd0f1e3f7e7019b131a7a679eb60841fd2.pdf.

[99] Ministry of Railways, “Indian Railways - Indian Railways,” 01 Feb 2015. [Online]. Available: http://www.indianrailways.gov.in/railwayboard/uploads/directorate/finance_budget/Budget_2015-16/White_Paper-_English.pdf.

[100] Ministry of Communication and Information Technology, “NATIONAL CYBER SECURITY POLICY 2013,” 02 July 2013. [Online]. Available: http://www.cea.nic.in/reports/isacpower/ncsp2013.pdf.

[101] Department of Electronics and Information Technology, “National Cyber Security Policy, 2013,” 2013. [Online]. Available: http://nciipc.gov.in/documents/National_Cyber_Security_Policy-2013.pdf.

[102] NCIIPC, “National Critical Information Infrastructure Protection Centre,” 01 Jan 2017. [Online]. Available: http://nciipc.gov.in/documents/NCIIPC_Newsletter_Jan17.pdf.

[103] S. Sharwood, “India sets up second new CERT in a year,” 13 Dec 2017. [Online]. Available:

https://www.theregister.co.uk/2017/12/13/india_creates_nic_cert_for_government_services/.

[104] J. Smith, “India creates a cyber police force,” 25 Aug 2011. [Online]. Available: https://www.itgovernance.co.uk/blog/india-creates-a-cyber-police-force/.

[105] L. Xiaokun, “India's drill report 'surprises' Chinese govt,” 01 April 2009. [Online]. Available: http://www.chinadaily.com.cn/china/2009-04/01/content_7636102.htm.

[106] D. JOSHI, “India UK Legal Regulatory Approaches,” 1 Nov 2016. [Online]. Available: https://cis-india.org/internet-governance/files/india-uk-legal-regulatory-approaches.pdf.

[107] “National Cyber Security Strategies: Global Trends in Cyberspace,” 5 May 2016. [Online]. Available: https://pdfs.semanticscholar.org/3176/5e8abe2766298eca548711493ad897293f6f.pdf.

[108] CESG, “10 Steps: Summary,” 16 Jan 2015. [Online]. Available: https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary#steps-to-cyber-security-at-a-glance.

[109] GOV.UK, “Working for JFC,” [Online]. Available: https://www.gov.uk/government/organisations/joint-forces-command/about/recruitment.

[110] UK Cabinet Office, “Report on Progress and Forward Plans,” 2014 Dec 01. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/386093/The_UK_Cyber_Security_Strategy_Report_on_Progress_and_Forward_Plans_-_De___.pdf.

[111] C. Vallance, “British Broadcasting Corporation,” 31 March 2014. [Online]. Available: http://www.bbc.com/news/technology-26818747.

[112] TheGuardian, “Thirty countries sign cybercrime treaty,” 23 Nov 2001. [Online]. Available: https://www.theguardian.com/technology/2001/nov/23/internetnews.

[113] HM Government, “NATIONAL CYBER SECURITY STRATEGY 2016-2021,” 2016. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

[114] ENISA, “National/governmental CERTs - Baseline Capabilities,” 17 Dec 2010. [Online]. Available: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/baseline-capabilities.

[115] FIA, “FEDERAL INVESTIGATION AGENCY,” [Online]. Available: http://www.fia.gov.pk/en/about.php.

[116] T. Amin, “Business Recorder,” 11 FEB 2018. [Online]. Available: https://fp.brecorder.com/2018/02/20180211342897/.

[117] FIRST, “FIRST Teams,” [Online]. Available: https://first.org/members/teams/.

[118] PakCERT, “Pakistan Computer Emergency Response Team,” 01 Jan 2018. [Online]. Available: http://www.pakcert.org/aboutus.html. [Accessed 4 12 2017].

[119] Pakwired, “Prospect of a Pakistani Computer Emergency Response Team,” 02 Feb 2016. [Online]. Available: https://pakwired.com/prospect-of-a-pakistani-cert/.

[120] PISA, “Pakistan Information Security Association,” [Online]. Available: https://www.pisa.org.pk/. [Accessed 18 April 2018].

[121] “Pakistan Hosizon,” 31 Dec 2015. [Online]. Available: https://pakistanhorizon.wordpress.com/2015/12/31/cyber-security-talk-by-mr-ammar-jaffri-and-barrister-zahid-jamil/.

[122] APCERT, “Asia Pacific CERT,” [Online]. Available: https://www.apcert.org/. [Accessed 02 Mar 2018].

[123] “OIC-CERT Annual Report 2016,” 31 Dec 2016. [Online]. Available: https://www.oic-cert.org/en/download/170301%20OIC-CERT%20Annual%20Report%20v2%20170310.pdf.

[124] CERT-In, “Indian Computer Emergency Response Team,” [Online]. Available: http://www.cert-in.org.in/.

[125] IndiaTimes, 11 Jan 2018. [Online]. Available: https://www.indiatimes.com/technology/news/an-online-researcher-hacked-into-aadhaar-s-official-android-app-to-show-how-poorly-it-s-secured-337425.html.

[126] “General Knowledge Today,” 31 Aug 2016. [Online]. Available: https://currentaffairs.gktoday.in/union-cabinet-apprises-mou-cert-in-cert-uk-08201635430.html.

[127] Cabinet Office, “GOV.UK,” 31 March 2014. [Online]. Available: https://www.gov.uk/government/news/uk-launches-first-national-cert.

[128] Cabinet Office, “The UK Cyber Security Strategy 2011-2016,” 01 April 2016. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf.

[129] C. WARD, “The UK’s Cybersecurity Regulatory Landscape: An Overview,” 13 Dec 2016. [Online]. Available: https://www.hldataprotection.com/2016/12/articles/international-eu-privacy/the-uks-cybersecurity-regulatory-landscape-an-overview/.

[130] K. Flinders, “UK government re-announces £1.9bn cyber security spend,” 01 Nov 2016. [Online]. Available: https://www.computerweekly.com/news/450402098/UK-government-re-announces-19bn-cyber-security-spend.

[131] Enisa, “How critical is a critical information infrastructure?,” 15 Feb 2015. [Online]. Available: https://www.enisa.europa.eu/news/enisa-news/how-critical-is-a-critical-information-infrastructure.

[132] CIPedia, “Critical Infrastructure Sector,” [Online]. Available: https://publicwiki-01.fraunhofer.de/CIPedia/index.php/Critical_Infrastructure_Sector.

[133] E. Luiijf, “Critical Information Infrastructure Protection for governmental policy-makers,” [Online]. Available: https://www.tno.nl/media/8578/gpg_criticalinformationinfrastructureprotection.pdf.

[134] K. WADDELL, “Why Elections Are Now Classified as 'Critical Infrastructure',” 13 Jan 2017. [Online]. Available:

https://www.theatlantic.com/technology/archive/2017/01/why-the-government-classified-elections-as-critical-infrastructure/513122/.

[135] D. Assaf, “Models of critical information infrastructure protection,” [Online]. Available: https://pdfs.semanticscholar.org/8e6d/11b8607d4bc93b0ca27d2c487f45da73cd09.pdf.

[136] National Assembly of Pakistan, “Prevention of Electronic Crimes Act, 2016,” 11 Aug 2016. [Online]. Available: http://www.na.gov.pk/uploads/documents/1470910659_707.pdf.

[137] R. Baloch, “How Pakistan's Critical Infrastructure Was Hacked? - Technical Analysis,” 01 Aug 2017. [Online]. Available: https://www.rafaybaloch.com/2017/07/how-pakistans-critical-infrastructure-was-hacked.html.

[138] TheHindu, “Pakistan’s infrastructure systems vulnerable: Cyber security expert,” 01 Nov 2016. [Online]. Available: http://www.thehindu.com/news/cities/chennai/Pakistan%E2%80%99s-infrastructure-systems-vulnerable-Cyber-security-expert/article15419881.ece.

[139] STATE BANK OF PAKISTAN, “THE PAKISTAN INFRASTRUCTURE REPORT,” 01 Dec 2010. [Online]. Available: http://www.sbp.org.pk/departments/ihfd/InfrastructureTaskForceReport.pdf.

[140] NCIIPC, “National Critical Information Infrastructure Protection Centre (NCIIPC),” 24 Feb 2018. [Online]. Available: http://nciipc.gov.in/.

[141] TheHindu, “The deadly new age war,” 03 April 2016. [Online]. Available: http://www.thehindu.com/opinion/op-ed/the-deadly-new-age-war/article7342982.ece.

[142] S. Datta, “The NCIIPC & Its Evolving Framework,” 26 Oct 2016. [Online]. Available: Power & Energy Banking, Financial Institutions & Insurance Information and Communication Technology Transportation E-governance and Strategic Public Enterprises.

[143] J. Diamond, “Guidelines for the Protection of National Critical Information Infrastructure: How Much Regulation?,” 31 July 2013. [Online]. Available: https://cis-india.org/internet-governance/blog/guidelines-for-protection-of-national-critical-information-infrastructure.

[144] CPNI, “Critical National Infrastructure,” [Online]. Available: https://www.cpni.gov.uk/critical-national-infrastructure-0.

[145] HSDL, “Homeland Secuirty Digital Library,” 26 Mar 2018. [Online]. Available: https://www.hsdl.org/?abstract&did=437453.

[146] Department of Politics and International Studies, “Centre for the Protection of National Infrastructure (CPNI),” [Online]. Available: https://warwick.ac.uk/fac/soc/pais/people/aldrich/vigilant/lectures/gchq/cpni/.

[147] UK Cabinet Office, “The UK Cyber Security Strategy,” 01 Nov 2011. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf.

[148] The Parliamentary Office of Science and Technology, “Cyber Security of UK Infrastructure,” 01 May 2017. [Online]. Available: http://researchbriefings.files.parliament.uk/documents/POST-PN-0554/POST-PN-0554.pdf.

[149] CPNI, “Who We Work With,” [Online]. Available: https://www.cpni.gov.uk/who-we-work.

[150] “COMSATS Institute of Information Technology, Abbottabad,” 1 March 2018. [Online]. Available: http://www.ciit-atd.edu.pk/Secure/academicprograms/Program.aspx?Program=105.

[151] Pakwired - WebDesk, “EDUCATIONCyber Security Education In Pakistan,” 27 Jan 2016. [Online]. Available: https://pakwired.com/cyber-security-education-in-pakistan-an-overview/.

[152] NUST, “NUST - MILITARY COLLEGE OF SIGNALS (MCS),” 1 Mar 2018. [Online]. Available: http://www.nust.edu.pk/INSTITUTIONS/Colleges/MCS/ap/pg/ms-phd-is/Pages/Course-Curriculum.aspx.

[153] “3D Educators,” [Online]. Available: http://www.3deducators.com/IT-Training/ITAudit-Security/CertifiedInformationSystemSecurityProfessional-CISSP.asp. [Accessed 20 Dec 2017].

[154] PNY, “PNY Trainings,” [Online]. Available: http://www.pnytrainings.com/ceh-ethical-hacking-course-in-lahore/. [Accessed 26 Feb 2017].

[155] SKANS, “CISA Certification,” [Online]. Available: http://www.skans.edu.pk/cisa/cisa.php. [Accessed 12 Mar 2018].

[156] APP, “Pakistan trained 12,458 individuals to control cyber crimes,” 24 Mar 2017. [Online]. Available: https://www.thenews.com.pk/latest/206371-Pakistan-trained-12458-individuals-to-control-cyber-crimes. [Accessed 03 Jan 2018].

[157] Moneeb Junior, “CYBER SECURE PAKISTAN 2018: INTERNATIONAL CYBER SECURITY CONFERENCE HELD IN ISLAMABAD,” 29 Mar 2018. [Online]. Available: http://moneebjunior.com/cyber-secure-pakistan-2018-international-cyber-security-conference-held-in-islamabad/. [Accessed 15 April 2018].

[158] CollegeDekho, “Cyber Security Colleges in India,” [Online]. Available: https://www.collegedekho.com/information-technology/cyber_security-colleges-in-india/. [Accessed 05 Mar 2018].

[159] iiitd, “Indraprastha Institute of Information Technology, Delhi,” 18 Feb 2018. [Online]. Available: https://iiitd.ac.in/academics/mtech/info-sec.

[160] AMRITA, “Ph. D. in Cyber Security Systems and Networks,” 04 Mar 2018. [Online]. Available: https://www.amrita.edu/program/ph-d-cyber-security-systems-and-networks.

[161] CompTIA, “CompTIA Security+,” [Online]. Available: https://certification.comptia.org/certifications/security. [Accessed 02 Mar 2018].

[162] ISACA, “Certified Information Security Manager (CISM),” [Online]. Available: http://www.isaca.org/Certification/CISM-Certified-Information-security-manager/Pages/default.aspx. [Accessed 02 Mar 2018].

[163] ISC, “Certified Information Systems Security Professional,” [Online]. Available: https://www.isc2.org/Certifications/CISSP#. [Accessed 03 Mar 2018].

[164] EC-Council, “Certified Ethical Hscker,” [Online]. Available: https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/. [Accessed 02 Mar 2018].

[165] GIAC Certifications, “Security Certification: GSEC,” [Online]. Available: https://www.giac.org/certification/security-essentials-gsec. [Accessed 03 Mar 2018].

[166] ISEA, “ISEA,” [Online]. Available: https://www.isea-pmu.in/home/About.

[167] Government of India, “Ministry of Electronics and Information Technology,” [Online]. Available: http://infosecawareness.in/home/index.php.

[168] SECURE, “Cyber Secuirty Summit,” [Online]. Available: http://cybersecuritysummitindia.com/. [Accessed 15 April 2018].

[169] Kenes Exhibitions India Pvt. Ltd, “Cyber Secuirty Confernence,” [Online]. Available: http://kenes-exhibitions.com/cybersecurity/why-to-attend/. [Accessed 20 Mar 2018].

[170] National Cyber Security Centre, “New talent,” 13 Mar 2018. [Online]. Available: https://www.ncsc.gov.uk/new-talent.

[171] NCSC, “NCSC Certified Degrees,” 13 Mar 2018. [Online]. Available: https://www.ncsc.gov.uk/information/ncsc-certified-degrees.

[172] “FindAphD,” [Online]. Available: https://www.findaphd.com/search/phd.aspx?CID=GB&Keywords=cyber+security. [Accessed 21 Mar 2018].

[173] “Arkwright Engineering Scholorships,” 12 Mar 2018. [Online]. Available: http://www.arkwright.org.uk/our-scholarships/arkwright-scholarships.

[174] IT PRO, “http://www.itpro.co.uk/careers/28212/a-guide-to-cyber-security-certification-and-training,” 12 Mar 2018. [Online]. Available: http://www.itpro.co.uk/careers/28212/a-guide-to-cyber-security-certification-and-training. [Accessed 12 April 2018].

[175] HM Government, “Cyber Discovery,” 20 Mar 2018. [Online]. Available: https://joincyberdiscovery.com/.

[176] “National cyber Security Center,” 14 Mar 2017. [Online]. Available: https://www.ncsc.gov.uk/events/cyberuk-2017.

[177] PopFlock, “Internet in Pakistan,” 04 Mar 2018. [Online]. Available: http://www.popflock.com/learn?s=Internet_in_Pakistan.