# INTRODUCTION

In the 21st century, the world politics is facing various complicated dimensions of threats. States are not only using traditional ways to achieve their objectives, but certain non-traditional tools are also being practiced. Recently, states have been heavily reliant on cyberspace for governance, resulting in a vulnerability of State systems at the same time. Consequently the probity of armed conflicts has been reduced that escalate the risk of hybrid warfare. Due to this enigma, non-traditional threats have gained more importance than traditional threats. The present has been labelled as the "Information Age," consisting of technological advancement and communication technology revolution, facilitating the emergence of Cyber warfare. Consequently, indicating a slow shift of the battlefield from land, air and sea towards the cyberspace. Cyber "is a contested term carrying different meanings for different people — and should not be taken as 'merely' interchangeable with the internet. Conceptually, cyber has two characteristics: electronic medium as its components and online communication as its capability".[1] Cyberspace "together with the characteristics of cyber, incorporates the characteristics of space, namely people or users and places for their communications."[2] Exploitation in term of cyber space is a new threat to a state's security; with no demarcation between governments, militaries and populations. An individual user can launch an effective and offensive cyber-attack against the enemy state or against the government. Cyber war is a serious threat to national sovereignty and national security, due to its wide-ranging domestic, international and trans-national implications. As cyberspace is free of cyber-borders, identification of an enemy is a troublesome task. Numerous Developed nations have become the victim of such cyber-attacks. Moreover, the emergence of similar trends is taking place in developing states, such as India and Pakistan.

---

[1] Muhammad Riaz Shad, "Cyber Threat Landscape and Readiness Challenge of Pakistan," *Strategic Studies*, accessed August 11, 2019, http://issi.org.pk/wp-content/uploads/2019/04/1-SS_Muhammad_Riaz_Shad_No-1_2019.pdf

[2] Muhammad Riaz Shad, "Cyber Threat Landscape and Readiness Challenge of Pakistan," *Strategic Studies*, accessed August 11, 2019, http://issi.org.pk/wp-content/uploads/2019/04/1-SS_Muhammad_Riaz_Shad_No-1_2019.pdf

The prolonged rivalry between India and Pakistan has resulted in a cyber-war. Hacktivism between two countries is not a new phenomenon, where hackers of both states frequently engage in hacking the governmental websites of each other. Although, both states are equipped with cyber capabilities, technologically, India is more sophisticated in comparison to Pakistan. Secondly, the Indian government is investing much more in the IT sector, in order to excel in the field, automatically creating difference between the two and a sense of insecurity for Pakistan. In recent years, various kinds of cyber-attacks have been reported from both sides.

Whenever a physical event occurs between these states, hackers of both states also play their part. For example: In August 2015, when the Kerala Eco Tourism park in southern India was sabotaged by Pakistani hackers, in response, the Indian Cyber Pirates, Indian Black Hats and the Mallu Cyber Soldiers attacked 120 Pakistani websites as vengeance.[3]

In the earlier months of 2014, hackers of Pakistani origin hacked and defaced the official website of Banglore city policy. Later, they launched an attack against India's Bharatiya Janata Party (BJP) websites, which led to the situation where the website has been blocked for all the users who are trying to access them from Pakistani IPs. In response, Indian "black hat hackers" defaced many government sites of Pakistan, most importantly ministry of defense, the ministry of railway, cabinet ministry and the national portal. Indian cyber security experts claim, they can hack the websites of Pakistan's critical infrastructure, if they were given 'go ahead' by Indian government.

The Election Commission of Pakistan (ECP) has sanctioned an agreement to acquire Electronic Voting Machines (EVMs) and Biometric Verification Machines (BVMs) that has already been used on experimental basis in pre-2018 by-elections. Later on, it will be used in general elections on a larger scale.[4]It will cost around RS 80 billion for the electronic ballot in general elections. For this, Pakistan will be in need of almost 360,000

[3]Max Metzger, "Pakistan India tensions go online," *SC Media UK*, February 12, 2016, accessed July 25, 2017,
https://www.scmagazineuk.com/india-and-pakistan-tensions-go-online/article/531450/
[4]Maheen kanwal, "Pakistan to test electronic voting machine for elections," *Tech Juice*, March 14, 2017, accessed July 25, 2017,
https://www.techjuice.pk/pakistan-to-test-electronic-voting-machines-for-elections/

electronic voting machines for general elections. For purchasing such advanced system, the pervious finance minister Ishaq Dar was granted huge funds. This highly developed system has been introduced by the USA in 2016 elections; where Russia hacked the Democratic National Committee campaign and used it against Henry Clinton. A similar scenario can smolder between India and Pakistan posing a serious threat to Pakistan's democratic system.

## Statement of the Problem

Arch-rivals India and Pakistan have forever been engulfed in a historical enmity. They have ever-lastingly strived with their hard power, but recently the tide has turned. Presently, states find non-conventional wars to come in handy unlike conventional mechanisms of obsolete times. One of the most prominent tools of these non-traditional wars is the curse of cyber-attacks. This curse has been let loose in the era of technology. Like other states, Pakistan and India are also engaging in this non-conventional confrontation. Mundanely, both hack each other's websites to access highly confidential information. In the midst of this cyber war, they are defacing one another's sites for the better public opinion.

An important concern is whether Pakistan capable enough to defend itself against cyber-attacks and it can secure its digital systems from unauthorized access. Furthermore, Pakistan has introduced electronic voting machines in its election system. Learning from the Russian example of cyber hacking into the US elections, one can predict that India can hack Pakistani elections once they are completely digitalized. Additionally, major sectors of Pakistan like banking, education, airlines, hospitals and nuclear sites are using online services. Providing maximum digital security to these sectors is very much challenging for Pakistan. In light of above mentioned context, this study intends to identify the conditions under which India can launch cyber-attacks against Pakistan. Furthermore, it analyzes the comparative offensive and defensive cyber capabilities of both states and the magnitude of threat posed by Indian cyber capabilities to the critical infrastructure of Pakistan.

## Objective of the Study

The study intends to achieve the following objectives:

- To study the cyber laws and strategies of India and Pakistan in comparison.
- To make a comparative assessment of the cyber capabilities of India and Pakistan.
- To examine the ways India poses cyber threat to Pakistan.
- To evaluate Pakistan's cyber preparedness vis-à-vis the Indian cyber threat.

## Research Questions

This study answers following research questions:

1. What are the respective cyber laws and strategies of India and Pakistan?

2. How do India and Pakistan differ in terms of cyber capabilities?

3. How do Indian cyber capabilities account for a cyber-threat to Pakistan?

4. How well is Pakistan prepared for counter response to the Indian cyber threat?

## Literature Review

This research is envisioned to explore the area of cybersecurity in Pakistan with upcoming threats. Cyber security also termed as "information technology security refers to the technologies, processes and practices "to prevent, detect and recover from damage to confidentiality, integrity and availability of information in cyberspace." Cybersecurity is assumed as a non-traditional threat at the global level. This research will discover the cybersecurity system, with reference to the digital attacks expected between India and Pakistan. India is paying considerable attention to the advancement of their cybersecurity system with protective measures taken by the government too. Accordingly, the impact of Indian cyber system on Pakistan will be analyzed that whether in reality, Indian expansion in cyberspace pops up peril for Pakistan. There is an additional need of interpretation upon hacktivism between both countries at individuals as well as governmental level. Many writers, analysts and cyber experts took this problem and gave their opinion with different dimensions. Some gave arguments in the favor of India as

well as several gave privilege to Pakistan. Analysis of this existing literature will be helpful in predicting future sequence of cyber threats.

Jeffrey Carr, in his book "Inside Cyber Warfare" (2010) provides a detailed description on how nations, groups, organizations or individuals throughout the world are using the internet as a weapon against others and acquiring military, economic, political and social rewards more than their adversaries. Many sophisticated state sponsored hackers are working on the behalf of governments and targeting anyone according to their requirements. Furthermore, in Chapter 6 he discusses when Pakistani hackers defaced the India Eastern Railway Site on 24 December 2008 with the following announcement. "Cyber war has been declared on Indian cyberspace by Whackerz-Pakistan". As a response to the Indian violation of Pakistani airspace the whackers, Pakistan again hacked the government and military sites and also destroyed the data of Indian customers from financial institutions. Even though the whackers Pakistan were not residents of Pakistan but they were strongly motivated by nationalistic or religious devotion. This same dedication is observed in the hackers of both sides with strong nationalist, religious and ethnic agenda with which they are targeting the sensitive sites of each other. There harmful agendas behind hacking have tendencies to affect the country on a large scale.[5]

Daniel R McCarthy, in his book, "Power Information Technology and International Relations Theory," (2015) resurfaces the idea of strategic narrative given by Professor Ben O Loughlin. It revolves around the "Communication Power and the new World Order." Within this order, whosoever will control the global communications infrastructure, will control the conduct of international relations. Furthermore, McCarthy constitutes a brilliant concept on the nexus of communication technology, foreign policy and structural power. Beside it, his critique of unequal capacities of states who are involved in internet construction alongside its entrenchment provides a shape of institutional power. Keeping in this view McCarthy smartly provokes an empirically well-off account for the role of hi-tech in international relations, which explain the role of American structural power. After that, he strives to make clear the role of advanced technological power in international relations through historical materialistic approaches.

[5]Jeffery Carr, *inside cyber warfare* (America: O' Reilly, 2010), 92.

As noted in chapter 4, developed and economically powerful companies have enough financial resources to develop a popular application and introduce them to a market, where under developed states only follow them. Which means the network is always influenced by financially well off actors. Due to this very reason, American companies are still dominating web browsers. "In India, the top 25 internet sites by traffic are dominated by American cooperation."[6] In response, developing states like China and India are also trying to oppose their structural disadvantages. They have used a strategy of state-led economic expansion in the advanced information and technology sector. When structural power role is applied in India and Pakistan, India is an economically well-off country and trying to compete with developed states like the U.S, in the field of Information Technology. On the other hand, a financially deprived Pakistan can only follow the internet to realize economic benefits, which make an unequal playing field in comparison to India.

In the context of cyber warfare, a debate about Indian cyber context has emerged in a research article written by Atul Kumar and Chiranshu Ahuja with a title of "Cybersecurity Research Developments Global and Indian Context". The writers discuss the emerging cyber security threats with reference to attacks that are affecting states in financial matters. They also explain the different strategies adopted by states for securing their cyberspace system. Within this ambit, Atul Kumar and Chiranshu Ahuja further provided Indian perspective about cybersecurity. Firstly, India tries to provide high economic growth for the welfare of its nation, but later emerging cyber challenges become more severe when it affects the national security and economic aspect of the country. Since those global patrons are a foremost factor for the economic enlargement of India.

Further, Majid Yar in his book "Cybercrime and Society" (2006), states that from the last decade the excessive proliferation of cybercrime is taking place globally. Here most essential issues are covered like child exploitation and online stalking, to name a few. As far as the world of cyber crime is concerned, it is taking place at a rapid pace. The most

[6] Daniel R Mccarthy, *Power information technology, and international relations theory* (London: Palgrave Macmillan, 2015), 81-134.

recent issues of Hi-tech crimes are a threat to vital infrastructure owned by individuals or groups who are motivated by any political or religious motivation, advance payment system and credit cards. To defy these attacks, Majid proclaims that we need a private and public cooperation to counter cybercrimes. As it is noted in the 3rd chapter of this book, most liberal democratic states are expanding their reliance on the internet using it as a tool for communication. Web defacement is prevalent, of which 70% defacement are pranks and remaining 30% used to target particular website for political, social and moral points.[7] Sometimes web hacking appears when there is tussle going on between two states like India and Pakistan. The governments are not only involved in an ongoing turf, but the public also becomes part of it. Furthermore, in late 2004, a child exploitation case was highlighted that could effect of creating cross-nation difficulties. Even in the current time period such type of cases are happening between India and Pakistan. Thus policy maker of both states are required to create suitable policies and strict laws against these cybercrimes. Because they are not only affecting the relationship between two states, but are also damaging state critical infrastructure.

**Research gap**

The above mentioned literature review is predominantly based on the analysis, opinions and understanding of different scholars about ongoing cyber issue between India and Pakistan. Some of them see India's upper hand in the field of cyberspace, with the capability to easily target essential sites of Pakistan due to poor Cyber security of Pakistan. Others have a contradictory view that India is not capable enough to pose a serious threat to Pakistan. The major gap in existing literature shows the intense involvement of both governments in cyber-attacks. Directly or indirectly, they are trying to undermine each other through their cyber capabilities. The point of discussion is whether new possibilities can emerge in future with reference to cyber confrontation between India and Pakistan. This aspect needs more attention in the view of prospective cyber warfare between India and Pakistan.

[7]Majid Yar, *Cyber Crime and Society* (London: Sage, 2006), 49-109.

## Theoretical Framework

The theoretical framework adopted for this research is the Theory of Securitization, formulated by Barry Buzan and Ole Waever, core contributors to Copenhagen School of Thought.[8] Both have largely worked on regional security complex theory. Copenhagen School contributed distinctively to the concepts of societal security and securitization.[9] Securitization is defined as "the process of presenting an issue in security terms, in other words as an existential threat."[10] There is a debate regarding the traditional and modern definition of security in post-cold war era. Traditionalists adhere to the realistic view of security threat, specifically dealing with objective threats and military threats. Stephen Walt who belongs to traditionalist school of thought defines it as "the studies of the threat, use, and control of military force."[11] Barry Buzan, the proponent of other school of thought, presented a more deep and wide concept to security. Buzan argued that in the post-cold war era, states face not only military threats but other threats such as political, societal, economic and environmental in other words, states individuals and social groups are considered as the referent objects.[12] Moreover, Barry Buzan in his book "People States and Fear*"* stated, that the notion of security was "too narrowly founded"[13] leading to Buzan contributing towards a broader framework of security.[14]

Although, the security remains the states' major concern, but dimensions of security have changed since the end of cold war. Under this consideration, securitization theory considered as best in facilitating the security analysis. Along with all these traditional security threats, cyber threat has emerged as a new non-traditional form of warfare. The cyber security threat emanates from advancement in information technology and communication network as well.

---

[8] Barry Buzan and Lene Hansen, *The Evolution of International Security Studies* (New York: Cambridge University Press, 2009), 212.
[9] Ibid.
[10] Ibid., 214.
[11] Vladimir Šulović, "Meaning of Security and Theory of Securitization," *Belgrade Centre for Security Policy*, October 5, 2010, accessed November 28, 2018, http://www.bezbednost.org/upload/document/sulovic_(2010)_meaning_of_secu.pdf.
[12] Ibid.
[13] Ibid.
[14] Ibid.

The securitization theory is applicable in case of India and Pakistan, as they share historical enmity and have fought three military wars. There is always a competition and tit-for-tat situation going on between them, such as if one goes for nuclearization, other responds in the same vein, followed by an arms race and now, as per the global trends, the military threats diverted into non-traditional threats. Among non-traditional security threats between Pakistan and India, cyber security is the most prominent one.

India and Pakistan being regional rivals since independence never enjoyed good relations. Their relations further aggravated by military threats emanating from each other. Moreover, cyber security threat is now considered to be a major source of tension between two states. Indo-Pak rivalry in cyberspace is best analyzed through the ideas put forth by Barry Buzan and Ole Waever in the theory of securitization. Although cyber security threat is an emerging phenomena and under study but appeared as disastrous in deteriorating Indo-Pak relations.

Both countries are trying to transform their security policies to counter evolving cyber security threats. India has been formulating its cyber security policies to address its persistent cyber security threats. However, Pakistan is far behind in cyber security capabilities when it comes to comparison with India due to its economic restraints and lack of central body to deal with cyber security threats emanating particularly from India. India has shifted its large part of economy on information and communication technology (ICT) which includes: information technology services, cyber espionage, commerce and banking sector and cyberattack.[15] Contrary, Pakistan is relatively a weak state and lack in capabilities to counter its evolving cyber security threats.

The theory of securitization further supported by the three models for cyberspace securitization presented by Lene Hansen and Helen Nissenbaum that are: hyper securitization, everyday security practices and technification. First model, hyper securitization focuses on “multinational cyber disastrous scenarios” that are interconnected in societal, financial and military prospects and need “excessive

[15] Reda Baig, “Could Offensive Cyber Capabilities Tip India and Pakistan to War?,” *The Diplomat*, March 26, 2019, accessed August 11, 2019, https://thediplomat.com/2019/03/could-offensive-cyber-capabilities-tip-india-and-pakistan-to-war/

countermeasures". Second model, everyday security practices means securing mobilization of normal individuals. The third model, technification primarily focuses on the role of information scientists and technical expertise to protect against cyberattacks. Unfortunately, Pakistan lacks in above mentioned cyber security discourse.[16]

In Indo-Pak security context, the cyber security threat has been becoming major concern over the past few years. Cyber warfare is in its infancy years, but is also gathering the interest of security analysts' as a major security threat to both countries. All the major powers have built their cyber domains and respective doctrines, but relatively Pakistan remains a weak state when it comes to tackling the cyber threats. It is historically evident that Pakistan has always stuck to a reactionary decision making process. But to deal with this new dimension of security threat, it needs to actively formulate cyber doctrines; to build strong detecting cyber capabilities in order to securitize the prevalent cyber security threat. India as compared to Pakistan spends more on its IT sector to develop its cyber capabilities. Furthermore, by targeting the sensitive sites of Pakistan, India is trying to defame Pakistan's image, internationally. Thus, Pakistan has to develop its strong cyber defense against its hostile neighbor so that it could enable Pakistan to avert any sort of criminal plan by India. Cyber security threat in Indo-Pak context needs to be securitized in Pakistan to counter this emerging threat by formulating specific cyber guidelines and laws.

## Research Methodology

The research design selected for this study is qualitative in nature, which deals with the collection and analysis of non-numerical data with reference to cyber threat between India and Pakistan. The research is mainly descriptive and analytical as it expounds history and gives critical analyses and futuristic scenarios regarding cyber security. Descriptive research is used to explain the problem in detail with positives and negatives. Since the current cyber security challenges faced by Pakistan are passing through their initial phase, the relevant data is not easily available. Data has been

[16] Muhammad Riaz Shad, "Cyber Threat Landscape and Readiness Challenge of Pakistan," *Strategic Studies,* accessed August 11, 2019, http://issi.org.pk/wp-content/uploads/2019/04/1-SS_Muhammad_Riaz_Shad_No-1_2019.pdf

collected from both primary and secondary sources. Among primary sources, interview was conducted of Dr. Tugral Yamin, Associate Dean of Department of Peace and Conflict Studies, National University of Sciences and Technology (NUST). The secondary sources of data include content analysis of books related to Cyber warfare, cybercrimes, and cyber politics in international relations and through related Research Journals and newspaper articles. The available literature was efficiently used in answering and interpreting the research questions.

## Significance of the Research

This research is significant in understanding the importance of cyber security in the current era. It provides detailed information about cyber threat as a non-conventional security threat. This area of cyber security is quite new and has not been investigated in detail with respect to India-Pakistan conflictual relations. Further, this study has reviewed the Indian cyber capability as a nontraditional security threat for Pakistan. Moreover, this study as a body of knowledge is primarily beneficial for academia, including students, teachers, researchers and think tanks. It is equally useful for policy makers as a source of knowledge regarding the seriousness of cyber threat to Pakistan. The study is finally of interest for private and public institutions/industries which depend on the cyberspace for their daily functions, such as NADRA, banking institutions, businesses and the energy sector.

## Delimitation

The thesis covers the issue of cybersecurity between India and Pakistan in the context of international relations. It does not provide the technicality of cyber threats posed by India to Pakistan nor Pakistan’s capacity to respond. It covers the historical background, current assessment of futuristic cyber scenarios between India and Pakistan.

## Organization of the Study

**Introduction:** Covering Statement of Problem, Research Questions, Objectives, Literature Review, Hypothesis, Theoretical Framework, Research Methodology, Significance of study, Delimitations, Organization of study, and Key terms.

**Chapter 1 "India-Pakistan Cyber Laws and Strategies in historical context"** Provides the history of cyber-attacks between India and Pakistan.

**Chapter 2 "A Comparison of India Pakistan- Cyber Capabilities"** Analyses of the cyber capabilities of both states.

**Chapter 3 "Indian Cyber Threat to Pakistan"** Examines how Indian cyber capabilities are posing nontraditional threat to Pakistan.

**Chapter 4 "Pakistan's Cyber Preparedness"** Provides major cyber security challenges faced by Pakistan and gives ways forwards for those threats.

**Conclusion** Summarizes the findings of the Thesis and provides recommendations of the study.

# CHAPTER 1
# INDIA-PAKISTAN CYBER LAWS AND STRATEGIES IN HISTORICAL CONTEXT

India and Pakistan have a very hostile relationship from the beginning. This relation became more complex due to some historic and political events. The major reasons causing these hostilities include: the British partition plan, political, cultural, social, economic factor, Kashmir conflict, division of asserts, and conflict on water between them. They have also fought three military wars. Another revisionist view is that they are rivals in their nature, because of Hindu-Muslim conflicts. Additionally, after acquiring nuclear weapons, there are enhanced chances of a disastrous war in the South Asian region. With the passage of time, non-conventional wars became more prevalent as compare to conventional warfare. India and Pakistan have also started following the new trends of conflict in which cyber-attacks are very much common between them.

## 1.1 History of Cyber Attacks by India

The historical enmity between India and Pakistan has split into a new form of digital war, in which Indian hackers are playing their vital role in cyber space. Whenever a tangible incident happens in India, it is considered that Pakistan is involved in it. In response, Indian hackers take out their anger in form of hacking or defacing websites of Pakistan. Following are events that have taken place in order to deface Pakistan by Indian hackers.

The first time ever India used cyber frontiers for war with Pakistan happened as a response to Kargil war controversy. Defacement of Bhabha Atomic research center was done by Pakistani hackers. In the year 2000, a group called “Patriotic Indians” claimed for hacking the official websites of the Pakistani government. This was just the start of a new kind of war. Initially, 7 websites of Pakistan were hacked in 1999, but by 2000, the numbers had increased to 18.

In 2011 three consecutive bomb blasts happened in Mumbai. As retaliatory move, a group of Indian hackers hacked the national high way authority website. After hacking they left a message, the defacement is just a reminder for Pakistan about those 20 people who were killed in Mumbai bomb blast attack. The group involved in website defacement is known as Indian Cyber Army with the name of 'Ashell' and another group, defaced the first 3D center in Karachi the Atrium Cinemas.[17] The owner said PTA was not available to respond to us. Internet experts shared their opinion that, PTA unable to stop these types of cyber-attacks organized by international servers.

When Kulbhushan Jadhav was arrested from Balochistan, he was accused of being an agent of RAW and was involved in some suspicious activates against Pakistan. Although, the Indian government believed that he was arrested from Iran and not from Pakistan. They accepted that he was a retired officer of navy and did not have any kind of links with the government, as an agent of RAW; He was given the death penalty by Pakistan. After the news of the penalty, Indian hackers became more active and hacked 30 governmental sites of Pakistan. Indian hackers also said that all these cyber-attacks on Pakistani sites are part of their operation against Pakistan. After this, another group of hackers known as Telangana Cyber Warrior claimed that they hacked and infected the governmental hospital in Karachi. They were able to monitor the record of patients. Later Kerala Cyber Warrior group of hackers from India hacked the website of Pakistan academy of Rural Development. After hacking, they left the message regarding justice for Kulbhushan Jadhav ji.[18]

Mahesh Haxor, the member of the group K9 Network Cyber Army affiliated with Anonymous, has defaced the site Pakistan.gov.pk, the official website of the Pakistani government. Cyber News reports that the hacking comes in response to the recent bomb attacks in Hyderabad where more than a dozen people were killed and 100 others injured.

---

[17]Web Desk, "Indian Hacker defaces National highway Authority website," *The Express Tribune*, July 7, 2012, accessed August 19, 2018, https://tribune.com.pk/story/404965/indian-hacker-defaces-national-highway-authority-website/

[18]Mail Today Bureau, "Surgical Cyber Strike! Hackers take down 30 Pakistani sites to revenge Kulbhushan Jadhav's death penalty," *Mail Online*, April 24, 2017, accessed August 19, 2018, http://www.dailymail.co.uk/indiahome/indianews/article-4441462/Surgical-cyber-STRIKE-Hackers-attack-30-Pakistan-sites.html

Some believe that a group with links to Pakistan is behind the attacks. On the defaced website, the hacker threatened to attack more sites and to leak data from the databases. "Government of Pakistan, you have failed, you have no power, no capacity, you are just trash, it's sad, but it's true," said the hacker.

Moreover, a similar group called ICA hacked over 36 most sensitive websites of Pakistan in which NADRA, Pakistan Navy, NAB, the ministry of foreign affairs and council of Islamic ideology were included. All these 36 governmental websites were relying on a single server which makes Pakistani websites more vulnerable and easy to access from Indian hackers. It shows the aggression level of Indian hackers on the Mumbai attack. They considered that Pakistan was behind this event. Two groups were involved in it, Jack4xor and LuCkY. Many well settled professionals are part of Indian Cyber Army. They were not promoting this kind of cyber-attacks between India and Pakistan, but just wanted to give a message to Pakistan that such kind of terrorist attack is disturbing their neighbor country. So it's better for Pakistani people to avoid it in future.[19]

Digital attacks are a common practice between the Indian Cyber Army and Pakistan Cyber Army. In 2010, Indian Cyber Army said that they got access to around 375 websites of Pakistan. Mostly websites are related to the government sector, well known organizations and even famous personalities as well. Earlier a group called Pak Cyber Army hacked almost 300 websites of India, as an act of revenge. After that warning, Pakistani government took the matter more seriously, creating a special chamber under the supervision of FIA and named The National Response Center for cybercrimes (NR3C). The basic purpose was to protect Pakistani websites from further digital attacks. For that FIA tried to re-implement the Prevention of Electronic Crimes Ordinance (PECO) with the coordination of PTA and ministries of information and technology. The bill was reacted by the president of Pakistan after the 18$^{th}$ amendment. The major problem of cyber-attacks is the single insecure server because majority servers do not physically exist in Pakistan. That's why hackers can easily find out the loophole in the

[19]Jahanzaib Haque, "Cyber Warfare: Indian hackers take down 36 govt websites," *The Express Tribune*, December 1, 2010, accessed August 29, 2018, https://tribune.com.pk/story/84269/cyber-warfare-indian-hackers-take-down-36-govt-websites/

cyber system and access its targets. To avoid further cyber-attacks the Pakistani governmental institutions and other sectors needed to relay on those servers which are physically available in Pakistan. This is less risky as compared to those servers which do not exist in Pakistan.[20]

Additionally in 2017, a group of Indian hackers took down Multan, Islamabad, Peshawar and Karachi airport website, a reaction from Indian hackers. Because a day before Pakistani hackers called 'Alone Injector' hacked the official website of an elite national security guard (NSG). As a reaction, Indian hackers not only hacked the website, but also spread ransom ware virus in their system. Later Indian hackers demanded cryptocurrency to unlock the website or data. They paid the bitcoin as per demand and resumed their websites. Moreover, Thiruvananthapuram airport website was hacked as a response by 'Mallu Cyber Soldier' a group of Indian hackers. They got access into Sialkot international airport and also obtained login information for the website. It did not end here. Indian hackers also shared the passwords and leaked the private information with the public. It created more dangerous situation for Pakistan. After these cyber-attacks, cybercrime gave an opinion about these ongoing attacks. Kislay Choudhary said that Indian hackers are not only hacking on the critical infrastructure of Pakistan, but also spying on Pakistani sensitive information. Apparently, this cyber defacement was just a revengeful act by Indian hackers, but in future it can create a more vulnerable condition for Pakistan. Apart from that the tools/types which is used by India for cyber-attacks against Pakistan are Website defacement, spear, phishing and malware.

## 1.2 History of Cyber Attacks by Pakistan

Pakistan hackers are much active on cyber space as Pakistani forces are on borders. These hackers are always ready to launch cyber-wars against India whenever Indian hackers try to show some massive defacement against the government and any other institution of Pakistan. Pakistan's Cyber Army warriors give a proper response to India as revenge.

[20] Asad Kharal, "Cyber War Continue: 375 Pakistani websites under threat," *The Express Tribune*, December 11, 2010, accessed August 27, 2018, https://tribune.com.pk/story/88730/cyber-war-continues-375-pakistani-websites-under-threat/

The first ever cyber offensive attack was launched by Pakistan in 1998. When India officially announced its nuclear test in Pokhran, a group of hackers called Mailworm, hacked the website of Bhabha Atomic Research center and left negative remarks about India. A similar practice was done by Pakistani hackers during the time period of most controversial kargail war. Pakistan hackers took control over armyinkashmire.com site. Through this, they exploited the situation and posted photos of Indian troops and their brutal acts. Furthermore, Pakistani hackers increased the number of hacking from 4 in 1999 to 72 in 2000. In 2001, Pakistani hackers hacked 150 websites of India. Later they continued attacking each other sites and began an unended war.[21]

A group of techies, Pakistan Cyber Army (PCA) hacked Indian defense website, as a response to the Indian initiated digital battle through the defacing of Pakistan's Defense site. PCA said that it was a preplanned defacement to give a warning to Indian hackers that again don't dare to mess with Pakistani web sites. Otherwise, you will face the similar response from Pakistan.[22]

Some Pakistani hackers who hacked the national police website of India, after hacking they left the negative comments about India with pasting Pakistani flag of their website. Another group of techies called Predators PK hacked over 200 websites of India. Whilst, Independent Computing Architecture (ICA) hacked Pakistani websites, their full focus was on the government sector. That's why when Predator PK took revenge; they also focused on Indian central Bureau of the investigation, NGOs, Indian multinational companies and religious sites as well. As ICA did this as retaliation for 26/11. But Pakistani hackers did not have a similar ideology. They hacked the websites to give a strong message to Indian hackers: do not deface the Pakistani websites. Before this event Pakistani hackers also hacked 1200 websites in which BJP, Nehor websites and some top hacker's forums were hacked. Pakistani techies claimed that it were attacks as a response

---

[21]Rishadullah Shaikh, "The futility of Indo-Pak cyber wars," *Dawn*, July 28, 2011, accessed August 29, 2018,
https://www.dawn.com/news/647571

[22]Muhammad Ali Raza, "Tit for tat: Indian Defence.com hacked to revenge Defence.pk Defacement," *The Express Tribune*, September 1, 2011, accessed August 19, 2018,
https://tribune.com.pk/story/243388/tit-for-tat-indiandefence-com-hacked-to-avenge-defence-pk-defacement/

to Indian hackers, who previously launched cyber-attacks. Moreover, Pakistani hackers said that the Pakistani government lacked cyber security as it relied on weak servers. It became easier for Indian hackers to target the Pakistani websites. Although, Pakistani hackers have more expertise in th cyber space and can better defend their country in terms of cyber war, but the Pakistani government should take some strict measures for the protections of its server system.[23]

Furthermore, almost 4,600 sites in India were deforested. Who made it? A Pakistani group "Pak Cyber Pyrates" claiming for their country the disputed territories hundreds of years ago in Kashmir or Kashmir was responsible. How they did it? in an organized way through Twitter by taking advantage of vulnerabilities of different sites whose administrators never patched.

According to Hackers Media, the site Pakistan.gov.pk/gop/ can be used as a proxy. The hacker used this proxy to show his own website and make it look as if the Pakistani parliament website was defaced. Seven websites of the Government of India have been hacked by Pakistan Cyber Army. Pakistan Cyber Army (PCA) hackers have attacked and modified 7 websites belonging to the Indian government, according to Hack Read. The affected websites are those of Bihar Tourism of the Ministry of Tourism of India (bihartourism.gov.in), Mitigating Poverty in Western Rajasthan (mpowerraj.gov.in), the Directorate of Medical Education of the Government of Kerala (nurses.kerala. gov.in), and the Kerala Government Wage Review Commission (src.kerala.gov.in).

The main objectives are government sites. As can be seen, in the cyberspace many wars are almost hidden, in which apparently there are no bullets, blood, or dead, but some of the attacks carried out in this way could endanger human lives if an infrastructure were attacked as critical as a nuclear power plant. Some countries are already drafting policies to protect their critical infrastructure and how to act against such an attack, other countries could perpetrate an attack on another using the infrastructure of a third party

[23] Jahanzaib Haque, “Cyber war escalates: Pakistani hackers ‘take revenge’,” *The Express Tribune,* December 4, 2010, accessed August 27, 2018, https://tribune.com.pk/story/85746/cyber-war-escalates-pakistani-hackers-take-revenge/

making it appear that the attack came from it and not from its true origin. A new battlefield is brewing and we are in it without knowing it.

## 1.3 Cyber Crime Laws in Pakistan

Cyber security is very much important for national security due to illegitimate cyber activities. South Asian states especially Pakistan is important in this emerging challenge. Pakistan has an excessive number of internet users. Previously, cybercrime laws did not exist in Pakistan. Although, national media indicates the growing cybercrimes in Pakistan like illegally accessing credit card, harassment and blackmailing are common. In 2009, the Prevention of Electronic Crimes Ordinance was lapsed without becoming a proper law. After that, no ruling government tried to reinforce it. Without legislation, some other preventions in Pakistan like Electronic Transaction Ordinance 2002 and Penal code 1860 are working for registered complains related to illicit online activates. Although, Pakistan badly needs a national cyber security policy which has been absent up until 2015. In 2016, the national assembly of Pakistan passed the act of Prevention of Electronic Crimes. The act got proper legislation on 18 August 2017. The law works offensively in unauthorized access, copying data, and data transformation of the system. It also introduces an offensive act on cybercrimes. In term of cyber terrorism if a person committed a crime to affect the critical infrastructure of the state. Hence, will be in prison for 14 years and pay Rs 5 million. Other than cyber terrorism crime the Prevention of Electronic crime act is also applicable to hate speech, on those who provide aid or motivate terrorism and recruitment for further attacks.

The act also provides the power of investigation to another agency. As per section 26 which gives power to the Federal government to create a proper agency that looks after this act; the main aim of the investigating agency is to see that laws are working as per prevention of electronic crimes act. In 2016, federal cabinet makes FIA as an investigating agency under the supervision of cybercrime act. Section 34 of the law gives a legal authority to PTA to block and remove any sort of information, page or website trying to harm the dignity of Islam, defacement of Pakistan national security, against military and decreasing the morality or social values.

After the implementation of the law, an opposing reaction was seen. Many human rights and so called liberalists were denying from prevention of electronic crime act because they were considering that it is affecting the freedom of expression. On their reaction, a founder of digital rights foundation Nighat Daad said, the basic problem of the Pakistani citizen is that they fully do not understand the language of the bill. The language used is quite difficult so human rights organizations and freedom of speech activists took advantage from it and explained it as per their perception. That's why these activists are considering that the law is taking the power of freedom of speech from them. Anusha Reham, the previous minister for information and technology & telecom and in the parliament Nighat Daad said, the criticism of cybercrime bill is totally baseless. Some non-governmental organizations and private sectors are just exploiting the bill due to a particular agenda and hence, opposing the cybercrime bill.[24] Apart from that, many political oppositional parties are also giving negative remarks about the cyber bill because as per their opinion the bill is giving more power to the government and government will use it negatively.

But the government is arguing that the basic aim of giving more power to Telecommunication authority, so it can prevent online harassment, terrorism and cyber stalking activities. As per cybercrime bill, the agency has the authority to track an individual's online activity, therefore, if any sort of negative activity is going on, PTA can block or remove the content from the internet. Besides, the government is facing a lot more criticism. Some lawmakers even said that the punishment in the cybercrime bill is too much harsh. Even the member of PTI Ali Muhammad Khan said that previous government should end politically motivated section because it is discouraging Pakistani youth, who is getting involved in political affairs.[25] Such type of criticism put government as well as the cybercrime law under serious circumstances. So the government of Pakistan should review the bill and do some amendment in it as per the

---

[24] Tariq Ahmed, "Pakistan: National Assembly Passes New Cybercrime law," *Library of Congress*, September 21, 2016, accessed August 31, 2018, http://www.loc.gov/law/foreign-news/article/pakistan-national-assembly-passes-new-cybercrime-law/

[25] Vasudevan Sridharan, "Pakistan Passes 'draconian' cybercrime law threatening civil liberties," *International Business Times*, August 11, 2016, accessed August 31, 2018, https://www.ibtimes.co.uk/pakistan-passes-draconian-cybercrime-law-threatening-civil-liberties-1575530#

practical requirement because just making such a strict law cannot prevent the cybercrimes. When mostly non-governmental and civil sector is non-serious and opposing the law, then the real implementation of the bill will be a most difficult thing for the government.

## 1.4 Cyber Crime Laws in India

The usage of technology is taking place in the daily life of human beings, but at the same time the excessive dependency on cyberspace has resulted in some pros and cons. States such as India needed cybercrime law to address the growing cyber-criminal activities. The very first cybercrime was recorded in 1820. In 2000, India introduces its first cyber law as Indian IT law. It was amended in 2008 and implemented in 2009. India is one of the biggest countries whose economy is dependent on electronic transactions. So it can be targeted at a higher level. That's why the protection of transaction and computer system security is the major concern of the Indian state. Since the 1990's, an organization was active in the cyber law in India. The initial effect of that organization was to spread awareness in public about cyber laws and how much India needed that kind of laws. As a result in 1999, the information technology bill was presented in the parliament of India. After some changes in 2000, the information technology act got the legislation. Still, the organization of cyber law in India was playing a very important role in exposing the draw backs in the information technology act.

## 1.5 India-Pakistan Cyber Laws in Comparison

In general, the public of both countries like India and Pakistan are not aware of the secure usage of the internet. Cyber criminals in both countries are taking advantage of it. Both developing states are trying their best to make proper laws for cyber criminals and counter the growing cybercrimes in every aspect, but there are many lacking in the cyber security bill of both countries.

In Pakistan, the bill of Prevention of Electronic Crime is having very hard punishments for digital criminals. Penalties are difficult to implement in reality. The other major drawback of Pakistan's cybercrime bill is that the government is having some unlawful

authority rights. By using that authority PTA can restrict and remove any kind of material from the internet without court orders. It can affect the right of privacy of Pakistani people and freedom of speech. In which the other institutes and stake holders are claiming that government is corrupt and is using the cyber laws for its personal interests. Other than that, Pakistan is having a national respondent center for cybercrimes but still no government authority or any other law is present to deal with financial frauds. India is planning to establish a center which deals with online financial frauds and the name of that center will be Indian Cybercrime Coordination Center (I4C). Moreover, in Pakistan the cyber security policy is still in the process and not implemented yet. The prevention of electronic bill was presented in the parliament but in reality, it is not workable yet.

## 1.6 Comparison of Cyber Crimes in India and Pakistan

In the case of Pakistan, the cybercrimes reports are not in the access of common public and if you want to access the data you need indirect sources to get the data. Even the government of Pakistan is not showing proper reasonability to handle the official sensitive data. But if it is compared with India, the cybercrime reports data is easily available on the internet. The cybercrime rate is rapidly increasing in Pakistan as compared to India. In Pakistan, a very low progress was seen in between 2014 to 2015. In which Pakistani NR3C out of 2534 cyber criminals, declared 44 as offenders. Furthermore, among those 44 offenders only 4 were arrested. But recently the FIA said that its cybercrime wing has so far conducted 2,295 inquiries, registered 255 cases and have arrested 209 people in 2018 so far, which is the highest since the Prevention of Electronic Crimes Act (PECA) 2016 was passed. The corresponding figures for 2017 were 1,290 inquiries, 207 cases registered and 160 arrests made, whereas figures for 2016 stood at 514, 47 and 49. The FIA admitted that cybercrimes are on the rise in Pakistan but added that “the government’s recent measure to establish 15 new cybercrime reporting centers” will help control the situation.

On the other side, in India according to cybercrime report 2013, from 5693 people 1600 individuals were arrested. While the National Crime Records Bureau (NCRB) stated that India recorded 9,622, 11,592 and 12,317 cases of cybercrime in 2014, 2015 and 2016

respectively, experts stated that this data accounted for merely 1% of the cybercrimes that actually took place in the country.

## 1.7 India's Cyber Security Strategy

A survey conducted about the last 20 years, shows the number of internet users have increased from 16 million to 3.8 billion. The excessive usage of internet is not limited to a specific sector but it has revolutionized both public and private sectors. At the same time, it has created many cyber warfare threats such as cyber espionage, cyber-crime and cyber terrorism. That's why now it has become a global challenge for nation states. Cyber-attacks not only negative impact the socio-political aspect of a nation but also impact the economy as well. As per 2015, globally cyber-attacks estimated amount reached around $75 billion. Further prediction about future digital attacks cost will be nearly $175 billion.

India is one of those countries, that regularly faces severe digital attacks and the cost of those cyber-attacks has increased to Rs. 25,000 cores. That's why 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). 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. 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. India started regulating its IT sector in 1998. 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.

Hence, Indian government pays more attention to the emerging issue and ratifies the information technology Act 2000. The last amendment was made in the year 2008. The

Indian government also introduced the National Cyber Security policy in 2013. The basic purpose of the policy was to provide maximum security to both the public and private sectors. Therefore, within the national cyber security policy, government established some more societies to deal with cyber security issues separately. These are some major institutions established by the government under the supervisor of national cyber security policy. Most of the institutes under the Ministry of Home Affairs (MHA) also fall in this category. The National Intelligence Grid (NATGRID) which keeps all sorts of citizen data in a single database that can be accessed by officers from RAW, CBI, IB etc., comes under the MHA. The National Cyber Coordination Center (NCCC) and the National Crime Records Bureau (NCRB) also come under this ministry.

Other than this, the Home Affairs Ministry directly controls the Intelligence Bureau (IB), the National Investigation Agency (NIA), the Central Bureau of Investigation (CBI) and the Narcotics Control Bureau (NCB). All institutes under the MHA are in charge of internal security in some capacity. The NCB and IB are exempted under RTI. The Ministry of Communication and Information Technology controls CERT-In, the Indian Computer Emergency Response Team that performs emergency cybersecurity functions and releases annual reports of security incidents.

### 1.7.1 Indian Computer Emergency Respondent Team (CERT-IN)

The basic responsibility of CERT-IN is to handle the cyber security incident, analyzing incidents and collects the required information of the incident. Furthermore, it also gives an alarming sign to other institutes, whenever it feels the loophole in the system or there is an expected digital threat. It also cooperates with other cyber security societies.

### 1.7.2 National Cyber Crime Coordination Center (NCCC)

The main duty of NCCC is to monitor and handle the online cybercrimes. It is also accountable to make better policies to handle the emerging cybercrimes and capability to prevent them. NCCC strengthening the research and development sector of cyber security.

### 1.7.3 National Critical Information Infrastructure Protection Center (NCIIPC)

NCIIPC act as the most responsible institute of national cyber security policy. The aim is to protect the critical information infrastructure of the state in which telecommunication network, online payment, digital stock trade and cyber space infrastructure is in control of air and space system.

### 1.7.4 Cyber Swachhta Kendra

It acts as a protection shield of national cyber security policy, which analyses ransomware or malware attacks, especially those that can spread causing dangerous effects on the network system. It also guides the users in the cleanup of the system to prevent further cyber-attacks.

## 1.8 India's International Collaboration on Cyber Security

Under National Cyber Security Policy 2013, the Indian government is trying to cooperate with more countries to counter the issue of cyber security. Currently, India is collaborating with the USA, European Union and Malaysia. The US is not only promoting India in cyber security but at the same time sharing information between CENT-IN and US-CENT. The UK also agreed with India to collaborate on cybercrime and for that sake, the UK is developing a national cybercrime cooperation center in India. The UK is highly dependent on Indian database. Apart from that in 2012, Indian and Japanese foreign and defense sectaries met with each other in Tokyo, where it decided that they should cooperate in the cyber security sector as well. Moreover, in 2013, a British prime minister visited New Delhi, promising to collaborate with India to fight against digital attacks. The UK wants to protect itself from China, for that UK needs Indian partnership in the matter of cyber security. India is actively participating and collaborating with international countries on cyber security matter other than Pakistan.[26] India is highly non-cooperative with Pakistan on the cyber security issue, which makes a

[26] Jean-Loup Richet, *Cybersecurity policies and strategies for cyber warfare prevention* (America, information science reference: 2015), 236.

difficult situation for Pakistan to make foreign allies and figure out a better solution in relation to cyber-attacks.

## 1.9 Pakistan's Cyber Security Strategy

Most states in the world are digitalizing their national assets and critical infrastructures through cyberspace. They attach much importance to the digital security and, therefore, have developed cyber strategies. The neighboring of Pakistan like India has their National Cyber Security Policy, which was created in 2013. After making the cyber secure strategy, India stands in one of those countries whose government is very much concerned about the digital security. Even a small state like Qatar, with a total population of nearly 2 million has a national cyber security strategy in place. On the other hand, Pakistan transfers the most sensitive data on cyberspace (such as NADRA with a fully digitalized system), is not as digitally secure as it should be to prevent cyber-attacks. USA took millions of call records of Pakistani's through telecom companies like SKYNET and DEMONSPIT. Apart from that US Central Intelligence Agency (CIA) store the biometric data of Pakistani citizen in the branch of Terrorist Identity Datamart Environment. As Snowden's reveals the secret information of USA intelligence, agencies like CIA and NSA are getting secret information from the Pakistani citizens on regular bases. It means that Pakistani agencies like NADRA, PTA and other well-known organizations are sharing data with the US.

Furthermore, Turkish hackers were claiming that they access and steal private data of Pakistani citizens through using PTA servers. Henceforth, pushing Pakistan to realize the need for cyber security strategy; the National Cyber Security Council Act 2014 was presented in the senate of Pakistan as a document. Some steps were proposed in the document paving way for the Pakistani council to be in a position to develop a cyber-security strategy at both national and international level. The establishment of National Centre for Cyber Security (NCCS) has been commenced by Government of Pakistan in

June 2018. Leaving aside the international cyber security strategy, on the national level Pakistan has not contributed productively.[27]

### 1.9.1 National Cyber Crime Center

In 2007, Pakistan established the first ever national respondent center for cyber-crimes (NR3C). It is associated with FIA. The objective of establishing a separate department for dealing with cybercrimes is, to secure the increasing use of cyberspace by institutions as well as individuals. The government needs to build a department which counters the cyber illegal activates. Apart from that, the major purpose to establish a cybercrime center is the growing terrorists and their excessive use of internet. On the other side, India is paying more attention to its digital security and developing its cyber army as well to deal with cybercrimes activities in more effective ways.

### 1.9.2 Role of Senate Defense Committees

After Edward Snowden reported the NSA spying on Pakistan, through the use of SECONDDATA and gathered almost 13.5 billion pieces of information. The chairman of the senate committee arranged an important meeting with the representative from Pakistan information security association (PISA). The aim of the meeting was to generate a debate in parliament about Pakistan's cyber security strategy. In that meeting, it was mentioned that government should allot a separate budget for cyber security strategy. The senate defense committee presented seven points. By following those points Pakistan can handle cyber-attacks in much better ways.

- To establish a law that properly works for the prevention, protection and promotion of cyber security with in the country.
- The government of Pakistan should pay more attention to the digital security and take cyber threats as much seriously as terrorist attacks are.
- The national CERT should be renamed with PKCERT.

[27]Zaki Khalid, "Need for a National Cyber Security Strategy in Pakistan," *Pakistan Insider*, May 27, 2015, accessed September 2, 2018, http://insider.pk/opinion/need-for-a-national-cyber-security-strategy-in-pakistan/

- A new task force should be established associated with different public and private organizations. The basic determination is to give a secure system to Pakistan and work on drafting cyber security strategy for Pakistan.
- Furthermore, establish a separate center like “inter services cyber command center” which gives full cyber security to Pakistan’s army.
- Pakistan should take the matter into regional organizations such as SAARC. To discuss cyber security protection measures that should be taken by regional countries to avoid future attacks, protecting against indirect cyber-attacks.
- The Pakistan information security association committee should arrange some conferences on cyber security for policy makers and spread cyber awareness among common people.

The draft was accepted by other departments and in which it was decided that later it will also be presented in front of assembly and PISA will also present the general draft of Pakistan’s cyber security strategy. It was further decided that all other departments such as defense, military and citizens of Pakistan should come together and play their role in cyber security. After the completion of all the other suggestions, when the legislated draft was presented in the national assembly no further progress was shown on it. Although government and other cyber experts tried their best to make a cyber security strategy, unfortunately they were unsuccessful in it.

## 1.10 A Comparative Analysis of India-Pakistan Cyber Security Strategies

On a national level, Pakistan is not working on cyber security strategy as it should be. From 2013, PISA was trying to draft a cyber-security strategy but up till now it has not been presented. There have been many meetings, conferences but there is no outcome which shows that Pakistan will soon publish its Cyber Security Strategy. Pakistan, the policy makers are more concerned about the digital security of intelligence services. That is why Pakistan established a cybercrime center rather than a national CERT. Pakistan has not shown any kind of positive gesture to provide security to the finance sector from digital frauds. It shows the lack of development by Pakistani policy makers in cyber security.

The 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.

On the other hand, in 2013 India issued its first cyber security strategy. India is not only working on the betterment of its cyber security system, but has also arranged the cyber army exercise with the name of "Divine Matrix". Pakistan is not exercising such sort of activities locally. Pakistan is a nuclear state and it cannot afford any kind of ignorance about cyber security after the example of a Stuxnit attack. Other than that India and Pakistan are a part of information security treaty of Shanghai Cooperation Organization (SCO), but India has signed more treaties and MoUs then Pakistan.

## 1.11 Data Security Laws

The basic aim of data security laws is to handle the security measures for data sharing and transmission. It explains how personal information can be used by the government, any organization and business purpose. Every country is having its own data security laws. Therefore, a comparative analysis of the data security laws of India and Pakistan is quite useful.

### 1.11.1 Data Security Laws in Pakistan

In Pakistan, there is no data protection law present or authority to deal with data protection yet. The constitution of Pakistan highlights the fundamental rights of privacy individuals, but in the electronic transection order 2002, there are no separate authorities who deal with data protection. In section 36, punishment has been specified against those who access private information illegally. Within the ordinance, it is mentioned that the government would establish a proper separate department which deals with electronic documents and gives privacy protection to its users. No practical steps were taken by the government. Prevention of Electronic Crimes Act 2016 also has some laws related to individual data protection. Even the individuals of the state have no right to access the confidential and sensitive information of the government. Additionally, the government

officers are not allowed to share confidential information with anyone else and if they do so, similarly they will be punished by the prevention of electronic crimes law.

### 1.11.2 Data Security Laws in India

India does not have data protection laws. It has agencies which deal with data privacy. The information technology act and rules 2011, give legal rights to every individual about protection of personal information. Prior to accessing the personal information of any person, the government is to inform that person beforehand. The consumer's protection act of 2015, focus on the misuse of private information. Although in 2012 a report was presented to the government of India about privacy. In which it was requested by the experts to make some data protection laws separately. Later in 2017, the Indian government established a committee that gave possible suggestions to give better protection to the personal information. After some months, the committee presented a draft in which they provided the suggestion to get feedback from the Indian public to improve the level of data security, especially personal information. Although till now no separate data security law has been passed by the India government it seems India is very much near to passing the data protection law.

### 1.11.3 Comparison of India-Pakistan Data Security Laws

India and Pakistan both have no separate entity which deals with data protection. But as compared to Pakistan, Indian information technology act and rules are more comprehensive in terms of data protection. The Indian government established a committee which presented a draft related to the right of the privacy act. Indian government has a plan to make proper law on data protection. But unfortunately, Pakistan does not have any kind of draft related to data protection. As per prevention of electronic crime act 2016, the government of Pakistan has the authority to share the private information of a person with any foreign country without the consent of the individual. Whereas If Indian government has a need to use personal information of an individual, the government legally informs that individual; giving India an upper hand comparatively to Pakistan, in terms of providing protection to citizen’s personal information.

## 1.12 Conclusion

In a nutshell, the historical rivalry between India and Pakistan shows three conventional wars. A major transition came in the conflicting ways among states from traditional to non-traditional ways, where South Asia's most prominent states such as India and Pakistan followed the trends and became part of cyber wars. Leading to both countries attacking each other's websites almost on a daily bases.

To deal with these cyber-attacks both countries have their own cyber laws. In Pakistan cyber law gets legislation in very late stages and apart from that many private sectors are opposing the law. In their point of view, the law is gives too much power to the government and government is somehow corrupt, so they are using the law for their personal interests. According to the law the freedom of speech and right of privacy was also being compromised. On the other side, India has a better law in terms of implementation and addressing issues. They also take care of the right of privacy of the citizen and the pathways to follow if the state needs personal information of citizen. They first inform the concerned person about it.

Furthermore, the cyber security strategies of both countries have been discussed and analyzed to see the difference between them. India is one of those states which is very much anxious about its digital security. Indian government established a well-developed cyber security strategy and in which there are different departments who deal with cyber-attacks as per the requirements. But unfortunately in Pakistan, the government is not as concerned as it should be. Although the most sensitive data of Pakistani institutions and citizens are coming under digital attacks, some well-known organizations are involved in the leakage of data. But the government is still unable to establish a cyber-security strategy.

This is followed by a brief comparison of data protection laws of India and Pakistan. This comparison shows that India has an edge over Pakistan in this regard. This is so because India established a committee to draft data protection and is very much near to providing proper legislation to data protection law. Regrettably, Pakistan once again is lagging behind in terms of providing data security to other agencies and the common citizen.

Although, Pakistan is facing more data protection issues as compared to India. In this situation, the government of Pakistan is not the only one who is fully responsible for it. Other sectors or law enforcement agencies are equally responsible. The only way for Pakistan to address the cyber security issue is when both public and private entities will fully participate in making policies regarding digital protection. Then implement the cyber security laws in a more effective way.

# CHAPTER 2
# A COMPARISON OF INDIA- PAKISTAN CYBER CAPABILITIES

Foremost, the requirement lies in highlighting the security challenges facing the world today. The rising global security environment entails risks that are more non-military than military. These emerging risks are interconnected with one another and affect human life in multiple ways. The current world security environment is characterized by complexity. As a leading notion of "comprehensive security," the current most significant global security peril to states is cyber security.[28] It is directly or indirectly threatening the states, societies, nations and even the whole international system. That's how states should provide maximum security to their digital systems to protect them from illegal access.

Like the rest of the world, the South Asian states increasingly face the rising cyber security threat. Particularly, India and Pakistan are the most prominent in this regards. Because of their historical hostility, they are using non-traditional tools to harm each other, between which cyber security threats are on an increase. India is enhancing its information technology for offensive cyber security ability as per the standing point of national security. "It is rapidly establishing itself as a software development capital of Asia."[29] Currently, India is exporting products related to internet that cost US $9 billion and apart from that every year it is producing around 100,000 IT professionals. It is not enough they are also having hundreds of well-prepared hackers operation in India. In which H20 and Hindustan Hackers Organization is very much popular. Because they are attacking on Pakistan from 1999 till yet. A new group called "Indian Cyber Army" is very much active in digital attacks. In 2010, they hacked almost 36 governmental and official sites of Pakistan.

---

[28]Radoslav Lvancik, Pavel Necas and Vojtech Jurcak, "Theoretical View of Some Current Global Security Challenges," *Incas Bulletin,* no. 1 (January 2014): 99.

[29] Muhammad Shabbir, "Cyber Security in Pakistan: Emerging Threats and Preventive Measures," *ISSRA,* no.2 (2013): 25.

Although, it is not the case that Pakistan is sitting silently and doing nothing. Its hackers are also trying to influence on Indian cyber system. In which they also hacked two thousand websites of India and even the most sensitive site like central bank of India. But the major problem with Pakistan is to secure its own digital security. A very good offensive quality cannot provide a strong defense. Here it becomes the responsibility of government, major institutes and stake holders to sit together and make some strong polices to tackle the growing cyber space issue. This chapter compares the cyber capabilities of both states. Moreover, it makes a comparative analysis to determine who has more potential to affect the other.

## 2.1 Indian Digital Capability

For years, and for many reasons, India has been the focus of political, security and defense, economic and technological analysts of the international community. India, from the geopolitical point of view, supports a fragile balance that conditions not only its security and defense but also that of a large part of the Asian continent and, by extension, that of the rest of the world. The territorial and religious conflicts with their neighboring countries, Pakistan and China, as well as the closeness and influence of the war in Afghanistan, together with the need of the 'Western powers' to have a reliable ally in Asia, reinforce its strategic importance. Regarding its domestic policy, India faces very heterogeneous problems ranging from the growing energy demand of an expanding country to conflicts of religious nature between the Hindu and Muslim communities of the country.

On the other hand, in 2020, according to all forecasts, India will be the most populated country on the planet, as well as the second largest world economy and the worldwide new mobile subscriber. In which India already stands on second world's largest mobile market with 310 million new subscribers will be expected till 2020.[30]These predictions have not gone unnoticed by the governments of the United States, Russia or Germany that are working to strengthen their commercial, economic and cultural relations with

[30]Maheen Kanwal, "Pakistan will have 17 million new mobile subscriber by 2020, GSMA Report," *Tech Juice*, April 17, 2017, accessed April 16, 2018, https://www.techjuice.pk/gsma-mobile-economy-2017-report-pakistan-mobile/

India. But what is the role of cyberspace in the present and future complex of India? It is important to shed some light on this role. After the independence from the British Empire, Jawaharal Nehru, Prime Minister of India between 1947 and 1964, gave science and technology a leading role in the identity of 'modern India'. The creation of a network of universities and schools for the training of future scientific and technological talents in the country was one of the first measures adopted by the government. The maximum exponent of this network is the 16 Indian Institute of Technology (IIT) distributed throughout the country. The importance and prestige of IITs in Indian society are reflected in the fact that only one in 50 young people who aspire to be trained in them achieve their goal.

In the same way, India was a pioneer in the creation of technological management and control organisms. In 1975, the Indian government created the National Center for Information Technology (NIC) in order to provide Information and Communication Technologies (ICT) solutions. During the 1986-1988 trienniums, the NIC coordinated and promoted the implementation of India's first three telecommunications networks: INDONET, which interconnected the large IBM mainframes of the Administration; NICNET, whose function was to interconnect all the NIC delegations distributed throughout the country; and Education and Research Network (ERNET), which interconnected the academic institutions that promoted R + D + i in India. In 1998, India was also a pioneer in approving the Internet Act, through which the strategic importance of the Internet for the country's global development was recognized. During the first decade of the 21st century, the Indian government created a set of organizations dedicated to the management and security of its cyberspace. These organizations include the National Information Board (NIB), responsible for the state policy on cyber security; the National Information Infrastructure Protection Center (NIIPC), responsible for ICT security of critical infrastructures in the country; and the CERT-In, the operational center for responding to cyber-incidents.

The International Telecommunication Union (ITU), a specialized institute of United States for Information and Communication Technologies (ICTs) recently published a report on Global Cyber Security Index and cyber wellness profiles of states. In which as

per Global cyber security index India stands on the 5th rank and in a regional context comes on 3rd position. It shows the extent to which Indian government seriously addresses the emerging digital challenges and is working for the betterment of the prevailing cyber security threats.

## 2.2 India's Growing Cyberspace

Current situation of cyberspace despite the historical commitment to ICT and the efforts made by the Indian government, is not infrastructural mature and its level of cyber security is far from a known and controlled state of risk. This reality is common to most of the cyberspace for the rest of the nations, although in the case of India it is even more complex due to its vast geographical extension, its high population and its complex geopolitical situation.

Despite the difficulties, Indian cyberspace is growing at a slow but sustained pace as the following data shows:

- The ICT sector contributed 6.4 percent to India's GDP during 2011, which represents an increase of 33 percent over the contribution in 2006.
- During 2011, investment in R & D & I was 0.7 percent of GDP. Almost 70 percent of this investment was made by the State.
- 149 Internet and telecommunication service operators provide Internet and mobile telephony access to a potential population of 800 million people, approximately 75 percent of the Indian population.
- Ten percent of the population has stable access to broadband. Forecasts put this percentage at 14 percent in 2016.
- India occupies the first places, by a number of users, in such popular services on the Internet as Gmail, Yahoo, Facebook or Twitter.
- During 2011, electronic commerce experienced an average growth of 47 percent compared to 2008.
- According to the Cisco Visual Networking Index, an important growth in Internet traffic in India is expected, going from the current 1.6 Exabytes to 13.5 Exabytes in 2015. From the organizational point of view, the Indian government has a set

of bodies and organizations with competence in the management, management and security of their cyberspace.

Those agencies work in an integrated and coordinated manner under the guidelines of the National Information Board (NIB), a body that brings together representatives of the country's main ministries, armed forces and intelligence services. In practice, each agency works autonomously, which results in a lack of knowledge of the state of the Indian cyberspace, as well as the global, an absence of procedures that allow an effective sharing of information between the different actors involved in national cyber security and an absence of coordinated policies in R + D + i, as well as an inefficient framework of public-private collaboration. At the legislative level, the IT Act of 2008 regulates the powers of the government in the direction, management, control and security of Indian cyberspace, the Copyright Act, all issues related to intellectual property and the Data Protection Act, everything related to the Data Protection.

In the field of education, the Indian government has opted for the recruitment and training of cyber-talent in the IIT of the country. However, this ambitious move has not reached the expected results. Nearly 70 percent of graduates in IT who subsequently pursue postgraduate or doctoral studies in the United States or Europe do not return to India. This is due to the lack of stable ICT projects and, above all, to the exceptional working conditions offered by the main American and European companies and universities. The cyber-conscience policy is not effective either. The lack of resources and the transfer of educational competences to each of the regions of the country prevent the implementation of this policy. In the area of the Armed Forces and the intelligence services, there is cyber security initiatives aimed at the creation of a set of CERT equipped with defensive and offensive capabilities. The Indian armies have cybernetic units but their capabilities are still scarce.

## 2.3 State Support on Cyberspace in India

India’s industry grows rapidly on digitalization making it the most essential nation of cyberspace. After some time India will be in the position to decide the future of many technical giants as is it increasing online population around 450 million. That

makes India a progressive country in terms of cyberspace in either capacity or moral authority to formulate the global digital economy. Modi stressed that modern digital technology is the main mobile (driver) investor in the world economy and is an instrument for the socialization of people with limited capabilities. The prime minister said that in India, young authors of startups or emerging companies seek solutions to everyday problems to improve people's lives. “I invite you to invest in that area and be part of the history of startups in India," Modi mentioned another issue, the threats in cyberspace. “Cyber-attacks represent a great threat especially in the democratic world, and we must prevent vulnerable groups of the population from falling victim to cybercriminals," he warned. In Modi's opinion, "countries must also prevent the digital space from becoming the platform for the dark forces of terrorism and radicalism.

Therefore, a debate about Indian cyber context has been created in a research article written by Atul Kumar and Chiranshu Ahuja with a title of “cyber security research developments global and Indian context”. The writers discuss the emerging cyber security threats with reference to attacks that are affecting states in financial matters. They further explained the different strategies adopted by the states for securing their cyberspace system. In this scenario, Atul Kumar and Chiranshu Ahuja further provided Indian perspective about cybersecurity. Firstly, India tries to provide high economic growth for the welfare of its nation but later emerging cyber challenges become more severe when it affected the national security and economic aspect of the country. Since those global patrons are a foremost factor for the economic enlargement of India. The major attention given to cybersecurity by India is because of maintaining the confidence of global clients. Whereas, supporting the cyber ecosystem, through more attention, assets and capital that are also necessary for cybersecurity. India is investing much in research and development field but a lot more needs to be done with advanced technology occurrence globally.

Consequently, Indian government is paying special attention to the emerging issue of cyber security. For that sake, the world largest conference was held in India. The Prime Minister Narendra Modi institutes the fifth edition of Global Conference on Cyber Space (GCCS). It was the first time ever organized in India, where 124 countries’

representatives and 33 ministerial delegates came from 31 countries to attend the GCCS 2017 in India.[31] In that global event where a number of international leaders, policy makers, think tank or industry expert were present deliberately to discuss the issue of cyberspace and challenges that come from increasing internet usage, showing the concern of the state about the emerging issues.

## 2.4 Evolution of E-Commerce in India

In India E-Commerce is quickly developing the industry. It started from 2013 when consumers in India spend 12.6 billion dollars. The number rapidly increased in 2015 to around 13.31 billion dollars.[32] Two major retailers are in a tough competition in E-Commerce, Flipkart and Amazon. They compete in their aim to interact with small and independent business. Around 90.000 companies are selling their products to Flipkart in India. Major target of the company is to dominate the cash economy in India. Initially, the online transactions were a difficult task for individuals. But in 2011 a rapid boost came in credit card usage from 256 million to 24.5 million cards till 2016. Making Axis bank became the third largest private organization lender in India. According to Sangram Sing, a head of cards clearly said that Axis bank attaches one lakh cards in every month. The fast growing usage of credit cards in India also crafting cyber challenges for the banking sector as well as for the state. Banks are trying hard to adopt suitable policies for their digital system. The state also involved in it, recently in June 7, 2016 the Indian prime minister met with president Obama. In which they discussed the problem of cyber security and both agreed to work cooperatively to improve digital protection in their respective countries.

---

[31]General Knowledge Today, "PM Narendra Modi inaugurate 5th Global Conference on Cyber space," accessed April 2, 2018,
https://currentaffairs.gktoday.in/tags/cyberspace

[32]Minnie Ray Chaudhury, "The Growth of E-Commerce in India: Cyber security and Infrastructural Challenges," *The Henry M. Jackson School of International Studies*, September 12, 2016, accessed April 1, 2018,
https://jsis.washington.edu/news/growth-e-commerce-india-cybersecurity-infrastructural-challenges/

## 2.5 Cyber Security of Critical Infrastructure in India and Pakistan

The critical infrastructure of any country plays a vital role in both economy and society. If it comes under cyber-attacks then the country will face huge impacts. Further on, the researcher analyzes the cyber security measures of both India and Pakistan in terms of its critical infrastructure.

### 2.5.1 Indian Cyber Protection of Critical Infrastructure

Cyber-attacks against critical infrastructure represents one of the major concerns of the Indian government. India has a well-developed center for the protection of its critical infrastructure with the name of "National Critical Information Infrastructure Protection Center" (NCIIPC). In 2014, it was created under the supervision of Information Technology Act 2008. The NCIIPC also came under in the National Technical Research Organization (NTRO). The major purpose of NTRO is to find better measures for cyber security and in the same time period cooperate with other national security institutions. The major objective of the center is to provide protection to national critical infrastructure in more efficient way.

Because both the Indian public and private sectors are equally depending on cyberspace it is quite easy for law makers or policy makers to make good policies for both sectors NCIIPC is not just a protection entity for critical infrastructure but it also coordinates with other stakeholders and their involvement in it.

The growing energy demand of the country contrasts with the obsolescence and vulnerability of the ICT infrastructure of the systems, which must satisfy this demand. Many of the cyber-attacks that take place in Indian cyberspace are perpetrated by groups of hacktivists, national and international, sponsored by countries and criminal organizations. After the terrorist attacks in Mumbai in 2008, the Indian government approved the IT Act 2008, which authorized the government to take those measures it deemed appropriate to prevent criminal activities through the Internet. Recently, invoking the IT Act, the Indian government ordered the mobile telephony providers of the Assam region, in the northeast of the country, to temporarily disable the SMS service in order to

stop the exodus of 50,000 bodos (mostly ethnic minority). In the Assam region) allegedly scared, via SMS, by the pro-Bangladesh Muslim community of Assam.

In addition, the strong rivalry between the two major political parties in India; the Congress Party and the Indian People's Party, is being transported to cyberspace. Both political parties make use of cyberspace for propaganda purposes, which causes radicalization of their discourses, moreover, the proliferation of regional conflicts that confront the country's Hindu and Muslim communities in the border regions, such as Gujarat, Rajastan and Punjab. The extremist thoughts are instilled through such kind of cyberspace propaganda and creating a new kind of enmity between India and Pakistan, where the hackers of both countries are also involved. As Sardar Sikander revealed in his article, "Indian hackers defaced government website as the country marks independence." Indian hackers once again try to create a mess with Pakistan on its independence day. They hacked many vital sites like federal cabinet, law and IT ministries. In which they left the message "Happy independence day- August 15".[33] Such types of digital attacks are creating more vulnerability for the national security of Pakistan.

### 2.5.2 Pakistan's Cyber Protection of Critical Infrastructure

Pakistan does not pay the required attention to the matter at hand; hence, the government sector of Pakistan lacks input in the protection of its critical infrastructure. But under the national cybercrime law as prevention of electronic crimes act 2016, a separate section highlights the digital crime against information, data system and cyber terrorism. As per the section, strict punishment will be carried out against those who access critical information of sensitive infrastructure but no sole department is present to deal with it. In the law of cyber terrorism, it is mentioned that if any one who connects with the critical infrastructure of the country is liable to be punished as an act of cyber terrorism.

---

[33]Sardar Sikander, "Indian hackers defaced govt website as country marks independence," *The Express Tribune*, August 14, 2017, accessed august 15, 2017, https://tribune.com.pk/story/1481375/indian-hackers-deface-govt-websites-country-marks-independence/

Additionally, Pakistan geopolitically acquires a very important position in the south Asian region and also as a nuclear state. Continuous attacks to its critical information infrastructure will badly affect the economy of the country. Pakistan does not have a dedicated department for the security of CII. In 2016, Indian hackers claimed that they had access to the military infrastructure of Pakistan and they have power to destroy the military infrastructure, if the Indian government grants them permission. According to a report related to Pakistan's infrastructure, 40 percent of critical infrastructure under public sector remains under control of governmental institutions, meaning government of Pakistan has a strong hold over private sector.

Later the Hindu newspaper shared an article about "Pakistani infrastructure system vulnerable: cybersecurity expert." In which an official S. Amar Prasad Reddy, Additional Director General said in the seminar on national cyber safety and security standards, we have entered in the critical infrastructure of Pakistan and have the capability to destroy the defense system of Pakistan if our government allows us.[34] Furthermore, he said that if it's imperative, then they can destroy the digital assets of Pakistan and they are capable enough to do this. Besides, he added that for the future cyber protection of their critical infrastructure they needed almost 10 lakh cyber professionals.

## 2.6 India's Policy on Cyber Security

India started working on its IT sector from 1998 and it is continually developing the sector as per the requirements. Indian cyber experts are carrying out meetings with different countries over the world to improve its cyber security strategy, in order to compete with other developed nations in terms of cyber security policy. In 2013, India developed the cyber security strategy as a draft. Yet, India faces a lot more cyber-attacks, giving rise to the question of how will India provide security to its digital system?

How should India face the future of its cyber security? The private sector, the education community and the leading think tanks in India are calling on the government to take the

[34]Special correspondent, "Pakistani infrastructure system vulnerable: cyber security expert," *The Hindu*, November 1, 2016, accessed 26, October, 2017, http://www.thehindu.com/news/cities/chennai/Pakistan%E2%80%99s-infrastructure-systems-vulnerable-Cyber-security-expert/article15419881.ece

lead and develop a strong and effective policy on cyber security. This policy should aim to provide a secure cyberspace and generate a culture of cyber security that enables the social, cultural and economic prosperity of India, as well as its security and defense. The Indian government should create a national cyber security system, that is, a set of bodies, agencies and procedures that allow the direction, control and management of its cyber security. The main experts of the country defend the creation of this system based on the integration and coordination of existing organizations. The National Information Board (NIB), by competencies and means, should assume the role of the central organ of the system. In the same way, this system should be based on a legislative framework, a common work methodology for all the actors of Indian cyber security and a profound modernization of the ICT infrastructure of the country. The Indian digital security system must provide the Indian government with a set of capabilities and resources that make it possible to:

1. Have a reliable and up-to-date knowledge of cyberspace in order to face the risks exposed throughout this article, as well as what may arise in the future.
2. To have agile mechanisms for the sharing of information among the government, armed forces, intelligence agencies and the rest of the actors involved in the country's cyber security.
3. Improve and strengthen the public-private collaboration framework.
4. Centralize and optimize R & D & I policies.

The security of Indian cyberspace is not an exclusive task for the Indian government and society. The global nature of cyberspace requires close collaboration with the international community. For this, India will have to update and renew the agreements on cyber security with other countries. Currently, it has a collaboration agreement with the United States, the US-India Cyber security Memorandum of Understanding. In addition, the Indian government must work to reach similar agreements with the rest of its allies. From the educational point of view, the flight of national talents to the United States and Europe must be stopped. For this, it will be necessary to increase the technical and economic resources allocated to IITs, increase and encourage investment in R & D & I and improve public-private collaboration in cyber security. The cyber consciousness of

Indian society is an essential task. The competences in this matter should be assumed by the central government in order to develop an ambitious early cyber-awareness plan. The Indian government should work to improve the national resilience of the cyber threat and create and foster a culture of cyber security. In short, India's social, political and economic future, as well as its security and defense, is inextricably linked to cyberspace. At present, India is far from being able to face the innumerable risks that cyberspace poses. The national cyber security policy is playing vital role in giving security to the cyber system of the country as compare to any other South Asian state.

### 2.6.1 Indian Cyber Security Challenges

An Indian well known channel, Rajya Sabha with a talk show named “The Big Picture about India’s Cyber Security Challenges” discusses the government’s involvement in cyber security, its challenges and its financial matters. The guest of the show was Arvind Gupta, Head, BJP IT Cell, Karnika Seth, Cyber Law Expert; Srinivas Kodali, Cyber Law Expert; T K Arun, Editor, Opinion, The Economic Times.

Karnika Seth said, now it has become the primary concern of the government or parliament because most transactions are happening digitally. She also added that India needs an amended law because the present law is not sufficient enough to deal with parts of cybercrimes.

Srinivas Kodali said, we need the latest tools for securing cyber space and there are many areas those require a lot more effort. He claimed that the government is just saying that all skate holders are important but in GCCS conference not many civil entities were present to attend that conference, which shows the government words are different from its practical actions. He also added that government should listen to the cyber researchers’ suggestions. Those are not happing yet. Srinivas himself gave recommendations to both local and central level to secure cyberspace but the government has not responded.

T A Arun, says after 2013 cyber security strategy there are some positive changes but these are not enough to fully secure the cyber space of the country. Because cyber system is inter-linked, infecting one computer can affect the whole system. The capacity building

between national security and individual are absent. Although government is complaining that they are working on capacity building. We need international cooperation because if a server is attacked by a transnational actor, there is no jurisdiction to take action against the actor. Within India how can we monitor the cyber trafficking without compromising the privacy of an individual? In the name of national protection of cyber security you can compromise the individual privacy. Although in developed countries like UK or US if you cartel someone's privacy you need court orders, even this is required for securing national security. But in India there is no accountability, you can scope on anybody without informing them.

Arvind Gupta, Head of BJP cell, said the government is very much serious about cyber security issue. The first global cyber conference held in India is the proof of it. India has done a lot of efforts in multiple areas of cyber but fundamentally there are different fields involved such as cyber security, network security and enterprise level security etc. For all those, it is very much important to provide awareness to the common mobile or internet users. The government has launched a missive cyber security awareness program. Apart from that, India has both the support of the state and non-state organization and many individuals are involved in securing Indian cyber system from attacks. Later Guptal respond to Arun claim of individual privacy. He said privacy always being respected by the court but in some exception we compromise due to certain reasons, even in data analyzing without informing to the particular person. There is difference between data level, the data you can access, what you don't and where you can drill more.[35]

In the end it shows that India is progressing in the field of cyber security but still faces a lot of challenges because cybercrimes are one step ahead to the cyber laws of the country. Similarly, India is trying hard with the help of international cooperation to secure it system as much as possible.

---

[35]Rajya Sabha Tv, "The Big Picture- India's Cyber Security Challenge," Published on November 22, 2017, accessed September 29, 2018.
https://www.youtube.com/watch?v=ARmvM_UGq-k

## 2.7 Pakistan's Cyber Capacity

Pakistan seems to be concentrating its efforts on preparing for parity with Indian capabilities in cyber warfare. Pakistan poses a threat to the global network because of its growing population of young hackers. We can see that these are often politically active, they are found in the heart of real-world conflicts. They are active in Kashmir but also in coverage on theaters of operations involving Muslims. It is likely that in response to India, Pakistan is studying a way to more effectively exploiting its human resources in cyber warfare with the aim of causing severe disruption or even collapse of the Indian network. Moreover, according to the current Global cyber security index 2017, Pakistan stands on 23rd in a global context and in the regional framework it stands on the 13th positions along with Samoa. Alongside, Pakistan is also a member of ITU-IMPACT initiates to improve cyber security services. In the opinion of International Telecommunication Union (ITU) study finding, Pakistan has online protection legislation for children as per criminal code section 293. It is accepted without any reservation or declaration of article 16, 17(e) and 34(c) for the convention on the child rights.

It is to prevent the trafficking of children, child pornography and children prostitution. But the main problem is the lack of institutions which could support the implementations of this legislation. Furthermore, there is no agency who could take the responsibility for such issues and even in case of online child protection no mechanism is introduced to report these incidents. Apart from that, Pakistan hackers are ranked on 3rd position among world top hackers amongst whom, Shmeer Amir an ethnical hacker, is now earning almost $150,000 by reporting bugs in 300+Global organizations.[36]

## 2.8 Increasing Use of Cyber Space in Pakistan

Pakistan stands on 9th rank according to United Nation globally developing digital economy. From 2012 to 2015 for the first time almost 16 million Pakistani internet users went online. As per expectation in 2020 the number will be reached around 17 million.

[36]Samir Yawa, "One of the World best Hackers is from Pakistan & has Made 1.5 Crores in Bounties alone*," Pro Pakistani*, July 15, 2016, accessed April 5, 2018, https://propakistani.pk/2016/07/15/one-of-the-worlds-best-hackers-is-from-pakistan-has-made-1-5-crore-in-bounties-alone/

Till 2013 almost 30 million internet users in Pakistan which included 15 million use smart phones for web browser. As per survey Pakistan stands on 5th leading mobile market in Asia.[37] Additionally, Pakistan rank on second in developing internet user in SAARC countries. The current development of cyberspace in Pakistan is producing more productive and innovative business. That is why it has become the responsibility of the government to take maximum security measure to protect their digital systems.

## 2.9 Critical Infrastructure in Pakistan

Few years back, the use of cyberspace was an exceptional innovation, in which inter-connection among states as well as between public was very much popular. The developed states wanted to get rid of the manual system of critical infrastructure for upgrading their national economies. They shifted their manual system to digitalization. But the digital system is vulnerable by nature because of cyber-attacks. Furthermore, as per global trend Pakistan also adopted that system. The major critical infrastructure of Pakistan on cyberspace is hospital, military establishment, nuclear sites, NADRA, banking sector, educational institution, election commission of Pakistan, emergency services and many more other sites. Those are having their sensitive and confidential data available on internet. But unfortunately most of the critical infrastructure sites are being attacked. Now it should be the chief concern of the government of Pakistan and policy makers to take cyber security seriously because it can affect the national security of Pakistan.

## 2.10 E-Government in Pakistan

E-Government is also called digital government or electronic government. The basic purpose of it is to provide services to other governmental agencies, customers, and employees through electronic ways. The word E-Government was first presented when the computer was used in governance throughout the globe.[38] The government of

[37]Web Desk, "30m Internet user in Pakistan, Half on mobile: Reoprt," *The Express Tribune*, June 24, 2013, accessed April 17, 2018, https://tribune.com.pk/story/567649/30m-internet-users-in-pakistan-half-on-mobile-report/

[38] Sayyam Malik, "E-Government in Pakistan: Prospects and Challenges," *Pakistan kakhuda Hafiz*, February 3, 2017, accessed, April 3, 2018, https://www.pakistankakhudahafiz.com/e-government-pakistan-prospects-challenges/

Pakistan established e-government directorate under the ministry of IT. In 2000 the first National IT policy and action plan were approved by the federal cabinet. Since the year 2000, Rs. 3.68 billion funds in IT sector was utilized by the ministry. In which Rs. 281 million was specifically used in E-Government. Pakistan is trying hard to improve this sector according to the requirement of the world. In 2008 and 2010, according to UN, e-government world survey ranked Pakistan 131st and 146th respectively.[39] However, the South Asian region as per 2010 survey is still far away from world average e-government system.

### 2.10.1 Major Sectors of E-government

There is three basic sectors of E-Government.

- Government to Government (G2G)
- Government to business (G2B)
- Government to citizen (G2C)

### 2.10.2 Basic Goals of E-government

Following are the goals of E-Government in Pakistan.

- Increasing the effectiveness of the government.
- Enhancing lucidity and decision making liability.
- Increasing public service delivery in more cost effective way.

On the other side, there was one more purpose of E-Government in Pakistan. If you have to visit some governmental office even for a simple work, that is somehow not possible without the involvement of a degree of corruption. One purpose of E-Government in Pakistan is to avoid corruption especially in legal task fulfillment. Here some of the key success factors of E-Government in Pakistan.

- Top level sponsorship.
- In time availability of funds.
- A better relationship between private as well as public sectors.

---

[39]Muhammad Ilyas, "E-Governance Practices and Models; Options for Pakistan," *ISSRA*, no.1 (June 2016): 43.

- Permitting amendments torun laws and rules.
- Online payment of bills.
- Online shopping, booking of tickets.
- Transformation of money.
- Online business opportunities.
- Increasing the potential of government.
- Sharing important information with other official institutes.
- Most importantly keeping all records of the country online.
- The other major purpose was to increase public interest in the policies of the government and keeping them updated about coming projects and plans.

## 2.11 Challenges for E-Government in Pakistan

Now E-government is a foremost element of modernization in Pakistan. There are many governmental organizations active on E-government services and trying to provide fast favor to their customers, but disappointedly they do not have a proper mechanism to prevent illegal access. That's why in 2015 most of the E-government sites were infected. The most dangerous attack happened by NSA (national security agency) of the USA in which they stole the 13.5 billion pieces of confidential information of Pakistan. Such events occur due to the non-existing law on cybersecurity and this is one of the major causes of growing digital crimes in Pakistan. Besides now, the policy makers of Pakistan need to develop a suitable framework for cybersecurity purpose. Because there is already a cyber-war going on between India and Pakistan, hence, it is essential for Pakistan to provide security to their cyber system from Indian criminal access.

Moreover, other challenges in e-government are the low literacy rate in Pakistan. People are unable to use the services. Then management issues, like systems are not updated as per requirement. Furthermore, the network security and security of private data from unauthorized access, low level of collaboration between the institutes and training their employees. Most importantly a high level of digital specialists is required to manage the system.

## 2.12 E Jihad and its Impact on Pakistan

Many terrorist organizations are using social media for increasing the idea of cyber jihad. When a cyber-conflict is initiated, a situation arises where many parties are willing to actively help one of the sides. Temporary alliances are formed between disparate groups. Individuals from many parts of the world may be involved. There are signs that Islamic hacker movements from different countries and regions are organizing themselves and directing their activities at servers and websites in the Western world, and primarily at Israel.[40]

Governments are warned to be attacked by Al Qaeda through the use of internet technology. Therefore, states are remaking the strategies to counter terrorism, with which they are using more sophisticated technologies to check the social media activities to prevent repetition of cyber terroristic events such as 9/11. When terrorists used the internet for communication to share their further plan for attacking USA. Al Qaeda was not as much strong organization after the death of their pivotal leader like Usama Bin Laden.[41]

In Pakistan social media is not just a platform for expressing your opinions. It becomes a battlefield between two schools of thoughts. One is liberalism and other is extremism. Liberalists are focused upon the promotion of democracy, freedom of expressions and fulfilment of mandatory rights whereas; Extremists have a different agenda for using the internet and social media websites. They use it to spread their messages, to change the public opinion about government if it is not fulfilling the demands of extremists, online recruitment and most importantly to create confusion about Blasphemy law.

---

[40] Niklas Granholm, Madelene Lindström, and Johannes Malminen, ed., *China's Globalization of internet Affairs: Tibet and Xinjiang in world Politics* (Strategic outlook, 2010),1-112.

[41]"Facebook and other Social Media 'use for Cyber Jihad'," *BBC News*, July 12, 2012, accessed August 17, 2018,
https://www.bbc.com/news/uk-politics-14126514

### 2.12.1 Blasphemy Laws

In 2010, when Facebook announced a competition to "Everybody Draw Muhammad the high court of Pakistan made a Blasphemy law to ban social media sites like Facebook and YouTube. It was banned because of its disrespectful content. It was an American comedy center in which they celebrated "Everybody Draw Muhammad" to show the expression of so called freedom of speech. "South park" part in which they showed a character wearing a bear costume and it was called Muhammad. But American cables and television center censored the part from broadcasting because they faced threats of death from extremist groups. Many Muslim countries and Al Qaeda stood up in opposition. Facebook administration said that the page content is not violating their terms. Although Facebook administration agreed that the content is not legal in some countries. But they did not remove the page from Facebook. Radicalization and extremism have increased in Pakistan. Therefore, the Pakistani embassy in Washington D.C put the request to the government to take effective steps and remove the content from Facebook page. As a result Facebook apologized from Pakistan and they stopped the access to the page from Pakistan.

The two schools of thought; liberalist and extremist, supported different opinions on Facebook and YouTube ban creating a difficult and dangerous conflicting situation in Pakistan. Liberalists were against the content but they were not in the favor of a total ban. Due to some pressure the ban was lifted after two months. As a consequence the extremists group launched their own page with the name of "Millat facebook."

### 2.12.2 Millat Facebook Page and its Impact on Pakistan

After the ban was lifted from Facebook, those extremist groups continued the cartoon issue on social media. In which they almost attracted 7,000 members and mostly from Pakistan. After one year, the admin of millat Facebook, Omer Zaheer arranged a conference in Islamabad. In which mostly religious scholars were invited. They announced a boycott of the products of those countries that were supporting disrespectful content on Facebook.

Creating a problematic situation for Pakistan as the extremist group started spreading misunderstandings and propaganda against Pakistan. Subsequently, it showed that these extremist groups in Pakistan used social media platform for their own interests and ideology. Liberalist school never used its power for social change as the extremists did. Salmaan Taseer murdered case was the best example of extremist ideology. In which Salmaan Taseer, a Governor of Punjab was gunned down by his own security guard Mumtaz Qadri. As per Mumtaz belief Salmaan Raseer was blasphemer because he broke the rules of Blasphemy law of Pakistan. Mumtaz Qadri after the murder and surrendered himself to the police with the statement that he feels proud to kill Salmaan Taseer.[42]

Once again it created a divided situation between the opinions of people. Some English newspapers were condemning the murder and other Urdu newspapers were in his favor. The radicalized parties took benefits from the situation and entitled Mumtaz Qadri as a ghazi. Many religious parties rallied in his favor. His supporters were not only limited to street strikes. They also took their extremist ideological combat on Facebook.

### 2.12.3 India's Accusations and Pakistan's Protracted Cyber Attacks

India is claiming that Pakistani military groups are spreading cyber jihad in India. Due to those cyber jihadi groups, they send threatening text messages to leave the place. Otherwise they will be attacked. Therefore almost ten thousand people were forcefully migrated. Indian officials also said that they have identified the number of terrorists groups those are involved in cyber-attacks from Pakistan and Bangladesh. In which harkat ul jihad al Islami (HuJi) and Jamat e Islami are most prominent.

But officially Pakistan is denied such kind of news. As per the Pakistani opinion the picture shown in newspaper is not migrating people. India is just manipulating the situation through false images. The, pervious interior minister of Pakistan, Rahman Malik, said that his Indian counterpart told him that false text messages were produced in Pakistan. However, the foreign officials of Pakistan said the claim was baseless. There was no reality to it.

---

[42] Dr. Faizullah jan, "Social Media and Cyber Jihad in Pakistan," *Islamic Research Index*, (June 2016): 34-47.

Furthermore, a security analyst and senior official of RAW intelligence agency said that these cyber-attacks are some kind of "Psychological Jihad". Through this, these cyber jihadi are trying to cause a disorder type of condition in India. However, these psychological attacks are very much hard to control. India blames that military groups are connected with Pakistani jihadists, who are backing the cyber jihad campaign in India. But still there is no proof that Pakistani government is also with them and supporting them.[43]

It generates a very thoughtful situation for Pakistan. That even without proper evidence India is directly blaming Pakistan. It can globally affect the image of Pakistan, although globally states already have a negative perception about Pakistan and its link with terrorist organizations. Pakistan is being considered a hub of terrorists. Such kind of claims also creates more troubles for Pakistan. Especially in the process of developing good relations with others and portraying its better image to the entire world.

### 2.12.4 Thriving use of Social Media in Pakistan

Last couple of years, the use of social media is rapidly growing in Pakistan. Till the end of 2012, more than 114 million mobile subscribers were in Pakistan. Due to that mobile development Pakistan stands on 9$^{th}$ number on countries level and in regional level it stand on 5$^{th}$ position. In which 20 million internet users are coming online through their cell phones. Still the remote areas of Pakistan are unable to access internet, because of no broadband services. But government is not working on the growth of broadband services in Pakistan. It is not the only problem. The major issue is the increasing Facebook users in Pakistan. Within six months one million Pakistani got registered on Facebook. 55 percent youth is involved in it between the ages of eighteen to twenty four. It is shows that how youth are becoming active in social, political and religious matters through internet. That is creating a terrible scenario of Pakistan because cyber terrorist organizations are especially targeting the youngster to spread extremism in their

[43] Dean Nelson, "India blamed Pakistan for "Cyber Jihad" designed spark ethnic strife," *The Telegraph*, August 21, 2012, accessed August 16, 2018, https://www.telegraph.co.uk/news/worldnews/asia/india/9490007/India-blames-Pakistan-for-cyber-jihad-designed-to-spark-ethnic-strife.html

countries. In case of Pakistan where already terrorist organizations are very much active they can take benefit from this situation. They can hire maximum users from Pakistan to expand cyber jihad in their country as well as they spread the extremist ideology throughout the world. It is very much thoughtful movement for Pakistani government to engage its youth in some other side. So they can separate them from becoming members of any extremist cyber jihadi organization.

## 2.13 Issue of Cyber Security in Pakistan

In current time everything which is available on the internet is hackable. In that scenario, mostly digital sectors of Pakistan are vulnerable. Because the system is not as strong as it's required to be. As the finical sector is the most sensitive sector of any state. States try to give maximum protection to that sector. But in Pakistan, that sector is the most vulnerable due to lack of preventative measures. Couple a months ago, the latest cybercrime attack happened on a well know bank of Pakistan, Habib Bank Limited, where 599 accounts were hacked through ATM cards and Rs.10.2 million were stolen in china.[44] It is perhaps the negligence of the national institutes, government and banks that they are totally unable to address these kinds of online attacks. Some months before in Karachi, some Chinese national was caught installing skimming devices in ATMs of Habib Bank. Most recently Islamic bank was targeted, the most devastating attack. In which they lost millions and the hackers targeted debit cards users. The users claimed that money was withdrawn from their accounts, without their knowledge. First Islamic bank tried to deny the incident but after acknowledging the seriousness of the attack, they spoke about it.[45]Now Pakistan required a proper mechanism for banking sector security and some of the opinions related to cyber security issues related to Pakistan are discussed below.

---

[44]Zubair Ashraf, "In Pakistan, Banking Sector Most Vulnerable to Cyber Attacks," *The News*, December 18, 2017, accessed March 15, 2017,
https://www.thenews.com.pk/print/257280-in-pakistan-banking-sector-most-vulnerable-to-cyber-attacks
[45]Aamir Attaa, "Here's how and why bankislami Accounts were hacked," *Pro Pakistani*, October 31, 2018, accessed November 2, 2018,
https://propakistani.pk/2018/10/31/heres-how-and-why-bank-islami-accounts-were-hacked/

Mahir Mohsin sheikh gives his opinion in his article “Cyber Security: not being taken seriously in Pakistan” which explains that Pakistan is one of those countries who is increasing their access to information but the very next challenge for Pakistan is how to protect the information from cyber-attacks. The government of Pakistan and other organizations are at high risk of cyber threats due to lack of awareness of sophisticated technology. This suggests they are not securing parameters for the protection of their data from cyber-attacks. Pakistan is a reactive nation rather than proactive, in case of cybersecurity. In the banking sector, the ATM frauds are so easy, hackers install skimmer devices in ATM machines to hack card details and withdraw money from other people’s accounts. But banking sector does not worry about cyber-attacks because of having insurance policies as they can easily recover the loss. In the end, he suggests that in Pakistan there are many talented youngsters involved in hacking. Their expertise can be used positively in research or in the development sector. So they can help Pakistan to secure its cyber system.

Furthermore, the most sensitive site of Pakistan is National Database and Registration Authority (NADRA). Which has the private information of Pakistan public? That was also hacked by hackers and they left the message that next time you just wait for the bigger damage. Later Muhammad Ali Raza talks about the incapable services of national database and registration authority (NADRA) in his article “PKNIC Hacker Claim to Have Access to NADRA and FIA Servers” which Raza said that Pakistani hackers claim that the private data of NADRA is easily accessible in which all NICs personal and private data of Pakistani citizen is available. So it’s NADRA’s duty to secure the system from such type of illegal access. Pakistani hackers also claim that many major sites of Pakistan are not secure; they are accessible so it’s a great threat for Pakistan. This means when data is easily accessible for others in that case, the national security of Pakistan is undermining because as personal data is not secure from cyber threats.

Moreover, many Pakistani Governmental sites are available on the internet. They are most important sites of Pakistan. But their protection system is not as stronger as it should be because often these sites get hacked. Recently on 70$^{th}$ Independence Day of Pakistan, many governmental sites were hacked by Indian hackers. After hacking, they

posted Indian flag and national anthem on these sites.[46] In which they hacked the following sites: Ministry of defense, Ministry of information and technology, Ministry of water and power, Cabinet division, Ministry of food security and Ministry of environment change.

Furthermore, Talha Khan gives his opinion about Pakistani cyberspace vulnerabilities in his article "Cybercrimes: Pakistan lacks Facilities to trace Hackers." Which he describes that Distributed denial of services (DDoS) events taking place more efficiently in first six months of 2014 these attacks were double as compared to 2013. DDoS attacks now become a global threat, countries trying hard to resolve this issue. Where Pakistan is very much far behind to deal with this increasing issue, hackers from all over the world are launching attacks on Pakistani websites. Those attacks usually belong to the federal government, officials or security forces and later they leak the sensitive data. Even federal investigation agency (FIA) is the country leading watchdog of cybercrimes, lacking valuable capabilities to subsist these attacks. One of the officers said that country needs to work on its capacity building and till now no serious work has been done on cybersecurity. On a daily basis, Pakistani websites are being attacked and these attacks were initiated from India. As a result, most suffering sectors are private businesses, banking sector and BPO companies. The government of Pakistan needs to pay more attention to the rising issue and try to provide maximum security to these sectors.

## 2.14 Ransomware Cyber Attacks on Pakistan

Ransom ware is a kind of virus that affects the system in a dangerous way. In recent time period, it affects the global system. The researcher will provide analysis on what is ransom ware and how it works to affect the system further on, the extent of effects upon Pakistan.

[46]Mubashir Zaidi, "Major Pakistani Government Sites Hacked on 70th Independence Day," *The Hindu*, August 14, 2017, accessed April 4, 2018, http://www.thehindu.com/news/international/major-pakistani-government-sites-hacked-by-indian-hackers-on-70-independence-day/article19493079.ece

### 2.14.1 What is Ransomware?

Ransomware is a kind of malware which prevents or limits the user to access its own system. Where hackers do two kind of thing, they lock the computer screen or they lock the whole data. The user is totally unable to access the computers data till they pay the ransom.

### 2.14.2 How does it enter the System?

There are number of ways through which it can enter the system. The most common method which is practiced in ransomware is to send a spiteful link to the user. When users open the malicious link then the virus directly enters into the system. It is also called phishing. It can also be attached with a file that you download from a site. After completing the downloading process when the user opens the file then malware automatically enters the system. Sometimes users visited a website that is already malicious in nature, and then it can affect the system. But most commonly method was used in ransomware attack was phishing emails.[47] After locking the system hackers used a different way to get the payment. They asked for bitcoin currency to pay the ransom.

### 2.14.3 What is Bitcoin?

Bitcoin is basically a cryptocurrency that was created in 2009. Satoshi Nakamoto was the person who generated it. The main purpose of inventing bitcoin was "a new electronic cash system" which has "completely decentralized with no server or center authority". There is no other authority like government, bank or other institutions that regulate it. Because it's digital currency and its owners are unknown. A person can buy or sell these bitcoin through encryption keys.[48]

---

[47]TR Pakistan, "Global Data Held Hostage through Ransomware," *MIT TECHNOLOGY REVIEW*, May 15, 2017, accessed August 17, 2018, http://www.technologyreview.pk/global-data-held-hostage-ransomware/

[48]Justin Jaffe, "What is Bitcoin? Here's everything you need to know blockchains, bubbles and the future of money," *CENT*, February 12, 2018, accessed August 17, 2018, https://www.cnet.com/how-to/what-is-bitcoin/

### 2.14.4 How does it affect globally?

Ransomware was a horrible cyber-attack also called WannaCry. Within two days nearly 200,000 computer systems came under WannaCry ransomware attack and almost 150 countries got affected.[49] Mostly well-known companies around the globe were complaining to be attacked by WannaCry attack. In which they have no other option rather than paying ransom in form of bitcoin. After paying bitcoin the user will be able to get back its computer data. Otherwise hackers will simply delete the entire data of the effected computer. Microsoft was claiming that ransomware attack affected only those computer systems of which windows were not updated. Because once malware entered into the system the user has two ways to get back data safely. One to pay required ransom otherwise recovers your entire data from offline backup.

### 2.14.5 WannaCry Effects on Pakistan

Pakistan is also one of those counties who became the target of this WannaCry attack. As per the report published by Microsoft that Pakistan is in top countries of the world after Bangladesh who's computer system is most attacked by malware. It is quite terrible movement for Pakistan because 25% computers in the whole county were attacked by Malware. Apart from this the most amazing thing in the report was that almost 85% computers in Pakistan are not having security software in their computers.[50] It shows that how much Pakistan needs to work on the particular field. Here government is not the only one that is responsible for that but the people should also play their role in it. Educational and other institutes arrange some workshops regarding cyber security awareness. So they can not only secure the professional data but also be able to secure their personal systems as well.

---

[49]Jeffrey Born and Martin Dias, "Global Ransomware Attacks: The impact and the response," *D'Amore-Mckim school of business*, May 18, 2017, accessed August 17, 2018, http://www.damore-mckim.northeastern.edu/news/2017/05/18/14/59/global-ransomware-attacks-the-impact-and-the-response

[50]ProPak Staff, "One in the four computer in Pakistan are attacked by Malware: Microsoft," *Pro Pakistani*, September 19, 2017, accessed August 17, 2018, https://propakistani.pk/2017/09/19/one-four-computers-pakistan-attacked-malware-microsoft/

## 2.15 Institution's Lack of Preparation on Cyber Security

Pakistan is one of the developing states expanding their reliabilities on cyberspace. Mostly institutions are getting digitalize. But when we analysis the protection measures regarding cyber security, it is rather weak. As Pakistan's very sensitive institutions easily get hacked. Like government sites, banking sector and Nadra. Recently a seminar was organized by the Institute of policy studies, Islamabad with the title of "cyber threats: implications on national security". That was chaired by Ambassador (r) Ali Sarwar Naqvi, executive director, a center for international strategic studies. The main speakers were included Dr.Tughral Yamin, Syed Muhammad Ali, Dr Nadia Khadam and Ammar Jaffri. Dr Yamin said in his presentation that Pakistan lagged behind in security landscape in comparison to its neighboring countries like India and Iran in the form of leadership, infrastructure, and suitable legislation or well-designed policies to retort any kind of digital offensives. But in case of Pakistan "There is no designated lead agency in Pakistan at present which is responsible for cybersecurity in the country." Furthermore, he suggested that Pakistan, as stated by Snowden's leaks, is the second most spied country in the world. Due to this Pakistan should develop national cyber command or recruit cybersecurity forces like US and India. As Dr. Yamin informed that now India is planning to hire half a million IT professionals for cyber warfare in future. After that Mr. Jaffri also provided some suggestions in terms of cyber vigilance. According to him, stakeholders will cooperate with each other to develop a mechanism to fight against rising cyber world threats. Besides, he argued that government of Pakistan should invest more in capacity building of youth and provide them better equipment that they utilize their talent and come up with better solutions. Because when India is trying to strengthen its cyber landscape from illegal access so Pakistan also need to pay more attention in IT field and develop better digital infrastructure.

Later in the DAWN newspaper's staff reporter provided some authentic opinion of well-known personalities about government flows to handle cyber-attacks in the article "Government not Prepared to Handle Cyber Threats: Experts." The government of Pakistan and other stakeholders should require takes defending steps against the responsible attackers. According to the executive director, CISS retired Ambassador

Sarwar Naqvi said: “Cyberspace is an area where vulnerabilities of states against sub-state actors trying to achieve political objectives have become more apparent.” Furthermore, Mr Jafri, who heads Pakistan Information Security Association, said that law enforcement agencies should focus on gaining expertise in forensics for improving their capabilities in tracking criminals and to make such type of mechanism for dealing with internet attacks? Then the defense analyst Dr. Raffat Hussain made a point that cyber war is more attractive for attackers because here the criminal can hide his identity so Pakistan needs to create more sophisticated offensive defense in cyber warfare. At the end of the article, some experts share that the unintentional cyber war occurs between India and Pakistan. For this SAARC member must get together and do some serious work on cybersecurity.

## 2.16 Pakistan’s Policy on Cyber Security

Pakistan has regularly overlooked the cybercrimes portrayed by India. A state like Pakistan needs proactive developing and evolving mechanism to certify the cyber security on a national level. Government is trying to play its role in digital security and presented legislated draft in national assembly but unfortunately no further progress was shown in it. Then the NSA advisor wants to make some implementations to establish the National Pakistan Computer Emergency Response Team PK-CERT. it may be a combine retort structure of Government, military and the private sector. The major aim of the PK-CERT is to offer state of the art digital security services to Government, military and private institutes. The other most important concern is to be more reactive on the critical incident and fight back in more effective ways. Here Pakistan needs to start PK-CERT center in provincial level and it plays the role of a bridge between international CERTs for sharing better practice. Moreover, spread cyber security awareness in both public and the private sector.

## 2.17 Conclusion

In conclusion, it is analyzed Pakistan and Indian digital capabilities or lack in the cyber system. Where we see that how much Indian government taking digital threats seriously and make better policies to assure the digital system from illegal access. Even

they are planning to expand their IT sector and hire a more cyber professional. On the other hand, digitalization of critical infrastructure is rapidly increasing in Pakistan. But the Pakistani government is not paying much attention to cyberspace threats. The government of Pakistan is making laws but their implementation is missing. That shows Pakistan lagging behind from India in cyber security procedures.

As per Global cyber security index report, India stands on 15th and Pakistan on 23rd position in terms of global cyber security. On the regional level of the global cyber security report, India ranked 3rd and Pakistan at 13th.[51] According to that report, Pakistan has a lack of criminal legislation. Because the state does not have a single national permitted official and any sector which fulfils the international recognized standards of cyber security. There is no national authentic institute which certified digital security framework. Moreover, in Pakistan, there is no cyber security strategy accepted by official side. There is no national agency who takes the responsibility of cyber security. Furthermore on capacity building, no recognized states institute or R&D program or even project which gives better guideline or practices to meet the standard of cyber security. Although Pakistan officially accepted PK-CERT as cyber security repose team in reality still it is playing a very much limited role to spread cyber security awareness among public services. The major cyberspace sector was under the control of the governmental sector and only 40 percent was controlled by public sector. But government itself has no institution for the protection of its critical infrastructure.

On the other side, India has cyber-criminal legislations that include the penal code and the information act regarding digital crimes in the country. Indian CERT is officially acknowledged as CERT-IN. India also has a comprehensive cyber security policy. The Indian government makes the cyber security policies implications as a mandate in government institutes according to Information Security Management System (ISMS). Even the guideline of the Five Year Plan on Information Security also achieves the Global standards.

[51]Ahmed Raza, "Securing Cyberspace for Pakistan," *Technology Review*, accessed April 6, 2018, http://www.technologyreview.pk/securing-cyberspace-for-pakistan/

# CHAPTER NO 3
# INDIAN CYBER THREAT TO PAKISTAN

India and Pakistan do not have good relations from the beginning. In the past, they fought conventional wars but now there is an alteration in the international benchmark. States prefer nontraditional ways to harm each other. That's why digital warfare is becoming a popular phenomenon among states. Similarly, India and Pakistan also are a part of the digital warfare. Both are hacking each other important sites to get benefits from it. Here, we will compare the cyber capabilities of both states and followed by analysis to show how India is showing more cyber security threats towards Pakistan.

## 3.1 Threat to Pakistan's Digital Nuclear Security

Nuclearization in South Asia creates deterrence between India and Pakistan. Because it was gauged that nuclear weapons can ultimately bring peace and security in this region. This approach worked in the time of kargil war, boarder standoff in 2001, 2002 and in Mumbai attacks. The major crisis happened but both states restrained themselves because they knew very well the after effects of a complete war.

Nuclear weapon states face a great threat for non-nuclear states, regional states and even for international peace and solidity. In the case of South Asia, many schools of thoughts declared the place is the most dangerous place in the contexts of nuclear proliferation. Because of their political and economic usability, terrorism, extremism is very much common. On the other hand, the growing number of nuclear weapon in both countries are maintaining balance as well as creating a challenge for their future stability and peaceful situation.

For all these reasons, it is essential to pay attention to the nuclear situation in South Asia. However, as Islamabad and New Delhi are unlikely to halt the development of their nuclear weapons, given the long history of antagonism and distrust between the two sides, can anything be done to reduce nuclear risk in the region? Yes, we can highlight two types of initiatives with the potential to improve nuclear stability in South Asia.

- First, New Delhi and Islamabad could initiate bilateral cooperation on nuclear security.
- Secondly, the two parties could - with international help - seek to improve nuclear cyber security in the region. In turn, in one way or another India and Pakistan could make commitments in relation to the Comprehensive Nuclear-Test-Ban Treaty. A constant concern in South Asia is that terrorist groups gain access to nuclear materials, either for use in attacks or as negotiating elements against New Delhi or Islamabad.

According to the Nuclear Threat Initiative and its nuclear safety index, the work of both India and Pakistan in safeguarding their nuclear materials leaves much to be desired. However, in recent months, both countries have taken some promising steps. Before the fourth and last Summit on Nuclear Safety, which began in March, Islamabad ratified the amendment to the Convention on the Physical Protection of Nuclear Materials in 2005. At the same summit, New Delhi made commitments in relation to nuclear smuggling and other issues. For its part, in June, India committed itself to an important initiative known as the Joint Declaration for the Improvement of the Implementation of Nuclear Safety.

Even so, India and Pakistan face risks related to the safety of nuclear materials in their territories. Bilateral and cooperative mechanisms to address these challenges could benefit both parties, but at present this cooperation is minimal. It needed the framework for cooperation on nuclear safety that encourages the two sides to share best practices, knowledge and intelligence, and to carry out joint exercises of the police forces.

Fortunately, an existing format for nuclear confidence-building measures could be adapted to integrate a bilateral mechanism for the improvement of nuclear safety. Unfortunately, efforts to build trust in the subcontinent are usually interrupted by terrorist attacks in Indian Territory. The 2008 Bombay bombings resulted in the suspension of nuclear confidence-building measures for many years, and this year's Pathankot attack led to a stalemate in bilateral talks on a number of issues. Therefore, it is essential for India to strategically dissociate nuclear security from terrorism. Otherwise, it is unlikely that steady advances in nuclear safety can be made.

Improvement of cyber security, the subcontinent faces an urgent need to increase its capacity in terms of cyber security. The weak cyber security infrastructure makes the nuclear facilities of both countries vulnerable; neither India nor Pakistan has adopted the strong cyber security measures that their nuclear facilities require. India developed a national cyber security policy in 2013, but this is limited to exposing a broad view of cyber security, without establishing the type of detailed plans that require cyber security threats. For its part, Pakistan passed a cyber-security law in August, but the law has more to do with restricting the spread of extremist ideology than with protecting nuclear sites.

Of course, it is hard to imagine Pakistan and India cooperating on cyber security amid the frequent cyber-attacks that flow across the border. In addition, no country has the economic resources necessary to make the large investments required by reliable cyber security infrastructures. To be able to anticipate the latest threat scenarios it is necessary to make constant updates, so cyber security is a very expensive issue. However, cyber security in the subcontinent could be improved if the international community, led by the United States, helped ensure that South Asia's nuclear facilities are safe from, for example, a Stuxnet-style attack by hackers or groups terrorists. That was the most dangerous digital attack of the history in which Iranian nuclear facilities Natanz were targeted by the US and Israel. As per reported a rough destruction was about a fifth of Iranian Nuclear centrifuges was destroyed. But that was not the only attack on Iran, the first Stuxnet attack was just the detection of knowledge. Later after a couple of years, the second Stuxnet attack happened. What was actually considered the first cyber-attack? Later details were revealed that the effect of the first attack was much larger than the second attack where the hard components of computer were also effected. This shows that cyber attacks not only effect digitally  but also damage physically.

A couple of months ago, India and the United States signed an agreement aimed at improving cooperation between the two countries regarding best practices in cyber security and the identification of cyber threats. It is the first framework of this type established by either of the two countries. That automatically creates a sense of insecurity for Pakistan because last time the US attacked Iran with the consensus of Israel. Now it can use India for a similar purpose. As Pakistani Cyber Security system is not as strong

as Indian or the US digital security system. Pakistan needs more efforts to secure its system for such kind of dangerous future attacks.

## 3.2 Cyber Espionage between India and Pakistan

Espionage is as old phenomena as human history is. In the previous time period, states send their agents to other states to obtain private and confidential information. Cyber espionage is quite new among states. Cyber espionage can be defined as "The use of information technology systems and networks to gather information about an organization or a society that is considered secret or confidential without the permission of the holder of the information,"[52]

Cyber espionage is a kind transformation in a global system which follows the traditional conflicts in the much more effective way. In cyber espionage, the tangible boundaries among countries become a blur.[53] That way many governments get an advantage from it. They hire hackers from a different corner of the world and get confidential information without exposing themselves. Thus the cyber espionage is also called a new sort of cold war.

In current times, Cyber Espionage is not very much of a new phenomenon among states. But it is affecting states both politically and economically. These are some common tools used for cyber espionage.

- Malware attacks
- DDos attacks
- Viruses
- Worms
- Trojan Horses

[52] Frenklin D. Kramer, Stuart H. Starr and Larry K. Wentz. ed, *Cyber Power and National Security* (USA: National Defence University Press, 2009), 440.
[53]Emily Skahil, "War Games: Cyber espionage and the new 'Cold War'," *Brown Political Review*, January 6, 2018, accessed August 16, 2018, http://www.brownpoliticalreview.org/2018/01/war-games-cyber-espionage-new-cold-war/

With the help of these tools, hackers can use very much limited sources and can destroy or target larger. In cyber warfare the most complicated thing is to identify the cyber espionage. Throughout the world, states are carrying out cyber espionage.

Even the United States is building the largest espionage base in the world but not only the United States and China use this battlefield to wage a modern war, nor the first ones. The first data that one has of a cyber-war was between Russia and Georgia when territories were disputed in 2008.There are groups that specialize in attacking Israeli sites that had a lot of activity during the weekend attacking and defaceando (changing the home page) of dozens of sites but also attacking government sites and educational entities, obtaining administrator privileges over them.

Many states governments are taking an individual step to block the sites for their own spying purpose. Countries like Turkey and USA they also banned Facebook, twitter and YouTube. Pakistan, Iran and Turkey are one of those countries who can easily put a restriction on their internet users for using these sites. In the Zardari regime, the government put some restrictions on text messages and twitter tweets which, made fun of president or any government institution.

The real issue is not about banning these sites for public use. But states themselves are also involved in spying over its citizen or on other countries. As Edward Snowden revealed the secrets about USA national Security Agency who suck up millions of text messages, phone calls, emails throughout the world in every single day. It becomes great fallout for the government of the USA. The government is not taking care of the privacy of its citizen or other individuals. Later NSA declared that all countries are spying, and there is nothing in it to apologize for.[54]

In cyber espionage, we cannot execute India and Pakistan. According to Reuters reports both south Asia's major countries, Pakistan and India are the target of Cyber Espionage Company which describes that some suspicious state sponsored actors are involved. As

[54]Irfan Husain, "View from abroad: Cyber Jihad and espionage," *DAWN*, March 24, 2014, accessed August 17, 2018,
https://www.dawn.com/news/1095236

per the report, there are multiple groups behind this. The most interesting thing about it, the campaign has similar goals or under the same sponsor. It's very much difficult to identify the sponsor state.

In early 2017, India takes some effective steps against cyber threats. It created a malware analysis center for helping institutions and individuals to remove malware impacts from their system. India was on number 8 as per the report. But Pakistan considers the most at risk state of south Asia for malware effects.[55] Although one of the senior FIA officials gives the statement that up till now they did not receive any report from the governmental information technology department regarding malware attacks.

It puts Pakistan in such a hard situation because the cyber defensive mechanism of Pakistan is not as strong to prevent these malware attacks. Yet officials from Pakistan are denying about Symantec corporation report. In the end, Pakistan should face the reality and work more effectively on its digital system security. So in future, it can better protect its system from this malware espionage.

## 3.3 Hacktivism between India and Pakistan

Hacktivism is not a new phenomenon for global politics. In current time period it is used for gaining political or social agenda. Mostly powerful states or organizations are supporting them as per their interests. Like "Titan Rain" A group of Hackers breaking into official U.S. networks are not just using Chinese systems as a launch pad, but are based in China. Hackers sat down at computers in southern China and set off once again on their daily hunt for U.S. secrets. Since 2003 the group had been conducting wide-ranging assaults on U.S. government targets to steal sensitive information, part of a massive cyberespionage ring that U.S. investigators have codenamed Titan Rain. On this particular night, the hackers' quarry was military data, and they were armed with a new weapon to reach out across cyberspace and get it.

---

[55]Morgan Chalfant, "Cyber espionage campaign targets India and Pakistan: report," *The Hill,* August 28, 2017, accessed August 17, 2018, http://thehill.com/policy/cybersecurity/348253-india-pakistan-target-of-sustained-cyber-espionage-campaign-report

It is not just limited to the developed states but also developing states get affected through this. Hacktivism is very much popular between Indian and Pakistani hackers. Their hackers are always ready to hack sensitive sites of each other, whenever a political or social event occurs between them. It is a continuous exercise between them. That creates a difficult scenario like if such kind of hacking practice carries on between them. So later on they can launch a full flag cyber war.

## 3.4 Pakistan's Technological Electoral System and its Implications

The chairman of Nadra has announced the production of the electronic voting machine in elections. The cost of that machine will be round about Rs. 80 billion. Mostly developing states are using that system and currently, eleven countries are using that system which includes US, Canada, Australia, France and India etc.

For general elections of Pakistan almost 360, 000 Electronic Voting Machines (EVMs) will be required. The cost of one Biometric Voting Machine (BVM) is Rs 120,000 and EVM around Rs 180,000. The Election Commission of Pakistan (ECP) has almost purchased 250 machines for elections.[56] Pakistan needs 360,000 machines for the country wide elections. In the coming years of Pakistan, ECP is trying to introduce that system. But it is quite difficult to introduce such an advanced system. Even ECP said that there are two major reasons for not using EVM in coming years. First, the government is not giving the required amount for purchasing these machines and second it is not possible to train people. Apart from that in Pakistan very much low level of literacy making it more difficult because people can't easily understand the system.

Furthermore, the perception about EVMs is that they can make the election system much fairer and there will be fewer chances to manipulate the results. ECP information technology DG Muhammad Khizar Aziz arranged a demo related to EVMs usage. In which he asked that all other stakeholder should stand with the Election Commission for conducting next general election on the digitalized system. In this way, the common man

[56]Aamir Saeed, "ECP Requires Rs 90 Billion to buy EVMs and BVMs," *Business Recorder*, April 16, 2017, accessed April 29, 2018.
https://fp.brecorder.com/2017/04/20170416168962/

can know the usage of EVMs and further we will get the better result from that system. As an experiment in Peshawar by elections of NA-4, in which EVM was used. Where 100 EVMs were used and 35 polling stations were created in the history of Pakistan said by DG Khizar Aziz. The major purpose of EVMs was to make the elections more simple and effective in terms of the result. The government of Pakistan needed to work more on the security of EVMs and make the technology more constructive for the country because it is a sensitive system and those countries which are using the system are very much concerned about the security of it.

On the other hand, India has been using EVMs since 1999 but replaced it with the paper ballot. Election Commission of India took a lot of time for improving the security of EVMs. The inventor makes sure of the security and technical safeguards before introducing that system in elections. The EC never took a single decision without the approval of the high court. Even in the beginning of the digitalized system, a committee of five technical advisory professors of top IITs was invited. They gave their pleasing remarks about EVMs. After that when the court was fully satisfied with the non-tamper ability of EVMs. Then Karnataka High Court gave its remarks "This (ECI-EVM) invention is undoubtedly a great achievement in the electronic and the computer technology and a national pride."[57] India took a lot of years for introducing the system. Now around 1.4 million EVM machines are used in Indian elections. That cannot be possible without the help of the Indian government. Who donated a huge amount of funds for it? Currently, India is using EVMs successfully and trying their best to safeguard it.

Additionally many developed states switched from EVMs to traditional ways of elections. Because according to them paper ballot is more reliable than EVMs. In which hacking, tempering easily happens. As per states, it is nearly impossible to provide complete security to its digital system from hacking. Here we take the example of the two most powerful states the USA and Russia. Here the USA is claiming that Russia hijacked the whole campaign of 2016 elections. Even CIA, FBI and national security agencies of

[57]S Y Quraishi, "Shooting the EVM," *The Indian Express*, March 17, 2017, accessed April 30, 2018, http://indianexpress.com/article/opinion/columns/shooting-the-evm-electronic-voting-machine-controversy-election-commission-of-india-4572456/

America gave the statement with full confidence, that Russia used the technical tools and put their influence on the election campaign. The main purpose was to make a clear way for Trump to become president and defame the Hillary Clinton promotion. The whole process happened with the consensus of Russian president Vladimir Putin. All these three security agencies are highly confident that Russian intelligent services were involved in it and they targeted both the USA political parties. When Moscow got to know that secretary Hillary Clinton was likely to win the elections. Russia put its full focus on her campaign and undermined the expected presidency. Other than this, they also tried to weaken the opinion as well as the faith of the USA public about the democratic system. Apart from that Russia also had some other agendas like Russia wanted international counter terrorism coalition against ISIL and IS.

So for that Russia used its state funded media like websites, social media, twitter, Facebook, YouTube and radio. Russian organization linked to the Kremlin is known as the Internet Research Agency (IRA) is reported that it hired hundreds of people to spread fake news about Clinton on social media. The content of IRA was spread to more than 140 million users of them. This was not the first time when IRA wages a well resourceful campaign against the US. 2014 was the beginning of information warfare against the USA. Meanwhile, USA agencies also had doubts that in 2016 Russia also hacked their hundreds of emails and later on leaked them online. On the other side, the Russian Government is still denying about these allegations.

We can compare the same situation between India and Pakistan. In future India digital system will be much better than Pakistan. There are many chances that India also tries to hack the Pakistani elections as per its interests. That is because Pakistani EVMs can be manipulated easily due to some reasons, in which low literacy rate is most important because it will be difficult for government and other institutions to educate people about the proper usage of machines. Even in by-election held in Peshawar in October 2017, where EVM was used, the ECP was unable to provide more magnetic ink to voters for fingerprint verification results.[58] Secondly, for ECP, it is quite impossible to check 1.4

[58] "Electronic Voting machines to make debut in NA-4 by elections," *Pakistan Today*, October 19, 2017, accessed February 7, 2019,

million machines and come to know that which one is tempered. Additionally, the ECP officials should ask to Indian election authorities regarding how to avoid EVM tempering. They said till now there is no mechanism to escape from tempering. India itself became a victim of this.

## 3.5 Cyber Warfare Enigma Between India and Pakistan

In comparison with traditional warfare, "Cyber Warfare is the art and science of fighting without fighting; of defeating an opponent without spilling their blood."[59] The word "terrorism" brings to mind a picture of bearded men throwing a pouch filled with explosives. But in the context of IT security, terrorists can come in many forms such as politically motivated, anti-government, anti-world trade, and pro-environmental extremists. If given the opportunity, such activists would gladly disrupt trade and legislative agendas by attacking a facility's communication server, especially if the media were standing by to report what just happened. Also, a terrorist could try to interfere with IT resources controlling critical national infrastructures.[60]

A few years ago, a new kind of revolution came that was called the information revolution. With it, computer and mobile devices got more power than the traditional tools of fighting. In this way the global networking becomes telecom highway among states. The use of information technology becomes part of human life in every single way. The dependency has been increasing day by day in every sector whether it's banking, hospitals, airports, government sectors or military institutions. The rapid development of digital system is also posing a challenge in the shape of security of the cyberspace. Because every country is having millions of internet users and state should provide security of the digital data.

---

https://www.pakistantoday.com.pk/2017/10/19/electronic-voting-machines-to-make-a-debut-in-na-4-by-elections/

[59] Jaffrey Carr, *Inside Cyber Warfare* (Inc: O Reilly Media, 2011), 2.

[60] Janczewski, Lech J., and Andrew M. Colarik, *Cyber Warfare and Cyber Terrorism* (America: ICG, 2008),14.

States are moving towards digitalization. They must prepare themselves for the latest kind of war which is cyber warfare. Although many writers didn't accept the dilemma of cyber warfare because according to them still there is no full flag cyber war happened between any states. But it can happen between countries and will be more destructive for critical infrastructure of any state because cyber war is quite different from traditional war. In which state non-states actors both are involved to attack a nation's information network or computer system through different viruses and denial of services attacks. The major task of cyber war is to target the physical backbone of the internet that is submarine cables. Because these submarine cables carry around 97% of international data.[61] So if any one who attacks these cables of cutting down the internet traffic than it can create a great chaos for any states. That's why many states are very much concerned about their cable safety. Because cyber war is not just an internet base conflict, it is having political, religious, ethnical, sectarian motivations involved in it. The more chances of cyber war likely to happen between hostile states.

India and Pakistan have historical hostility, which decreases current likelihood of traditional wars. That's why if any war that will take place between India and Pakistan will be cyber war. That is already beginning between them in form of cyber-attacks on the critical infrastructure of each other. Here we need to analyze the capabilities of both states in terms of cyber offensive and defensive power.

Indian has the Defense Cyber Agency (DCA) a forerunner for cyber war. They should have both offensive and defensive cyber capabilities. DCA is also having the responsibility to protect the submarine cables. On the other side, Pakistan is not having proper cyber defense agency who took the responsibility of cyber security. That can make a difficult situation for Pakistan to fight back in case of cyber war. Here Uzair Younus expressed the seriousness of Pakistan and their approach to cyber warfare in his article "Cyber Warfare How Prepared Is Pakistan?" that Obama's administration facing very tough time related to the leakage of data and information. Even some other countries

[61]Prashant Mali, "Is India is ready for Cyber War," *Daily News and Analysis*, April 30, 2018, accessed May 6, 2018,
http://www.dnaindia.com/analysis/column-is-india-ready-for-cyber-war-2609937

those are under surveillance of cyber-attacks but it's surprising that Pakistan is the second high ranking of cyber-attacks. All other countries such as the U.S, China, India, and Israel know the importance of cyberwar. They are investing their resources in cyberwar while Pakistan is a slave to its armed forces. Some people blamed army forces because they have a hold on power and giving more importance to traditional threats rather non-traditional but as far as Pakistani civilians are concerned they have also blamed that leakage of data is a threat to national security.

Furthermore, Farzana Shah looks at the issue from a different angle and provides some sort of comparative study in her article "Cyber Warfare: Pakistan's New Battlefield." She describes that the new cyber warfare is trickier than the traditional threats between Pakistan and India. Pakistan is not paying much attention to its technology field but India is investing more in its technology field to create more challenges for Pakistan in cyber warfare. In this scenario, Israel is also proving a help to India against Pakistan. According to Shah, the cyber warfare is very much complex as compared to conventional warfare for Pakistan. The new cyber warfare is a great threat to the government of Pakistan as well as the Pakistani citizens because Indian and Israeli agencies are trying to defame Pakistan and its nuclear program. Still, cyber limited sticks are going on between India and Pakistan. Indian hackers deface the Pakistani website of a Ministry of Oil and Gas, Government personal data etc. as a response, Pakistani hackers defaced many Indian websites as a sign of retaliation.

Moreover, Muhammad Sabbeir gives a similar dimension in his article "Cyber Security in Pakistan: Emerging threats and preventive measures". That now cybersecurity is not the only concern of an individual but organization and even countries are beginning to suffer. Negligence in the cybersecurity can create terrible consequences. Pakistan is also one of those countries who is still having no cyber-criminal law and security policies. Because of that reason most important sites like OGRA, HEC, Pakistan air forces, Supreme Court, banks, and PIA are highly vulnerable to cyber-attacks. Because of lower cyber awareness in Pakistan, it is providing a great opportunity to India that they could easily arrange an attack on Pakistan. India is now trying to establish an offensive cyber-attacks ability, in this regards "It is rapidly establishing itself as a software development

capital of Asia". Later he describes that Indian internet export linked products are amounting to the US $9 billion and also producing further 100,000 IT professional in every year. Hundreds of well advance professional hackers are working in India and they hacked almost 36 government sites of Pakistan in December 2010. They are targeting the government's sites because of the low cyber security system of Pakistan. But we cannot say that Pakistani organizations and individuals are sitting idle. Pakistani hackers also hacked more than two thousand Indian websites even central bank of India is also included. According to Sabbire digital security is not just like military security, in which your strong offensive capability does not craft your defence stronger. At this point, Pakistani organizations and agencies are lacking of cooperation about cybersecurity. That's why India is taking advantage of it. Afterward, Sabbire explains that the cyber police of both the US and China are making different policies for securing their cyber system from any sort of attack. Similarly, in the case of India and Pakistan, Pakistan needed a well to develop policy so that it can effortlessly avoid Indian cyber-attacks in future.[62]

## 3.6 Cyber Terrorism

The FBI defines Cyber Terrorism as a "Premeditated, political motivated attack against information, computer system, computer programs and data which results in violence against non-combatant targets by sub national groups or clandestine agents."[63] Now the internet is becoming an unsafe place or we can say a developed digital weapon. That is a fastest growing threat not only for individuals, public or private sector but it also affecting the whole nations as well. The cyber space infrastructure of nations is getting vulnerable. Due to that security of government and civilian is at a stake. To counter these threats the nation needs more cyber professionals to handle the situation. Now, on the other hand, many terrorist organizations are developing their digital technologies or advance ways of attacking. As discussed in the book "Like War :The Weaponization of

[62]Muhammad Sabbeir, "Cyber Security in Pakistan: Emerging threats and preventive measures," *ISSPR PAPERS* 7 (2013), 25.

[63] Peter W. Singer, "The Cyber Terror Bogeymen," *Brookings*, November 1, 2012, accessed August 8, 2018,
https://www.brookings.edu/articles/the-cyber-terror-bogeyman/

Social Media" by P. W. Singer and Emerson T. Brooking, the attacks launched by terrorists through the Twitter wars have real consequences on people and events, the misinformation causing political effects. The new battlespace now involves tech, politics, and war that all happen on smartphones.[64]

While in the present scenario, we cannot say that terrorist organizations are not using cyber space for their act of violence. These groups are using the internet because it is less costly or less risky. The major potential of terrorism organizations is by using the internet to attract the other academic, governmental institutes for fulfilling their interests. Cyber terrorism is continually an ongoing process, where thieves, cyber terrorists and youngsters are getting involved in the usage of the internet and are becoming a part of it because these people are easily approachable.

Most famous terrorist organizations like Al Qaeda, Daesh, ISIL and ISIS are using the latest technologies for their own interests as well as to serve the desires of other states. Because practicing cyber space is more complex and a much effective way for recruitment. Further, it's much significant to reach people than they ever could. The basic reasons for using cyber space are to spread propaganda and to communicate with each other. Al Qaeda was the first well of a terrorist organization that starts using the internet for the promotion of its ideology.

Islamic State was, in the beginning, a military campaign as self-defender. However, after gaining control over the territory of Iraq and Syria, Islamic State started using the internet for their further interests. But they lost its control over territory and experience a military defeat from the hands of US. Then IS starts creating a cyber-weapon or exploiting social media platform building a counter narrative. Because they get to know that the legitimacy of their ideology will not take place in real space. So they have to change the strategy and putting their full focus on the internet. Through the internet, they can easily promote their ideology and extremism against their targeted states. In early 2016, the social media activates IS was very much greater, especially on twitter. Then around 125,000 accounts of IS, was shut down by the social media company. Still, they have a lot more influence

[64] Paul Adams and Emerson.T, Brooking, *Like War: The Weaponization of Social Media* (New York, Eamon Dolan/Houghton Mifflin Harcourt,2018), 12.

over the internet. As per ISIS defector Abu Abdullah al- Maghribi statement in which he said "The Media is a personis more important than soldiers, their monthly income is higher. They have better cars. They have the power to encourage those inside to fight and the power to bring more recruits to Islamic State."[65]

Al Qaeda is the very well-known organization who attempted many cyber-attacks to developed states as well as developing state like Pakistan and India. Pakistan and India are those countries who are affected by cyber terrorism. Cyber terrorism is making countries more vulnerable to protect their computer system from digital attacks.

India is facing so much trouble from digital terrorism. Indian youth comes on the third highest rank of using internet or social media after china and US. Still, it is not counter by the nation as it should be. Although India is having more advance technology still some Indian cyber experts considered that that they are unable to control cyber-attacks, those come from Pakistan and china. Pakistani hackers and other terrorist organizations are taking advantage of it and attacking the critical infrastructure of India. Cyber terrorisms are providing a new dimension to the ongoing conflict over Kashmir. In which pro Pakistani cyber terrorists and hackers those are recruited for targeting the Indian sensitive information. Even just after the 9/11incident, many people consider that mostly member of Al Qaeda is sympathizer of Pakistan. They are involved in spreading propaganda against G-Force and Doctor Nuker was defaces.[66] Even after the most famous attack was Mumbai attack 26/11, in which terrorist used internet service for communication and they carried around 12 shooting attacks in the whole city. A recent study was done by the Indian government proving that stolen phones are increasing in numbers and selling it to Pakistan. Because those phones are still valued in Pakistan, but their IP address or International Mobile Equipment Identity (IMEI) numbers are still registered in India. Due

[65] "How Terrorists Use the Internet," *OP*250, accessed August 13, 2018, https://www.operation250.org/how-terrorists-use-the-internet/

[66]Lidia Mariam Benoji, "Cyber Terrorism- Quick glance," *Legal Service India*, accessed August 12, 2018, http://www.legalservicesindia.com/article/1263/Cyber-Terrorism---Quick-glance.html

to that much fake news, messages, tweets are traced to Pakistan said by senior government officials.[67]

Now it is the time for the Indian government to take some strong steps and counter the growing cyber terrorism. Although after such kind of terrorist attacks the parliament of India take a legal step and pass a law against cyber terrorism. Some of those laws and their sections are here.

- That was IT Act, the section 66F of IT Act for those who are involved in digital terrorism activities will be in imprisonment or for life time imprisonment.
- Furthermore according to section 69A of IT Act give power to the center government of India or any of its authority have to power to block the access of information from the computer source used by the public. To prevent the sovereignty and integrity of the nation.
- Then as per section 70B of IT Act, the CENT in the team is having a responsibility to give quick respond or alert after knowing ant kind of cyber security challenge for the nation. But also provide an immediate security measure to tackle the cyber incidents.
- Unlawful Activities prevention Act 1967, this act gives the punishment to terrorist activities. The main purpose of it to focus on those organizations, those are recruiting people for terrorist activities.
- Cyber security policy 2013, first time introduced by India at the national level for its digital security. The basic purpose of this policy is to secure Indian cyber space from both terrorists and anti-social matters.[68]

Pakistan is also becoming a major victim of cyber terrorism. Daesh is recruiting youngsters from Pakistan and using them against Pakistan and many others. But the

---

[67]Meetu Jain, "Center Worried over Cyber Terrorism as Stolen Phones are finding ways into Pakistan," *India Today*, July 11, 2018, accessed August 12, 2018, https://www.indiatoday.in/india/story/centre-worried-over-cyber-terrorism-as-stolen-phones-are-finding-way-into-pakistan-1283199-2018-07-11

[68]Prathiksharavi, "How the Legal system Tackles Cyber Terrorism," *Pleaders,* April 16, 2018, accessed August 12, 2018, https://blog.ipleaders.in/cyber-terrorism-laws-india/

government of Pakistan is still denying that ISIS is existent here. Such kinds of statements are creating confusion between military and governmental statement. A conference held in Islamabad on 10 February 2016, in which Muslim religious scholars were there, they even admitted the existence if ISIS in Pakistan. They also maintained that the terrorist organizations like ISIS, Al Qaeda fighters are more risky Muslims rather than non-Muslims. But the foreign minister of Pakistan is denying and said "No Group like ISIS exists in Pakistan." On the other side, the Commander of NATO General John F Campbell said that the Islamic State is recruiting fighters from Afghanistan and Pakistan which were not functional up till now. There are many other reasons which are promoting Cyber Terrorism in Pakistan. Here are some of them.

- Unregistered Madrassas
- Unemployment
- Extremism
- Political differences
- External influence

Because of these reasons terrorist organizations are easily getting access to Pakistan. ISIS is offering 50,000 per month to their employees. That is quite a handsome package for Pakistani unemployed youngsters because in a current time period more than 20 million young people are unemployed in Pakistan.[69] They are providing training to cyber warriors through different motivational videos. That is very much common practice in Pakistan. They call it jihad to support Afghani and Kashmiri against America and India. Latest digital technology is playing important role in promoting online radicalization and terrorism in Pakistan.[70] Now undoubtedly the government of Pakistan is paying some importance to address the emerging issue.

The government of Pakistan understands the seriousness of the growing threat of cyber terrorism. That's why the government has established the National Cyber Terrorism

[69]Yunis Khushi, "ISIS in Pakistan: A critical Analysis of Factors and Implications of ISIS recruitments and concept Jihad-Bil-Nikah," *Art and Social Sciences Journal*, no.1 (June 2017): 13.

[70] Saqib Khan and Khalid Mmanzoor Butt, "Cyber Technology, Radicalization and Terrorism in Pakistan," *Journal of Indian Studies*, no. 2 (December 2017): 119-128.

Security Investigation Agency for a counter check on millions of online platforms and terrorism. For its establishment, Islamabad allocated around 100 million Pakistani rupees to the interior ministry's annual budget of the monetary years 2018 and 2019. Apart from that the government of Pakistan also gave 24 million rupees for the establishment of the cyber patrolling unit. The main purpose of the cyber patrolling unit is to track down militants guilty of hate speech, activities of extremis and their recruitments.[71] Moreover, Asif Ali Zardari regime set the death penalty for cyber terrorism. According to the law based on the prevention of electronic crime, it will be applicable upon all those who use the computer for committing a crime to destabilize the national security of Pakistan. The law will also be implemented on either Pakistani citizen or foreigners who are living abroad.[72]

In the era of the digitalized world, it is essential for Pakistan to pay more attention to the growing digital terrorism. For sake of that Pakistani government first time ever launched a cyber-security center. There are a number of other departments like police, Federal Investigation Agency (FIA), the National Counter Terrorism Authority (NACTA) working for terrorism and extremism. But the flaw between them is that they are empowered under separate laws and having less cooperation regarding the implements of laws.

To address the ongoing cyber terrorism challenges Pakistani government needs much more effort especially in case of law implementation. All other institutes which take care of terrorism should come together and make a proper cooperation to tackle extremism, terrorism or hate speeches because digital technology is gaining more and more advancement in it. Due to that cybercrimes are becoming more complicated so to address these crimes Pakistan requires more laws with the same speed.

---

[71] Aamir Shah, "Pakistan to establish Anti-cyber terrorism Agency," *Arab News*, May 6, 2018, accessed August 10, 2018,
http://www.arabnews.com/node/1297496/world

[72] Reuters Staff, "Pakistan sets Death penalty for "Cyber Terrorism"," *REUTERS*, November 6, 2008, accessed August 11, 2018,
https://www.reuters.com/article/us-pakistan-crime/pakistan-sets-death-penalty-for-cyber-terrorism-idUSTRE4A54AR20081106

Additionally, India's too much involvement in Afghanistan is creating a problem for Pakistan. Now India is the major trading partner and regional leading contributor in Afghanistan. They invested around $3 million since 2001. That is more than Pakistan's investment in it. That is also creating tensions between Pakistan and Afghanistan government.[73] It is creating quite a difficult scenario for Pakistan. India is funding more for development and any other project to promote cyber terrorists against Pakistan because it will be more beneficiary situation for India.

So Pakistan needs to tackle the situation in more efficient and better ways. Since India is having a more sophisticated digital system than Pakistan and as if it backs Afghanistan in terms of technology so it will automatically create more trouble for Pakistan.

## 3.7 Conclusion

To conclude, India is showing both tangible and non-tangible threats to Pakistan. In non-tangible threat, cyber threats are most prominent. Firstly, we see that after the Stuxnet attack how nuclear countries became conscious about their nuclear safety. In which Pakistan especially needed a lot more protection measure needed to secure its nuclear data from India. India has the latest technology, but also is getting assistance from the US and Israel. That creates a much more critical situation for Pakistan.

Secondly, cyber warfare is not a new dilemma between states. But in India and Pakistan, it presents a very interesting picture. The researcher comes to the point that Pakistan is till yet not fully prepared to handle the new kind of war. With the help of different writers Opinions, that how Indian hackers are targeting the most sensitive sites of Pakistan and government is still not fully able to control the threat.

Thirdly, it describes the cyber espionage situation in both India and Pakistan. As per Symantec Corporation, a digital security company published a report in which it was mentioned that how India and Pakistan are major targets of cyber espionage in South Asia. Multiple groups are behind this campaign but still, they are unable to locate the

[73]James Griffiths, "Who are the Key Players in Afghanistan," *CNN*, September 19, 2017, accessed August 14, 2018,
https://edition.cnn.com/2017/08/26/asia/afghanistan-pakistan-india-china-russia-us/index.html

sponsored state that is backing them. In the end, we see that how much India is taking the threat seriously as compared to Pakistan. India establishes a malware analysis center to address the malware impacts. On the other side, Pakistan is not even making any mechanism to counter the issue but also officially denying regarding this report.

Fourthly, we see that Pakistan is going to introduce the Electronic Voting Machines in coming elections. Only eleven countries throughout the world are using EVMs. But most of them are developed states but their systems still get hacked. The researcher states the example of developed states like the USA and Russia. That's how Russia hacked the full campaign of US election and it put great effects on the result. The researcher is trying to implement the same situation between India and Pakistan. India is already experiencing the system in its country and they have a better idea of how to deal with the system. But when Pakistan will introduce the system properly till then they will not have a proper idea about the system. India can get full advantage from it and hack the election as per its interests.

Lastly, the researcher tries to compare the cyber terrorism condition between India and Pakistan. Also considers the types of problem India is facing and what protection measures are taken by it against them. Later it is seen how Pakistan gets more affected by digital terrorist organizations and how India is trying to get more benefit from this scenario through its more involvement in Afghanistan. How Pakistani government is making policies and laws to handle the situation?

# CHAPTER 4
# PAKISTAN'S CYBER PREPAREDNESS

In the current Hi-Tech world, neglecting of the digital security can result in awful consequences not only for any individual but also for the state. It can create major chaos because security is the most fundamental requirement of every cyberspace network. It is just like the basic security of humans. If you are not providing security to the system then it is just like a bank, which is full of money but there is no security guard or cameras.

According to some surveys, Pakistan has not prepared to control the ongoing digital attacks because the coordination between cyber agencies and other security institutions are lacking. Due to this situation, hackers try to take a significant control over information, communication and intelligence system. They get access as soon as it comes in their access. To grip the condition, Pakistan needs to practice the following steps already followed by other developing countries to secure their digital realms.

But unfortunately, in this time period, Pakistan is one of those countries who is not having proper cyber-crime laws and policies related to cyber security. Because of that Pakistan becomes an easy target for cyber-attacks. The most important sites of Pakistan

## 4.1 Legal measures

It is very much easy to say that the 21st century is the internet century. Where hacking is being carried out owing to the weak cyber system. Pakistan is not well prepared to counter these attacks. As per a survey by our prevailing institutions like communication network, internet service providers, Nadra, Bank, PIA and educational institutes reveals that their digital system is highly vulnerable to cyber-attacks. Here are some of the relevant areas where the researcher will try to analyze the cyber preparedness measures and their capacity building.

Whole world is dependent on small devices and through them people can easily fulfill tasks in a limited time period. But now the internet has become more vulnerable rather than reliability. Excessive usage of the internet is also increasing the rate of online

crimes. Due to exceeding rate of cybercrimes, countries throughout the globe are making cyber laws for the prevention of online crimes. Similarly, Pakistan took an initiative but rather not so early. But before coming to the main laws related to cyber-crimes it's necessarily important to understand the background and developing steps of electronic laws in Pakistan.

In 1885, the Telegraph act was the first ever telecommunication law in Pakistan. That law gives much power to the center government of Pakistan. Where a person needs permission from the govt to use a telegraph or the central government issued a license to the person who can work on telegraph in any part of Pakistan.[74] But the major drawback of that act was the government and telegraph officer were not responsible in case of any loss. Later in 1933, the wireless telegraph act came into existence.[75] But similarly it was not much effective.

Furthermore, in 1996, the Pakistan telecommunication act was adopted. That was the first ever regulated law in Pakistan which dealt with internet activities. Starting from providing a license to misuse of the internet, the basic aim of the act was to reorganize the telecommunication system of Pakistan. In which the major rights of telecommunication authority of Pakistan was explained and who so ever will disobey the law will be punishable.

Then in 2000, the first and major Electronic Transaction Ordinance (ETO) was created. That was recognized at the national level. The basic purpose was to protect the digital system in both the local and global level. The law was inspired by foreign law related to digital criminal activities. At that time President Pervaiz Musharaf was legalized legislation to the ETO 2002.

Before that law, there was no acknowledgement of electronic records and documents. There was no center for online transaction safety nor was data recovery taking as much serious issue. ETO 2002 comprised 43 sections and the most important parts were related

[74] The Telegraphy Act, 1885, accessed August 17, 2018, http://www.fia.gov.pk/en/law/Offences/26.pdf
[75] The Wireless Telegraphy Act, 1933, accessed August 17, 2018, http://pklegal.org/pdf/Wireless-Telegraphy-Act-1933.pdf

to defilement privacy or security information, damage the information system like delete, modify and steal private data etc. but after getting legal legislation all electronic documents and records were also legalized.

Moreover, in 2007, the payment system and electronic fund transfers act were established. This law gives the safety to banking services and consumer protection was provided. The major aim of the act was to facilitate and create a regular framework for money transaction and electronic fund transfer.

Later in 2007, the cabinet approved the bill related to prevention of electronic crimes. That was the first ever regulated law related to the cybercrimes. In which 17 kinds of cyber-crimes were discussed and their punishments were maintained. The more serious crimes like electronic fraud or electronic forgery will be punished with almost seven years in prison and with no right of bail. But in case of data damaging, data stealing, or misuse of personal information will be punished around three years with having the right of bail.[76]Apparently, the law seems perfect but it faces a lot more criticism.

After that, Electronic Documents and Prevention of Cyber-Crime Act emerged in 2014. The government of Pakistan decided to establish a special court for cyber authority. The basic purpose of that law was not only to do some changes in existing laws but it required major amendments in Pakistan Telecommunication Reorganization Act of 1996. The Electronic Documents and prevention of cyber-crime law also provide a well-developed system for authentication of digital documents, records and digital signature. Under the constitution article 10, a committee was established upon seven members. The five members were from the private sector and remaining from the public sector. The basic intention of introducing this unique system for both public and private, so in case of any change happened in documents, forms or signature then cyber authority can easily detect them. As a result, all kind of transactions will be recognized by legal cyber authority and it will also be safe as a record for future recertification. Besides that, the government of Pakistan will establish a Cyber Emergency Response Team work under by secretary of

[76]R.S, "Pakistan's Cyber Crime Bill 2007," *ICT4D South Asia*, January 20, 2007, accessed October 19, 2018,
https://southasiaict4d.wordpress.com/2007/01/20/pakistans-cyber-crime-bill-2007/

Information technology. Where two cyber experts will be required to give a quick response of national or cyber security issues and it will also play the role of a bridge between government and cyber authority.[77]

August 2016, the National Assembly passed the law known as Prevention of Electronic crime Act. The law was unanimously approved through the senate with a lot more amendments. The main purpose of this law is to prevent illegal access, copying and transfer system. In which international cooperation is also required. The law also gives excessive power to the central authority so they can better check the system and reduce cyber-crimes. Still if someone is involved in such kind of digital criminal activities then they will face harsh penalties. Besides that, the bill also faces a lot of criticism. Some said the punishments are too harsh as per crime and the major stakeholders were badly ignored during the development of this law. The existing laws related to cyber security come under the influence of prevention of electronic crime act or the law gives too much power to the government to get the personal information of anybody without informing the particular person. The law enforcement agencies are missing and so is the center authority, who has the right to remove or block online material without court orders.[78]

In an interview, Dr. Tugral Yamin agreed that prevention of electronic crime bill only deals with cyber-crimes, not with cyber security issue he said "There are no measures as far as cyber preparedness is concerned. The lethal measures that have been taken, is within the ailment of Pakistan Electronics Crimes Act. It is just to prevent the electronic crimes and not to prevent cyber-attacks, so there are no measures. For instance, how would a hacker – who actually breaks into (God-forbid) NADRA's database (National Database and Registration Authority), how will he be trialed? We need a special, legal framework for cyber preparedness. I am sure that the agencies concerned are aware of the threats but everybody is operating in solos, there is not a wholesome governmental approach to it, even the punishments, are very harsh in law. But the harsh punishments

[77] Khaleeq Kiani, "Govt to set up Cyber authority, court," *DAWN*, January 12, 2014, accessed October 20, 2018,
https://www.dawn.com/news/1079918/govt-to-set-up-cyber-authority-court
[78] Tariq Ahmed, "Pakistan: National Assembly Passes new cybercrime law," *Library of Congress*, September 21, 2016, accessed October 21, 2018,
http://www.loc.gov/law/foreign-news/article/pakistan-national-assembly-passes-new-cybercrime-law/

are for the political victimization. You cannot victimize people for their political views, you can victimize people if they are blogging, but it's not for cyber security. That is the issue when the digital activists, like *Bolo Bhi* etc. campaign for digital rights, that is a completely different perspective, it is not cyber security preparedness"[79]

Comparatively, in 2000, India formulated its first every Information Technology Act. The basic purpose of the law was to provide protection to the e-commerce of the country from cyber-crimes. But there was some lacking in that law, for that it needs amendments. In 2008 the bill came again in the amended form. In which cyber security deals with a number of issues like hacking, data protection, unauthorized access, stolen personal information etc. Till then there was not only the IT act working but at some points, Indian Penal Code (IPC) was punishing those who committed cyber-crime. There were some cases but IPC did not address them in a very well way. That's why the act was criticized because it reduces the punishments of cyber criminals, as well as the body, was not strong enough to give safety to the individuals. Additionally, India also creates a data protection laws with the support of Information Technology Act and Rule in 2011 and the Consumer Protection Act 2015. The law was first ever drafted in 2010 or 2011 but it remained under discussion till 2014. In 2017, the Indian government created a committee who create a draft on data protection act. The draft is also completed but the law did not pass yet. But it's quite near to the passing process.

Later on, the Indian home ministry said that they have the plan to establish an "Indian Cyber-Crime Coordination Center" (I4C). It will specifically deal with financial frauds and also restrict the pornographic content within India. The I4C center will work with the government of India and observe social media activities. It also has the right to block all those websites that are working against cyber law. That is how India is making laws and working for its betterment. Not only are public, but also private institutions working with full cooperation of the government to protect the cyber system from illegal access. Indian government itself is very much serious about its digital system and they are not only supporting those entities who are working for cyber but also financially providing them support.

[79] Dr. Tugral Yamin (HOD, NUST), In discussion with Sadia Rasool, October 2018.

Whereas it seems the condition of the Pakistani government about cyber security is not as supportive as it should be. Pakistan is making laws but they are not as effective as they should be. The present laws are only addressing cyber-crimes and not working on cyber security matters. Pakistani government need to pay more attention to that area and create a well-organized framework, through which they can prevent cyber security attacks. Furthermore, develop a proper governmental institute, which deal with digital data in the case of any sort of loses. The institute will be responsible for that event and try to recover as much data as they can. In this way, Pakistan can progress in a more effective way in case of cyber protection through legislation measures.

## 4.2 Technical Measures

Globally countries are working hard for technical measures. In the case of Pakistan, it is not working the way it should be and paying little attention to taking some technical measures to improve the security of its digital system. PISA CERT is the first ever public computer emergency respondent team in Pakistan. In which qualified and professionally certified security experts are working and their basic aim is to control the misuse of the internet. PISA CERT is a private entity not governmental. Still, it's representing Pakistan in international cyber drill organization that was APCERT.

But till now there is no central authority in Pakistan who took the responsibility in case of any swear cyber-attack. As digitalization has become very popular in Pakistan, for the sake of its security government needs more effective tools to protect it. The most important e-government components like NADRA, Banking sector, FBR, Pakistan stock exchange and FPSC etc. are attractive target sites for hackers. Even most recently FIA issued a report about Pakistani banks that almost all banks data has been hacked. In which around banks credit card and debit cards were used outside the country within the black market. Islamic bank lost almost Rs. 2.6 million from its accounts and nearly 100 cases were registered in FIA. Such kind of incidents shows how much these institutes are seriously taking technical measures to secure their system.[80]

[80]Agency, "FIA says data from almost all Pakistani banks hacked," *Daily Times*, November 7, 2018, accessed November 8, 2018,

It shows that Pakistan is ill-prepared because there are things that are happening which need to be controlled, e.g. we know that the Result Transmission System failed; we do not know why it failed. There was some newspaper article which said that somebody made a mysterious call and instructed everybody to stop using it or freezing its operations or whatever, but all of this is part of cyber security. Are there any means to authenticate, or anybody who calls you up just-like-that! The jury is still out: you don't know what went wrong Further there were a number of attacks on the I-Voting System. The Pakistani expatriates who voted from outside, there were numerous attacks which were reported. Pakistan is ill-prepared because the government is not prepared to take this up as an issue – as a major security issue. This is a major security issue because this is all about data and data protection. If somebody steals someone's personal identity and breaks into his/her bank account, it's a tremendous loss. Same goes for if somebody is able to break into the data of businesses, banks or into the data that is meant for official use. It means that if you lose data then that's a very bad news because the country is not prepared. Our political leaders have very little idea about cyber security and cyber security is not just erecting firewalls, you have to have a proper policy, you have to allocate funds, there must be sufficient number of trained people, not only computer scientists but also men and women who are aware of how to frame a cyber policy.

So for the sake of maintaining confidential data, the government of Pakistan needs to establish a National computer emergency respondent team with the collaboration of CERT. Besides that Pakistan is also required to become part of OIC and SCO to bring better cyber protection system. Because cross border cases cannot be trace due to lack of governmental involvement and had no international or bilateral treaties for the persecution of cyber-crime.

On the other side, India established the National Technical Research Organization for protecting the critical infrastructure of the country and controls all kind of cyber incidents. Beside that Indian Computer emergency, Response Team develops in order to

---

https://dailytimes.com.pk/319389/fia-says-data-from-almost-all-pakistani-banks-hacked/

deal with financial matters. That's why it's called CERT-FIN. The basic objective of that institution to analysis the financial incident and report it to the national CERT about it.[81]

Moreover many Indian national cyber security institutes come under Ministry of Home Affairs (MHA) like the National Intelligence Grid (NATDRID) who keep all kind of citizen information on a single database and can only be accessed by RAW, CBI, IB and the National Cyber Coordination Center (NCCC) and National Crime Records Bureau (NCRB) also came under MHA. Department of Electronic and Information Technology (DEITY) are responsible for cyber security and the other major responsibility of it to deliver government services online and promote the IT sector.[82]

Beside that Indian military established an entity the Defense Cyber Agency (DCA) for defensive, deterrence and offensive aspect of cyber warfare. At the beginning around 1,000 people were drawn from Indian Navy, Army and Air force so in future they better serve up on cyber commands. Initially, the body is engaged in defending military assets or resources from non-state actors and terrorist organization. The DCA established for strengthening the national capabilities for big issues like cyber warfare. It did not deal with cyber-crimes or any other agencies like that.[83]

This is how India is preparing itself in cyber protection through taking different technical measures. The Indian government is very much concerned about the growing issue of digital security but unfortunately, the Pakistani government is not doing the required amount of effort to secure its cyber system.

---

[81]Samaya Dharmaraj, "The current state of cyber security in India," *Open Gov*, August 1, 2018, accessed November 11, 2018, https://www.opengovasia.com/the-current-state-of-cyber-security-in-india/

[82]Vivek Pai, "An overview of Indian cyber security agencies," *MEDIANAMA*, April 15, 2016, accessed November 11, 2018, https://www.medianama.com/2016/04/223-indias-cyber-security-agencies/

[83]Sanjib KR, "Military to get new body to tackle cyber warfare soon," *The Asian Age*, June 28, 2018, accessed November 12, 2018, http://www.asianage.com/india/all-india/280618/military-to-get-new-body-to-tackle-cyber-warfare-soon.html

## 4.3 Organizational Measures

In the current time period, cyber security is not just a threat to states but it also becomes a new area that required detail study. As per the requirement of time mostly developed states are offering cyber security as a regular course in their educational institutes. In this way, they can better secure it digital system and spread cyber awareness. Where mostly organizations are becoming part of it and conducting conferences and doing seminars about cyber security.

US government is formulating the cyber security strategy on the state level. Even developing state like India knows the seriousness regarding cyber security issue that's why India is collaborating with Israel. Israel is expecting that cyber security market will reach around $1 billion by the end of 2020. As a result, those countries also started PhD level programs regarding cyber security.

In 2013, the university Grants Commission of India asked the number of universities and colleges to teach cyber security as a proper course not only for the Postgraduate level but also in undergraduate level. Later in 2015, Indian university of NIIT started two years program in cyber security. Even in more recent times, the India state of Karnatake said that all universities with in the territory will offer cyber security courses in their institutions. That statement was given by Mr. T.B. Jaychandra, who is a minister of higher education. So as per Indian cyber security policy they have around 500,000 cyber professionals and by the end of 2025, they will reach around 1 million cyber security experts. That is why Indian institutions are contributing more so they match the required number as per policy.

On the other side, Pakistan has limited itself around the previous understanding of information security. Even the Pakistani universities are also not promoting cyber education as per requirement. Here are some of the universities who took little bit initiative. NUST University took the initiative and offered MS and PhD program related to Information Security curriculum. But their student tells PakWired that once university arranges a work shop about cyber warfare only a very small number of students took interest in it. As a consequences university never took the initiative again. LUMS

University is not offering any program about cyber security. UET is not offering specialization in cyber security.[84]

Now the first ever cyber security center is lunched at Air University for the protection of state digital infrastructure, economy from cyber-attacks. The previous federal minister of interior Ahsan Iqbal said its really good initiate taken by Air University and effective measures of cyber security can reduce the risk of cyber threats. The major aim of National Center for Cyber Security (NCCS) is to build up the latest tools and technologies to secure Pakistan cyberspace, sensitive information, and data from illegal cyber-attacks. The NCCS also has the aim to involve the other universities in this initiative. In which Bahria University, NUST, ITU, LUMS, university of Peshawar, University of Engineering and Technology Peshawar NED university of Karachi, University of Engineering and Technology Lahore and Taxila also included. Furthermore, Air University tried to increases the awareness and knowledge about cyber security in Pakistani students. For that sake it is offering four years BS cyber security program so through that course they can develop the latest cyber security skills. In future, they can apply those techniques in managing a computer system and networks from cyber-attacks.[85]

Moreover, in an interview by Dr.Tugral Yamin, gave his opinion about organizational performs or role in spreading cyber awareness was “Very little, I am afraid. There are conferences, people organize them.” Even till now only two universities, NDU and Air University, took the initiative to spread cyber-awareness through programs**.** “We also did so, a few years back, but more ought to be done. And it should not only be in the domain of computer sciences, but it ought to be also discussed as a policy matter in terms of international relations, bilateral relations. All those things need to be spoken about. The book that I’ve written, it is International Relations and International Law – CBMs between India and Pakistan, because I think there is no bilateral agreement between these

[84] Web Desk, “Cyber Security Education in Pakistan- An Overview,” *Pak Wired*, January 27, 2016, accessed October 21, 2018,
https://pakwired.com/cyber-security-education-in-pakistan-an-overview/
[85] Aqsa khunshan, “Pakistan gets its first ever National Center of Cyber Security,” *Tech Juice*, May 21, 2018, accessed October 21, 2018,
https://www.techjuice.pk/pakistan-gets-its-first-ever-national-centre-for-cyber-security/

two countries about what will be construed as a cyber-attack and what would entail a retaliation by the other party? These are the issues that ought to be on the negotiating agenda."

Apart from that, the Pakistani government presents the National Internal Security Policy (NISP) 2018-2023. It was the very first policy document which emphasized more on securing the digital system. It started in 2014 and the basic aim of it was to identify the future threats and give suggestion about how to deal with them. The report was released by NIPS, where the top most threat to Pakistan was mentioned. The most national security threat was Tehreek-Taliban-Pakistan (TTP), Islamic State (IS) presence in Afghanistan, the return of militants from Syria and Iraq, violent extremism in the educational sector and cyber-attacks. But after a long time, cyber security got attention by NISP. It formulates the national cyber security policy and established a civil and military cyber command forces. It also gives more power to FIA and National Counter Terrorism Authority (NACTA) in case of cyber-crime along with spreading cyber threat awareness in public. Besides that, much more strategies were introduced but were not explained in regards to how they will be applicable.[86]

It shows that now Pakistani educational sector and some of the governmental organizations are paying little attention to a cyber-security issue. That's why some of the well-known universities are offering cyber security as a subject for post graduate level. It's very much positive step taking by the higher education system. But still, Pakistani organizations need additional determination for improving the cyberspace system. That's because only one or two organizations will not enough to secure the digital system, much more is needed. Pakistan will then be able to meet the proper safety measures of cyber security.

[86]Fahad Nabeel, "National Internal Security Policy 2018-20123 a Critical Assessment," *Daily Times*, August 2, 2018, accessed November 1, 2018, https://dailytimes.com.pk/276539/national-internal-security-policy-2018-2023-a-critical-assessment/

## 4.4 Capacity Building Measures

As fast as Pakistan is moving towards digitalization, similarly it needs to enhance capacity building measures. Government and other stakeholders should understand the importance of cyberspace. Commonwealth and Telecommunication Organization (CTO) organized a conference about "Tackling cybercrime in the telecommunication sector in Pakistan" with the help of ministry of Information technology and Telcom. In which 53 members countries were included as mandates. The basic part of that workshop was about the capacity building measures taken by the member states. Apart from that, another focus was on global cybercrimes, data protection etc. in which the high commissioner of UK said that we need to collaborate with each other to prevent cybercrimes. Here minster of senate IT and Telcom Anusha Rahman said that Pakistan is now having Prevention of Electronic Crime act (PECA). It deals with online crimes and monitors them. Still, the ministry of Information and Communication Technology (ICT) accepts that they need a lot more effort to develop the capacity for stopping cybercrimes. Beside that Anusha Rahman highlight that with in ICT; they are having some more projects for underdeveloped areas like Baluchistan and Fata for their infrastructure. Furthermore, 226 schools of Islamabad trained their girls in coding or cloud computer. So in future, they can play their role in developing cyber security system.[87]

Moreover,Microsoft announced that they have the plan to open digital training and development center in Pakistan. The plan was disclosed by GM of Microsoft North Africa, East Mediterranean and Pakistan (NEPA). They believed that through introducing Microsoft technologies and training within Pakistan, it will be helpful for the local sector, service sector, and to progress HR capacities. After that Microsoft decided that they will invest more in ICT of Pakistan. So this way they can provide better data protection, cyber security in the country.[88]

---

[87] Correspondent, "Experts Highlight threats to cyberspace," *The Express Tribune*, March 17, 2018, accessed November 8, 2018, https://tribune.com.pk/story/1662213/2-experts-highlight-threats-cyberspace/

[88] Web Desk, "Microsoft to open new training, development center in Pakistan," *Pakistan Press Foundation*, February 2, 2016, accessed November 8, 2018, https://www.pakistanpressfoundation.org/microsoft-to-open-new-training-development-centre-in-pakistan/

The government of Pakistan should take some serious capacity building measures. As per Dr.Tugral Yamin opinion, he said "I think they should have, just as sort of an indicator that how serious we are about cyber security: I know and it appeared in the newspaper that the FIA has an organization called the NRCC"[89]

Later somebody ousted to the senate and said that there are only fifteen forensic experts in Pakistan. So, if Pakistan has only 15 forensic experts to investigate cybercrime, it means that we don't have a proper body or organization, which can show the cyber defenses of the government. There's a requirement that there should be a proper team, there should also be a computer emergency response team at the national level which should be able to respond to national emergencies. Pakistan does not know what parts of our critical infrastructure have to be protected from cyber-attacks. So, all those things need proper attention, proper focus, proper funding, and proper administration management.

It's the current status of Pakistan cyber capacity building measures that show that Pakistan required more effort to improve its capacity building measures. Those measures are not enough to protect the cyberspace system properly.

On the other side, Indian information security education and awareness programmers are trying to spread cyber security awareness through both formal and informal programmers. The cyber security program was recognized by national or sector specific standards of research and development. Apart from that cyber security training facilities has been trying to train law enforcement agencies and facilitates cyber-crimes. EU has been leading on international cyber security capacity building measures. The basic purpose of it is to collect the view of civil society and EU partner countries that how to more effectively work on the area of capacity building. In which India also shares its view. The conference was funded by EU and it was arranged in New Delhi.[90] So India is

[89] Dr. Tugral Yamin (HOD, NUST), In discussion with Sadia Rasool, October 2018.
[90] Press Releases, "EU-India Innovation meet-Innovation Platform Launched in New Delhi," *EEAS*, October 11, 2018, accessed January 23, 2019.
https://eeas.europa.eu/delegations/india/52023/eu-india-innovation-meet-%E2%80%93-innovation-platform-launched-new-delhi_en

not only doing national level but also doing international level cooperation to strengthen its cyber capacity measure.

## 4.5 International Cooperation

Cyber security is a regulating threat for every nation. That's why states need cooperation among them to prevent the threat. Mostly developed and developing states are making alliances or treaties about their cyberspace protection. But Pakistan is lagging behind in making cooperation between states.

As per Global Cyber Security index conducted by International Telecommunication union in 2017, Pakistan ranked at 67$^{th}$ position for digital security. In the regional level of analysis regarding Global cyber security index in Asian pacific context, Pakistan ranked on 13$^{th}$ with Samoa. After that the current national cyber security index 2018, Pakistan ranked 68$^{th}$ out of 86 countries. Since 2009, Pakistan was assumed to be victimized by 11 cyber operations against the government and non-governmental institution. Mostly hacking appears from Indian side and remaining from foreigner countries. From 2016 to 2018, above 18,000 cyber-crimes were reported. It is undermining the cyber security position of Pakistan.[91]

This situation shows that Pakistan needs relentless effort to secure its digital system in both public, the private and critical infrastructure of the country. Additionally, Pakistan Academy of Engineering (PAE) arranged a conference on Cyber Security- where we stand? In which many speakers shared their opinions regarding the critical situation of Pakistan's cyber system. All the spokesperson agreed that Pakistan should establish a state level cyber command body, which deals with all kind of digital affairs. After that speakers also said that the member states of SAARC should come together and make proper policies or platform to address the growing threat of cyber security.

The Asia Pacific Computer Emergency Respondent Team (APCERT) cyber drill was organized by the Pakistan Information Security Association (PISA). One main point

[91]Fahad Nabeel, "Need of a Robust Cybersecurity Regime for Pakistan," *CSCR*, October 2, 2018, accessed November 1, 2018,
https://cscr.pk/explore/publications/articles/cybersecurity-pakistan/

arose in it, that if some serious kind of cyber incident ensues then which governmental department will take responsibility for it? Moreover, APCERT develops a national level Computer Security Incident Response Teams (CSIRT) for Asian Pacific countries. The basic purpose of CSIRT is to collaborate among member states and share information regarding cyber security. 21 countries are part of it even India, Bangladesh, Sri Lanka, Myanmar is a member of it but unfortunately, Pakistan is not. APCERT arranges a cyber conference every year in which not only member states participate but it also invites OIC-CERT (Organization of Islamic Cooperation). As Pakistan doesn't have its own CERT that's why PISA registered its computer emergency respondent team slot in OIC-CERT. That is basically a private entity and government of Pakistan is not making any remarkable progress in the digital security system.[92]

Even Dr.Tugral Yamin agreed that Pakistan is having no international cooperation measures in the matter of cyber security and even he said "I have presented my book to the foreign minister - the book is a few years old now and I gave it to the minister of IT, but nobody has any interest. I said this should be on the agenda and we should be talking to other countries about it because Aziyan, for example, they have treaties, agreements within the member-states about cyber security, they organize conferences, share best practices; that kind of thing absolutely lacking in our context. For example, SAARC is absolutely silent about it; we can easily do it within their framework or SCO also".

The current status of Pakistan in making alliances and becoming part of any international treaty related to cyber security. That shows a critical scenario that Pakistan is not able to develop a relationship with other developed countries to improve its own digital system. Like other states, they are doing an agreement with advance states to get better technology and information related to their system safety. Similarly, now it's time for the Pakistani government to take the threat as seriously as it is and build up relationships with technical advance states for the protection of its own cyber systems.

---

[92]Zeeshan Munir, "Cyber Security Issue in Pakistan," *Global Village Space*, April 20, 2018, accessed October 27, 2018,
https://www.globalvillagespace.com/cyber-security-issues-in-pakistan/

Comparatively as per Global Cyber security index 2017, India rank on 23rd out of 165 countries of the world. The global report was issued by ITU. In information technology's national cyber security policy 2013, believed in information sharing and cooperation. Because cyber-crimes are not the problem of one state rather it is a global issue and needs global consciences on it. That's why Indian government is collaborating with a number of countries like the US, European Union, Malaysia on cyber security. The close cooperation between US and India on cyber security strategy shows their common interests in which the US will help the government of India to secure its national cyber system, capacity building in the research and development center. Even both countries agreed to strengthen the critical information infrastructure, share the cyber threats, develop a joint mechanism to prevent digital threats and promote each other's law enforcement agencies.[93]

China also agrees to cooperate with India on cyber security. It happened in Vivkananda international foundation, basically a think tank in New Delhi, where a joint trilateral meeting was held among the representative of China, US and India. The basic purpose was to develop a relationship on cyber security and socio economic.[94]

Recently 4th cyber dialogue took place between UK and Indian. In which both countries shared their views about international cyber threats to the national security of the states. Then they were in favor of international law and international internet governance. They signed the agreement of the commonwealth cyber declaration for cooperation of implementation of plans through their capacity building. The fifth UK and India cyber dialogue will be held in the UK in 2019. Besides that UK has agreed to establish a proposed National Cyber-crime Cooperation Center in India.[95]

---

[93]Office of Press Secretary, "Fact Sheet: Framework for the U.S-India Cyber Relationship," *The White House*, June 7, 2016, accessed November 13, 2018, https://obamawhitehouse.archives.gov/the-press-office/2016/06/07/fact-sheet-framework-us-india-cyber-relationship

[94]ANI, "India, China, US agree to cooperate more on cyberspace security," *The Economic Times*, July 12, 2018, accessed November 13, 2018, https://economictimes.indiatimes.com/news/defence/india-china-us-agree-to-cooperate-more-on-cyberspace-security/articleshow/61685145.cms

[95]British High Commission New Delhi, "The 4th UK-India Cyber Dialogue," *GOV.UK*, August 9, 2018, accessed November 14, 2018, https://www.gov.uk/government/news/the-4th-uk-india-cyber-dialogue

India is busy in developing its strong ties with developing states regarding cyber security. The Indian government is very much concerned about its digital system security. But besides that Pakistan is lacking because the government is not taking the issue as seriously as it should be.

## 4.6 Conclusion

Resultantly, Pakistan's cyber preparedness and how much Pakistan is taking safety measures to secure the digital system. As globally states are moving towards an advance system of the internet but similarly the ratio of cyber-crimes are increasing more rapidly. That is why states are making cyber-crimes laws to deal with those criminals. In the case of Pakistan, it is doing a gradual effort in making cyber laws and their implementation. But the major issue of cyber laws in Pakistan that the punishment is too harsh and very much difficult to practice in reality. Secondly, those laws are just dealing just with cyber-crimes, not cyber security like if any critical cyber-attack happened than no governmental institute takes the responsibility. Because of that government of Pakistan should take the issue more seriously. Comparatively India government is very much concerned about its digital security for that sake they are making cyber laws and doing amendments with the passage of time as per the requirements. Secondly, not only public but private institutes are also collaborating with the government in the matter of cyber security.

In the field of technical measures Pakistan is also lagging behind. PISA CERT is the first computer emergency response team in Pakistan. It's not governmental but a private entity. The e-government components like NADRA, FPSC, and banking sector are a very much attractive target for hackers. Even recently FIA issued a report in which it was declared that all Pakistani banks data has been hacked. They lost a huge amount through their credit and debit cards. Here the government of Pakistan needs to essentially develop a national computer respondent team who deal with such sort of cyber-attacks and try to trace them. On the other side, India established the National Technical Research

Organization for securing the critical infrastructure of the country. Furthermore, develop a CERT-FIN to deal separately with financial frauds.

Furthermore, the developing countries know the importance of cyber security that it's not just about making laws or strategies. Now cyber security needs a detailed study about it. That's why organizations become part of it. They are offering cyber security courses for higher education in which not only developed but developing states like India is taking a very much active part. Indian higher education system said all colleges and universities will offer cyber security as a subject in their institutes so at the end of 2025 they will be able to produce around 500,000 cyber professionals. Pakistani organizations are now doing some efforts, in which universities like NDU, Air, NUST are taking part or offering cyber security as a subject for MS and PHD. Apart from that the government of Pakistan should encourage the efforts of those organizations and provide them full support where ever required.

Moreover, ICT is the major entity in Pakistan which is working for capacity building measures. ICT was the representative of Pakistan in OCT international conference. In which higher commissioner of UK said we need to collaborate with each other for preventing cybercrimes. ICT is also having a plan, that 226 Islamabad school girls will be trained for coding and cloud computer. Apart from that Microsoft announced that they have a plan to establish a training and development center in Pakistan. That will be effective for both local and private sector to secure their cyber system. But the government is separately not doing any kind of effort to improve the country's capacity measures. On the other hand, Indian information security education and awareness programmers are trying to spread cyber security information in both formal and informal ways. India is the member state in EU organization on cyber security capacity building measures. In which also share its view about how to protect the digital system.

Lastly, the government of Pakistan is not a part of any international organization or making alliances with other developed countries on cyber security. Although it's not just one country problem it's a global issue and requires global concern. So states need to work together to address the issue and until the government of Pakistan not taking it into serious consideration, the matter will remain unresolved. But India is comparatively quite

active in developing international relations with more developed states like the UK, US, Malaysia and China for getting better assistances for protecting its national cyber system. Because the Indian government believes in it that cyber security or cyber-crimes are not the problem of one state, it's a global problem and needs a global consensus on it.

# CONCLUSION

The study analyzes the cyber capabilities of India as a non-traditional threat for Pakistan. As both countries have historical enmity, due to previously fought military wars. With the passage of time, the trend of traditional wars has converted into non-traditional wars. To avoid cyber-attacks states take different measures and frame laws to prevent further attacks. India and Pakistan also have cyber laws to protect their digital system. In the case of India, the government of India is much concerned about cyber laws developed to deal with a number of cyberspace issues. Apart from that, they are much conscious of the privacy of individuals. Unfortunately, Pakistan is lagging behind in terms of making cyber laws and their implementation. Even years back Pakistan gave legislation to cyber law, but criticism prevailed in the private sector. As per their opinion, the law gives too much power to the government and affects the privacy of the citizens.

Furthermore, both states are rapidly converting their critical infrastructure into digital systems. The Indian government is paying more focus to its IT sector and planning to expand it through hiring more cyber experts. Pakistan is increasing its dependency on cyberspace, but the government is not taking much security measures as required. In global cyber security index and on a regional level, India ranked at 3$^{rd}$ and Pakistan on 13$^{th}$. Pakistan does not have a single institute to control the cyber criminals activities as per the international standard. Although 40% cyberspace sector is under the control of private sector remaining comes under the control of the government. Even now there is no cyber security strategy that is acceptable by the government. PK.CERT is the only official institute which responds to the cyber-criminal activities. India has a proper cyber-criminal law in which penal code and information technology act, are addressing the cyber-crimes of the country. Indian CERT is officially acknowledged entity and in the next five years plans about information security. The Indian government is trying to meet the global standards of digital security.

The security of critical infrastructure becomes the primary concern of states. Here India and Pakistan are also doing some efforts to secure the cyber system. That is because, after the Stuxnet attack, nuclear states are worried about their nuke safety. Pakistan needs to do

a lot more effort to protect its nuclear digital system from cyber threats. The two major reasons Pakistan has to secure its digital system are: first globally, the image of Pakistan's nuclear aspect. Secondly, India is posing a potential threat to Pakistan's nuclear because it is getting the latest technical assistance from US and Israel. Both those states were already involved in Stuxnet attack and they are also defaming the image of Pakistan's nuclear aspect to the world.

Cyber warfare is not a new dilemma between India and Pakistan. The hackers of both countries are targeting the sensitive sites of each other. Up to now there is no full-fledged war that has happened between them, but there are some chances that it can happen. Many writers give their opinions through articles, in which they mention that Pakistan is not fully prepared to deal with cyber warfare. The Pakistani government is not taking the issue seriously. On the other side the Indian government is fully working on its cyber arms, so that in future, they will be able to deal with cyber warfare if it ever happened.

Additionally, a Symantec corporation, a digital security company published a report about South Asian regional cyber espionage in which India and Pakistan are the main target of hackers? India is taking the maximum measures to avoid cyber espionage. It has established a malware analysis center to address the malware threats. Pakistan is not making any effort to prevent further cyber espionage and even the Pakistani officials are denying from the report.

Pakistan is planning to introduce the Electronic voting machine in coming years. Although throughout the globe only eleven countries are using the EVMs system and most of them are developing states. Still, after having advanced technologies, their EVMs system got hacked. As a developing state it's quite difficult for Pakistan to use the EVMs system and prevent hacking during the process. The developing states prefer the USA the whole campaign of the current election was hacked by Russians. So a similar case can happen between India and Pakistan. India is already using that system and is well aware from the technical lacking in that system. But Pakistan is for the first time ever trying to introduce it so it's quite hard for it to understand the complications of EVMs system.

In the end, in terms of cyber preparedness, Pakistan is lagging behind especially in these fields like technical measures, legal measures, organizational measures and international cooperation. The government of Pakistan is not taking the issue seriously. On the other side, India is working hard in all the above fields because the Indian government is well aware of the consequences of it.

Cyber threats gained prominence globally in literature as well as at policy level. Majority of states are enhancing its security of law and strategies to counter cyber threats. Although Pakistan is expanding its cyber reach at national level but presently far behind when it comes in comparison with India. The steps Pakistan has taken to counter its cyber threats have not adequately addressed the issue.

Pakistan should not only has to formulate laws and strategies to curb Indian cyber threat at policy level but also need to work at lower level .i.e. educational institutes. Pakistan's universities should develop separate departments at specifically deals with cyber studies. It is real need of Pakistan to counter evolving cyber security threats. Thus, Pakistan educational institutes should produce individuals those can contribute to enhance Pakistan's cyber capabilities.

Additionally, as cyber security threat is seriously threatening Pakistan security therefore Pakistan should have to collaborate with international organizations dealing with cyber security issues. Pakistan need not only proper legislation , policy making but also strict implementation. The role of academia and education in cyber security is integral thus the study is a step in that direction.

**FINDINGS**

- Both India and Pakistan have cyber laws but for Pakistan it is difficult to implement those laws due to lack of implementation mechanism. While India is very much concerned about the protective measures taken for the privacy rights of the citizen, it is badly missing in Pakistan cyber law.
- India has devised a well-developed cyber secure strategy with the involvement of number of institutions but Pakistan is still struggling to devise a proper strategy for securing its digital system.

- At government level, India is taking the cyber security issue more seriously but unfortunately the Pakistani government is least concerned in addressing the cyber security issues.
- Pakistan is deficient cyber crime legislation such that it does not have a single national office that follow the international standards of cyber security. But on the other side, India is having well established cyber criminal legislation for their country.
- When it comes in comparison with other states, Pakistan still lack in national agency which particularly address cyber space issues and take the responsibility of any cyber attack.
- Keeping Stuxnet attack into consideration (USA and Israel's cyber attack on Iranian nuclear facility), India could take cyber assistance from Israel and USA with the aim to attack on Pakistan's nuclear capability as it already in cooperation with these two states.
- The introduction of Electronic voting machine is a plan in Pakistan which will be implemented in coming years while India has already introduced it in past. Here, on the basis of hacking activity of Russia observed in US elections, the same scenario can happened between India and Pakistan.

**Recommendations**

Pakistan is trying to meet the modern globalization criteria. For that Pakistan must identify the vulnerable cyberspace threats to its national security. To secure Pakistan's national security, few recommendations are proposed.

- Pakistan should establish a national cyber security strategy as soon as possible and then establish some institutes who determent the national role and responsibility of the state.
- Government itself strictly observes the institutes that are competing for the required conditions of national information security policy. If they are unable to meet the criteria so the government need to take solid steps against them

- Governmental, military and other institutions must plan an information security course. That must be attended by all the employees so they have basic knowledge about cyber security. Then gradually all these departments will be flourished in terms of cyber security.
- HEC also need to take the initiative to encourage university sector to do more work on cyber security including: offering courses related to cyber security. In this way number of Pakistanis will be trained in cyber security development.
- The government of Pakistan needs to establish a friendly relationship with developing states to acquire technical guidelines from them.
- Pakistan should join regional and international treaties regarding cyber security.
- The government of Pakistan must create an institute that arranges conferences and spreads cyber awareness in both the public and the private sector.
- The government should create a group of cyber experts who analyze the digital critical infrastructure of the state and later come up with the basic loophole within the cyber system. Then they recommend some suggestions those should be taken seriously by law makers.

# BIBLIOGRAPHY

Asmi, Fahad, Rongting Zhou, and Maoqian Wu. “Measuring E-Reading among Non-Users of Internet Banking in Pakistan: By TAM with CRM as External Factor.” *European Journal of Business and Management*, No. 29 (2016): 2222-2839.

Awan, Imran. "Cyber-extremism: Isis and the Power of Social Media." *Society*, No. 54 (April 2017): 138-149.

Awan, Imran. "Islamophobia on Social Media: A Qualitative Analysis of the Facebook's Walls of Hate." *International Journal of Cyber Criminology*, No.1 (January 2016): 1-20.

Bakshi, Preshant. “Se curity Implications for a wired India.” *Strategic Analysis,* No. 1 (April 2001): 105-117.

Baker, White Elizabeth. “A Model for the Impact of Cyber Security Infrastructure on Economic Development in Emerging Economies: Evaluating the Contrasting cases of India and Pakistan.” *Information Technology for Development*, No. 2 (April 2014): 122-139.

Blakemore, Brian. *Policing cyber hate, cyber threats and cyber terrorism*. London: Routledge, 2016.

Blakemore, Brian. *Extremism, Counter-terrorism and Policing*. New York: Routledge, 2016.

Broadhurst, Roderic, and Lennon YC Chang. “*Cyber Crime in Asia: trends and Challenges*.” In Handbook of Asian Criminology, pp. 49-63. Springer, New York, 2013.

Broadhurst, Roderic, and Peter Grabosky, ed. *Cyber Crime The Challenge in Asia*. Hong Kong: Hong Kong University Press, 2005.

Carr, Jaffery. *Inside Cyber Warfare*. Inc: O’Reilly, 2010.

Carr, Jeffrey. *Inside cyber warfare: Mapping the cyber underworld*. Inc: O'Reilly Media, 2011.

Choucri, Nazli. *Cyber Politics in international Relations*. London: MIT Press, 2012.

Chandio, Khalid. “Cyber security/warfare and Pakistan.” *IPRI*, August 13, (2015)

Chen, Thomas M. "Stuxnet, the real start of cyber warfare?[Editor's Note]." *IEEE Network*, No. 6 (November 2010): 2-3.

Colarik, Andrew M. *Cyber terrorism: political and economic implications*. America: Igi Global, 2006.

Dahan, Michael. "Hacking for the homeland: Patriotic hackers versus hacktivists." In *ICIW 2013 Proceedings of the 8th International Conference on Information Warfare and Security.* America: Academic Conferences Limited, 2013.

Devi, Sushma. *National Security in Digital age: a Study of Cyber Security Challenges in India*. London: Academica Press, 2018.

Ganguly, Sumit, Manjeet Pardesi, and Nicolas Blaral. *The Oxford Handbook of India’s National Security*. New Delhi: Oxford University Press, 2018.

Guiore, N. Amos. *Cyber Security Geopolitics, law and policy*. New York: Routledge, 2017.

Gudgel, E. John. “Cyber War Versus Cyber Realities: Cyber Conflict in International System.” *Small Wars and Insurgencies*, No. 3 (April 2016): 550-552.

Heickero, Roland. “Cyber Antagonism Between Hacker Groups Develops new ChaHenges.” *Leading Issues in Information Warfare and Security Research*. No.1 (2011): 54.

Langner, Ralph. "Stuxnet: Dissecting a cyberwarfare weapon." *IEEE Security & Privacy*, No. 3 ( May 2011): 49-51.

Lewis, Andrew James. “ Sustaining Progress in International Negotiations on Cyber Security.” *CISC*, No.1 (July 2017): 1-7.

Lindsay, Jon R. "Stuxnet and the limits of cyber warfare." *Security Studies*, No. 3 (July 2013): 365-404.

Ilyas, Muhammad. “E-Governance Practices and Models; Options for Pakistan.” *ISSRA*, no.1 (June 2016):43.

Ivancík, Radoslav, Pavel Necas, and VojtechJurcák. "Theoretical view of some current global security challenges." *Incas Bulletin* 6, no. 1 (January 2014): 99.

Janczewski, Lech J., and Andrew M. Colarik. *Cyber Warfare and Cyber Terrorism*. America: ICG, 2008.

Jan, Faizullah. “Social Media and Cyber Jihad in Pakistan.” *Islamic Research Index*, (June 2016): 34-47.

Jaishankar, Karuppannan, ed. *Cyber criminology: exploring internet crimes and criminal behavior*. London: CRC Press, 2011.

Kenney, Michael. "Cyber-terrorism in a post-stuxnet world." *Orbis*, No. 1 (2015): 111-128.

Khan, Saqib, and Khalid Mmanzoor Butt. “Cyber Technology, Radicalization and Terrorism in Pakistan.” *Journal of Indian Studies*, No. 2 (December 2017): 119-128.

Khushi, Yunis. “ISIS in Pakistan: A critical Analysis of Factors and Implications of ISIS recruitments and concept Jihad-Bil-Nikah.” *Art and Social Sciences Journal*, No.1 (June 2017): 13.

Mateen, Ahmed, and Qaiser Abbas. “Tsunami of Cyber Crime: Analysis of Cyber Crime New Trends, Causes and Remedies in Future Prospectus.” *International Journal of Computer Applications*, No. 8 (October 2016): 29-32.

Mccarthy, R Daniel. *Power, Information Technology, and International Relations Theory*. London: Palgrave macmillan, 2015.

Moore, Stephen. “Cyber Attacks and the Beginning of an International Cyber Treaty.” *North Carolian Journal of International Law and Commercial Regulation*, No. 1 (2013): 223- 257.

Nazir, Maryam. “Cyber security and Pakistan.” *IPRI*, (January 2017).

Naseer, Rizwan, and Musarat Amin. “Cyber Threats to Strategic Network: Challenges for Pakistan’s Security.” *South Asian Studies*, No. 1 (June 2018) : 35-48.

Prichard J. Janet, and Laurie E. MacDonald. “Cyber Terrorism: A Study of the Extent of Coverage in Computer Security Textbooks.” *Journal of Information Technology Education*, No. 3 (2004):279-289.

Rasool, Sadia. “Cyber Security Threat in Pakistan: Causes, Challenges and Way forward.” *International Scientific online Journal*. No.12 (2015): 21-32.

Richet, Loup-Jean, ed. *Cybersecurity policies and strategies for cyber warfare prevention*. IGI Global. 2015.

Sabbeir, Muhammad. “Cyber Security in Pakistan: Emerging threats and preventive measures.” *ISSPR PAPERS*, No.7 (2013): 25.

Schaap, Arie J. "Cyber warfare operations: development and use under international law." *AFL Rev.* No.2 (2009): 121.

Shabbir, Muhammad. “Cyber Security in Pakistan: Emerging Threats and Preventive Measures.” *ISSRA*, No.2 (2013):25.

Singh, Onkar, Priya Gupta, and Roushan Kumar. “A Review of Indian Approach towards Cyber Security.” *International Journal of Current Engineering and Technology*, No. 2 (2016): 644-648.

Taylor, Robert W, Eric J. Fritsch, and John Liederbach. *Digital crime and digital terrorism*. America: Prentice Hall Press, 2014.

Yar, Majid. *Cyber Crime and Society*. London: Sage, 2006.

Zlateva, Tanya, and Virginia Greman. *Proceeding of the 11th International Conference on Cyber Warfare and Security*. USA: Academic conferences and publishing limited, 2016.