NATIONAL SECURITY IN THE AGE OF CYBERSPACE:

A CASE STUDY OF PAKISTAN

By

MUHAMMAD ASLAM

A THESIS SUBMITTED IN PARTIAL FULFILMENT OFTHE
REQUIREMENT FOR THE DEGREE OF

MASTER OF PHILOSOPHY

Department of International Relations

To

FACULTY OF SOCIAL SCIENCES

NATIONAL UNIVERSITY OF MODERN LANGUAGES, ISLAMABAD

August 2021

NATIONAL UNIVERSITY OF MODERN LANGUANGES FACULTY OF SOCIAL SCIENCES

THESIS/DISSERTATION AND DEFENCE APPROVAL FORM

The undersigned certify that they have read the following thesis, examined the defense, are satisfied with the overall exam performance, and recommend the thesis to the Faculty of Social Sciences for acceptance.

Thesis/ Dissertation Title: **NATIONAL SECURITY IN THE AGE OF CYBERSPACE: A CASE STUDY OF PAKISTAN**

Submitted by: Muhammad Aslam **Registration #: 1667 MPhil/IR/F18**

Masters of Philosophy
In International Relations

International Relations
Discipline

Dr. Rizwana Abbasi ____________________
Signature of Research Supervisor
Research Supervisor

Dr. Rizwana Abbasi ____________________
HOD (IR) Signature of HOD (IR)

Prof. Dr. Mustafeez Alvi ____________________
Dean (FSS) Signature of Dean (FSS)

Prof.Dr Muhammad Safeer Awan ____________________
Pro-Rector Academics Signature of Pro-Rector-ACAD

CANDIDATE DECLARATION FORM

I Muhammad Aslam

Son of Sttar Bukhash

Registration # 1667 MPhil/IR/F18

Discipline International Relations

Candidate of **Masters of Philosophy** at the National University of Modern Languages do hereby declare that the thesis: **NATIONAL SECURITY IN THE AGE OF CYBERSPACE: A CASE STUDY OF PAKISTAN** submitted by me in partial fulfillment of MPhil degree, is my original work, and has not been submitted or published earlier. I also solemnly declare that it shall not, in future, be submitted by me for obtaining any other degree from this or any other university or institution.

I also understand that if evidence of plagiarism is found in my thesis dissertation at any stage, even after the award of degree, the work may be cancelled and the degree revoked.

Signature of Candidate

Dated

Muhammad Aslam

Name of Candidate

Table of Contents

ACKNOWLEDGEMENT

I am thankful to Allah Almighty who gave me wisdom, knowledge, potential and courage to seek and search the facts existing in our surroundings and bestowed me Determination to go through the complicated and obscure facts hidden in our world; gave me the sense of judgment to finalize it with my precise and justified find-outs for the complicated environment of international politics in my research work. Special appreciation goes to my supervisor, Dr. Rizwana Abbasi for her supervision, patience, sound judgment and constant support. Her invaluable help of constructive remarks, recommendations, advice, and direction revealed me throughout the thesis works have contributed to the success of this research.

Last but not least, my deepest gratefulness goes to my beloved parents and also to my siblings for their endless love, supports, prestigious prayers and best wishes and to those who indirectly contributed in this research, your compassion means a lot to me. Thank you very much.

Muhammad Aslam

DEDICATION

With utmost devotions, I dedicated my whole work to my beloved and affectionate Parents, Sisters, Brother, Friends and Respected Staff of International Relations Department who have always been source of encouragement, knowledge, illumination and wisdom for me, whose pray and guidance showed me the right path and made the blessing of Allah shower on me.

LIST OF ABBREVIATION

5GW	Fifth Generation Warfare
C2	Capability 2
NR3C	Center for Cyber Crime
CNBC Pakistan	Watch Live Watch Live Gourmet News Network
CVE	Common vulnerabilities and exposure
CNO	Computer Network Operations
CERT	Computer Emergency Response Team
CBMs	Confidence-building measures
CTF	Cyber-taskforce
DoD	Department of Defense
DOS	Denial of service attacks
DDoS	Distributed Daniel of services
GIS	Geographic Information System
GPS	Global Positioning System
PKCERT	Establishment of Pakistan Computer Emergency Response Team
FIA	Federal Investigation Agency
HUBCO	Hub Power Company Limited
ICT	Information and Communication Technology
IT	Information Technology
ISRT20	Internet security threat report
ICS	Information Control Systems
IAEA	International Atomic Energy Agency
INGOs	International non-governmental organization
ICAN	International Campaign to Abolish Nuclear Weapons
JUI-F	Jamiat Ulema-e-Islam
NHS	National Security Services
NACTA	National Counter Terrorism Authority
NGOs	Non-governmental organization
NTISB	National Telecommunications and Information Technology Security Board
NCSB	National Communication Security Board
NSA	National Security Agency
C412SR	Pakistan’s command, control, communications, Computers, intelligence, information, surveillance, and Reconnaissance
PTA	Pakistan Telecommunication Authority

PLC	Programmable logic controllers
PPP	Pakistan Peoples' party
PML-N	Pakistan Muslim League
PIAIC	Presidential initiative for Artificial intelligence and Computing
PECA	Prevention of Electronic Crimes Act, 2016
PECO	Prevention of Electronic Crime Ordinance 2009
PK-CERT	Cyber Security Company in Pakistan
PTCL	Pakistan Telecommunication Company Limited
RAT	Remote Access Trojan
RAND Corp	Research and development
SCADA systems	Supervisory control and data acquisition
SCO	Shanghai Cooperation Organization
RADARS	Radio Detection and Ranging
SAARC	South Asian Association of Regional Cooperation
SWIFT	Society for Worldwide Interbank Financial Telecommunications
NRC3	The National Response Center for Cyber Crimes
UN	United Nations
USCYBERCOM	United States Cyber Command
WAPDA	Water & Power Development Authority

ABSTRACT

Pakistan is a least prepared country against cyber warfare from hostile nations/elements. Cyber warfare is a domain that poses major challenge to the national security of Pakistan. Indeed, the digital domain determines the defeat and triumph of rival parties whether it's in politics, business, or battlefield. More so, the enemy in cyber domain is invisible and unpredictable, therefore, it becomes very hard for nation states to identify the actual enemy. Although there is no dearth of literature in this field, however there seems insufficient scholarly literature on the case study of Pakistan. The main objective of the research is to evaluate the challenges and threats faced by the national security of Pakistan in the Age of Cyberspace and recommend viable solutions to protect cyberspace to meet future challenges. Moreover, this research is an attempt to make an addition to the existing body of knowledge while comprehending cyber challenges to national security of Pakistan and its response to mitigate such threats. The thesis discusses as to how Pakistan should carefully complete its cyber threat mapping, and craft a new strategy to overcome such threats.

INTRODUCTION

Cyber threat and cyber warfare are new kinds of threats. The hostilities are launched by communication and electronic systems. Cyber warfare is the shift in the paradigm of warfare. Traditional army and armaments such as bombs and bullets have no role in it. With the transition of the world into the age of information, the number of threats has emerged to the national security. With our transition into the information and the technology age, the door to the series of cyber threats to the national security of the states has been opened. The advance development of the technology and more dependence on the computers cause changes in the ideology of national security not only for our nation but for all the nations. The nations have this fear and threat that their information data base may be hacked, changed or debilitated by any other attacking or offensive advance technology. Threats may occur by new and advance technology and effects on the national security in cyber domain. Nevertheless, the cyber threat is a threat to Pakistan's national security in the contemporary age.[1]

Cyber security is a serious matter to the national security of Pakistan because it is open 24/7 having no borders. Cyberspace of any country can be penetrated anytime and sensitive information and data are at risk.[2] Whole systems of any country can be paralyzed through cyber warfare. [3]

National Security of Pakistan always remained a matter of grave concern for its security agencies due to its eternal enmity with its neighboring country, India. Pakistan strengthened its defense on every ground to cope with any internal or external threat. In traditional domain, Pakistan has robust weapon system and capability to maintain it national security and survival.[4]

[1] Anthony Craig and Brandon Valeriano, "Realism and Cyber Conflict: Security in the Digital Age," E-International Relations, last modified February 3, 2018, https://www.e-ir.info/2018/02/03/realism-and-cyber-conflict-security-in-the-digital-age/.

[2] Quoted in, Donna Lee and Paul Sharp, *The New Public Diplomacy: Soft Power in International Relations*, ed. Jan Melissen (London: Palgrave Macmillan, 2005).

[3] Gabriel Weimann and Bruce Hoffman, *Terror on the Internet: The New Arena, the New Challenges* (Washington, DC: US Institute of Peace Press, 2006).

[4] Ibid.

In cyber warfare, attackers can intrude in Pakistan's commercial sector, security sector via gadgets of information technology.[5] Many incidents have occurred between India and Pakistan where the hackers of both the countries have hacked many sensitive websites of each other and stolen sensitive information and major threats for each other's national security.[6] Indian hackers hacked the website of the ministry of foreign affairs and Pakistan hacked the CBI website which is considered as the direct attack on the national security.[7] Hundreds of other officials' websites are being penetrated from both sides reciprocally.[8] So a cyber-war is being fought between both countries and making the national securities at risk. Pakistan is not only prone from the Indian sides but it is also being spied from many other countries due to their hidden interests such as USA and UK.[9] India and USA have been attempting to seize the data through cyber-attacks to defeat China and its strategies on the regular basis.[10] Consequently, cyber-security is necessary for the national security of Pakistan.

In order to make national security of Pakistan imperious, there is a need to concentrate on the strategies related to cyber threat because the threat is growing rapidly with the passage of time. In order to build meaningful and commanding infrastructure relating to cyber security in Pakistan, there are recognizable barriers, such as absence of central authority to educate the Premier of Pakistan to take decisions and allocate funds to strengthen the national security. This creates a deep gap in the policy circles on need and urgency of growing cyber threats. Although the government has introduced the cyber-crime laws, there is a deficiency in the legislation and policies of cyber security. The players are not clearly identifiable; therefore, their turfs are not marked out adequately.

[5] Fred Schreier, *On Cyberwarfare* (Geneva: Geneva Centre for the Democratic Control of Armed Forces, 2015).

[6] Center for Strategic and International Studies, "Significant Cyber Incidents | Center for Strategic and International Studies," *Center for Strategic and International Studies* |, 2021, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

[7] Naveed Siddiqui, "Ministry of Foreign Affairs Website Hacked, Inaccessible in Several Countries," *DAWN*, February 16, 2019, https://www.dawn.com/news/1464217.

[8] Ibid.

[9] Rizwan Naseer, Musarat Amin, and Kinza Shaheen, "Cyber Security Challenges in South Asia and Room for Cyber Diplomacy," *NDU Journal*, 2020, https://ndu.edu.pk/ndu-journal/articles/ndujournal2020/07-CYBER-SECURITY-CHALLENGES-IN-SOUTH-ASIA-AND-ROOM-FOR-CYBER-DIPLOMACY.pdf.

[10] Mubeen Ashraf, "Cyber threats to Digital Pakistan," *THE NATION*, December 31, 2019, https://nation.com.pk/31-Dec-2019/cyber-threats-to-digital-pakistan.

This research is an attempt to illustrate the threats and problem being faced by security and governmental sector of Pakistan on the cyber space ground and theme by Pakistan to strengthen its national security in the age of cyber space and to recommend a viable way forward for Pakistan.[11]

Statement of the Problem

Researchers are highly passionate to conduct research on this vary issue which has been spreading rapidly because of its personal interest in the security and defense subject. Due to the continuous evolution in the field of cyber technologies, cyber systems and growing adaptation in Pakistan at both levels, military and civil sectors have presumed to expose the possible cyber threats from hostile components or nations, and the serious implications of cyber attacks. There is a massive growth of cyber infrastructure and structures, providing Pakistan with new security challenges or known enemies. This study identifies existing policy gaps, known or unknown challenges and threats have been analyzed in the context of Pakistan's national security in the cyber space era, proposing feasible cyber security measures to preserve and protect the sensitive and confidential data or information from the state.

Objectives of Study

- This study aims at adding new perspectives into the existing body of knowledge on comprehending seriousness and challenges faced by Pakistan in cyber domain and new mechanism that Pakistan may take as a guiding post towards policy contributions.
- To evaluate the challenges and threats faced by the national security of Pakistan in the Age of Cyberspace.
- To recommend viable solutions to protect cyberspace to meet future challenges.

Research Questions

Q 1: How is the evolving cyber space threatening National Security of Pakistan?

Q 2: How robust is Pakistan's existing policy mechanism and infrastructure against Cyber threat?

[11] Marie Baezner, "Hotspot Analysis: Regional rivalry between India Pakistan: tit-for-tat in cyberspace," *Center for Security Studies (CSS)* 1 (August 2018), https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2018-04.pdf.

Q 3: Why Pakistan fail in order to perceive the Cyber Security?

Q 4: How can Pakistan confront/respond to the futuristic challenges emerging from Cyberspace?

Literature Review

Literature has been examined on cyber-threats, cyber-crimes and vital infrastructure. Pakistan's vital infrastructure case study has been taken into consideration. Cyber risks to CIs have been identified after evaluating Pakistan's vital infrastructure. The research further reduced cyber manipulation by Pakistan's cyber-space attackers and also addressed significant tactics / instruments utilised by cyber-attackers. The Government of Pakistan has evaluated countermeasures to preserve vital infrastructure and the ability of International Organizations to address cyber attacks. The critical infrastructure literature demonstrates that the definition of CI for every nation remains the same.[12] The discussion on cyber war, cyber space terror, cyber espionage, cyber dangers, physical threat to CIs, which continue to evolve, are still in progress. However, the existing literature about these topics and their major outlines offered a good insight into this paper.

In addition to facilitating nation-states, cyber space has powered non-state actors, cybercriminals and hackers as well. They are able to influence the political arena governed by national states. Cyber space also allows these cyber attackers to disguise their identity and therefore raises vulnerabilities when manipulating Internet space. Cyber warfare and cyber espionage continue to be a challenge, according to the author, because governments are major risks to key infrastructure, which lead to the collapse of the nation-state. In terms of defining the word cyberspace, an overview of contemporary cyberspace activities and of the difficult cyberspace crimes and/or threats is of great importance. This study focuses on those who are using cyberspace due to various chances. Nevertheless, cyberspace is the ideal platform to manipulate. The paper addresses cyber space dangers and problems offered by cyber citizens or cyber users.

[12] John Moteff and Paul Parfomak, *Critical Infrastructure and Key Assets: Definition and Identification*, (USA: Resources, Science, and Industry Division, CRS Report for Congress, 2004), https://sgp.fas.org/crs/RL32631.pdf.

This paper provides a comprehensive analysis of current cyberspace literature and finally analyses many key and significant cybernatal activities.[13]

Stefan Fenz discusses contemporary daily lives issues through cyber risk (online banking, fiscal computing, on-line health and care, critical infrastructural control) and highly demands enormous security efforts in his paper "Cyberspace Security: A Definiture and A Description of Remaining Problems" (2005). The article also defines 'cyberspace' and explains safety here.[14]However, the impacts on the national security of Pakistan are not discussed in the literature.

The European Union Agency for Network and Information Security publishes the ENISA Threat Landscape Report 2016. Details of the major threats evaluated in 2016 are provided in the following report. In the third chapter of this paper, which focuses on the cyber menace in general as well as the cyber danger to critical infrastructure in particular, the most sophisticated and persistent cyber threats of 2016 have been identified here.[15]The hindrance in way of strong national security is not discussed in the report.

The Internet landscape of Pakistan is a Yahanzaib Haque study that describes the rules and practises of Pakistan's online system. It describes the government's online mechanisms. The study also points out the historical point of view, internet monitoring, means, impact and aim of such monitoring. The paper attempts towards the end to find out how various stakeholders are examining the Internet infrastructure. The study gives an overview of this issue, however the cyber manipulation is not properly mapped and threats to the national security due to cyber-warfare are not incorporated.[16]

[13] Ahmed Alnagrat, Shakirat H. Sulyman, and Nur Adlya B. Muktar, "An Overview of Contemporary Cyberspace Activities and the Challenging Cyberspace Crimes/Threats," *Research Gate* 12, no. 3 (May 2014), https://www.researchgate.net/publication/311953165_An_Overview_of_Contemporary_Cyberspace_Activities_and_the_Challenging_Cyberspace_CrimesThreats.

[14] Stefan Fenz, *Cyberspace Security: A definition and a description of remaining problems*, (Information Society & E-Government, 2005), https://www.univie.ac.at/frisch/isegov/aushaengUniWien/CyberpaceSecurity_Fenz.pdf.

[15] ENISA, *ENISA Threat Landscape Report 2016*, (European Union Agency for Network and Information Security, 2017), https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016/at_download/fullReport.

[16] Jahanzaib Haque, *Pakistan's Internet Landscape*, (Islamabad: Bytes for All, Pakistan, 2013), https://www.academia.edu/9731697/Pakistans_Internet_Landscape.

In his work "Information Warfare Understanding and its Relevance to Pakistan," Khurshid Khan has given a thorough assessment of the information war and its relevance to Pakistan. The article detailed the idea of war on information, its features, the situation of war on information worldwide and how Pakistan faces IW challenges today. This paper is an excellent effort for the examination of accessible literature.[17]Other aspects including infrastructure and military related are not explored in the literature.

A Situational analysis and way ahead, Zibber Mohiuddin's work is one of Pakistan's rare literature on the role of Pakistan in the cyber industry. It begins with background information on the roots of internet and cybercrimes, cybercrimes kinds and cybercrimes objectives. It also addresses cyber laws, Pakistan's position in the cyber world in contrast with Pakistan, and worldwide issues of cyber law.[18] On the contrary, the threats to the military, infrastructure, and public are not addressed in the paper.

Andrew Futter, in, *Hacking the Bomb: Cyber Threats and Nuclear Weapons*, explains that states continue to modernize their nuclear weapon systems and grapple with cyber security policy.[19] Historically, strategists had no need to consider cyber threats aimed at disabling, tampering with, or launching nuclear weapons, because nuclear systems were more isolated than other defence systems. Today, in an increasingly interconnected world, more convenience comes with more security vulnerabilities. Although interagency officials may be inclined to modernize the nuclear triad in a more integrated manner, the fact that these systems remain independent is vital to their security and ours. Futter reveal show the net-working of U.S. nuclear systems could leave the U.S.'s arsenal vulnerable to cyber-attack. A thorough read of this well-researched text is likely to influence the thinking of policy makers, increasing the likelihood that they take more seriously the grave threats posed by cyber actors to strategic weapon systems.[20]*Hacking the*

[17] Khurshid Khan, "Understanding information warfare and its relevance to Pakistan," *Institute of Strategic Studies Islamabad*, 2011, http://www.issi.org.pk/wp-content/uploads/2014/06/1379480610_58047454.pdf.

[18] Zibber Mohiuddin, "A PAPER PRESENTED ON: CYBER LAWS IN PAKISTAN; A SITUATIONAL ANALYSIS AND WAY FORWARD," *Ericsson Pakistan (Pvt).*, 2006, https://nanopdf.com/download/cyber-laws-in-pakistan-supreme-court-of-pakistan_pdf.

[19] Andrew Futter, *Hacking the Bomb: Cyber Threats and Nuclear Weapons* (Washington: Georgetown University Press, 2018).

[20] Ibid.

Bomb is not all doom and gloom. Futter note show nuclear espionage by cyber means could actually lead to increased stability with respect to nuclear weapons. In the event that an adversary discovers that its rival possesses more advanced nuclear capabilities than previously known, the adversary may seek policies that reduce the chances of escalation and enhance the credibility of deterrence. Furthermore, cyber operations may even aid in counter proliferation efforts. Futter quotes journalist Eli Lake, who say-sit best: “The specific benefit of [cyber] sabotage is that it makes countries [and terrorists] wary”. However, the national security aspect is not discussed in the work.

Dean Cheng in Cyber Dragon: Inside China's Information Warfare and Cyber of purchasing crucial [nuclear-related] materials on the black market.[21] Operations provides a framework for assessing China's extensive cyber espionage efforts and multi-decade modernization of its military, not only identifying the "what" but also addressing the "why" behind China's focus on establishing information dominance as a key component of its military efforts.[22] China combines financial firepower—currently the world's second largest economy—with a clear intent of fielding a modern military capable of competing not only in the physical environments of land, sea, air, and outer space, but especially in the electromagnetic and cyber domains. This book makes extensive use of Chinese-language sources to provide policy-relevant insight into how the Chinese view the evolving relationship between information and future warfare as well as issues such as computer network warfare and electronic warfare written by an expert on Chinese military and security developments, this work taps materials the Chinese military uses to educate its own officers to explain the bigger-picture thinking that motivates Chinese cyber warfare. Readers are able to place the key role of Chinese cyber operations in the overall context of how the Chinese military thinks future wars are fought and grasp how Chinese computer network operations, including various hacking incidents, are part of a larger, different approach to warfare. The book's explanations of how the Chinese view information's growing role in warfare

[21] Ibid.
[22] Dean Cheng, “*Cyber Dragon: Inside China’s Information Warfare and Cyber Operations”*(Santa Barbara: Greenwood, 2016).

benefit U.S. policy makers, while Students in cyber security and Chinese studies better understand how cyber and information threats work and the seriousness of the threat posed by China specifically. It provides a detailed overview and thorough analysis of Chinese cyber activities; Makes extensive use of Chinese-language materials, much of which has not been utilized in the existing Western literature on the subject. It enables a better understanding of Chinese computer espionage by placing it in the context of broader Chinese information warfare activities. They Analyze Chinese military modernization efforts and provide a context for the ongoing expansion in China's military spending and reorganization. It offers readers policy-relevant insight into Chinese military thinking while maintaining academic-level rigor in analysis and source selection. The literature does not focus on threats to the infrastructure and commercial sector of state due to Cyber-warfare.

Martin Libicki, in *Conquest in Cyberspace: National Security and Information Warfare* book takes a different, broader, and possibly more realistic view of the classic info war scenario.[23] Libicki -- a senior policy analyst at the RAND Corp. argues that hostile conquest of the global network is not as big a threat as some believe because of the incredible difficulty to taking control of information systems owned by others, corrupting their data, and/or shutting those systems down. He also argues that the globally connected cyberspace presents an excellent opportunity to drive the actions and attitudes of others.

Media is an essential part of life when it comes to the effects of media. The security dynamics of Pakistan keep changing according to the international environment. The "effects of media" is a crucial function as it may degrade or upgrade the implementation process of cyber security. This is a huge challenge for the concerned authorities. Index portrays a negative image more than the positive image for protective measures. The media highlights human rights violations and excessive investigation rather than issues related to cyber security. The knowledge about cyber security has limited the country as it is a new phenomenon. Now it is the responsibility of media and other involved actors

[23] Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (Cambridge: Cambridge University Press, 2007).

to use media for activating positive aspects and threats of cyberspace. Media is an ideal platform and must be utilized for achieving political support and spreading information about protective measures. But content is not analyzing the impacts on national securities of states, and the impacts on commercial and military sectors of the states.

This is not ahead in the sand analysis that suggests that cyber attacks are not possible; Libicki's premise is more about the practicality and efficacy of such efforts and, therefore, the book is about policy as much as it is about technology. The Internet was developed as the result of U.S. Department of Defense (DoD) research efforts yet has realized its greatest success as means for peaceful commerce and personal intercourse. Its success is the very reason that we even think of the possible impact of hostile actions that might occur. Yet this book is very clearly about hostile conquest *in* -- rather than *of* -- cyberspace, suggesting that while isolated attacks within the Internet can and do occur, what do such attacks mean to the physical world?[24]

Jason, Andress and Steve Winterfeld explains that how cyber attacks and defense intersect with each of the classic war fighting domains of land (Army), sea (Navy), air (Air Force), space (Joint, with Air Force in the lead), and cyber (ubiquitous, with US Cyber Command [USCYBERCOM] just getting organized).[25] Cyber Warfare covers the doctrine being developed today and lays out the tactics, techniques, and procedures of Computer Network Operations (CNO) including attack, defend, and exploit (the military term for reconnaissance or spying), plus the new aspect of social engineering.[26] On a personal note, it is easy to read about social engineering and think “yeah, yeah, yeah”, but I, am on many others, friended Robin Sage, a fake personality created by a security researcher to see how much data could be collected, on Facebook. Switching from the “what” to “how” in the later chapters, Cyber Warfare considers the “why,” as the authors explore the ethics and legal issues of this new battlefield. Then the book defines and analyzes the challenges facing cyberspace. Finally, it looks at

[24] Ibid.

[25] Jason Andress and Steve Winterfeld, *Cyber warfare : techniques, tactics and tools for security practitioners* (Rockland: Syngress, 2014).

[26] Ibid.

trends in this arena. Cyber Warfare provides readers with a strong foundational understanding of a threat they see every week in the news.[27] However, it ignores the impacts of cyber-warfare on general public and commercial sector.

In the field of security securitization theory proposed and analytical and evaluative method that consist of segregating the "complex whole" into different departments and sectors For example military, societal, economic, environmental and political in order to identify particular patterns of interaction since all these sectors lack the "distinctive quality of independent existence". This segregation is done to achieve its core objective and that is to reduce the number of involved variables. In Pakistan, the problem is the vast scope of the cyber securitization where securitizing agent and actor are striving hard to deal with the great number of variables at the same time. Therefore, there must be a securitization wing to deal with cyber threats in all sectors ranging from basic cyber threats of malware attack and identity theft to much complex cyber threats to national critical infrastructure.[28] The content securitizes the cyber warfare; however, it ignores the impacts on the commercial sector of Pakistan.

Sushil Jajodia, in, Cyber warfare Building the Scientific Foundation says that Modern society’s increased reliance on computer systems, smartphones, and the Internet has provided a new target in a time of conflict. Indeed, cyber-warfare has already emerged as an extension of state policies—one needs to look no further than the headlines produced by Stuxnet, Aurora, or the cyber-attacks during the Russian- Georgian war than to gain an understanding of the emerging impact this domain has during a conflict.[29] It covers the threats to the state and military; however, ignores the impact on the commercial sector due to cyber warfare.

The main objective is to steal national security secrets and essential information of the country.[30] The technology is used as a "cyber-weapon" to control and command the available data during wars and conflicts. All the above-mentioned incidents are proof that the security policy of Pakistan is vulnerable due to which cyber attacks are increasing

[27] Ibid.

[28] Jason Andress and Steve Winterfeld, *Cyber warfare : techniques, tactics and tools for security practitioners* (Rockland: Syngress, 2014).

[29] Sushil Jajodia et al., *Cyber Warfare: Building the Scientific Foundation* (Basingstoke: Springer, 2015).

[30] Ibid.

each day. On the other hand, the situation is difficult for policymakers to establish a security framework due to the limitations and regulation of cyberspace. There is a need to rebuild the legislative bodies, formulate strong policies, implementation mechanisms to overcome the threats of cyberspace and digital infrastructure in the country. Furthermore, the collaboration and consensus-building among government and stakeholders would bring effective policies against cyberspace. A comprehensive plan, implementation strategies ensure a balance between the rights of the citizens and security.

While we have seen a plethora of advanced engineering concepts that directly affect cyber-warfare such as the inventions of the firewall, Metasploit, and even advanced malware platforms such as Flame, many of these concepts are built around best practices, rules-of-thumb, and tried-and-true techniques. While these inventions have been of high impact and significance, history has repeatedly taught us (in other disciplines) that the establishment of scientific principles leads to more rapid and remarkable progress.

Hence, this volume is designed to take a step toward establishing scientific foundations for cyber-warfare. Here we present a collection of the latest basic research results toward establishing such a foundation from several top researchers around the world. This volume includes papers that rigorously analyze many important aspects of cyber-conflict including the employment of botnets, positioning of honeypots, denial and deception, human factors, and the attribution problem.[31] Further, we have made an effort to not only sample different aspects of cyber-warfare, but also high-light a wide variety of scientific techniques that can be used to study these problems. The chapters in this book highlight game theory, cognitive modeling, optimization, logic programming, big data analytics, and argumentation to name a few. It is our sincere hope that this volume inspires researchers to build upon the knowledge we present to further establish scientific foundations for cyber-warfare and ultimately bring about a more secure and reliable Internet.[32]

Jeffrey Carr, in Inside Cyber Warfare: Mapping the Cyber Underworld,

[31] Dep Chief of Staff for Intelligence, *Cyber Operations and Cyber Terrorism, Handbook Number 1.02* (Leavenworth: US Army Training and Doctrine Command, 2005).

[32] Ibid.

explains that cyber security has become an increasing strategic and economic concern.[33] Not only have major corporations and government agencies continued to be victimized by massive data thefts, disruptive and destructive attacks on both public and private entities continue and show no signs of abating. Among the publicly disclosed targets of cyber attacks are major financial institutions, entertainment companies, cyber security companies, and US and foreign government agencies, including the US Department of Defense, the US Senate, and the Brazilian and the Malaysian governments. Many of these cyber penetrations are aimed at theft of identity or financial data for purposes of criminal exploitation. These cannot simply be regarded as a "cost of doing business" or tolerable losses; such episode sunder mine the public trust, which is the foundation for business transactions over the Internet. Even more significant is the threat posed by cyber theft of intellectual property. Every year, economic competitors of American businesses steal a quantity of intellectual property larger than all the data in the Library of Congress. As a result, these rivals are gaining an unfair advantage in the global economy.[34]The literature overemphasis on the economic competition and cyber warfare to gain economic gains and ignores the other social, commercial and military aspects. Moreover, the threats to the national security phenomenon are not bothered in the literature.

Dr Tughral Yamin, in "The Evolution of Nuclear Deterrence in South Asia" suggested that there is an urgent need for well-defined national cyber security architecture. The powers of coordinating all issues related to cyber security may be vested in the office of a cyber-security coordinator working directly under the prime minister. He may be provided secretarial services by the NSC. The NSC could be one forum, where all cyber security measures may be discussed. Second, a cyber-taskforce (CTF) as suggested by Senator Syed may be placed under the NSC.[35] The mandate of the CTF should include issuing policy guidelines on cyber security. Third, the creation of PK- CERT is a long outstanding issue. The national CERT should be established and asked to practice cyber emergency regularly.

[33] Jeffrey Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld* (Sebastopol: O'Reilly Media, 2011).
[34] Ibid.
[35] Tughral Yamin, *The Evolution of Nuclear Deterrence in South Asia* (Islamabad: The Army Press, 2014).

Fourth, cyber funds should be allocated in the national budget and their proper utilization ensured by the national cyber security coordinator. Fifth, cyber security cooperation with other countries, particularly those belonging to the South Asian Association for Regional Cooperation (SAARC) would have been ideal but unfortunately, this association has become moribund due to Indian intransigence. Pakistani may consider raising the issue of regional cooperation in cyber security at the forum of the Shanghai Cooperation Organization (SCO). This cooperation should be meaningful and expand beyond the brief reference made in the joint statement issued after the visit of the former Prime Minister Nawaz Sharif's visit to the White House in 2015. Last but not the least, a cyber-security debate in the parliament may help setup along term plan.[36] The content is over emphasis the threats to national security of states due to cyber-warfare. Although, it also impacts the life of public of the states.

Amy Zegart and Herb Lin in Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations presents a ground breaking discussion and exploration of cyber weapons with a focus on their strategic dimensions. It brings together many of the leading specialists in the field to provide new and incisive analysis of what former CIA director Michael Hayden has called "digital combat power" and how the United States should incorporate that power into its national security strategy.[37] The literature ignores the impacts of cyber warfare on the economic and commercial sector of the states.

Paulo Shakarian in Introduction to Cyber-Warfare: A Multidisciplinary Approach Provides a multidisciplinary approach to Cyber Warfare analyzing the information technology, military, policy, social, and scientific issues that are in play. This book presents detailed case studies of cyber-attack including inter-state cyber-conflict (Russia-Estonia), cyber-attack as an element of an information operations strategy (Israel-Hezbollah,) and cyber-attack as a tool against dissidents within a state (Russia, Iran).It also explores cyber-attack conducted by large, powerful, non-state hacking organizations such as Anonymous and Lulz Sec. It

[36] Ibid.

[37] Herbert Lin and Amy Zegart, *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations* (Washington: Brookings Institution Press, 2018).

covers cyber-attacks directed against infrastructure such including but not limited to water treatment plants, power-grid and a detailed account on Stuxent.[38]

Paul J.Springer in Encyclopedia of Cyber Warfare says that Cyber space is definitely not the same as the physical realm, and using it as a means of conflict does not always follow the same approaches used in the physical world. In some ways, warfare in the cyber domain is less terrifying than conflict on land, at sea, or in the air, in part because, to date, no humans have been killed by a cyber attack. Currently, cyber activities tend to be an enabling mechanism supporting conflict in other domains, rather than being an entirely separate vector for violence. However, as more devices are connected and societies become more dependent upon cyber networks, the possibilities for causing harm grow in proportion. Further, because the Internet is by definition an international network that does not halt at national borders, it blurs the line between domestic and global activities, pushing past the assumed limitations of domestic and international law. Because a nation may choose to respond to a cyber attack by retaliating in the physical domain, cyber warfare offers a certain potential for cross over effects. Ultimately, whether an attack is perceived as an irritant or an act of war largely depend on the preferences.[39] The content focused on the human security rather than economic, commercial, and national securities of the states.

Clarke and Knake, in the book "The Fifth Domain", revels about the realm in which nobody should ever want to fight a war: the fifth domain, the Pentagon's term for cyberspace.[40] Our guides are two of America's top cyber security experts, seasoned practitioners who are as familiar with the White House Situation Room as they are with Fortune 500 boardrooms. Richard A. Clarke and Robert K. Knake offer a vivid, engrossing tour of the often unfamiliar terrain of cyberspace, introducing us to the scientists, executives, and public servants who have learned through hard experience how government agencies and private firms can fend off cyber threats.

[38] Paulo Shakarian, Jana Shakarian, and Andrew Ruef, *Introduction to Cyber-Warfare: A Multidisciplinary Approach* (London: Newnes, 2013).

[39] Paul J. Springer, ed., *Encyclopedia of Cyber Warfare* (Santa Barbara: ABC-CLIO, 2017).

[40] Richard A. Clarke and Robert K. Knake, *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats* (London: Penguin Books, 2019).

Clarke and Knake takeus inside quantum-computing lab sracing to develop cyber super weapons; bring us into the boardrooms of the many firms that have been hacked and the few that have not; and walk us through the corridors of the U.S. intelligence community with officials working to defend America's elections from foreign malice. With a focus on solutions over scaremongering, they make a compelling case for "cyber resilience"--building systems that can resist most attacks, raising the costs on cyber criminals and the autocrats who often lurk behind them, and avoiding the trap of overreaction to digital attacks. A Above all, Clarke and Knake show us how to keep the fifth domain a humming engine of economic growth and human progress by not giving in to those who would turn it into a wasteland of conflict. Backed by decades of high-level experience in the White House and the private sector, *The Fifth Domain* delivers a riveting, agenda-setting insider look at what works in the struggle to avoid cyber war. It more focuses on the commercial sector in comparison with the aspects including military and infrastructure. Hundreds of Books and thousands of Research Articles have been written on National Security in the age of cyberspace but insufficient work has been done in case of Pakistan. This research would be an addition to existing knowledge and also be comprehensive research in case of Pakistan.

Research Gap

Based on the literature available internationally and from Pakistan and the identified gaps, the discussion leads to the following points.

a) There isn't a single paper, book, or study on the subject of National Security in the Age of Cyber Space; A Case Study of Pakistan. There are a few articles and books that describe cyber threats, cybercrime, and cyber terrorism, but none of them can be found in one place.

b) Pakistan has yet to complete its cyber threat mapping, and no work has been done on the weaknesses of Pakistan's national security in the age of cyber space. There is a pressing need to plan Pakistan's vital interests, as well as to counter cyber threats.

c) The analysis benefits from case studies of Pakistani government agencies, the lack of cyber policies, and available literature on international best practices to identify the main steps in establishing a cyber-defense in Pakistan.

Theoretical framework

Offensive realism, put forward by John Mearsheimer in response to defensive realism (same family with slightly different strands), this is an international relation's theory which expresses that states are able to compete and encounter because to gain optimizing control, self-interests, and threat and fair from other states. [41] Furthermore, it claims, in the international system, states are obligated to function the way to facilitate the survival. States use all the available resources to harm the rival states for the maximization of their national interests and gains. States had always invented new means and ways to harm other rival states and to protect their national interest through coercive means. Cyber threat/warfare is the most recent coercive mean which is the product of offensive realism, is being used to harm other countries and halt their sensitive and confidential infrastructure as well as data, by posing a greater threat to national security. Cyberspace, has become battlefield influenced by the offensive design, is being used to fulfill the national interest and psychological operations are being conduct just to maintain their power and supremacy on other nations. Future wars fight through the cyberspace. The cyberspaces of other countries are being penetrated on the bases of offensive realism in the anarchic international system with an intention to steal or manipulate the sensitive data and information.

The proliferation of cyber attacks is showed the realist intensions of the states. The reasons behind the rapid spread all across the world is to exploit the information of other state, maximize owns power, and shatter the economy of the other states (business nature has changed and now companies and firms deals through internet); furthermore, by knowing and revealing the official data of government and higher institutions of the other states including defense and security related departments, it is easy to defeat the state in every battle to achieve its own goals and objectives.

In the contemporary world, the war patterns have changed due to the innovations in the field of science and technology. This change also gives a chance to the states to

[41] Quoted in. André Munro, "John J. Mearsheimer," *Encyclopedia Britannica,* December 2020, https://www.britannica.com/biography/John-Mearsheimer.

adopt offensive realism policy to achieve its ambitions in the globe. The 21st century is the age of technology; however, there are severe threats because of it. Cyber threats are not only restricted to the major powers and super powers, they are equally threatens the small and developing states. Pakistan is also affected due to the cyber warfare.

Therefore, in case of Pakistan there are many rivals of Pakistan, not only outside the region, but within the region. However, India is on the top. India wants to control the region and struggle to gain the status of hegemon in the region of South-Asia.[42] One of the main hurdles in its way is Pakistan; therefore, India has been launched Cyber attack on Pakistan to know its secrets and achieve its goals by weakening nationalism and unity. Moreover, United Kingdom has launched attacks on Pakistan to defeat America's agendas in the region and keep an eye on the activities of Americans.[43] Every state has a purpose to gain supremacy and defeat or destroy the other state. The ISPR report has also declares the details of cyber attacks to the higher officials and government of Pakistan from India.[44]

So, there is a race going on between and among the states to defeat one another and be a hegemon of the region and the super power of the globe. This all depicts the realist's thoughts and philosophy.[45]

Core Argument

Cyber threat leads to severely undermine the military and civil sector of Pakistan in the next decade. Cyber threat is more acute then the military threats. So, Pakistan needs to act seriously against it and make proper strategies to mitigate such challenges.

Research Methodology

It is necessary to be aware of the research technique and its importance in the area of international relations in order to carry out research. The fact that social science research is not as identical as natural science research as it is described by

[42] Quoted in, Ravi D. Bajpai and Swati Parashar, "India in the 'Asian century': Thinking like a hegemon?," *DOC Research Institute – Dialogue of Civilizations*, July 4, 2019, https://doc-research.org/2019/07/india-in-the-asian-century-thinking-like-a-hegemon/.

[43] Ibid.

[44] Ibid.

[45] Laiq U. Rehman, "Security Agencies Foil Indian Cyber Attacks Against Govt, Defence Officials: ISPR," podcast audio, August 12, 2020, https://arynews.tv/indian-cyber-attacks-defence-ispr/.

many scholars and worldwide specialists is vital to grasp. While this study is primarily based on qualitative and analytical research approaches, the theory of complex interdependence which makes this study based on deductive thinking seeks to explain diverse cyber safety occurrences by critical examination of available data. Deductive reasoning therefore offers its conclusion logically convincing backing. As an independent variable in this research cyber security, Pakistan's risks and problems rely on them. After a comprehensive analysis of the data gathered from diverse sources, a research would attempt to develop a basic overview of the risks to Pakistan's national security. There is therefore an effort to add a new aspect to the link between cyber dangers and Pakistan's national security. The data collecting approaches comprise secondary sources such as books, research articles, reports from international and research think-tanks, reviews of documents, indirect observations, research journals, newspapers, Web sources, and other social media reports, as required. The study closely examines Pakistan's government's official comments and news releases on the subject of cyber security and its policy guidelines in future.

Significance of Study

The study is expected to help the Security Agencies, Governmental organizations, Think Tanks and the cyber security researches as well as cyber professionals to understand the emerging threats posed by the cyberspace to the national security as well as different elements of the national power of Pakistan and develop an understanding of enhanced need for cyber security of the country. Moreover, Pakistan is least prepared against cyber warfare from hostile nations/elements that pose a major challenge to the national security of Pakistan.

Delimitations

Pakistan’s National Security is facing several challenges but the research would focus on the challenges which are emerging from cyberspace. Hundreds of tools are being used against rival states but the study would include tools which fall in the domain of cyberspace specifically against Pakistan. Moreover, due to the sensitive nature of subject the researcher has failed to collect data from primary sources.

Organizational Structure

The research would be divided into four chapters.

Chapter One: Evolving Nature of Cyber threat and Cyber warfare in Contemporary Times

The chapter explains the broad perspective of Cyber Warfare and its threats in the contemporary age. This chapter provides the knowledge about Cyber warfare, Cyber Security, tactics and strategies of cyber security to understand the cyber threats.

Chapter Two: Pakistan's National Security in Cyber Domain

The chapter explains the effects of cyber-warfare faced by Pakistan due to cyber-attacks. The attacks hurt feelings, emotions, and sentiments of Pakistan's public against their government and institutions; moreover, the norms, culture, and religion are the main targets of the attacks. The nation of Pakistan has seen social media use for various political and religious movements like facebook, youtube, twitter, and Instagram etc.

Chapters Three: Pakistan's Existing Infrastructure against Cyber Threat

The chapter explains that one of the most intense transformations of this era is the digital revolution. Almost all fields of life are somehow dependent on technology now. Vulnerabilities are one of the most consequences of interconnectedness. Moreover, the individuals and states have compromised their privacy Digital platforms are considered more effective to judge state and state citizen's relations. The communication, computing, governance military and civilians rely on digital networks which can be attacked from any part of the globe.

Chapter Four: Reasons of Pakistan's Failure in Order to Preserve Cyber Security

This chapter explains the failures in the policies and strategies of Pakistan to counter cyber threats and maintain cyber security in the state. Pakistan has designed Cyber policies time to time to maintain the security of the state; however, due to lack of awareness among public and illiteracy the state faces plethora of issues in the implementation of policies.

Chapter Five: Pakistan’s Effort to Counter Cyber Terrorism

This chapter explains that there is still no cohesive cyber command or national cyber policy established to counter Pakistan's regional cyber challenges. While Pakistan has established a cyber security auditing and assessment laboratory recently, it remains in its formation stages. Increased tools and research capabilities are also available to help defend Pakistan's cyber-space, confidential data, and local economies from cyber attacks while limiting illegal access.

Conclusion and Recommendation

This section concludes the debate that the Cyber-attacks are accomplished due to military equipment’s failure, electric blackouts, and ruptures of secrets. Thief steals the important and sensitive information and uses it against the country, organization and, individual (have access on the data of the person). The attackers paralyze the system, disconnect the networks, and corrupt the important information. The cyber threats have been becoming intense and increasing day by day. Moreover, recommendations are mentioned in the end.

Chapter I

Evolving Nature of Cyber Threat and Cyber Warfare in Contemporary Times

1.1 Introduction

Before the emergence of the internet, everything was being done manually from business to the governmental affairs to the wars on the battlefield. But the emergence of the internet made everything possible on just one click. It has changed the ways of life and facilitated human life in many aspects; nevertheless, it creates problems and challenges in every field of life. Every record and affair was converted from papers to the virtual space called the cyberspace. With the passage of time internet become the need of individuals, businesses, governments, militaries, multinational corporations and national and international organizations. Everything including records and classified data of governments and organizations was converted to the digital information and was shared to the cyberspace for further storage, transformation and communication. At present, there would be hardly any company to run its affair with our using the internet. This is the era of digitalization and everyone is dependent on the internet. Cyberspace has created easiness in doing business, running the state affairs and fighting the wars virtually. Where it has facilitated all the ways of life it has also created much vulnerability which has been a grave concern for the world. On one side it is facilitating us and on the other hand, it is creating vulnerabilities which are more severe in nature. The world has become more concerned about these vulnerabilities and threats. Cyberspace is posing many threats and vulnerabilities to the national security and almost everyone prone to these threats which are being posed by the cyberspace. Therefore, the countries have been compelled to take drastic measures to mitigate these threats and vulnerabilities. The dependency on internet opens ways to the progress and prosperity; however, the cyber threats and attacks which are emerged as a result of internet are fatal for the national security of the states. Now days, the threat is not restricted to few states, it becomes threat to the national security of states all across the world. In this chapter, we will be discussing the vulnerabilities and threats being imposed by the cyberspace.[46]

1.2 Cyber Attack

The life dynamics are also changed due to the revolution of technology. In every facet of life, people depend on technology whether, business, education, social activities, and politics. The technology eases the life of people on one hand and put them in danger on the other hand. Cyber-warfare and Cyber Attacks are originated from the internet, computers, and information technology.

In the contemporary age the data has been gathered, transmitted, and processed with the speed, flexibility, and capacity. There are eight technologies which are very significant in terms of scientific and technical revolution, such as advance computing, wireless transmission of data, satellites and networking are on the top. Due to these advancements in technology; cyber threat has been emerged.[47]

Cyber threat is described in a plethora of ways such as misuse of intellectual property. Research and Development work, trade secrets, proprietary, disruption of services, product espionage and destruction of physical property are actually threats to the national security. Cyber Attacks are easier, cheaper, and convenient in comparison with physical attacks.[48] That is one of the reasons behind rapid increase in cyber-attacks in the current scenario. Attackers need internet connection and computer to install and accomplish their goals. Distance and geography do not matter in launching the attack and it is not easy to accuse and reach to the attacker because of internet's unconfined nature.

Any action which has used to hijack computers, networks, and digital technology and have wrong intensions to control over them such as misuse of data is called cyber threat. There are authorities to take legal action against unfriendly users of computer and hackers by international and municipal law. The fundamental purpose of Cyber Attacks is

[46] Check Point Research, *2021 Cyber Attack Trends Mid-Year Report | Check Point Software*, (US: Check Point Software Technologies LTD, 2021), https://pages.checkpoint.com/cyber-attack-2021-trends.html?utm_term=cyber-hub.

[47] Jessica Haworth, "Data breaches are costing more than ever, as organizations take longer to detect attacks, apply patches – report," *The Daily Swig*, July 28, 2021, https://portswigger.net/daily-swig/cyber-attacks#top.

[48] Alvaro A. Cardenas, Saurabh Amin, and Shankar Sastry, "Secure Control: Towards Survivable Cyber-Physical Systems," *2008 The 28th International Conference on Distributed Computing Systems Workshops*, July 2008, doi:10.1109/icdcs.workshops.2008.40.

destruction, deaths, killing, fear, and damage, etc. in few cases, the computers or gadgets are not the target of hackers; however, they controls airports, banks, and other sensitive places like power grids to accomplish their goals.

The cyber threat also defined as the hostile action taken by anyone against information technology like computers and networks. The reason behind the action is to destruct and exploit the information, and misuse the information, and leak the information which has stored in the system.[49] Since dawn of computing, the knowledge protection and sacrosanctity of the data has not gain momentum in anticipation of the exponential growth. The web machines have been providing real sandbox and hackers test their abilities through this by stealing information, downloading websites and committing fraud. This exposes the nature of Cyber Crime in today's world. There are approximately 3.4 billion people have been using internet world wide and the percentage of whole population is 46% and the users are increasing day by day. So, the cyber threat chances are going to be increase; therefore, the prevention and the phenomena of cyber threat are going to be the complex and difficult.[50]

The term exploitation in cyber threat means to make copy of information and use it for negative purposes and provided the information to the advisory; moreover, advisory has taken the advantage of the data.

A plethora of words used to define the Cyber threat such as hack, attack, intrusion, penetration, Compromise, exploit, and breach. In light of Symantec Cybercrime Report 2012, US$ 114 billion each year spend on Cyber Attacks. The companies spend US $385 billion for recovery from Cyber Attacks each year. Symantec conducted survey and collect information from twenty thousand people and 24 countries. He reported, there are 69% victims of Cyber Attack in life time. Every day there are approximately 14 adults of victims of Cyber Attack and one million attacks overall in the world.[51]

Social, political, economic, and cultural conflicts are the causes behind Cyber Attacks; therefore the attacks has occurred due to political conflicts, extremism, religious belief,

[49] Julian Jang-Jaccard and Surya Nepal, "A survey of emerging threats in cybersecurity," *Journal of Computer and System Sciences* 80, no. 5 (2014), doi:10.1016/j.jcss.2014.02.005.

[50] Australian Computer Society (ACS), "Cybersecurity - Threats, Challenges, Opportunities," ACS - The Professional Association for Australia's ICT Sector, last modified November 2016, https://www.acs.org.au/insightsandpublications/reports-publications/cybersecurity-threats-challenges-opportunities.html.

[51] Ibid.

and few are in a result of anger and revenge. It is to conclude that there are two kinds of Cyber threats. One is against the information infrastructure and other is cyber based (exploitation of technology) like hacking tools. Hacking tools are basically are programs and scripts that assist you in identifying and exploiting flaws in operating systems, web apps, servers, and networks.[52]

1.3 Cyber Warfare

In the current scenario, the grounds for battles and wars have changed. The old fields of war like sea, land, and air are not remaining influential and prominent because of modification in war fares. The new battlefield, cyber space has discovered or invented. Now the digital world decides the defeat and triumph of rival parties whether in politics, business, and individual conflicts. It is beyond the boundaries of geography and reach of conventional or customary means like Geneva Convention. It is a real game changer not only for a region, but worldwide. This completely changes the policies, challenges, threats, and dynamics of war; therefore, the enemy is unpredictable due cyber warfare[53].

In light of Jeffery Carr definition, cyber warfare is the warfare in which fight conducted without a real fighting and parties defeat rival parties defeat without spilling the blood.[54]

There is a difference in Cyber Attack and cyber Warfare. Series of attacks refers to cyber warfare and one attempt by the hacker refers to Cyber Attack. The concept of cyber warfare is not limited to a use of computer against computer. The phenomenon is about attack to rivals from digital means and space. The attack has been sponsored by the state to distract the system and to draw statements and outcomes regarding politics. Individual are used or hired to execute or launched attack.

It has totally changes the concept and connotation of traditional wars which was tangible. In this warfare, the enemy is unpredictable, invisible and hidden. The attack and

[52] Krishna Rungta, "25 Best Ethical Hacking Tools & Software for Hackers (2021)," *Meet Guru99 - Free Training Tutorials & Video for IT Courses*, 2021, https://www.guru99.com/learn-everything-about-ethical-hacking-tools-and-skills.html.

[53] Peter R. Trim, *Cyber Security Culture: Counteracting Cyber Threats Through Organizational Learning and Training* (London: Routledge, 2013)

[54] Quoted in. Michael Robinson, Kevin Jones, and Helge Janicke, "Cyber warfare: Issues and challenges," *Computers & Security* 49 (March 2015), doi:10.1016/j.cose.2014.11.007.

happenings are not tangible like traditional wars where soldiers firstly identify the enemies and then use guns, bombs to defeat or destroy enemies.[55]

In this kind of warfare a single person can controls and execute attacks on the rival party. For the other party it is difficult to unveil the attacker easily. Therefore, the current situation is quite challenging for every sector such as military and business, etc.

The liabilities give basis to the cyber weapons and numerous systems have the vulnerabilities. Drive health care, power generation, manufacturing, and transportation has affected due to impact on network. It is difficult for militaries to secure the systems and identify the attackers during war and conflict. Biometrics is also shifted from papers to digital. The new dynamics effected national security, impacted intelligence, and war fighters.

1.4 Politically and Economically Motivated Attacks

Extremist groups are cyber criminals and they motivate Cyber Attacks through websites and networks against political rivals or enemies. The agenda behind that attack is to steal money and propagate propaganda, and connects with physical world crime. On the other hand, the slowdown of economy leads to distress and pressure inside the country. Most of Information Technology (IT) professionals has been lost substantial amount at stock markets such as China, China is the state tilting towards IT and due to this Cyber Crime probability has been increased in China. Financial greed both personal and corporate and economic conditions are the facts behind Cyber Attacks. Greed, needs, and poverty are reasons and motivations of the Cyber Attack.[56]

Due to the sophisticated attack is done by the hacker, the power grid or system has hacked or failed without external influences. Whether the failure in computer causes due to criminals, terrorists, or human mistake; however, it has a domino effect. The domino effect has linked to interdependencies. The gaps in the system allow attackers to control over the system.

Human attack is very significant in terms of national security and threat politics; therefore, techniques have been designed and tailored as per need. The responses have

[55] MarieO’ N. Sciarrone, "Cyber Warfare: The New Front," *George W Bush Institute*, no. 6 (Spring 2017), https://www.bushcenter.org/catalyst/modern-military/sciarrone-cyber-warfware.html.

[56] Robin Gandhi et al., "Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political," *IEEE Technology and Society Magazine* 30, no. 1 (2011), doi:10.1109/mts.2011.940293.

been taken at levels; technical, long term strategies have different levels, and midterm strategies have different. In case of attack by the state actor, military activates and responses to the threats or attack; however, in case of sub state actor, law-enforcement measures have been taken initially. The attacker identity has not cleared due to the global information infrastructure.[57]

Cyber incidents have impacted the field of economics. ICT opens new doors for the market and business and the source of income which become foundation of rapid increase in growth. That's why threat of Cyber Attacks is the genuine issues not only for economy, but also for the national security of the state. There are multiple approaches of Cyber Economics.

There are very few governments that show the real cyber threats and guidance in their annual reports; however, 75% organizations use in an appropriate way and take advantages of the information.[58] In 2017 report, UK business has highlighted the cyber threats.[59] Substantial percentage of businesses has lack of security controls; however, majority of businessmen have increased the budget to get rid of the issue. The corporate issues are linked with duplicitous emails. Firms identifies the attacks successfully are approximately 72%; moreover, 33% of attacks are related with viruses, malware, and spyware. The 27% are related with mimicking emails and 17% are correlated to ransom ware. The organization and individual has been experienced a plethora of direct and indirect harms to their national security.[60]

1.5 Adversary in Cyberspace

The purpose of adversary to exploit information is advisory in cyber space. This is completely an offensive action. Unfriendly and strict actions have been being taken place by the advisory against information technology and networks. Such as computers, mobile phones, and Tabs, etc.

[57] Myriam Dunn Cavelty, "Cyber-Security and Threat Politics: US Efforts to Secure the Information Age," *Journal of Information Technology & Politics* 1, no. 4 (January 2008), https://www.researchgate.net/publication/277714726_Cyber-Security_and_Threat_Politics_US_Efforts_to_Secure_the_Information_Age.

[58] Ciaran Martin, *The Cyber Threat to UK Business 2017-2018 Report*, (UK: National Cyber Security Center, 2018), https://www.ncsc.gov.uk/information/the-cyber-threat-to-uk-business-2017-2018-report.

[59] Ibid.

[60] Ibid.

The scope of cyber security has been increasing rapidly because of unpredictable nature of cyber threat. This is a contemporary and 21st century challenge faced by industries, individuals and governments. Everyone has a threat of fraud, scamming, and hacking.

1.5.1 Cyber Exploitation

The information has been escaped or steals from storage and given to the unauthorized parties illegally is called cyber exploitation. The sensitive data has stolen from the digitally stored data like criminal records, telephone numbers, intellectual property, blue print, and other sensitive information such as classified information, contract information, and forbidden information then provided it to irrelevant person or party is exploitation of cyber.[61]

The exploitation has made by intelligent or good profile people covertly or surreptitiously. The exploitation key feature is its surreptitious nature. It is useful before discovery because after discovery of exploitation, the person prevent the use of cards, code, and numbers with the help of concerned authorities. The hacking and Cyber Attack can be implemented through iPhones and apples. There are a number of users of apple and iPhone; therefore, most of the people have been using iPhone in an organization or company. So, it is difficult and complex in the contemporary age to counter Cyber Attack.

The major cyber exploitation has been discovered since 2013. The information of 70 to 10 million people have stolen and leaked.[62] It contains email addresses, credit card numbers, and names and has sold on black market websites. It is also used for blackmailing victims.[63] For example, criminal has taken control over the Webcam of personal computer of Miss Teen USA and has been taken pictures to blackmail the victim since 2013.[64]

[61] Logsign Team, "What Are Real Time Security Threats?," *Logsign: Next-Gen SIEM, SOAR and Value Added Services*, January 10, 2021, https://www.logsign.com/blog/what-are-real-time-security-threats/.

[62] Juliana D. Groot, "The History of Data Breaches," *Digital Guardian*, December 1, 2020, https://digitalguardian.com/blog/history-data-breaches.

[63] Ibid,

[64] Committee on Developing a Cybersecurity Primer: Leveraging Two Decades of National Academies Work et al., *At the Nexus of Cybersecurity and Public Policy Some Basic Concepts and Issues (2014)*, (Washington, DC: National Academy Press, 2014), https://www.nap.edu/catalog/18749/at-the-nexus-of-cybersecurity-and-public-policy-some-basic.

The term Cyber has been used for understanding the movement and control of animals and machines since 1950s; however, it has been used for computerization. After 1990s the terminology has become cyber space and the connotation about the term has totally changed. Now, it is defined as the computer devices and electronic activities performed through the computer devices to control the devices and data.

1.6 Cyber Threats in the Modern Day

The term is related to the security issues of information stored in the electronic devices. It’s difficult to expose and envisage over the data transformation and movement and understand and observe the phenomena of travelling of information through wires. It is not possible to visualize the phenomena physically and represent the attack. So, the nature of threats to the national security is also changed in this age.

Cyber Attack has been launched to destroy the data, steal the data, copy the data and misuse the data from the computers against any legal body. Cyber space is the phenomena used to explain the aim behind this process; furthermore tells us about new kind of weaponry introduced by the Cyber Attack, commonly called digital weaponry. The attacker’s purpose is to harm human lives. They have Nuisances, serious attitude, and annoying nature.[65]

This is the age of cyber. The world has been engaging in the cyber warfare, cyber espionage, and cyber terrorism. This is totally a new kind of war and more dangerous and complex than physical war because it is difficult to identify the enemy. There is a huge rise in the quantity as well as quality of the cyber incidents. During 1990s the connotation of the cyber security was terrorism and protection of critical infrastructure. It was gaining impetus and the term cyber security was under flash. United States had given much attention to the issue and it was reached on the top threats of modern age. International relations are also impacted due to the revolution in the field of technology and information. The technology has gained prominence and dominance in our lives. Cyber threats are not only threats, it’s a reality today.

According to the Critical Infrastructure Readiness Report, Aspen Institute and Intel Security, 2015, the half of the security professionals surveyed and predicted that the

[65] Hugh Taylor, "What Are Cyber Threats and What to Do About Them," *The Missing Report*, June 16, 2021, https://preyproject.com/blog/en/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them/.

infrastructure will be taken down and there will be severe loss of lives in coming three years.[66]

There are a lot of modes, tools, and intents used for launching Cyber Attacks for example Trojan horses. The benign programs and applications are launched to devastate the set up. That's the reason hacker enters to the system through viruses and worms, etc. In light of Risk Based Security report; in 2019, 7.9 billion records have been exposed by data breaches. The malicious are behind the majority of Cyber Attacks. US Department of Justice has accused the organization's leader of cybercriminal that they are involved in global assault on Dridex malware attack in 2019. The Public, infrastructure, and government, have been impacted all across the world due to this malicious movement.

Dridex has a number of capabilities and is a finical Trojan. It has affected victims by infecting computers via phishing emails in 2014. The financial loses are caused due to it and have worth hundreds of millions. Deceitful transections have been made by stealing passwords, bank information, and personal data. So, to cope with the crisis and back up of data, National Cyber security UK advised public to install anti-viruses.

FBI has warned the public about romance scams. Chat rooms, data sites, and apps are used by the cybercriminals and fraud with public of USA in February 2020. The people who are looking for new relationships are the targets of the culprits because it is easy to get personal information through this tactic. Moreover, FBI estimated the total victims who are affected because of romantic Cyber Attacks in the Mexico are 114 and they have lost round about 1.6 million dollars[67].

Australian cyber security centre advised the nation-wide official domes in 2019 about global cyber threat from malware from Emotet. It is a sophisticated and advance torjan which steals information and transmitted and saved to the malware. Safe passwords have ability to defend against Cyber Attacks. Unsafe and unsophisticated passwords are easy tasks for Emotite; therefore, safe passwords are very significant to fail the attack. It's the prediction of international data cooperation that the spending on the cyber security in 2022 is going to reach at 133.7 billion dollars.

[66] Vanson Bourne, *Critical Infrastructure Readiness Report Holding the Line Against Cyberthreats*, (Santa Clara, California: The Aspen Institute Homeland Security Program and Intel Security in advance, 2015), https://www.thehaguesecuritydelta.com/media/com_hsd/report/43/document/Critical-Infrastructure-Readiness-Report---Holding-the-Line-against-Cyberthreats.pdf.

[67] Ibid.

According to Kaspersky Lab

“In 2016, 758 million malicious attacks occurred (an attack launched every 40 seconds) and the cost of cyber crime damage is expected to reach $5 trillion by 2020”.[68]

With the WannaCry and NotPetya attacks, ransomware was under the spotlight in 2017, which briefly crippled several major businesses and organizations. The major hacking of its IT infrastructure was revealed by Adobe in October 2013. Data information was stolen from 2.9 million accounts (logins, passwords, names, credit card numbers and expiration dates).[69] Another file later found on the internet took the number of attack affected accounts to 150 million (only 38 million active accounts) Sony's PlayStation Network was targeted in April, 2011. The Japanese brand's multiplayer gaming operation, online gaming purchase and live content delivery contained the leaked personal data of 77 million users.[70] Banking data was also compromised for tens of thousands of players. PSN, as well as Sony Online Entertainment and Qriocity, were closed for one month after the detection of the intrusion. Sony paid $15 million in restitution and a few million dollars in legal fees to appease their users, in addition to having to reimburse the people whose bank accounts have been illegally used. In 2014, Sony Pictures Entertainment, a subsidiary, was targeted again by malware and, more specifically, by a computer worm.[71]

The Guardians of Peace stole 100 terabytes of information, including vast amounts of sensitive data. In January 2014, the South Koreans discovered that, over many years, data from 100 million credit cards had been stolen. Furthermore, 20 million bank accounts have been compromised, too. More than 2 million South Koreans have blocked or replaced their credit cards for fear of having their bank accounts vacated.

In December 2013, Target, the second-largest US discount retail chain, was the victim of a large-scale cyber attack. Between November 27 and December 15, data from 110 million customers was hijacked, including bank data from 40 million customers and

[68] Outpost24, "TOP 10 of the World's Largest Cyberattacks, and How to Prevent Them | Outpost 24 Blog," *Full Stack Risk Based Vulnerability Management Platform | Outpost 24*, December 3, 2018, https://outpost24.com/blog/top-10-of-the-world-biggest-cyberattacks.

[69] Adam Gabbatt, "Adobe Warns 2.9 Million Customers of Data Breach After Cyber-attack (Update5)," *DataBreaches.net*, October 3, 2013, https://www.databreaches.net/about/.

[70] Wikipedia, the Free Encyclopedia, s.v. "PlayStation 3," in *Wikipedia, the Free Encyclopedia* (2001), accessed March 7, 2020, https://en.wikipedia.org/wiki/PlayStation_3.

[71] BBC, "Credit card details on 20 million South Koreans stolen," *BBC*, January 20, 2014, https://www.bbc.com/news/technology-25808189.

personal data (names, postal addresses, telephone numbers and email addresses) from another 70 million customers.[72]

The marketing analytics company left an unsecured online database that publicly revealed confidential data to 123 million US households.

For each household, data covered 248 fields of knowledge, ranging from addresses and income to ethnicity and personal interests. Data include contact data, ownership of mortgages, financial history and whether a dog or cat enthusiast was included in a household. The dating site was raided for the first time in 2015[73]. Details on 4 million accounts (pseudonyms, dates of birth, postal codes, IP addresses, and sexual preferences) has made available on a forum accessible only on Tor. It had malicious actors recovered it, the information may have been used for spam campaigns, identity theft or blackmail. No banking data, however, was hijacked.

Data, including banking details, from up to 500 million guests at the Marriott-owned Starwood hotel group has been compromised. The rift was opened in 2014 and was first spotted in September 2018. Even though, as Marriott notes, the number of customers who have experienced a personal information breach is close to 327 million somewhere, the effects are huge. Accessed information includes payment information, names, postal addresses, telephone numbers, email addresses, passport numbers, and even Starwood Preferred Guest (SPG) account data, a high-end card newly introduced for frequent travellers by the American Express credit card issuer[74].

In August 2014, the IT security company Hold Security announced that 1.2 billion logins and passwords on 420,000 websites around the world had been compromised by Russian hackers. This could probably have helped the 'CyberVor' group of hackers to access 500 million email accounts. In order to exploit SQL injection vulnerabilities, hackers have used engineered botnets to visit sites and perform vulnerability tests.[75]

[72] Jim Finkle and Dhanya Skariachan, "Target cyber breach hits 40 million payment cards at holiday peak," *Reuters*, December 19, 2013, https://www.reuters.com/article/us-target-breach-idUSBRE9BH1GX20131219.

[73] Ibid.

[74] Brian Barrett, "Hack Brief: Marriott Got Hacked. Yes, Again," *WIRED*, March 31, 2020, xx, https://www.wired.com/story/marriott-hacked-yes-again-2020/.

[75] BBC, "Russia gang hacks 1.2 billion usernames and passwords," *BBC News*, August 6, 2014, https://www.bbc.com/news/technology-28654613.

Yahoo! revealed in 2014 that it experienced a cyber attack in 2014 that affected 500 million user accounts, the largest massive hacking of individual data targeted at a single company. Although the company told customers that banking details had not been affected, caution was nonetheless advised. Prior to this case, the "Peace" hacker sold 200 million usernames and passwords for $1900 million in 2012.[76]

The prediction is made in the Critical Infrastructure Readiness Report become true. States has gained the power to destroy infrastructure through technology. The myth has become a reality. Now, there is a list of countries whose infrastructure has been destroyed with the help of cyber-attacks. The attacks are;

Tanks had sent to Georgia by the Russia in 2008. It was a Cyber Attack for the computation of infrastructure. This was considered as the first Cyber Attack. In 2008, the US and Israel had developed the stuxnet and crippled the Iran's enrichment program of nuclear. In 2014, hackers had breached the Germany steelworks and the furnace had not worked properly and not shut downed. Another Cyber Attack had been seen in 2015, it was an attack in Ukraine, and two lac thirty thousand people lost supremacy and power. Attackers seized the system and system was controlled by the remote. The attack was launched from the Russia.

The incidents conclude, the war strategies, tactics, and methods are changed now. The weapons such as Guns, bombs, animation are no longer sustains the deterrence and fear. Keyboard is the new weapon to control, destroy, devastate, and defeat enemy or exploit the national security of any state.

Conclusion

The Cyber-attacks are accomplished due to military equipment's failure, electric blackouts, and ruptures of secrets. Thief steals the important and sensitive information and use it against the organization and person (have access on the data of the person). The attackers paralyze the system, disconnect the networks, and corrupt the important information. The cyber threats have been becoming intense and increasing day by day.

In opinion of Gartner,

[76] Nicole Perlroth, "Yahoo Says Hackers Stole Data on 500 Million Users in 2014," *The New York Times*, September 22, 2016, xx, https://www.nytimes.com/2016/09/23/technology/yahoo-hackers.html.

“Risksfrom Cyber Security has encompassed that not every organization has under the direct control of IT.[77]The strategies and techniques are used to protect computers, websites, and networks from unauthorized attacks or access and minimizes or destroyed the manipulation by the attacker is called cyber security.

Nothing has saved and secure in the contemporary world. it is more difficult to secure the national security of state than the past. A plethora of people are using mobile phones and internet. Good and intelligent guys can also launch Cyber Attack to full fill his aim. In the light of network security and services company fortinet, the attacks against its network are approximately 500000 in every minute.

The advancement and modifications has been done in the field of digital business strategies by the businessmen. A lot of risks have been taken by businessman every day to protect and secure the data; however, cyber threat is not completely eliminated.”

Cyber threats are evolving with time. The methods, systems and techniques are going to be advance day by day. So, the threats are boosted with time. Old phenomena’s to prevent and defend one’s self from cyber threats are not enough and useful in the current scenario such as Zero day is the new generation introduced and it cannot be detectable in the sign detection technology.

[77] Ibid.

Chapter II

Pakistan’s National Security in Cyber Domain

Pakistan has been facing the effects of cyber-warfare in the form of minor cyber attacks and use of cyber space violently for five years, this includes hate speeches, abuse the norms, culture, and religion, hurt feelings , emotions, and sentiments of Pakistan’s public against their government and institutions. The nation of Pakistan has seen social media use for various political and religious movements like facebook, youtube, twitter, and Instagram etc.

Now, danger of violence, propaganda, and extremist views spread is not so strong to affect the state through social sites, but in future it could escalate to a substantial level if left untapped.[78] Pakistan’s government has been developing the policies to counter cyber attacks since 2013, but it has not been implemented in true meanings. Over time, the realm of cyber space is exploited by the cyber criminals; however, it has also become the greatest safe haven for cyber terrorists to recruit and use contact, data collection, mobilization networks, and psychological warfare.

2.1 National Security

The national security means to safe and manage a country through multiple channels including diplomacy, economic, political power, and intelligence agencies. The aim is to achieve the protection of our country's most basic and long-term needs: safeguarding people's lives and safety; preserving the sovereignty, including its values, institutions, and territory; and ensuring the nation's prosperity.

Pakistan has been facing challenges in terms of national security since inception. However, the nature of the challenge varies with time. Since partition, Pakistan national security faced challenges including infrastructure, economy, weak military capacity against a hostile hegemonic neighbor, and human security concerns as a consequence of extreme migrations and refugee settlement.[79]

[78] Muhammad I. Ayub Khan, "Cyber-Warfare: Implications for the National Security of Pakistan," *NDU Journal 2019*, 2019, https://ndu.edu.pk/ndu-journal/pub/06-Cyber-Warfare.pdf.

[79] Mudassir Mukhtar, Waseem Ishaque, and Muhammad S. Malik, "Natioanl Security Paradigm of Pakistan-Retrospective Analysis," *NDU Journal2019*, 2019, https://ndu.edu.pk/ndu-journal/pub/11-National-Security-Paradigm.pdf.

Pakistan is confronted with a complex security landscape and significant national security concerns.[80] Intrinsic and extrinsic, explicit and implicit, direct and indirect, harsh and soft, old and new, conventional and quasi factors all contribute to this. Some of these issues are unintentional consequences of Pakistan's previous actions, but many are the consequence or causal factors. A matrix based on sectors of Comprehensive National Security has been used to group this vast range of issues.

2.1.1 Challenges to National Security

When it comes to recognising security issues, two referents spring to mind: the state and the person. While the human is the fundamental object, most political scientists, such as Barry Buzan and Weaver, believe that the state remains the key reference for providing security that also meets human security concerns.[81]

2.2 Types of National Security Threats

There are multiple types of national security threats including economic threats, military threats, societal threats, religious threats, information and technology threats, and threats in environmental sector and political threats; moreover, it's been integrated with the social sector. Because the areas described by all of them are interconnected, well-knitted, and overlapping, precise borders between them cannot be formed. Instead of delving into every element of state operation, just those sectors that have the greatest impact on Pakistan's state have been highlighted. Analyses are conducted with the intention of determining the causes as well as their manifestations. Due to their intertwined nature, it's impossible to draw clear lines between internal and external challenges of the Pakistan's national security.

The political aspects of Pakistan includes relations with Afghanistan, India, governance, FATA and Baluchistan circumstances, etc. moreover, military aspects of Pakistan concerned with the security of maritime, terrorism and extremism, threat from rival states. Economic aspects of Pakistan include water issue, struggling economy, and food security.[82] Societal aspects are concerned with the security of human beings and

[80] Ibid.

[81] Barry Buzan, Ole Waever, and Jaap D. Wilde, *Security: A New Framework for Analysis* (Colorado: Lynne Rienner Publishers, 1998).

[82] Aarish U. Khan, "The Terrorist Threat and the Policy Response in Pakistan," *Stockholm International Peace Research Institute SIPRI* , no. 11 (September 2005), https://www.files.ethz.ch/isn/13595/Policypaper11.pdf.

population growth in Pakistan. The difficulties in the informational realm arise from the subtle and destructive using all types of data, such as media, ranging from cultural co-option to mass perception management and the propagation of despair. Cyber threat and cyber warfare are added in the threats of national security of Pakistan in the contemporary age.

2.3 National Security of Pakistan: The Role of Cyber-warfare and Cyber-security

In order to avoid hacking, digital surveillance, and online incitement, the participation of Pakistan in war against terror and the rivalry of Pakistan with India have increased the need of effective security from cyber threat. There are so many events in the recent past of Pakistan's history, such as hacktivism, digital surveillance, and Cyber Jihad indicates the cyber channel abuse.[83] These are comes under cyber warfare's umbrella and have potential to weaken Pakistan's national security. In visualization, adequate legislation, leadership, infrastructure, and consolidate dogmas to respond cyber attack, as comparison of neighboring countries Iran and India; it is lagged behind. India, the rival of Pakistan has been invested much in it and activated the Defense Cyber Agency (DCA) for two to three years.[84] Several occasions have pointed out by the lawmakers and researchers about threats to Pakistan's national security due to cyber attacks. There are three kinds of cyber attack which are examined around the sphere. Unregulated Cyber space is of them. Anyone who has even a minimum knowledge of information technology can evade the cyber space of Pakistan easily. First time, Pakistan has been ordered to block the anti-Islamic material on the internet; however, the system used was not effective because a very low quality and free software's has used which can easily by pass the telecommunication blocking system of Pakistan. Pakistani government has blocked the access to several websites containing pornographic, blasphemous, and material based on anti-state, but this is ineffective due to inadequate mechanism of

[83] E. S. M Akerboom, *Jihadists and the Internet 2009 update*, (Netherlands: National Coordinator for Counterterrorism (NCTb), 2010), https://fas.org/irp/world/netherlands/jihadists.pdf.

[84] Cyber Defense Agency, "India is quietly preparing a cyber warfare unit to fight a new kind of enemy," *The Economic Times*, October 19, 2017, https://economictimes.indiatimes.com/news/defence/india-is-quietly-preparing-a-cyber-warfare-unit-to-fight-a-new-kind-of-enemy/articleshow/61141277.cms?from=mdr.

blocking.[85] At ICON (The Internet Corporation for Assigned Names and Numbers), Pakistan ranked quite low rated. For maintaining internet data flow records, the system is very weak and power.[86] The real identity and location of a user can easily be obscured through freeware apps, which is very disturbing indeed. The threatening concepts have originated through uncontrolled cyber-space.

2.3.1 Cyber-Terrorism

The effect of terrorism has been fuelled by uncontrolled cyberspace, where terrorist groups use the digital media to spread aggression, fear, and ideology very easily. Due to terrorism, Pakistan has been suffered a lot for twenty years. By eradicating conventional threats of terror; the considerable success have achieved by the forces of Pakistan army, but because of its craftiness nature, cyber terrorism threat is now posturing a more powerful threat. In 2016, terrorists have used the soil of Afghanistan and network of Afghanistan telecommunications; this has planned and conducted an assault on University of Bacha Khan at Mardan.[87] Moreover, Janduallah based in Afghanistan has reported the Safoora bus attack, Karachi.[88] The attack has been motivated by the ISIS individuals including Saad Aziz, Tahir Hussain Minhas and Asad-ur-Rehman, all of them are university students. The surprising nature of attacks has made them more dangerous and violent for the national security. Furthermore, the medical student of second year, Noreen Leghari had inspired and then joined the ISIS through facebook usage. Pakistan army apprehended her later.

[85] Malahat Rab, *PTA Blocks Access to Anti Islamic Video in Pakistan*, (Pakistan: Pakistan Telecommunication Authority, 2012), https://pta.gov.pk/index.php/en/media-center/single-media/-pta-blocks-access-to-anti-islamic-video-in-pakistan.

[86] Ibid.

[87] Ashish Shukla and Yaqoob U. Hassan, "PAKISTAN NEWS DIGEST A Selected Summary of News, Views and Trends from Pakistani Media," *New Media and Mass Communication*, July 2016, https://www.google.com/search?q=Ashish+Shukla%2C+%22PAKISTAN+NEWS+DIGEST%3A+A+Selected+Summary+of+News%2C+Views+and+Trends+from+Pakistani+Media%2C%22+Institute+for+Defence+Studies+and+Analyses+%7CIDSA%2C+last+modified+January+2016.&rlz=1C1GGRV_enPK921PK921&oq=Ashish+Shukla%2C+%22PAKISTAN+NEWS+DIGEST%3A+A+Selected+Summary+of+News%2C+Views+and+Trends+from+Pakistani+Media%2C%22+Institute+for+Defence+Studies+and+Analyses+%7CIDSA%2C+last+modified+January+2016.&aqs=chrome..69i57.1312j0j4&sourceid=chrome&ie=UTF-8.

[88] M. I. Khan, "Pakistan gunmen kill 45 on Karachi Ismaili Shia bus," *BBC*, May 13, 2015, https://www.bbc.com/news/world-asia-32717321.

2.3.2 Cyber-Propaganda

Cyber propaganda has used by individuals, religious, and political parties to promote violence, a narrative of extremism, and an anti-state agenda. So, this sort of propaganda puts tremendous pressure on any government. In foreign events, the effects of cyber propaganda have been seen. For example, the exploitation has done in presidential elections of Russia in 2016. Fake news and figures are used in the situation to engineer the minds of the electorate using social media. The fairness of every election is compromised by this sort of act using the electronic media. Pakistan has been suffering from same issue for last two to three years. There are numerous political movements and religious propagandas has witnessed in the territory of Pakistan through social media. The rise and spread of Tehreek Labaik Pakistan has caused violence and extremism in 2017 and 2018 and push Pakistan towards danger and instability.[89] The agenda of TLP has spread through social media. The mental and physical illness has been diagnosed in the general public due to the situation. The government could not be able to control the situation and fails to maintain law and order. Moreover, the important case which has emerged in the last two years to manipulate and harm the sentiments of Pashtuns in the Federally Administered Tribal Area of Khyber Pakhtunkha by the Pastun Tahafuz Movement (PTM)[90]. In this crucial stage of ongoing war against terrorism, the anti-state slogans campaign created a soft power forum to instigate hate. The event's scale can easily make it a platform for anti-state components to take advantage of participants' flaw to stimulate the anti-state agenda. Similarly, fake news has flooded the international and social media many times to generate panic among the public. The lack of public awareness about usage of social media and internet sites is the most important issue faced by the Pakistan in the cyber domain instead of knowing what they see on their screens even now, lack of information persuades mostly under educated classes to accept fake news or rumors. Cyber bullying stalking, robbery or being terrorized frequently stems from a lack of knowledge of cyber ethics.

[89] Asad Hashim, "Pakistan: Thousands protest blasphemy acquittal, ignore PM's call," *Aljazeera*, November 1, 2018, https://www.aljazeera.com/news/2018/11/1/pakistan-thousands-protest-blasphemy-acquittal-ignore-pms-call.

[90] Ibid.

2.3.3 Cyber Harassment

It is also called cyber bullying. Cyber domain has been used by the individual through a plethora of ways such as social media sites to intimidate public. Social media users are commonly the victims. Attackers blackmail them and use them for various purposes. There are various consequences of cyber bullying; however, evidence suggests that it has disproportionate impact on youngsters relative to adults and teens. If they begin to develop physically and psychologically, youth suffers the most. Anxiety, loneliness, and depression have been visible in cyber victims.

2.3.4 Economic Disruptions

In the contemporary times; trade, e-banking, and e-commerce have reliant on ICT.[91] These terminologies have made life incredibly quick and brought enormous improvements to current life habits, although these activities have become susceptible to cyber attacks. Cyber domain economic disruption is considered to the most critical because the purpose behind the cyber attacks is to destroy country's economic system, which could create panic and chaos in public. The attacks are perhaps leads to direct money theft or intended to inflict damage. The main targets of the cyber attackers are banks to destruct nation's economy completely because economy is the one of the pillars of national security. Pakistan has been the victim of small-scale attacks targeting several bank account holders in 2018; however, concerned attacks in this area have a devastating effect. This impacts on the individual's life and has had a significant effect on the national security.

2.3.5 Cyber-Theft

Trading and internet based trading and banking firms have been stealing through cyber-theft. Such attacks have been observed in Pakistan since 2018. Millions of rupees have robbed and transferred illegally through online facilities. So, Pakistan authorities are powerless to justify the events. No criminal has been identified so far and dilemma has been created where people have been losing confidence in the use of internet banking systems, which will put Pakistan back in this domain again. Many online payment firms have been led by internet scammers and hackers to ban Pakistan from using its services

[91] International Institutions and Global Governance Program, "Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms," *Council Foreign Relations*, February 23, 2018, https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms.

such as PayPal, Google AdSense, skill and others. Debit cards and credit cards abuse in Pakistan has undermined the trust of individuals. In light of latest report, there are almost 20,000 attackers who have sold the stolen data to the hackers. So, there is a serious threat of Cyber Attacks not only Pakistan but to every country's national security.

2.3.6 Crypto-Currencies

Because of the stealthy and secure nature, the mysterious rise of crypto currencies has been attracted the investment from last few years from major investors. Crypto currencies have complex transaction systems; therefore, these are projected to be widely used in terrorist financing. It is difficult for developing countries like Pakistan due to less efficient e-payments systems to prevent the attack and track the activities related to finances. National security has linked with it by the anti-state organizations. In the entire world, there are a plethora of crypto currencies, although most of them are not registered. Terrorist groups are drawn by stealth transections to use uncontrolled currencies, in cases. The unregistered crypto currencies are the reason behind the money laundering spread. In terms of statics, approximately 2073 crypto currencies with a potential of market are of almost 1.4 trillion dollars are in operation. Crypto currencies' legalization varies from region to region. However, due to lack of effective mechanism against Pak-coin or the consumption of crypto currencies resulted in a 60% rise in first crypto currency of Pakistan. In the broader sense, they are use in extremism, money laundering, and tax evasion. So, it causes a serious threat for both national security and economy.

Usually, the attackers claim the money in crypto currencies because it is difficult to trace attackers by use of it. When the NHS system of UK has targeted in 2017, these forms of attacks became popular.

2.3.7 Ransom wares

It is software of virus. It is used to infect the target machines and encrypt their impracticable information before the anonymous attackers are paid off by a specified ransom to decrypt the data to reuse.[92] WannaCry is the name of the virus which has used to access the medical system of UK. It is used by attaching with emails. After clicking on

[92] Conner Forrest, "NotPetya ransomware outbreak cost Merck more than $300M per quarter," *Teach Republic*, October 30, 2017, https://www.techrepublic.com/article/notpetya-ransomware-outbreak-cost-merck-more-than-300m-per-quarter/.

it, the information is blocked and virus spreads in the system and it becomes convenient for the hackers to make online money transections by accessing the required files. There are around three lack computers which are affected due to the virus WannaCry. The United Kingdom’s National Security Services (NHS) has remained inactive for several days because twenty two years old Devon security researcher has been able to find a kill switch and restores the access to the system. During its conflict with Russia, the same type of attack dubbed was used to hack computer systems in Ukraine using a virus called “Petya”.

2.3.8 Cyber-Physical Attacks

The attacks in which hacker or attacker has entered from virtual computer environment to the real world and resulted in disastrous consequences is called cyber-physical attacks. The usage by the American and Israelis of the computer virus Stuxnet, which infected Iranian nuclear program computers and disrupted thousands of programmable logic controllers (PLC) running the centrifuges used to enrich uranium. These attacks are known by countries like US as top level attacks and the attacks are vital for the automated SCADA systems (Supervisory control and data acquisition) and Information Control Systems (ICS). For power grids, water management, and critical infrastructures; ICS and SCADA systems are used. Physical cyber assaults come into the following cyber activities.

2.3.9 Sabotages

Cyber warfare sabotage is known as an assault or attack, but in which the attackers’ target is computer system that controls vital infrastructures including Nuclear Power Grids, Automated Production Systems, Nuclear Weapons, Transportation Systems, Electric Distribution Systems, and many others. Fortunately, Pakistan has not experienced such kind of attack and there are two reasons behind this. Pakistan has established both suitable security system and nuclear program that has been seemed adequate by the International Atomic Energy Agency on several occasions IAEA. Second, Pakistan has not established industrial control system and remained underdeveloped. This will improve in future with the implementation and growth of new technology‘s possibility will increase. Iran has faced such kind of attack, the stuxnet virus has destroyed its nuclear program; therefore, this form of advancements in the field of technology gathers the attention of attackers worldwide and has a chance of being attacked.[93]

2.3.10 Data Breaches

The crucial failures have been emerged due to data breaches in information and communication networks. Such as the personal data of people using social media on the internet has been infringed and illegally exploited on several occasions for last three years. The steal data has sold on the internet, then used in cyber abuse in turn. Many analysts have called these kinds of breaches as important as this data can be critical in influencing the public's ideology using fake news as per defined agenda. In 2005, data breaches have been identified; however, in 2017 and 2018, the critical data has breached. A Cambridge Analytica whistleblower has been reveled since 2018 that Cambridge Analytica, which is used to manipulate the American voters, which had exposed data from 50 million of Facebook users.[94] A significant factor which linked with events, for example, US presidential elections in 2016, Arab Spring, and Brazilian presidential elections in 2018 is described as data breaches. With this in mind, it is significant to clarify that 60 million Pakistani users have access to the internet in light of the Telecommunication Authority of Pakistan. 40% people have registered social media user profiles. If data has violated unlawfully, this could lead to an undesirable circumstances in future.

2.3.11 Relying on Foreign Equipment

One of the most ill-fated areas of research in cyberspace is the use of foreign equipment in the field of information and communication technology. The computer systems used worldwide are developed by majority powers and used in many countries' vital infrastructures. When manufacturers leave a back door, RAT (Remote Access Trojan), and backchannel, etc. in computer equipment, the use of such devices could be abused. Like other countries all across the world, Pakistan is also dependent on computer

[93] Robert McMillan, "Siemens: Stuxnet worm hit industrial systems," *Computerworld*, September 14, 2010, https://www.computerworld.com/article/2515570/siemens--stuxnet-worm-hit-industrial-systems.html.

[94] Carole Cadwalladr and Emma G. Harrison, "Revealed: 50 million facebook profiles harvested for Cambridge Analytica in major data breach," *The Cambridge Analytica Files*, March 17, 2018, https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

equipment, from small microprocessors to heavy duty industrial computer systems, which is the real threat to the national security at some stage in the future.

2.4 Pakistan's Endeavors to Counter Cyber Warfare

There is actually a very low level of Cyber Crime legislation in Pakistan, which is expected to tackle low-level cybercrime. Pakistan is expected to tackle low level Cyber Crimes. There is no capacity to cope with cyber warfare at large, national, and global level; furthermore, the strategies are also unproductive.in addition, the new laws, rules and regulations are obsolete and public has no knowledge about them. Pakistan has launched the Electronic Transactions Ordinance in 2002.[95] The purpose is to fix problems related to Bank. On the other side, for dealing with terrorism, electronic device abuse, electronic encryption misuse, and electronic falsification; the "Pakistan's Cyber Crime bill 2007" has passed.[96] The prevention of Cyber Crime act has passed in 2015. In the constitution of Pakistan to tackle Cyber Crime; Prevention of Cyber Crime is the only first level response to any cybercrime in Pakistan has adopted. It describes the stated areas of Cyber Crime and penalties and punishments related to it in Pakistan. In the Pakistan cyber space, the bill represents the various forms of crimes which come under umbrellas of cyber crimes. The National Response Center for Cyber-crime (NR3C) has been mandated by Federal Investigation Agency (FIA) since 2007[97]. The agenda behind is to tackle technical crimes in Pakistan. In Pakistan, it's the one and only unit; however, it also allows other law enforcement agencies in their own affairs to receive complaints directly. After the advent of NR3C, in comparison with the modern world developments at cyber crime on the basis of technical research, NR3C's statistics on its implementation have been weak. Neither is it regulated properly, nor up to the mark. As contrasted with other agencies in the world, even the simple setup of the agency is not standard.[98]

[95] DAWN, "Electronic Transactions Ordinance promulgated," *DAWN*, September 12, 2012, https://www.dawn.com/news/56846/electronic-transactions-ordinance-promulgated.

[96] Ghulam M. Kundi, Allah Nawaz, and Robina Akhtar, "Digital Revolution, Cyber-Crimes And Cyber Legislation: A Challenge To Governments In Developing Countries," *Cyber Crime and the Victimization of Women* 4, no. 4 (February 2014) https://www.researchgate.net/publication/283316038_Digital_Revolution_Cyber-Crimes_And_Cyber_Legislation_A_Challenge_To_Governments_In_Developing_Countries.

[97] Federal Investigation Agency, *National Response Centre for Cyber Crime*, (Islamabad: Federal Investigation Agency, 2016), https://www.nr3c.gov.pk/about_us.html.

[98] Mehwish Khan, "7-Point Action Plan Proposed for Cyber Secure Pakistan," *ProPakistani*, 2013, https://propakistani.pk/2013/07/09/7-point-action-plan-proposed-for-cyber-secure-pakistan/.

Conclusion

Pakistan’s government has been developing the policies to counter cyber attacks since 2013, but it has not been implemented in true meanings. Over time, the realm of cyber space is exploited by the cyber criminals; however, it has also become the greatest safe haven for cyber terrorists to recruit and use contact, data collection, mobilization networks, and psychological warfare. Pakistan has launched the Electronic Transactions Ordinance in 2002.[99] “Pakistan’s Cyber Crime bill 2007” has also passed to counter cyber attacks.[100].Moreover, The National Response Center for Cyber-crime (NR3C) has been mandated by Federal Investigation Agency (FIA) since 2007.[101] One of the major reasons behind the cyber threat in Pakistan is lack of awareness among public about cyber threats and cyber warfare. Tehreek e Labaik (TLP) and Pastun Tahafuz Movement (PTM) have been raised in Pakistan for few years are due to cyber propaganda and real threat to the national security of Pakistan.

[99] Ibid.
[100] Ibid.
[101] Ibid.

Chapter III

Pakistan’s Existing Infrastructure against Cyber Threat

3.1 Introduction

In the contemporary world cyber warfare is very dangerous. Many powerful countries using cyber space as a military. Now we are living in modern age world we can't see our future by the crystal ball although we are in age where any organization government can engage cyber war and cyber crime. In 1950 that time nuclear weapons maintained the balance of power but now nation state cyber warfare is becoming an equalizer shifting the balance of power in the world. Cyber warfare means the use of technology and cyberspace for the interests of a state against the enemy's state or nation. Digital battle by attacking computer networks, hacking, websites, and digital operations are involved in cyberspace. The purpose of cyber attacks is to espionage and sabotages the security and finance system of a state. There is no proper definition for cyber warfare; it is a continuous war without any end. The developing era of information and technology is raising danger. To counter these threats, nations and developing capacities to defend themselves.[102]

Cyber space is increasing day by day due to use of information technology and telecommunication. That technology invites the hackers to misuse and disrupt the use of cyber space. Hackers are hack the networks and system is become paralyze. In recent hackers cyber attacked on infrastructure and services but Pakistan don't have accessibility to counter the cyber attack. Hackers attacks and earn money after that they hide their identity by the internet. Pakistan must adopt the policy against the cyber security because cyber security defines the body of technology rather all system is running by the cyber security like, software program, infrastructure, military command and control system. Pakistan should be protecting from disruption, hacking and cyber attacks. In the last ten decades world became change and now in contemporary world is called "information age" everyone realize more and more on internet. Pakistan is facing threats from the cyber world. Modern communities are relying on cyber space and trying to give the people flexibility in their lives but it can be challenge and threats for the people. Cyber

[102] Aamna Rafiq, "Challenges of Securitising Cyberspace in Pakistan," *Institute of Strategic Studies Islamabad* 39, no. 1 (2019), https://prdb.pk/article/challenges-of-securitising-cyberspace-in-pakistan-1538.

security is protects computer, database program and network from unauthorized access change or destruction. Many researcher analyzed cyber security issues increased those who create the nation's security policy. Cyber security is a big challenge for Pakistan rather for world. Pakistan’s policy maker should be adopting the policy to prevent the cyber boundaries of countries.

3.2 Cyberspace Vulnerabilities of Pakistan

To check the vulnerabilities of any country systematic cooperation is responsible to maintain all the comprehensive databases. The recorded database vulnerabilities are more than 66,400. According to the Internet security threat report (ISRT20), one-third of websites were scanned back in 2014 by this corporation. And find out loopholes in 20% of them. The corporation also made up 57.6 million at lack sensors via its Global Intelligence Network. According to the reports of 2014, none of the companies is secure in the era due to security threats of the internet.

This report also highlighted the emerging cyber threats linked to smartphones. As per the report, people only link cyber security with the computer system and neglect the protection of mobile phones. The entranced and extensive use of IT and technology has given easy access to hackers. They are able to misuse and disrupt the use of cyberspace all across the world. 39% of the total population of the country uses mobile phones. It is expected to reach 50% in 2025. This emerging use of technology is giving rise to a new threat to cyberspace security.[103]

Till now the PECA is the most significant plan which was presented in 2016. The purpose was to ensure security against unauthorized data, illegal information, interception, and transformation of critical data. It was also responsible to stop the spread of hate, fraud, data-stealing, etc. via the internet.

In 2017, International Telecommunications Union ranked Pakistan at number 67th on the Index of Global Cyber security.[104] According to the index, the technical and organizational measures of Pakistan are still a long way away to go. Pakistan is one of the

[103] Muhammad R. Shad, "Cyber Threat Landscape and Readiness Challenge of Pakistan," *Institute of Strategic Studies Islamabad ISSI*, April 2019, http://issi.org.pk/cyber-threat-landscape-and-readiness-challenge-of-pakistan/.p

[104] Amin Yusufzai, "Pakistan Ranks 67th in Index Measuring Commitment to Cyber Security," *ProPakistan*, 2017, https://propakistani.pk/2017/07/18/pakistan-ranks-67th-index-measuring-commitment-cyber-security/.

highest in terms of malware-hosting sites. Through malware personal information and data are being stolen from infected computers Distributed Daniel of services (DDoS) attack comes at the number to in terms of cyber threat for the country.

In 2018, the banking sector of Pakistan suffered a huge loss due to cyber-attacks. On the Dark web, the personal data of eight thousand people are available with their banking details. India is considered one of the main enemies of Pakistan.

Pakistan and India have been involved in biological, chemical, conventional, non-conventional, and nuclear warfare. Now India has initiated cyber warfare in the "Cold Start Doctrine".[105] Cyber warfare is all about various tools and techniques for the purpose of destruction. The computer system is being damaged at tactical operational and strategic levels. All the critical information and data related to nuclear command and control can be hacked or destroyed easily. India included cyber warfare as an essential component of the Hybrid or fifth warfare Generation. Now cyberspace is a new dimension for future wars and conflicts.[106]

The growing cyberspace, which incorporates the increased usage of IT and Telecoms, attracts hackers to misuse and disrupt the use of cyberspace. The area for attacking hackers has also increased to a degree where networks can be disabled. Imagine what happens if a country's financial, power grid, transport, military control and control system are immobilised.[107]

Millions of cyber assaults on infrastructure and services have occurred throughout the past several years. Hackers often utilised ransom products to earn the victims money. It is also essential that we be able not just to protect ourselves against such assaults, but also to undertake counter cyber strikes. This is easier said than done, as it is difficult to identify the identity of the attacker in most of situations. The nature of the Internet allows for all infrastructures to be hidden behind it. In particular, cyber assaults are supported by the state. The hackers also enjoy anonymity due to the asymmetry of assaults.[108]

[105] Gurmeet Kanwal, "Strategic Stability in South Asia: An Indian?s Perspective," *Institute for Defence Studies and Analyses (IDSA)*, June 2010, doi:10.2172/1367405.

[106] Abdullah R. Butt and Amna Tauhidi, "Cyber Vulnerabilities of Pakistan," *CASS - Centre for Aerospace and Security Studies*, February 2020, https://casstt.com/post/cyber-vulnerabilities-of-pakistan/147.

[107] Hermann Kaponig, "Austria’s National Cyber Security and Defense Policy: Challenges and the Way Forward," *Connections: The Quarterly Journal* 19, no. 1 (2020).

[108] Tobias Calås, "Quality of Governance and Cybersecurity A quantitative study into Securitization-theory and Cyberspace," (master's thesis, Uppsala University, 2019).

Countries, however, must take adequate cyber security measures. Cybersecurity is described as a collection of technologies, procedures and policies to prevent attack, damage or illegal access to the networks, computers, programmes and data. Safety covers cyber security and physical security in a computer setting. In order to prevent disruption and hacking, cyber-attacks, cybersecurity envelopes Computer Networks, infrastructure, software programmes, military command and control systems, utility services etc. As the technology progresses quickly, domestic gadgets may potentially be hacked and disrupted. [109]

Over the past 100 years, the methods States and non-state entities practise the art of war have changed significantly. The "information era" is widely termed this century, but not without its drawbacks. As the world relies more on Internet, links and technology, the possibility of breaches of cyber security is growing and tends to inflict significant damage. Similarly, Pakistan is also facing cyber-world dangers. Pakistan is likewise confronted with a cyber space issue. Cyberspace threats have been expanded in Pakistan in banking, education and telecommunications, military and government organizations.[110]

3.2.1 Dangers of Digital Revolution and Weaknesses of Pakistan

One of the most intense transformations of this era is the digital revolution. Almost all fields of life are somehow dependent on technology now. In start the purpose of cyber technology was communication and computing. But now it has expanded and part of banking, transport, food, management, and governing bodies' people of all fields from across the world are connected now which make the world "Global Village". However, vulnerabilities are one of the most consequences of this interconnectedness. Moreover, the individuals and states have compromised their privacy Digital platforms are considered more effective to judge state and state citizen's relations. The communication, computing, governance military and civilians rely on digital networks which can be attacked from any part of the globe. Then vulnerabilities are rising due to

[109] Rubab Syed, Ahmed A. Khaver, and Muhammad Yasin, "Cyber Security: Where Does Pakistan Stand?," *Sustainable Development Policy Institute (SDPI)*, February 2019, https://www.think-asia.org/bitstream/handle/11540/9714/Cyber-security-where-does-pakistan-stand%28W-167%29.pdf?sequence=1.

[110] William H. Dutton et al., "Cyber Security Capacity: Does It Matter?," *SSRN Electronic Journal* 9 (2019), doi:10.2139/ssrn.2938078.

complex networks.[111] A study conducted by an organization named Broimum showed that digital crime revenue reached 1 Trillion dollars annually in illicit profits. In the 21st century, every nation is facing problems of cyber security in domains of economy, politics, environment, and military, etc. The digital infrastructure that is easy to organize, difficult to trace, and asymmetric in nature is always more vulnerable to cyber-attacks. Pakistan is easy prey to cyber-attacks.[112] Pakistan comes at number 7 in the vulnerable countries to cyber disruption. The most common cyber attacks are data-stealing, website hacking, and denial of service attacks (DOS). There is a number of incidents that revealed the weakness of Pakistan's cyber security framework. In 2008 the finance minister of Pakistan reported that the services of the state bank of the country have been freeze for 21 days. The banking system of the country was once again targeted in 2018. The ATMs of Habib Bank Limited and Bank Islamic Limited were once again targeted in December 2018.[113] There are many loopholes in regards to cyber security in many institutions of the state in the country. The official website like the ministry of interior, ministry of foreign affairs, District court Gujranwala, Faisalabad police department, Lahore high court, and website of the government of Pakistan were affected by cyber due to cyber attacks.[114]

Moreover, the footprints of these attacks were linked with rivals of India on 2nd March 2019 the passport tracking application of Pakistan and their website were hacked. In this attack, the visitor's data was stolen by using the scan box framework. The media platforms and political parties are also among the main targets of cyber technology. Likewise, the websites of Jag Tu, CNBC Pakistan, SAMMA FM, PPP, PML-N, JUI-F were hacked to sabotage their image.[115] The hackers inserted anti-Pakistan slogans and material on the homepages of these websites. The military and security agencies of

[111] Muhammad M. Sadiq and Rasa Daugėlienė, "ASSESSMENT AND ENHANCEMENT OF CYBERSECURITY RISKS IN PAKISTAN," *Institute of Strategic Studies Islamabad ISSI*, December 2019, https://www.researchgate.net/publication/339051655_ASSESSMENT_AND_ENHANCEMENT_OF_CYBER_SECURITY_RISKS_IN_PAKISTAN.

[112] Ibid.

[113] Dunya News, "Card data of 20,000 Pakistani bank users sold on dark web: report," *Dunya News*, November 6, 2018, https://dunyanews.tv/en/Crime/465384-Card-data-Pakistani-bank-users-sold-dark-web-report.

[114] KPMG, "Dealing with cyber threat is a complex challenge," KPMG, last modified March 1, 2017, https://home.kpmg/qm/en/home/about.html.

[115] Ibid.

Pakistan are not safe in this regard. However, the nature of attacks may differ according to the objectives of these attacks.

3.3 National Security Secrets

The main objective is to steal national security secrets and essential information of the country. The technology is used as a "cyber-weapon" to control and command the available data during wars and conflicts. All the above-mentioned incidents are proof that the security policy of Pakistan is vulnerable due to which cyber attacks are increasing each day. On the other hand, the situation is difficult for policymakers to establish a security framework due to the limitations and regulation of cyberspace. There is a need to rebuild the legislative bodies, formulate strong policies, implementation mechanisms to overcome the threats of cyberspace and digital infrastructure in the country. Furthermore, the collaboration and consensus-building among government and stakeholders would bring effective policies against cyberspace. A comprehensive plan, implementation strategies will ensure a balance between the rights of the citizens and security.[116]

3.4 Irresponsible Media Reporting

Today, there's not, at this point such thing as "the consistent pattern of media reporting" — everything is a day in and day out. Because of innovative changes and lower costs, people and associations are perpetually dependent on electronic correspondence. Today, the space of the internet is similarly available by first world countries to Taliban guerillas and ISIS individuals. This straightforward entry creates a strong danger, which should be made preparations for. The term Cyber War had been begotten to portray the new sort of fighting, which centers on the threatening electronic and correspondence frameworks. "This is another worldview of fighting", in which not many PC infections and projects might be more valuable than developments of soldiers and may cause a widespread disappointment of electronic hardware of C4I2SR frameworks, RADARS, PCs, weapon frameworks, reconnaissance and all objective electronic frameworks as exhibited during the Gulf War, wherein the United States outsmarted Iraq by applying Cyber Warfare principles. Cyber warfare goes before the genuine battling and may even forestall it before it can take a beginning. The advancements in Cyber warfare have made the cutting edge multitudes of the world to

[116] Ibid.

think and accord due to accentuation, as simple entry by unfriendly electronic and correspondence frameworks can be abused to upset military readiness just as the economy of the country and should be prepared for.[117]

3.5 Abuse of Information

Any activity which has used to commandeer PCs, organizations, and computerized innovation and has wrong expectations to control them, for example, abuse of information is known as a digital danger. There are specialists to make a lawful move against threatening clients of PCs and programmers by worldwide and civil law. The key reason for Cyber Attacks is demolition, passing, executing, dread, and harm, and so forth in couple of cases, PCs or contraptions are not the objectives of programmers; in any case, they control air terminals, banks, and other touchy spots like force lattices to achieve their objectives.

3.6 Lack of Security Framework

The forecast is made in the Critical Infrastructure Readiness Report become valid. States has picked up the ability to obliterate framework through innovation. The legend has become a reality. Presently, there is a rundown of nations whose foundation has been devastated with the assistance of digital assaults. The assaults are; Tanks had shipped off Georgia by Russia in 2008. It was a Cyber Attack for the calculation of the framework. This was considered the main Cyber Attack.

In 2008, the US and Israel had built up the capacity and disabled Iran's enhancement program of atomic.[118] In 2014, programmers had breached the German steelworks and the heater had not worked appropriately and not shut downed. Another Cyber Attack had been seen in 2015, it was an assault in Ukraine, and 230,000 individuals lost matchless quality and force. Aggressors held onto the framework and the framework was constrained by the far off. The assault was dispatched from Russia. The occurrences close, the war techniques, strategies, and strategies are changed at this point. The weapons, for example, Guns, bombs, activity are no longer supports prevention and

[117] Ibid.

[118] Julia Masterson, "Timeline of Nuclear Diplomacy With Iran," *Arms Control Association | The Authoritative Source on Arms Control Since 1971*, July 2021, https://www.armscontrol.org/factsheets/Timeline-of-Nuclear-Diplomacy-With-Iran.

dread. The console is the new weapon to control, obliterate, decimate, and rout adversary.[119]

With our change into the data and the innovation age, the entryway to the arrangement of digital dangers to our public security has been opened. The development improvement of the innovation and more reliance on the PCs will cause changes in the philosophy of public security ideas for our country as well as for all the countries. The countries have this dread and danger that their data information base might be hacked, changed, or debilitated by some other assaulting or hostile development innovation. We should be completely mindful and have a full exploration of all the dangers that may happen by new and advanced innovation and its results on the public security in digital space. This paper would give an occasion to investigate digital fighting measurement bases after arising innovations and electronic methods.

It has changed the lifestyles and encouraged human existence in numerous perspectives. Each record and undertaking was changed over from papers to the virtual space called the internet. With the progression of time, we become the need of people, organizations, governments, militaries, worldwide companies, and public and global associations. Everything including records and grouped information of governments and associations were changed over to the computerized data and was shared to the internet for additional capacity, change, and correspondence. As of now, there would be not really any organization to run its issue with our utilizing the web. This is the time of digitalization and everybody is subject to the web. The internet has made effectiveness in working together, running the state issues, and battling the wars essentially. Where it has encouraged all the lifestyles it has additionally made a lot of weakness which has been a grave worry for the world. On one side it is encouraging us and then again, it is making weaknesses that are more extreme in nature.[120] The world has gotten more worried about these weaknesses and dangers. Cyberspace is presenting numerous dangers and weaknesses and nearly everybody inclined to these dangers which are being presented by the internet albeit each nation has been constrained to take radical measures to alleviate

[119] OSAC, *Pakistan 2020 Crime & Safety Report: Islamabad*, (Islamabad: OSAC, 2020), https://www.osac.gov/Content/Report/f36dd7e9-8cf3-489c-b9b4-187819994ff8.

[120] Ibid,

these dangers and weaknesses. In this section, we will examine the weaknesses and dangers of being forced by the internet.

There are three primary sort of Cyber Security.[121] The reconnaissance has been accomplished for the monetary profit or disturbance. There are a plenty of alternatives and strategies of assault for malevolent entertainers. There are numerous sorts of Cyber dangers, for example, Malware ,Phishing(email-borne assault ,the information has hacked by tapping on connection), malware on versatile applications, man in the center assault (the data has commandeered by the programmer between the sender and collector), stick phishing, Trojans (malevolent code inside the framework), Denial of Service assault or Distributed Denial of Service Attack DDoS, Ransom product ,Data Breaches (information penetrated by a vindictive entertainer), and assaults on IOT gadgets .

3.7 Security Sector

Pakistan Army has confirmed that the Indian intelligence services have carried out a massive cyber attack on government officials. The assault involved hacking cell phones and electronics by officials of the government and military staff. The attack was directed at misleading manufacturing. Despite his recent interception, he expressed grave concerns about India's danger of warning Pakistan from hacktivism and full-scale digital sabotage to propaganda.[122]

The above-mentioned instance of cyber spying is not unusual. Earlier in 2019, the Israel spyware firm NSO Group, which used spyware named Pegasus, was allegedly hacked by two dozen cell telephones from senior defense and intelligence officials. The technology which was apparently created to control crime has been accused of being used for state sponsored spying by its operators. It is worthy of noting that India-Israel strategic cooperation is a fact. Indian officials rejected any NSO contracts or possessed Pegasus. Cooperation extends from weapons supplies and military technology to high-tech sharing. There are many loopholes in regards to cyber security in many institutions of the state in the country. The official website like the ministry of interior, ministry of foreign

[121] Bill Rosenthal, *The Three Elements of Cyber Security*, (Logical Operations, 2016), https://logicaloperations.com/insights/blog/446/the-three-elements-of-cyber-security/.

[122] Aneeqa Safdar, "The Emerging Threat of Indian Cyber Warfare Against Pakistan," *Daily Times*, August 28, 2020, https://dailytimes.com.pk/660092/the-emerging-threat-of-indian-cyber-warfare-against-pakistan/.

affairs, District court Gujranwala, Faisalabad police department, Lahore high court, and website of the government of Pakistan were affected by cyber due to cyber attacks.

Hackers have targeted Pakistan's Foreign Ministry and Army bases. The ministry received multiple reports from different countries, according to Spokesperson Mohammad Faisal, announcing that, from 16 February 2019, websites were unavailable. The assault is suspected to have come from India, Dawn reports from Pakistan's news section. The attack was a result of the terrorist strike that killed 40 Indian CRPF workers in Pulwama, Kashmir on 14 February 2019. The terrorist group Jaish-e-Mohammed from Pakistan took charge of the attack.[123]

On February 10, US-based cyber security firm Lookout reports that the Pakistani military has been spying on two malware programmes on an Android based network that originated in India. In a tweet, Lookout said he discovered the Hornbill and SunBird malware used by an online community called Confucius which first emerged in 2013 as 'a state-sponsored pro-India player targeting primarily Pakistani and other Southern Asian goals. The Analytical Support and Sanctions Monitoring Team has said in a Feb. 3 briefing at the U.N. Security Council that, between July and October 2020, the terrorist group carried out over 100 cross-border attacks from Afghanistan to Pakistan.[124]

The ISPR on Wednesday said Pakistani intelligence agencies had detected a major cyber-attack by Indian intelligence agencies targeting government officials and military personnel's cell phones and gadgets. The Military media wing has said in a statement that the cyber attack involves "a variety of cyber crimes, including misleading deception by punching government and military officials' personal mobiles and technological gadgets." The statement added that some objectives were examined by "hostile intelligence services."[125]

Likewise, India has invested extensively in its military modernization, from the acquisition of sophisticated weapons to the production of state-of-the-art technologies in the area of artificial intelligence and outdoor space. The revived Indian Defense

[123] Ibid.

[124] Islamuddin Sajid, "Pakistan says probing pro-India malware 'attacks'," *Politics*, *Asia Pecific*, February 25, 2021, https://www.aa.com.tr/en/asia-pacific/pakistan-says-probing-pro-india-malware-attacks/2156362.

[125] Ibid.

Policy, the 2017 Joint Doctrine of Indian Armed Forces, which establishes defense technology as a core strategic weapon to enable military forces, represents a change in paradigms. Indian strategic circles concentrate on the advancement of digital weaponry to achieve cyber-supremacy as an institutional imperative for the future.

3.8 Commercial sector

In November 2018, when hackers targeted nearly all the country's banking websites, Pakistan had a similar incident. Anyone keeping a bank account could have been vulnerable to Internet attacks because data from almost every bank in the country has been hacked in a security violation. Captain (retd) Mohammad Shoaib, the director of the cybercrime Federal Investigation Agency (FIA), announced the incident. "Nearly all [Pakistani] bank data has been broken in an interview with Geo News. Much of the banks have been hit, according to the data we have."

According to an investigation carried out by Pakistan's Emergency Response Team (PACCERT), dates from 19,864 cards of customers from 22 Pakistani banks have been placed on sale on the dark website. All began in mid-October when some of Bank Islami's clients sent text messages alerting them about purchases, which they did not do. Bank Islami blocked its foreign payment scheme on the 27th October, with notice of irregular transactions of Rs. 2.6 million. This was a concerted cyber attack that affected Bank Islami's payment network and the international payment system. Hackers used the cards provided by the bank to carry out these transfers on overseas ATMs.[126]When the HBL ATMs were attacked, a large skimming attack occurred. Any arrests have been made but banks are still vulnerable to such attacks. The problem has been illustrated. PakCERT reports that data on stolen cards will be published on its website in both dumps. Meanwhile, several banks have banned international debit and credit card transactions, while others have sent customers text messages informing them their accounts are safe. No bank has officially stated other than Bank Islami whether any money has been taken from its account so it is unknown which customers are at risk.

Access to the network of Pakistan International Airlines, according to vulnerability analysts in Israel, is offered for sale on the cyber underground. A KELA Spokesman

[126] Farooq Baloch and Iftikhar Firdous, "Pakistani banks hit by biggest cyber attack in country’s history," *SAMMA*, November 6, 2018, https://www.samaa.tv/news/2018/11/pakistani-banks-hit-by-biggest-cyber-attack-in-countrys-history/.

told Info security Magazine on November 9, "We have been monitoring the threat actor who published domain access for sale last week to the network of Pakistan International Airlines.[127]There is no exception to the financial sector of the region. They are still faced with grave cyber attacks. The most frequent occurrence is the skimming of the accounts, abuse of ATM cards, hacking, and online theft. Around 8,000 to 10,000 out of 25 million bank investors have been defeated by hackers in the industry. Pakistani banks have lost significant sums of money from cyber attacks.[128]

To check the vulnerabilities of any country systematic cooperation is responsible to maintain all the comprehensive databases. The recorded database vulnerabilities are more than 66,400. According to the Internet security threat report (ISRT20), one-third of websites were scanned back in 2014 by this corporation. And find out loopholes in 20% of them. The corporation also made up 57.6 million at lack sensors via its Global Intelligence Network. According to the reports of 2014, none of the companies is secure in the era due to security threats of the internet.

In 2017, International Telecommunications Union ranked Pakistan at number 67th on the Index of Global Cybersecurity.[129] According to the index, the technical and organizational measures of Pakistan are still a long way away to go. Pakistan is one of the highest in terms of malware-hosting sites. Through malware personal information and data are being stolen from infected computers Distributed Daniel of services (DDoS) attack comes at the number to in terms of cyber threat for the country.

In 2018, the banking sector of Pakistan suffered a huge loss due to cyber-attacks. On the Dark web, the personal data of eight thousand people are available with their banking details. India is considered one of the main enemies of Pakistan. Moreover, the footprints of these attacks were linked with rivals of India on 2nd March 2019 the passport tracking application of Pakistan and their website were hacked. In this attack, the visitor's data was stolen by using the scan box framework. The media platforms and political parties are also among the main targets of cyber technology. Likewise, the websites of Jag Tu, CNBC Pakistan, SAMMA FM, PPP, PML-N, JUIF were hacked to sabotage their

[127] Sarah Coble, "Hacker Sells Access to Pakistani Airlines' Network," *Info-security Magazine*, November 10, 2020, https://www.infosecurity-magazine.com/news/hacker-sells-access-to-pakistani/.

[128] Wade Trappe and Jeremy Straub, "Journal of Cybersecurity and Privacy: A New Open Access Journal," *Journal of Cybersecurity and Privacy* 1, no. 1 (2018), doi:10.3390/jcp1010001.

[129] Ibid.

image.[130] The hackers inserted anti-Pakistan slogans and material on the homepages of these websites. The military and security agencies of Pakistan are not safe in this regard. However, the nature of attacks may differ according to the objectives of these attacks.

Pakistan and India have been involved in biological, chemical, conventional, non-conventional, and nuclear warfare. Now India has initiated cyber warfare in the "Cold Start Doctrine".[131] Cyber warfare is all about various tools and techniques for the purpose of destruction. The computer system is being damaged at tactical operational and strategic levels. All the critical information and data related to nuclear command and control can be hacked or destroyed easily. India included cyber warfare as an essential component of the Hybrid or fifth warfare Generation. Now cyberspace is a new dimension for future wars and conflicts.[132]

The International Peace Research Institute (SIPRI) in Stockholm has produced a special study on computer security norms that shows a number of engineered networks worldwide that are 'hack able' dependent on digital computing. The States have been attempting to address these flaws for several years and defense development is known as IT or security systems. In this speech, honesty is part of the 'CIA Triad,' which is a crucial secrecy, integrity and availability of the IT-security mechanism.

3.9 Fifth Generation Warfare

Digital dangers are developing with time. The strategies, frameworks, and procedures will be developed step by step. In this way, the dangers are supported with time. Old wonders' to forestall and safeguard one's self from digital dangers are sufficiently not and valuable in the current situation, for example, Multiday is a new age presented and it can't be noticeable in the sign discovery innovation. A number of elements include advancing Cyber dangers like individuals, spots, and settings. The models are Nation-states, programmers, fear-based oppressors, criminal gatherings, business contenders, and desirous gatherings. The country's undercover work has been done to know the insider facts of another state utilize their touchy data against them. In the appointments establishment article, Chris Painter of the USA office said that North

[130] Ibid.

[131] Gurmeet Kanwal, "India’s Cold Start Doctrine and Strategic Stability," *Institute for Defence Studies and Analyses (IDSA)*, July 2010, https://www.idsa.in/idsacomments/IndiasColdStartDoctrineandStrategicStability_gkanwal_010610.

[132] Ibid.

Korea and China have been utilizing the digital capacity to achieve their objectives all over the world. Both states have their destinations in the globe; in this manner, both are attempting to improve Cyber abilities. Digital weapons are utilized to achieve advanced burglary. There are a number of tombs and criminal associations, knowledge offices, programmers, and programming designers chipping away at the digital secret activities. Insight gathering proceeds amplifies, envelops, develops, and impacts the computerized world; nonetheless, it is hard to separate among knowledge assortment and assault to hold onto the framework arranging or getting ready to capture the system.[133] For occurrence, as a feature of traditional surveillance data assortment, a foe could disturb. The digital war tolls are dispatched to constrain the rival to achieve the longings of a rival; be that as it may, if the gathering opposes achieving the objective, Cyber Attack or Cyber war has dispatched to control and achieve the objective. In the contemporary age, public security has subject to data climate, even it is considered as the structure of get-togethers.[134] That is the reason solid establishments and savvy people are needed to save society from digital war tolls and digital danger and make a move against control on the grounds that the contentions through digital will build step by step. Along these lines, there is a need to fight back against assaults. The 5GW is more damaging because of the cutting edge innovation and methods. The dangers and difficulties will increment in the future as the 5GW is as yet advancing. There is no legitimate meaning of 5GW, notwithstanding, throughout the time it is totally changing into crossbreed war. The idea of the 5GW is continually changing and assessing. A wide range of means, innovations, and strategies are utilized in this sort of fighting. This is a time of progression and innovation is spread in each field of life including the military the worldwide legislative issues structure is presently multi-polar and the dangers of 5GW are expanded due to multi-extremity. Due to the multi-polar climate, there is no superpower. What's more, power is scattered in various locales of the world. Consequently, security concerns expanded to beat these issues states are gaining more innovative strategies for their safeguard The skirmish of stories is expanding because of the internet. The internet gives incredible occasions to go

[133] Raja T. Hassan, "Cybersecurity Threats: Policy gaps, challenges and way forward," *Daily Times*, February 7, 2019, https://dailytimes.com.pk/352011/cybersecurity-threats-policy-gaps-challenges-and-way-forward/.

[134] DAWN, "Pakistan being subjected to 5th-generation warfare in 'massive way' but we are aware of threats: DG ISPR," *DAWN*, December 3, 2020, https://www.dawn.com/news/1593804.

into strife circumstances. The atmosphere is ceaselessly hanging which causes a worldwide temperature alteration .the deficiency of water is driving the world towards water battles in the coming future there are odds of the forthcoming battle between Pakistan and India will be for assets of water. The dangers of 5GW are mind-boggling and can't be crushed by previously existing strategies to confront any unordinary challenge or warlike circumstance. Present-day issues require current answers for improving the circumstance.[135] A few strategies and methodologies are should be presented for the arising difficulties of the new fighting ages. The mental strategies are utilized to acquire profits by focused regions. The financial and security emergency is the ideal approach to squeeze the rival coalition or network. The contentions about the difficulties and security dangers of the new fighting age contrast; a few scholarly people are supportive of this thought as there are uncommon odds of direct war. In any case, the outcomes of these strategies and negative utilization of innovations will be more damaging than direct war. The rise of psychological oppressors associations got one of the greatest emergencies of the 21st century, the nations embraced this as a new strategy and completed fear mongers activities against their rivals. Psychological oppression turned into an instrument for the fifth era of fighting; other non-assailant apparatuses are additionally utilized for the effective accomplishment of objectives. The utilization of vicious instruments is proof that the rise of new fighting is dangerous for the harmony and dependability of the globe. The monetary weight, digital assaults/tasks, utilization of current innovation, and so on offers ascent to the flimsiness and undesirable rivalry among states. It is difficult to handle a haze adversary as in this fighting foe isn't obviously characterized. The force conveyance is additionally not satisfactory and this makes an issue in approach-making measure. The rival network or nations would be not able to confront the difficulties. The focused on network and state is controlled through broad communications by getting out the phony word which establishes an unstable climate. Digital assaults are one of the significant devices utilized during new fighting techniques. The information is taken or totally devastated by the PCs of targets. The sites and records of authorities and organizations are hacked to get data. In spite of the fact

[135] Asmaa Patel, "Fifth-Generation Warfare and the Definitions of Peace," *The Journal of Intelligence, Conflict, and Warfare* 2, no. 2 (2019), doi:10.21810/jicw.v2i2.1061.

that spying is anything, but an advanced procedure, yet it is utilized normally to get data and watch out for the exercises of the objective. To harm the adversary intellectually mental assaults are completed. Typically bogus claims and getting out phony word assists with attacking the positive picture of the adversary to make them intellectually wiped out. In such cases antagonism won in social orders. The incendiary activities are additionally done to invert or modify accepted practices, political structure, and regulatory choices. These exercises are completed cautiously so nobody could mention criticisms. The deadly danger is raised by featuring the strict and social contrasts among individuals of the same zone or spot. Afterward, these distinctions offer ascent to the common wars. The separatists' developments arose if there should arise an occurrence of common wars.[136]

As immediate intrusion of the war isn't important for technique thus, to accomplish objectives of making agitation in the focused on zone intermediary wars are started. For this reason the assaulting state give assets and military help to the radical gatherings of the region, this assists with making war like circumstance. The nations having atomic force use it to deflect other non-atomic and atomic states. The danger of beginning of atomic war is greatest test that is the reason non-[proliferation arrangements were established. The world of politics and world structure are not steady and it is evolving constantly. These progressions upgrade the dangers of shakiness. The war isn't announced, the assaulting state can receive any of the previously mentioned and different strategies to wreck the objective. This makes it hard for focusing on state to embrace arrangements against it. The objective network or nations are misused with the end goal of their pulverization. In the period of globalized world and present day advances negative picture of the states lead them towards disengagement. This makes the endurance of focused satisfies unimaginable. Every one of these difficulties is making security dangers for the entire world.

If there should be an occurrence of customary undercover work, the political and lawful audits are initiated; notwithstanding, regular military line falls because of the

[136] Shafaat U. Shah, "Fifth Generation Warfare and the Challenges for Pakistan2019," *Pakistan Politico*, January 15, 2019, https://pakistanpolitico.com/fifth-generation-warfare-and-the-challenges-for-pakistan/.

computerized assault. The digital fighting and Cyber Attack develops with advancement in the field of data and innovation.

The development of fifth war fare generation has changed the elements of contention and vital procedures. The nations received various procedures and strategies to start battle against adversaries without starting direct wars. The advanced innovation is utilized and states in a roundabout way attack. Generally, time the objectives are ignorant of the circumstance and get captured without any problem. The India and Pakistan are rivals since their development as a different state. India and Pakistan has been associated with wars straightforwardly since their rise for various reasons. Crossover war has changed the components of the contention. Both adversary states received digital assaults, illegal intimidation, and use if atomic weapons as a danger, helping separatists' gatherings, and foundation of ports, and so on to conquer the expanding impact of one another. Subsequently, the opposition and contention has been expanded to secure all the more incredible assets and vital strategies.[137]

Conclusion

Pakistan is vulnerable to a wide range of cyber attacks including computer viruses, identity theft, financial data theft, cyber crime, critical infrastructure monitoring, and intelligence on critical infrastructure. Unless these challenges are successfully met, Pakistan cannot guarantee robust national security. Technology, however, has also, in recent decades, been a major national security concern to the Member States. Current threats have been revolutionized by the state dependence on cyberspace and digital networks. Cyber warfare was finally realized by the generalized digital revolution of states and populations. All the countries which are aware of this danger use their ability to projected power in this region. The main opponent of Pakistan, India, is also among those nations who strive to a widespread culture of cyber weapons and militarize cyber space.

The technological development has posed new threats and challenges to states' stability, because the cyberspace between government agencies, telecommunications providers, militant facilities and bank infrastructure is continuously being breached by hostile states and even non-state actors. Developing countries such as Pakistan also face serious

[137] Ibid.

cyber-related problems that should be dealt with immediately. The infringement of public information, the hijacking of government websites, the penetration of government officials in WhatsApp personal reports, the evasion of financial institution cyber security, the effective use by terrorist organizations of ICT and a well-organized international malicious cyber campaign against Pakistan by hostile countries, such as India are serious warnings against politicians. In order to strengthen cooperation between civil and defence agencies, the State also has to establish a 'National cyber coordination centre.' Thus, improved coordination among law enforcement agencies will enhance Pakistan's cyber security environment and contribute to the strict implementation of cyber security policies.

Chapter IV

Reasons of Pakistan's Failure in Order to Preserve Cyber Security

The art of warfare is a dynamic phenomenon that is always evolving. Because of their scientific and technical advancements, humans have had a great deal of success in reviving the means of combat. Information and computer technology (ICT) has made it possible for information to move quickly. On the other side, it has revealed new threats to state cybersecurity, rendering countries like Pakistan and their citizens even more exposed. More than half of the world's population is now connected to the internet, which exchanges information and data in real time. With such a large population, internet security becomes a natural worry for any country. According to Symantec, a globally recognised cybersecurity organisation, "Pakistan is among the top 10 countries most vulnerable to cyberattacks." To combat this danger, new views must be taken, indigenous cyber technology must be improved, and capacity-building methods must be improved.

In terms of cyberattacks, 2018 was a perilous year for Pakistan. According to the Federal Investigation Agency (FIA), nearly every bank in Pakistan has been subjected to a cyberattack. According to a PakCERT assessment, over 20,000 ATM card numbers were stolen and sold on the dark web. In the same year, the Pakistan Air Force was subjected to a devastating cyber attack. It was codenamed Operation Shaheen, and it involved the use of phishing methods to obtain sensitive data from the Air Force. In 2019, Rattlesnake, an international group, attempted a similar attack on Pakistan's Naval Public Relations Bureau for stealing crucial information. In addition, numerous Pakistani high-ranking officials claimed that their iPhones had been hacked for surveillance purposes.

The aggressive actions of non-state actors and separatist movements on the internet are another problem for Pakistan. These groups use social media sites such as Twitter, YouTube, and Facebook to disseminate hatred, misunderstanding, and anti-Pakistan propaganda. Pornographic content and morally reprehensible data are also openly distributed on the internet in an attempt to appeal to Pakistan's young. Due to a lack of knowledge and poor laws, online gambling, drug trafficking, web spoofing, digital piracy, and cyber stalking are all common in Pakistan.

4.1 Reasons of Pakistan's Failure in Order to Preserve Cyber Security

Cyber dangers have become an unavoidable reality as linked digital technologies have grown and proliferated. Massive data fraud and theft were named the fourth most likely global danger in the World Economic Global Risk Report 2019, with cyber-attacks coming in fifth. Cyber-attacks on key facilities were identified as the sixth greatest risk in the same study issued in 2020. This highlights the rising potential of the cyber domain, where governments, political parties, non-state actors, and businesses may use it for espionage, conflict, and terrorism.

There is an ever-increasing threat of cyber-based assaults on critical infrastructure systems, according to numerous governmental and privately verified reports. Critical infrastructure systems, being the lifeblood of contemporary society, are critical for both national and economic security, since their dependable and secure functioning is essential for a state's seamless operation. All modern governments adopted emergency measures to strengthen their cybersecurity after recognising it as a global and national security threat.

The cyber-attack on K-Electric, Pakistan's largest power distribution utility, in late 2020 reignited the long-running discussion about enacting proper cybersecurity legislation and governance structure, but to no result.

In Pakistan, cyberspace legislation and governance are still mostly undeveloped. The ransomware assault by Net walker placed the data of 2.5 million K-Electric customers at danger, with names, addresses, CNIC, and NTN numbers published on the dark web when the business failed to pay the $7 million ransom. Although K-Electric officials claim that the attack was not harmful and that their data is safe, the consequences of any future attack could be even more disastrous because Pakistan lacks an effective redressal mechanism for cyber infiltrations and data protection laws that strengthen digital privacy.

The cyber-attack on K-Electric, as well as a slew of other instances, highlight Pakistan's vulnerability to cyber-threats. In terms of cyber readiness, Pakistan was rated 94th out of 193 nations in the Global Security Index 2018.

Since then, the situation has become worse, owing to a lack of commitment in the areas of legal, technological, organisational, and capacity building, as well as a lack of interagency/sector collaboration in the cybersecurity domain.[138]

4.1.1 Pakistan's Cyber Laws Lack

To control and regulate cyberspace in Pakistan, the government has established a number of computer and internet-related legislation. The "National IT Policy and Action Plan of 2000," "Electronic Transaction Ordinance 2002," "Electronic Crime Ordinance 2004," "Pakistan Electronic Crime Ordinance 2007," "Prevention of Electronic Crimes Act (PECA) 2016," "Data Protection Bill 2018," and "Citizen Protection (Against Online Harm) Rules 2020" are among the most important. Despite the fact that all of these laws were intended to address internet and computer-related crimes to some extent, none of them fully recognises the increasing complexity of cyber-attacks.

While enacting effective national legislation to punish cybercrime is a positive start, Pakistan's cybercrime laws are only one component of a robust and safe cybersecurity system. Unfortunately, Pakistan falls short of meeting some of the most important requirements for a robust cybersecurity system. A national cybersecurity plan, according to the International Telecommunication Union (ITU), is a critical first step in tackling cyber-security problems. In Pakistan, there is no security agency that establishes a national cybersecurity strategy and framework other from the "Prevention of Electronic Crimes Act 2016." There is also a lack of consistency in criminal law proceedings and the administration of justice.

Furthermore, there is a lack of intelligence exchange and collaboration frameworks across national entities, hampereding national cybersecurity efforts. Pakistan also lacks a proactive national Computer Emergency Response Team (CERT) to detect and respond to cyber-threats and assaults in real time. Another important component of a strong cyber-security framework is capacity-building in the domain of cybersecurity, and efforts in this area are still in their infancy.[139]

4.1.2 Lack of Collaboration

As a result of the foregoing, Pakistan appears to be very vulnerable to cyber-attacks and

[138] Amna Tauhidi and Aneeqa Safdar, "Is Pakistan's Cyber Security Strong Enough to Protect the Country?," *Center for Aerospace and Security Studies*, 2021, https://casstt.com/post/is-pakistan-s-cyber-security-strong-enough-to-protect-the-country/358/j.ctvrnfqsx.8.

[139] Ibid

lacks an adequate reaction mechanism. Given the growing risks to national security, which have intensified during the COVID-19 epidemic, Pakistan must address its policy inadequacies in terms of cybersecurity and readiness. Any delay in implementing cyber-security infrastructure might be expensive. It is critical to neutralise any potential cyber intrusion, and Pakistan's cyber security legislation must be updated to deal with th To guarantee coordination between government, military, and intelligence partners, a "National Cyber Security Agency" should be established. A committee should be established to analyse the cyber risk of vital infrastructure and set protective levels. Most significantly, present digital legislation, notably PECA, has to be overhauled from a broader perspective to address online issues. Any apathy, procrastination, or delay in developing a comprehensive and active cyber defence will be to Pakistan's detriment.e evolving cyber threat environment.

Pakistan is used to dealing with security threats from both within and outside its borders. The problem of security remained at the forefront of its foreign policy due to regional instability and risk on both the eastern and western frontiers. However, it is said that Pakistan is still unfamiliar with current counter-soft-threat techniques.

4.1.3 Lack of Addressing Unconventional Security Threats

Afghanistan's civil conflict and insecure administration will have a knock-on impact in Pakistan. Pakistan must properly equip its institutions and population to battle the effects of climate change, particularly along its borders and in areas prone to extreme weather. To guarantee a robust defence against cyber-attacks, cyber security for financial institutions and defence installations will become increasingly important. War is a national endeavour, and that was best demonstrated in 1965, when all elements of society came together to confront the enemy. "We are living in the era of hybrid warfare, which are fought on several fronts at the same time, including cyberspace, propaganda, and fake news."

With aggressive and coordinated methods, we must address all of these issues. The National Counter Terrorism Authority (NACTA) idea has failed, and Pakistan must regain public trust through clear and coordinated tactics. Around our borders, many risks are arising that must be addressed together. Parliament, the public, and the media all have a role to play in achieving national strategic goals. Pakistan's defence would be strengthened at all levels if it has a robust intelligence system and a strong economy.

Following the emergence of the Covid-19 epidemic throughout the world, including in Pakistan, which has pushed ordinary people as well as government officials to use internet resources more frequently, cybersecurity and data protection have become even more critical.

4.1.4 Lack of Public Care

Pakistan appears to be considerably more permissive in terms of data privacy; the sentiment is not as strong as it is in the West. There were several reasons for this, one of which was the continued use of tangible papers or identities as the key resource for any official action. People believed that their personal information was of little value to others; nevertheless, a rapid-paced information or Internet of Things (IoT) revolution was underway, and failing to grasp privacy would entail allowing others to control what they could do and view online.

4.1.5 Cyber Exploitation

The sensitive data has stolen from the digitally stored data like criminal records, telephone numbers, intellectual property, blue print, and other sensitive information such as classified information, contract information, and forbidden information then provided it to irrelevant person or party is exploitation of cyber.[140]

The exploitation has made by intelligent or good profile people covertly or surreptitiously. The exploitation key feature is its surreptitious nature. It is useful before discovery because after discovery of exploitation, the person prevent the use of cards, code, and numbers with the help of concerned authorities. The hacking and Cyber Attack can be implemented through iPhones and apples. There are a number of users of apple and iPhone; therefore, most of the people have been using iPhone in an organization or company. So, it is difficult and complex in the contemporary age to counter Cyber Attack.

The major cyber exploitation has been discovered since 2013. The information of 70 to 10 million people have stolen and leaked.[141] It contains email addresses, credit card

[140] Logsign Team, "What Are Real Time Security Threats?," *Logsign: Next-Gen SIEM, SOAR and Value Added Services*, January 10, 2021, https://www.logsign.com/blog/what-are-real-time-security-threats/.

[141] Juliana D. Groot, "The History of Data Breaches," *Digital Guardian*, December 1, 2020, https://digitalguardian.com/blog/history-data-breaches.

numbers, and names and has sold on black market websites. It is also used for blackmailing victims.[142] The term Cyber has been used for understanding the movement and control of animals and machines since 1950s; however, it has been used for computerization. After 1990s the terminology has become cyber space and the connotation about the term has totally changed. Now, it is defined as the computer devices and electronic activities performed through the computer devices to control the devices and data. Pakistan has ranked 79th in the International Telecommunication Union's Global Cyber Security Index. The country's existing cyber law, the 'Prevention of Electronic Crime Act' (PECA), is ineffective.[143]

4.2 Poor Track Record

Pakistan has ranked 79th in the International Telecommunication Union's Global Cyber Security Index. The country's existing cyber law, the 'Prevention of Electronic Crime Act' (PECA), is ineffective. To name a few instances, the federal government has failed to establish a digital forensics laboratory that will give expert opinion to the court independent of the investigating agency, as required by Section 40 of the PECA.[144] Similarly, under Section 49 of the PECA, the federal government was obligated to appoint national and sectoral CERTs for critical infrastructure protection. The most difficult aspect of the policy is its execution. A national cyber security policy is followed by a strategy document that includes an action plan for achieving the policy's objectives. Prioritization of action items, deadlines, and roles and duties of organizations responsible for achieving the policy's objectives would all be included in the strategy document. The government must establish an institutional structure comprised of dual civil-military agencies: That would be raised specifically for the purpose of executing the aforementioned policy objectives and sustaining national cyber defenses in the government, commercial, and military sectors.[145]

[142] Ibid.

[143] Vikki Davies, "New cybersecurity policy for Pakistan," *Cyber*, August 8, 2021, https://cybermagazine.com/cyber-security/new-cybersecurity-policy-pakistan.

[144] Emma Woollacott, "Pakistan government approves new cybersecurity policy, cybercrime agency," *The Daily Swig (Cyber News and Views)*, August 5, 2021, https://portswigger.net/daily-swig/pakistan-government-approves-new-cybersecurity-policy-cybercrime-agency.

[145] Ibid.

Millions of cyber-attacks on infrastructure and services have occurred in recent years. Many times, hackers utilised ransomware to extort money from their victims. As a result, it is critical that we develop the power of not just fighting against such assaults, but also of launching counter-cyberattacks. This is easier said than done since, in most situations, determining the attacker's identity is difficult. Because of the nature of the internet, it is easy to hide behind its open infrastructure. This is especially true when cyber-attacks are supported by a state. Hackers also benefit from anonymity due to the asymmetry of assaults.

Cyber Attack has been launched to destroy the data, steal the data, copy the data and misuse the data from the computers against any legal body. Cyber space is the phenomena used to explain the aim behind this process; furthermore tells us about new kind of weaponry introduced by the Cyber Attack, commonly called digital weaponry. The attacker's purpose is to harm human lives. They have Nuisances, serious attitude, and annoying nature.[146] Cyber dangers have become an unavoidable reality as linked digital technologies have grown and proliferated. According to the World Economic Global Danger Report 2019, enormous data fraud and theft are the fourth most likely global risk, with cyber-attacks ranking fifth.[147]

Cyber-attacks on vital infrastructure were ranked as the sixth greatest risk in the same study issued in 2020. This demonstrates the rising potential of the cyber sphere, in which governments, political organisations, non-state entities, and businesses may conduct espionage, warfare, and terrorism.[148]

Rapid digitalization and the widespread adoption of Information and Communication Technologies (ICTs) have exposed nations to new and developing cybersecurity risks. Data and network security has become a must-have for governments. While many responsible nations have created comprehensive policies and procedures to combat imminent cyber threats, Pakistan has struggled to build a coordinated national

[146] Hugh Taylor, "What Are Cyber Threats and What to Do About Them," *The Missing Report*, June 16, 2021, https://preyproject.com/blog/en/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them/.

[147] Amna Tauhidi, "Is Pakistan's cyber security strong enough to protect the country?," *Global Village Space*, May 1, 2021, https://www.globalvillagespace.com/is-pakistans-cyber-security-strong-enough-to-protect-the-country/.

[148] Business Recorder, "All set to implement 'Cyber Security Policy' by next year," *Business Recorder*, September 17, 2021, https://www.brecorder.com/news/40120703.

cybersecurity policy or plan. Although cybersecurity and governance guidelines for certain sectors (such as banking and defence) were in existence, a comprehensive national-level strategy to cybersecurity was lacking.

4.3 Adversary in Cyberspace

The purpose of adversary to exploit information is advisory in cyber space. This is completely an offensive action. Unfriendly and strict actions have been being taken place by the advisory against information technology and networks. Such as computers, mobile phones, and Tabs, etc.

The scope of cyber security has been increasing rapidly because of unpredictable nature of cyber threat. This is a contemporary and 21st century challenge faced by industries, individuals and governments. Everyone has a threat of fraud, scamming, and hacking.

4.4 Pakistan Lack a Security Framework

The forecast is made in the Critical Infrastructure Readiness Report become valid. States has picked up the ability to obliterate framework through innovation. The legend has become a reality. Presently, there is a rundown of nations whose foundation has been devastated with the assistance of digital assaults. The assaults are; Tanks had shipped off Georgia by Russia in 2008. It was a Cyber Attack for the calculation of the framework. This was considered the main Cyber Attack.

In 2008, the US and Israel had built up the capacity and disabled Iran's enhancement program of atomic.[149] In 2014, programmers had breached the German steelworks and the heater had not worked appropriately and not shut downed. Another Cyber Attack had been seen in 2015, it was an assault in Ukraine, and 230,000 individuals lost matchless quality and force. Aggressors held onto the framework and the framework was constrained by the far off. The assault was dispatched from Russia. The occurrences close, the war techniques, strategies, and strategies are changed at this point. The weapons, for example, Guns, bombs, activity are no longer supports prevention and

[149] Julia Masterson, "Timeline of Nuclear Diplomacy With Iran," *Arms Control Association | The Authoritative Source on Arms Control Since 1971*, July 2021, https://www.armscontrol.org/factsheets/Timeline-of-Nuclear-Diplomacy-With-Iran.

dread. The console is the new weapon to control, obliterate, decimate, and rout adversary.[150]

With our change into the data and the innovation age, the entryway to the arrangement of digital dangers to our public security has been opened. The development improvement of the innovation and more reliance on the PCs will cause changes in the philosophy of public security ideas for our country as well as for all the countries. The countries have this dread and danger that their data information base might be hacked, changed, or debilitated by some other assaulting or hostile development innovation. We should be completely mindful and have a full exploration of all the dangers that may happen by new and advanced innovation and its results on the public security in digital space. This paper would give an occasion to investigate digital fighting measurement bases after arising innovations and electronic methods.

It has changed the lifestyles and encouraged human existence in numerous perspectives. Each record and undertaking was changed over from papers to the virtual space called the internet. With the progression of time, we become the need of people, organizations, governments, militaries, worldwide companies, and public and global associations. Everything including records and grouped information of governments and associations were changed over to the computerized data and was shared to the internet for additional capacity, change, and correspondence. As of now, there would be not really any organization to run its issue with our utilizing the web. This is the time of digitalization and everybody is subject to the web. The internet has made effectiveness in working together, running the state issues, and battling the wars essentially. Where it has encouraged all the lifestyles it has additionally made a lot of weakness which has been a grave worry for the world. On one side it is encouraging us and then again, it is making weaknesses that are more extreme in nature.[151] The world has gotten more worried about these weaknesses and dangers. Cyberspace is presenting numerous dangers and weaknesses and nearly everybody inclined to these dangers which are being presented by the internet albeit each nation has been constrained to take radical measures to alleviate

[150] OSAC, *Pakistan 2020 Crime & Safety Report: Islamabad*, (Islamabad: OSAC, 2020), https://www.osac.gov/Content/Report/f36dd7e9-8cf3-489c-b9b4-187819994ff8.

[151] Ibid,

these dangers and weaknesses. In this section, we will examine the weaknesses and dangers of being forced by the internet.

There are three primary sort of Cyber Security.[152] The reconnaissance has been accomplished for the monetary profit or disturbance. There are a plenty of alternatives and strategies of assault for malevolent entertainers. There are numerous sorts of Cyber dangers, for example, Malware ,Phishing(email-borne assault ,the information has hacked by tapping on connection), malware on versatile applications, man in the center assault (the data has commandeered by the programmer between the sender and collector), stick phishing, Trojans (malevolent code inside the framework), Denial of Service assault or Distributed Denial of Service Attack DDoS, Ransom product ,Data Breaches (information penetrated by a vindictive entertainer), and assaults on IOT gadgets .

Pakistan is vulnerable to a wide range of cyber attacks including computer viruses, identity theft, financial data theft, cyber crime, critical infrastructure monitoring, and intelligence on critical infrastructure. Unless these challenges are successfully met, Pakistan cannot guarantee robust national security.Technology, however, has also, in recent decades, been a major national security concern to the Member States. Current threats have been revolutionized by the state dependence on cyberspace and digital networks. Cyber warfare was finally realized by the generalized digital revolution of states and populations. All the countries which are aware of this danger use their ability to projected power in this region. The main opponent of Pakistan, India, is also among those nations who strive to a widespread culture of cyber weapons and militarize cyber space.

The technological development has posed new threats and challenges to states' stability, because the cyberspace between government agencies, telecommunications providers, militant facilities and bank infrastructure is continuously being breached by hostile states and even non-state actors. Developing countries such as Pakistan also face serious cyber-related problems that should be dealt with immediately. The infringement of public information, the hijacking of government websites, the penetration of government officials in WhatsApp personal reports, the evasion of financial institution

[152] Bill Rosenthal, *The Three Elements of Cyber Security*, (Logical Operations, 2016), https://logicaloperations.com/insights/blog/446/the-three-elements-of-cyber-security/.

cybersecurity, the effective use by terrorist organizations of ICT and a well-organized international malicious cyber campaign against Pakistan by hostile countries, such as India are serious warnings against politicians. In order to strengthen cooperation between civil and defence agencies, the State also has to establish a 'National cyber coordination centre.' Thus, improved coordination among law enforcement agencies will enhance Pakistan's cyber security environment and contribute to the strict implementation of cyber security policies.

4.5 Threats to National Cyber Security Policy

While National Cybersecurity Policy had been a long-standing strategic necessity, it was the Pegasus affair that accelerated its implementation. A consortium of media organisations conducted a collaborative investigation that revealed how a hacking software – Pegasus – licenced by an Israeli firm NSO to its client governments for tracking terrorists and criminals was used to target world leaders, human rights activists, and journalists, among others. Hundreds of Pakistani phone numbers were on the list, including one used by Prime Minister Imran Khan once. Surprisingly, and most concerningly, India—archrival—was Pakistan's one of NSO's most devoted customers.

The aim of the 2021 policy is to 'build a safe, strong, and constantly developing national digital ecosystem while assuring responsible confidentiality, integrity, and availability of digital assets.' Its major guiding concepts include citizen data privacy and security, giving the necessary support and system to concerned public and commercial entities, establishing a national response structure, and, last but not least, implementing best practises to preserve national digital sovereignty.

The policy intends to'strengthen national cybersecurity capabilities via the creation of necessary and well-coordinated procedures, implementation of security standards and regulations within a policy and legislative framework' in order to enhance the national cybersecurity perspective.

Pakistan fared badly in global ICT rankings as a result of its scant attention to cybersecurity (ICT Development Index value of 2.42). As a result, one of the policy's primary aims is to enhance Pakistan's ICT ranking. Pakistan is also ranked 14th out of 18 Asian countries on the Global Cybersecurity Index (GCI) 2020. The total GCI score for the country is 64.88. The policy will also boost Pakistan's GCI ranking.

Another important aspect of the policy is the indigenization and development of cybersecurity solutions through R&D initiatives. This, too, was a critical issue that required attention. Adequate local resources, both in terms of personnel through Centers of Excellence and HRD programmes, and technology, would alleviate our over-reliance on external sources, which exacerbates the country's cyber vulnerabilities. However, officials did not define how much money or resources would be set aside for this critical purpose.

Nonetheless, far more emphasis has been placed on information security rather than cybersecurity. This is largely due to the fact that the incorrect stakeholder is in charge of this policy. Because cybersecurity is considerably wider than information security, it should be assigned to the National Security Division (NSD) for a more substantial perspective and breadth. According to the Information Minister, the National Cyber Security Policy is divided into two parts: cyber security and cyber crimes. The development of a framework to counter offensive cyber activities was a long-overdue move. Existing information and data security law (often referred to as cyber legislation) failed to address the rising need to protect and deter cyber assault.[153]

While the present policy does not provide a response system with well defined roles and duties, it does say unequivocally that the state of Pakistan will respond to any aggression. As a result, a cyber-attack against Pakistan's Critical Infrastructure or Critical Information Infrastructure will be considered an act of aggression against national sovereignty, and the state will respond appropriately. The decision to form a national reaction team is also critical in this regard.

[153] Amna Tauhidi and Aneeqa Safdar, "Is Pakistan’s Cyber Security Strong Enough to Protect the Country?," *Center for Aerospace and Security Studies*, 2021, https://casstt.com/post/is-pakistan-s-cyber-security-strong-enough-to-protect-the-country/358/j.ctvrnfqsx.8.

In terms of context and substance, the policy is an essential and much-needed document that addresses both offensive and defensive requirements. Priorities and necessary activities are clearly stated, but there is no action plan in place to attain those objectives and deliverables. Nonetheless, the policy includes the decision to form a Cyber Governance Policy Committee (CGPC) for implementation and supervision. The Committee will be entrusted with developing a specific strategy and action plan. Given Pakistan's dismal track record of policy enforcement and selective policy implementation, all eyes are on the CGPC to fulfill its mission and fulfill the obligation of safeguarding Pakistan's national cyberspace. The policy is being implemented to the point where a national level umbrella committee would offer the governance structure for the entire country.

Critical infrastructure systems, as the contemporary world's lifeblood, are critical for both national and economic security, since their dependable and secure functioning is critical for a state's seamless operation. Recognizing it as a global and national security threat, all contemporary governments implemented emergency steps to strengthen their cybersecurity.

The government has passed many computer and internet-related legislation to manage and regulate cyberspace in Pakistan. The key ones are the "National IT Policy and Action Plan of 2000," the "Electronic Transaction Ordinance 2002," the "Electronic Crime Ordinance 2004," the "Pakistan Electronic Crime Ordinance 2007," the "Prevention of Electronic Crimes Act (PECA) 2016," the "Data Protection Bill 2018," and the "Citizen Protection (Against Online Harm) Rules 2020."

Despite the fact that all of these laws were designed to target internet and computer-related crimes to some extent, none of them effectively addresses the rising complexity of cyber-attacks. While punishing cybercrime through effective national legislation is a positive start, Pakistan's cybercrime laws are only one factor of a robust and safe cybersecurity system.

Unfortunately, Pakistan falls short of meeting some of the most important requirements for a robust cybersecurity system. A national cybersecurity plan, according to the International Telecommunication Union (ITU), is an essential first step in tackling cyber-security problems. Aside from the "Prevention of Electronic Crimes Act 2016," there is no security agency in Pakistan that establishes a national cybersecurity strategy and framework. In addition, there is a lack of coherence in criminal law procedures and regulations for dealing with cybersecurity issues.

Furthermore, there is a lack of intelligence sharing and collaboration frameworks across national agencies, which stymies national cybersecurity initiatives. Pakistan also lacks a proactive national Computer Emergency Response Team (CERT) to detect and respond to cyber-threats/attacks in real time. Capacity-building in the domain of cybersecurity is another critical component for a strong cyber-security framework, and initiatives in this area are still in their early stages. To guarantee coordination among government, military, and intelligence partners, a "National Cyber Security Agency" should be established. A committee should be established to undertake a cyber risk assessment of vital infrastructures and to set protective levels. Most significantly, there is an urgent need to rethink present digital laws, notably PECA, through a larger lens of dealing with online issues. Any apathy, procrastination, or delay in building a comprehensive and active cyber defence will be at Pakistan's cost.

According to the policy, any cyberattack on a Pakistani institution will be deemed an act of aggression against national sovereignty, and all necessary and punitive measures will be implemented. The committee will execute the policy at the national level, develop a plan, and take action in a timely way. The secretaries and senior officials of 13 different departments/organizations make up the committee. Previously, many organisations dealt with cyber security concerns in silos. The National Cyber Security Policy is designed to combat events involving hostile use of information and communication technology in cyberspace, which represent a serious financial and security danger to Pakistan. The policy includes support for the creation of an internal framework for the protection of the cyber ecosystem, the security of national information systems and infrastructure, and the protection of all national ICT infrastructures in all public and commercial organisations.

Conclusion

However, as digital services became more connected, mobile, and versatile, they became more vulnerable to cyber security attacks. As a result, increasing cyber dangers and vulnerabilities in the digital world necessitate a comprehensive and coordinated framework to ensure people and companies have a secure cyberspace. A cyberattack on Pakistan will be classified as category I or category II aggression against national sovereignty, according to the policy, and the country will defend itself with necessary countermeasures. To counter these threats, the IT ministry will assist in the establishment of active cyber defence and cyber security governance, the protection of internet-based services, the protection and resilience of national critical information structures, the protection of the government's information systems and infrastructure, the development of an information security assurance framework, increased cyber security awareness, and the development of cybercrime response mechanisms and regulations, according to the policy.

Chapter V

Pakistan's Effort to Counter Cyber Terrorism

Pakistan is vulnerable to a wide range of cyber attacks including computer viruses, identity theft, financial data theft, cyber crime, critical infrastructure monitoring, and intelligence on critical infrastructure. Unless these challenges are successfully met, Pakistan cannot guarantee robust national security. The technological revolution brought new challenges to security. Hence the pros and cons of cyber warfare are increasing every day. In the domain of Cyberspace, Pakistan has secured improved indicators of the fastest growing digital economics of the world. Pakistan's indication towards digital technology, internet and cell phone have got significant growing trend. In this age of globalization, it has become fundamentally necessary for every nation to work on cyberspace. This interconnectivity between the states has also given birth to various crisis, crimes and conflicts with respect to nature occurrence and power. Pakistan is no exception to this inevitable phenomenon.[154] It is exposed to multidimensional Cyber threats like computer malware, Identity theft, Economic data theft, Cyber frauds threat to personal privacy and the most importantly espionage attempts on critical infrastructures. However, the concerned departments in Pakistan are ineffective to formulate and execute a comprehensive national cyber security framework to counter these threats. The nature and security of these above mentioned cyber threats to the national security of Pakistan must be infringed with effective policies in order to attain the cyber security. In the modern era, war has been revolutionized due to rapid advancements in technology. As a result, cyber security along with its pros and cons is contributing increasingly to modern warfare. Pakistan, however, is still in the developmental phase of cyber security. Although Pakistan has passed its first law related to cyber-crimes, in the form of the 2016 Prevention of Electronic Crime Act, the overall legislation related to cyber security is still vague and not as strong to deal with the dynamic and broad-

[154] Jawad H. Awan et al., "Security of eGovernment services and challenges in Pakistan," *2016 SAI Computing Conference (SAI),* 2016, doi:10.1109/sai.2016.7556112.

ranging nature of threats that emanate from the realms of cyber security.

Pakistan has been ranked at ninth position in maintaining digital economy by UN. In Pakistan with the increase access to the 4G technologies' the internet penetration rate has increased up to more than 30 percentage, it was earlier when there were no 3G and 4G technology that stood at 6.3 percentage in 2005. In Pakistan 40 percentage of its population is internet user. According to Pakistan Telecommunication Authority (PTA), the cellular internet penetration rate 30.32 percent with 60 million subscribers. The teledensity in Pakistan is 70.90 percent with 148 million cellular subscribers. Pakistan is currently ranked 10th globally with respect to increased mobile subscriptions. By 2025, it is expected to reach fifty percent in Pakistan and 60 percent of the global subscriber market. In 2017 Pakistan was ranked at 67th among 193 countries in the global cyber security Index (GCI), Pakistan is lagging behind in the areas of technical and organizational measure through which she can confront her cyberspace threat.[155] Some are the steps through which Pakistan can confront the challenges emerging in cyberspace.

In last one decade or two not more than that, In the relevance with cyberspace electronic media has been a key power brakes and has played a role in the social construction of cyber security threats in Pakistan the media most highlight the importance of psychological, economic, social, cultural, and political settings in which cyber securitizations are introduced and media is the platform through which the audience can react towards these securitizations. Audiences can be affected significantly through media. Moreover, "effect of media" makes it a crucial functional actor with the ability either to play down or amplify the cyber securitization moves.

The cyber security phase of Pakistan is still under development. Pakistan passed its first law "prevention of Electronic Crime Act 2016 to fight against cyber warfare. Only one law is not enough as the problems are emerging in various dynamics from the realms of cyber security. Pakistan has started an initiative by PAK-CRT, Presidential initiative for Artificial intelligence and Computing (PIAIC) and National Vocational & Technical training to build capacity.[156] Big powers like Russia, China, and the U.S.A are not capable of handling the evolved spectrum of cyber threats. States are totally dependent on

[155] Ibid.

[156] Jawad H. Awan et al., "Security of eGovernment services and challenges in Pakistan," *2016 SAI Computing Conference (SAI)*, 2016, doi:10.1109/sai.2016.7556112.

the technology which has enhanced the security concerns. In the case of Pakistan, the challenges are more because the country depends on others for technology. Symantec is a leading global Cyber security firms are they revealed that Pakistan is among the top 10 targeted countries. After all these challenges and threats Pakistan has not developed cyber command centers and cyber policy plans for security. The establishment of cyber-security and evaluation lab has not completed yet. To restrict the threats of cyberspace there is immense space to develop more powerful tools and techniques. The purpose of the newly established National center for cyber security is to increase the number of security professionals in the government sector. To support civilian and military infrastructure it is necessary that Pakistan must develop its own cyber security policy. After all these initiatives Pakistan will not be able to wage a strong offensive policy in near future. Pakistan is still a long way away to lay a strong cyber security foundation.[157]

5.1 Securitization on the Behalf of Nation

Mostly, in the process of securitization one is more privileged than others. If a state has well-defined rules and laws then such problems less likely to happen. Moreover, the problem of legitimacy will not occur. However, in the case of Pakistan, due to a lack of rules in the process of security issue still exist. The involvement of the nation will make rules more flexible than the state. The rules on the behalf of the nation are usually on the values and logic of identity. For instance, securitization is done on the behalf of the nation when it comes to terrorism. The state played a positive role by demolishing the confusion between the US war of terror and Pakistan war on terror. The government of Pakistan along with the establishment won the trust of the nation by clarifying the image of the real enemy. As a result, it became easier for the government to eradicate violent actors from society. Moreover, the NACTA was handed over the command of internal security, and the temporary courts were established for military special anti-terrorist courts. Rapid response forces by federal and provincial governments were also established and carried out military operations all across Pakistan. Hence the process of securitization will be more effective if carried out by involving the nation rather than just the government.

[157] Ibid.

5.2 Synthesis before Segregation

The scope of securitization is the broad and "complex whole" in Pakistan. The challenge is to tackle a number of variables at the same time. There are many actors like military societal, economic, environmental, al, and political to identify the dimensions of cyber security. The challenges are complex due to the non-distinguish quality of existence.

In the field of security securitization theory proposed and analytical and evaluative method that consist of segregating the "complex whole" into different departments and sectors For example military, societal, economic, environmental and political in order to identify particular patterns of interaction since all these sectors lack the "distinctive quality of independent existence". This segregation is done to achieve its core objective and that is to reduce the number of involved variables. In Pakistan, the problem is the vast scope of the cyber securitization where securitizing agent and actor are striving hard to deal with the great number of variables at the same time. Therefore, there must be a securitization wing to deal with cyber threats in all sectors ranging from basic cyber threats of malware attack and identity theft to much complex cyber threats to national critical infrastructure. [158]

These must be more complex instead of simple, manageable and clear. The securitizing authorities must synthesize the sectors in cyberspace before even segregating them. The authorities must understand and the must clearly identify the specific patterns of relationships, subjects and objects that shape the entire threat-survival matrix which is operating in the cyber space of Pakistan. The purpose of segregation is to reduce the number of variables by involving all the actors. Now the objective is to introduce a single security program to handle all the threats of cyber security. But in Pakistan authorities are synthesizing the sectors in cyberspace without even segregating them. They are unable to identify separate patterns, shaping subject and object of the entire threat Survival matrix which is operating cyberspace in Pakistan.

[158] Sadia Rasool, "Cybersecurity threat in Pakistan: causes Challenges and way forward," *INTERNATIONAL SCIENTIFIC ONLINE JOURNAL*, no. 12 (August 2015), http://sociobrains.com/website/w1465/file/repository/21_34_Sadia_Rasool_Cyber_security_threat_in_Pakistan_causes_challenges_and_way_forward.pdf.

5.3 Role of General Public

The process of securing a country from cyber warfare is an inter-subjective agreement. That is the reason for the role of the general public. One of the biggest challenges is the absence of narration and link between the general public and authorities of national cyber security. The concerned authorities only present cyber warfare as a threat to general public of the country. This cannot be termed valid measure protection and will never result in securitization. All the responsible actors and concerned authorities of cyber security need to argue the case for the resolute acceptance. There is a lack of balance between the speech act of government and the process of inter-subjective. Due to the inability of construction of balance the general public is overly simple regards cyber security. As the government claims that cyber security is an inter-subjective agreement but on the other hand, it has become an act of speech. The necessity of balance should be promoted by the political and security institution of Pakistan. The main issue is that all the cyber problems are being dealt with by utilizing traditional ways and techniques. All modern problems require modern strategies to attain balance.[159] All traditional techniques are highly formal and based on conventional rules and procedures. This negates all the components of the process of inter-subjective. This initiates a crisis of legitimacy for the regulation of a national plan to stop cyber warfare.

5.4 Media Framing

Media play a substantial role to socially construct the security threats of Pakistan Electronic and social media play a key role in society. The media is capable of introducing the psychological, social, financial, and cultural securitization against cyber warfare. Moreover, media is solid ground to deliver measures of securitization for the awareness of the general public.

This is the main point where lies the problem or challenge. Media should compel the audience to focus on human rights violations and excessive investigative powers instead of highlighting the growing execrated cyber threats. The audience has limited information because this cyberspace is new realm of security. Therefore, in Pakistan the securitizing actor or government of Pakistan must use media framing to create a desired and suitable context by activating the positive aspects of cyber security initiatives. Media must work

[159] Ibid.

indiscriminately and this platform must be used to achieve the support of the political opposition's neutral actions and human rights watch dogs and other related institutions.

Media is an essential part of life when it comes to the effects of media. The security dynamics of Pakistan keep changing according to the international environment. The "effects of media" is a crucial function as it may degrade or upgrade the implementation process of cyber security. This is a huge challenge for the concerned authorities. Index portrays a negative image more than the positive image for protective measures. The media highlights human rights violations and excessive investigation rather than issues related to cyber security. The knowledge about cyber security has limited the country as it is a new phenomenon. Now it is the responsibility of media and other involved actors to use media for activating positive aspects and threats of cyberspace. Media is an ideal platform and must be utilized for achieving political support and spreading information about protective measures.[160]

5.5 Establishing Relevant Institutions

The dynamics of security have some boundaries and limitations. The phenomenon of security is based on this and only the state decides what should be protected. But newly emerging security challenges always come up with controversies with respect to the state of emergency. Hence the construction of relevant institutions for such issues is crucial. Generally, the entire cyberspace has been securitized in the country. All the issues related to cyberspace automatically considered as a part of terrorism. Consequently, this is resulting in the emergence of several types of securitization. To deal with all the cyber threats government of Pakistan established The National Response Center for Cyber Crimes (NRC3). This was established as a result of the Electronic crimes ordinance in 2007 and 2008 for the purpose of providing security against such crimes. But later it was turned into a special branch under the assistance of the Federal Investigation Agency (FIA).

Security paradigms and culture of security of state has its own specific dynamics and boundaries which decide what can be prioritized on utmost basis if we talk of security. FIA in Pakistan is chiefly responsible for the dealings in cyberspace. FIA has also an

[160] Rehman Malik, "Cyber security challenges and solutions for banks, national institutions — II ," *The International News*, December 16, 2018, https://www.thenews.com.pk/print/406447-cyber-security-challenges-and-solutions-for-banks-national-institutions-ii.

active branch to deal with cybercrimes and that is cybercrime wing. Now holistically the new problem are discovered with the passage of time and with this all the nation's feel threatened because of this internet penetration and cyber interconnectivity. This also poses a threat and become controversial with respect to the state of emerging and this has instigated the nations to establish of new relevant institution. So, in addition to FIA, another institution is also under consideration and that institution is NACTA (National Counter Terrorism Agency). NACTA and FIA should work efficiently to unveil the serious threats by making and executing the effective policies.[161]

It should have been given the status of special institutions. Furthermore, all the extensive powers were given to the investigation officer in the PECA 2016. According to this investigation, the officer has the authority to officer and he/she can access, use, preserve, and seize all the data. This content might be required to carry out an investigation against cyber crimes. Furthermore, he also has the power to call any person that is involved in stealing or decoding information. But this is not enough to fulfill the requirements of the institution. Currently, officials are debating about the establishment of a cyber security agency for the implementation of laws. Moreover, the establishment of the National Counter-Terrorism Agency is also under consideration to make a security framework. The Inter-Ministerial committee of the PM office will finalize and design the rules to operate PECA 2016. There is a need to formulate a Cyber Emergency Response team and a special court for prosecuting cybercrimes. However, this is still pending and will be under construction soon. Now all the process of future security depends on these designated institutions and courts.[162] The security culture of Pakistan needs to be handled by the institutions to stop the reappearance of cyber threats.

5.5.1 Cyber Landscape of Pakistan:

Pakistan is gradually becoming aware of increasing importance of cyberspace developments and how these affect national security. Government of Pakistan is now increasingly encouraging E governance to use web based technologies to conduct the

[161] Center for Global & Strategic Studies and National Security Division, government of Pakistan, *Cyber Secure Pakistan Policy Framework*, (Islamabad: Center for Global & Strategic Studies (CGSS), 2018), https://cgss.com.pk/publication/Publications/pdf/Event-Report-Cyber-Security.pdf.

[162] Ibid.

business of the state.[163] However Cyber landscape of Pakistan remains very scattered and effort seems to be disjointed. Salient aspects of Pakistan's Cyber landscape are as under:-

a) Ministry of IT

In Pakistan awareness about Cyber aspects came in August 2000 when realizing wadding speed in IT, Pakistan's minister for science and technology, Dr Ataur Rahman, started Pakistan's first IT policy and action plan.[164] It was to assist the development of IT and computerization in Pakistan by putting foundation of IT universities intensifying the country's present IT institutes and modernizing the already present telecomm computerized infrastructure. Today Pakistan is connected with 4 undersea cables with rest of the world having 30,000 pk domains and approximately 40 million registered internet users, while MoIT is working on development of secure intranet to provide cyber connectivity to 42 government organizations with a central data center to work as nerve center of the central government.[165] A website www.pakistan.gov.pk has been created for all government ministries and organizations to promote and facilitate E governance along with issuance of a policy for internet usage. In private sector there are more than 200 software development firms which are registered with Pakistan software houses association for IT.[166]

b) Senate Standing Committee on Defense

Since Pakistan is located in the region where there is clear and higher alert of danger related to its national security through cyber warfare as revealed by Edward Snowden, it was felt that initiatives should be taken by the institutions to fight this war.[167] Senate standing committee on Defense took the initiative by introducing many actions including the seminars on cyber security task force and publishing the

[163] Cabinet Division, "E-MAIL & INTERNET POLICY FORTHE FEDERAL GOVERNMENT," Cabinet Division, accessed August 8, 2020, https://cabinet.gov.pk/SiteImage/Policy/internet-and-emails-policy.pdf.

[164] Fasih Ahmed, "UAVs'Potent Force Multiplier," *Hindustan Times*, March 18, 2006, xx, https://webcache.googleusercontent.com/search?q=cache:BFgjIVQVvyIJ:https://www.hindustantimes.com/india/uavs-potent-force-multiplier/story-WU4HnMcT4ItCyGI3a5IxUK.html+&cd=1&hl=en&ct=clnk&gl=pk.

[165] United Nations High Commissioner for Refugees, "Freedom on the Net 2016 - Pakistan," *Refworld*, November 14, 2016, https://www.refworld.org/docid/5834007d6.html.

[166] Ibid.

[167] MUSHAHID H. SYED, *[AS INTRODUCED IN THE SENATE] A BILL to provide for the establishment of a National Cyber Security Council*, (National Cyber Security Council, 2014), https://www.senate.gov.pk/uploads/documents/1397624997_197.pdf.

manuals for the media on cyber security and it introduced the National Cyber Security Council Bill, 2014. This committee has become the lead in creating Cyber warfare awareness in the country and even making suggestions to ministry of IT.

c) National Cyber Security Action Plan

Senate Committee on Defense and Defense Production headed by Senator Mushahid Hussain proposed a 7 point plan for cyber secure Pakistan in Jul 2013.[168] Mr Syed said "national security of Pakistan is vulnerable to the threats related with the cyber warfare which can affect Pakistan's defence, security, diplomacy, and nuclear programme, the economic and industrial sector". Salient's of proposed 7-point Action Plan are as under:

i. To introduce relative legislation so as to preserve, protect and promote Pakistan cyber security.

ii. Acceptance of Cyberwarfare as a potent threat equivalent to military threats, terrorism and aggression.

iii. Establishment of Pakistan Computer Emergency Response Team (PKCERT).

iv. Establishment of Cyber-Security Task Force in collaboration with MoD, MoIT, MoI, MoFA, Ministry of Information, security organizations and security professionals from the private sectors to formulate a Cyber Policy.

v. Armed Forces Inter-Services Cyber Command should be established to coordinate cyber security and cyber defence, under the office of the CJSC.

vi. Take initiative to start dialogue among member states of SAARC particularly India to establish acceptable standards in cyber security to prevent Cyber warfare among the SAARC countries.

vii. Educate leaders and promote awareness in the masses through media workshop on importance of cyber security.

d) National Cyber Security Council

Ecommerce and internet usage has grown rapidly in Pakistan but there are no cyber crime laws in place and some provisions of Pakistan Penal Code 1860 are used for

[168] Ibid.

investigating crimes relating to cyber activity.[169] The National Cyber Security Council Act, 2014 was presented in the parliament on 14 Apr 2014 for constitution of *National Cyber Security Council*to create appropriate conditions supporting the researches and analytical procedures, directing different sectors of the State educational departments to help the private sector to meet up the challenges of the cyber warfare, to help the individuals organization to take the responsibilities for protecting own cyber zone.[170] However State Minister for Information Technology Anusha Rehman termed the bill impracticable.[171] Proposed functions of the Council are as under:-

i. Promote research and initiatives in the field along with developing policy and rendering advice.

ii. Formulate National and international Cyber Security strategy and periodically review it after every three years.

iii. In accordance with section 6 of the bill take initiatives in the field of cyber.

iv. In line with emerging Cyber Security threats, draft policy guidelines and develop strategies Adviser to the Senate and the National Assembly, Judiciary and all Ministries, Departments and branches of Government on policy and legislation with respect to Cyber Security;

v. Facilitate legislation by providing advices reflecting international best practices in the field of Cyber Security.

vi. Advise and monitor implementation of security recommendations related to Cyber in government departments.

vii. Suggest policies for synchronization, homogeny and authorization for critical information infrastructure at government level.

viii. Act as coordinating body for implementation of policies, initiatives and legislation on Cyber Security at all levels.

ix. Act as a link between official and private sector entities, academic circles, and Cyber experts by holding frequent meetings.

[169] Tughral Yamin, *Cyberspace CBMs Between Pakistan and India* (New Mexico: Cooperative Monitoring Center Sandia National Laboratories, 2013).

[170] Ibid.

[171] Farooq Baloch, "Hackers and cybersecurity," *The Express Tribune*, January 12, 2015, https://tribune.com.pk/story/820463/hackers-and-cyber-security.

x. Institute an Advisory Groups to provide input for National Cyber Security Council which may be non binding and sought from time to time.

xi. Especially work as a team with national security mechanism to advise and assist in improving the cyber security of State.

xii. Maintain liaison and Coordination with international organizations and institutes in the field of Cyber security.

xiii. Initiate and guide R & D in accordance with international norms and obligations, in line with threat.

xiv. Create and promote awareness for responsibilities of individuals in the field of Cyber Security besides focusing on business houses and organizations.

xv. Buildup a long-term vision for Cyber Security to cater for next ten to twenty year.

xvi. Carryout necessary legislation for the functioning of the Council and other affiliated bodies, as required.

xvii. Incorporate all sectors and stakeholders to achieve the desired ends.

e) National Response Centre for Cyber Crime (NR3C)

National Response Centre for Cyber Crime (NR3C) is a unit of FIA dedicated to fight cyber crime, identify and curb the phenomenon of technological abuse in society.[172] National Response Centre for Cyber Crime (NR3C), is the latest introduction to mandate of the FIA, primarily to deal with technology based crimes in Pakistan. It is the only unit of its kind in the country and in addition to the directly received complaints also assists other law enforcement agencies in their own cases.NR3C has expertise in Digital Forensics, Technical Investigation, Information System Security Audits, Penetration Testing and Trainings. The unit since its inception has been involved in capacity building of the officers of Police, Intelligence, Judiciary, Prosecutors and other Govt. organizations. NR3C has also conducted a large number of seminars, workshops and training/awareness programs for the academia, print/electronic media and lawyers. Cyber Scouts is the latest initiative of NR3C, in which, selected students of different private/public schools are

[172] Farieha Aziz, "Pakistan’s Cybercrime Law: Boon or Bane? | Heinrich Böll Stiftung," *Heinrich-Böll-Stiftung*, February 14, 2018, https://www.boell.de/en/2018/02/07/pakistans-cybercrime-law-boon-or-bane.

trained to deal with computer emergencies and spreading awareness amongst their fellow students, teachers and parents.

f) National Telecommunications and Information Technology Security Board (NTISB)

Formerly it was known as National Communication Security Board (NCSB), and performs following functions:

i. Act as adviser for Federal Government on matters related to security of information and computer technology.
ii. IT regulates security systems induction related to information technology.
iii. Random checking of communication centers.
iv. Exercise control over communication security.

g) PECO (Prevention of Electronic Crime Ordinance 2009)

It was aimed at defining the crimes and punishment in cyber domain. It was required to be re-promulgated but expired in February 2010. At present there is no law pertaining to cyber crimes in the country. It addressed following issues:-

i. Access and damage to system or data with criminal intent.
ii. Fraud and forgery by cyber means.
iii. Misuse of cyber devices and encryption
iv. Use of various hacking and intercepting techniques for stalking and spreading malicious malwares.
v. Use of cyber for terrorism.
vi. Cyber war to cause effects in conventional war.

h) Prevention of Electronic Crimes Bill 2015[173]

A new bill has been sent to the National Assembly Standing Committee on IT and Telecom on 2 Apr 2015, which has been criticized by various experts as a draconian law as it curbs individual liberties and gives more power to government for regulating the use of IT. However it has not been passed as yet and envisages special courts to deal with cyber crimes as well an emergency unit to counter cyber attacks against Pakistan’s interests.

[173] PEMRA, "PEMRA grants non-commercial FM Radio licence to NUMS," *Digital Association Press of Pakistan*, December 9, 2020, https://www.app.com.pk/national/pemra-grants-non-commercial-fm-radio-licence-to-nums/.

- An overview of the cyber landscape suggests though a lot of initiatives have been taken in the field of cyber policies to safeguard national and individual security, but it is segmented effort in bits and pieces and needs to be galvanized by concerted effort of all elements of the government to produce unified response.

5.5.2 National Cyber Security

There is no globally agreed upon definition of 'national cyber securities.It is commonly employed by government spokespersons without ever being defined. However for the purpose of this paper it is defined as security of computer based equipment, systems and organizations against hostile actions of espionage, theft, destruction and disruption. Various threats to National Cyber security are as under:-

a. Indian Cyber Warfare Program

India has one of the fastest growing IT industries in the World. She is well poised to play a significant role in the 21st century due to the availability of top-notch talent in IT sector.There is a perception that, in future, IT is to India what the oil is to the Gulf. A combination of factors, some global and some of their own doings, have created an environment which is favourable for India for enhancing and practising various forms of Cyber Warfare. India is attempting to use Information Technology to enhance offensive Cyber war abilities from the standpoint of national security[174] which is a serious threat for Pakistan.

b. Intelligence and Espionage

The Internet has revolutionized intelligence and espionage activities. Spy agencies all over the globe are fully engaged in Cyber Warfare. US security agencies like National Security Agency (NSA) and other are spending huge amounts and time to find out ways and means to infect hostile or potential target systems with viruses and programmes which can be activated at the time of their choice. CIA is also collaborating with private firms to in fact hardware before it is sold to other countries.

c. System Vulnerabilities

Various government setups of Pakistan are becoming technology dependent leading to more vulnerability with regards to electrical and electronic equipment. The

[174] Beena G. Pillai, and Madhurya J. A, "A Decentralized Data Privacy for Mobile Payment using Blockchain Technology," *International Journal of Recent Technology and Engineering (IJRTE)* 8, no. 6 (March 2020), doi:10.35940/ijrte.2277-3878.

reliance on computers and computer-based equipment is increasing, which is leading to increased vulnerabilities and threat. In Pakistan, lack of indigenous production of sophisticated electronic and other related systems and raw human resources assets has made us more vulnerable to Cyber threat. Our electronic and computerized systems are mainly vulnerable due to following: -

i. Lack of awareness of the danger of cyber warfare.

ii. Lack of computer literacy and know-how.

iii. Poor management of the computerized systems and inadequate security to prevent unauthorized access/intrusion.

iv. Use of low-grade security codes, which can be easily compromised.

v. Poor defense of the most of the modern communication and electronic systems and microprocessor controlled units, which have their vulnerability to cyber techniques.

vi. Inadequate electromagnetic pulse protection / shielding of the structures, housing computer systems.

vii. Use of hired transponders for satellite communication.

viii. Lack of indigenous production base and dependence on foreign equipment and exports for modification/repairs.

d) Economic Vulnerabilities

Likely vulnerabilities in this category are Financial Institutions, Private and Government Industrial Plants and Private Enterprises which includes Karachi, Lahore and Islamabad Stock Exchanges, all major banks such as State Bank, National Bank, UBL, HBL and Citibank, currency control and depositories databases.

e) Civil Infrastructure Targets

It includes all civil communication system such as PTCL and mobile communication. There infrastructure includes digital switches, repeater stations, node centers and computer controlled system. Energy resources and powerhouses to include WAPDA and other private Power producers such as HUBCO and their distribution system, Nuclear power plants such as Chashma and Karachi are also vulnerable being dependent on computers system. Moreover all civil traffic signals, sea ports such as Karachi Port Trust, Port Qasim, Gwadar and all air traffic is being controlled by computer system and remains vulnerable to cyber threat.

f) Military Vulnerabilities

Pakistan's all military systems are becoming computer dependent and thus becoming more vulnerable to cyber threats. Computer controlled weapon systems, command and control systems, global position systems and early warning systems and communication systems are major vulnerabilities in military field.

Cyber Terrorism

It is widely accepted that after the industrial revolution of 18th century, IT revolution is the most significant step in global evolution.[175] However, increased dependence of military, economic and other national systems on IT has turned them into high value targets for cyber attacks. Easy acquisition of these targets is well identified by the terrorist as only one PC can level the playing field between otherwise not so equal adversaries.IT provides terrorists an opportunity to gather intelligence, plan terrorist action and create chaos in societies by targeting critical systems, without spending huge resources. IT and networking of critical systems has provided an opportunity to terrorist to exploit its vulnerabilities without any risk of physical harm to them. Cyber-terrorism is still under discussion as to; whether it is a new concept or just an extension of IO by the terrorists. However it is a difficult asks as boundaries between cyber terrorism and cyber crimes remains very blurred. Few of the definitions are as under:-

In USA, the FBI describes cyber-terrorism as: "Cyber-terrorism is a criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social, or ideological agenda."

Another definition by Kevin Coleman, a former chief strategist at Netscape who writes a Homeland Security focused column for Directions magazine is: "The premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives or to intimidate any person in furtherance of such objectives."

[175] Defense Intelligence Agency, *Statement for the Record: Worldwide Threat Assessment*, (USA: Defense Intelligence Agency, 2021), https://www.dia.mil/News/Speeches-and-Testimonies/Article-View/Article/2590462/statement-for-the-record-worldwide-threat-assessment/.

Significant Aspects of Cyber Terrorism

Significant aspects of cyber terrorism as highlighted in Handbook 1.02, Cyber Operations and Cyber Terrorism of US Army Training and Doctrine Command are as under:[176]

- It includes offensive IT potential used in isolation or in collaboration with other types of terrorism and is different form of terrorism.
- Cyber terrorism can cause destruction of equipment and hardware by means of IT resources. It can cause train accidents or disrupt road rail and air traffic by overriding the control systems besides causing economic destruction through falsified communications.[177]
- Since the cyber networks provide cyber terrorist the requisite medium for executing their tasks, they are most likely to keep their actions discrete and destruction caused limited; so that networks keep working and they remain viable to exploit the opportunity.
- Cyber terrorism is dependent on internet for transmitting malwares, disruptive commands, exploiting information and making counterfeit transaction.
- Hacking, crashing and defacing websites of adversary and spreading panic through financial disruption is the essence of cyber terrorism and is dependent on the fact that despite these entire actions target remains viable for further exploitation.
- However total crashing of networks is also possible if a terrorist group feels that it had gained maximum and now can afford the loss of this inlet into enemy systems.[178]
- Besides Computer systems, terrorists can also target communication hubs to disrupt national communication systems, which may have direct influence on military operations. These may be resorted to support physical attacks or adopted in isolation to project their power and control.

[176] Dep Chief of Staff for Intelligence, *Cyber Operations and Cyber Terrorism, Handbook Number 1.02* (Leavenworth: US Army Training and Doctrine Command, 2005), https://www.hsdl.org/?view&did=465926.

[177] Ibid.

[178] Ibid.

- Other than causing physical destruction, cyber terrorism can be used for non physical effects like data modification or manipulation or influencing perceptions and even electronic theft which are not in physical domain.
- Defacing of website is a major activity of terrorists as it helps them in creating negative impression about target while projecting own power.

Cyber Support to Terrorist Operations

Cyber domain has been fully exploited by terrorist organizations to facilitate their operations and promote their agenda.[179] Few of the major aspects are as under:

- **Communication & Planning**

Cyber infrastructure provides terrorist an opportunity to plan their actions while communicating with each other through internet while using low cost encryption methods to maintain secrecy by using pictures or making comments in chat rooms which are only under stood and opened by those who are required to open them. They also use such encryption programes to scramble their telephone conversations.

- **Donations & Recruitment**

Terrorist organizations are always searching for new recruits and donations for their cause. This is greatly facilitated by using social networking sites and promoting own organizational website which are made lucrative to attract new memberships and funds.

- **Intelligence Gathering**

Making use of internet and search engines terrorist can gather a huge amount of intelligence about any desired targets. Availability of maps, photos, Google and Wikipedia, etc. has made their job very easy. This fact is well realized by the terrorist and a recovered document of Al Quaida states: “Using public sources openly and without resorting to illegal means, it is possible to gather at least 80% of information about the enemy." It was in this back drop that Donald Rumsfeld issued a memo stating: "One must conclude our enemies access DoD Web sites on a regular basis."[180] He asked all military departments to remove any confidential data from websites as this provided terrorists an opportunity to retrieve information without ever leaving their bases.

[179] Mithilesh K. Singh, *Cyber War And Terrorism* (New Dehli: Prashant Publishing House, 2009).

[180] Ibid.

- **Perception Management**

Christopher Harmon thinks that, “Propaganda is a veritable terror group standard.”[181] It is actually the backbone of all terrorist entities which helps in projecting own cause and facilitate recruiting besides undermining the target country or government. Availability of internet and social media websites have provided great leverage to terrorist and they are no more heavily dependent on handouts and International Institutions and Global Governance Program.[182] Internet provides terrorists to be instantly available to millions of audience and spreading terror through horrific videos.

- **Cyber Terrorism vs. Physical Terrorism**

Till to date cyber terrorism has not manifested in its worst form of causing crashes and destruction, etc. but still terrorist have the ability to exploit the internet to their advantage. Director FBI for National Infrastructure Protection Center in 2002 said, “The event I fear most is a physical attack in conjunction with a successful cyber-attack on the responders’ 911 system or on the power grid.”[183] The FBI’s Cyber Division is of the view that cyber-terrorism will emerge as a better option in future against traditional terrorism, as it ensures anonymity while engaging divers targets with no risk of injury and very low cost and risk involved.[184]

4.5.3 Pakistan government approves new cyber security policy

The Pakistan Ministry of Information Technology announced the adoption for the country of South Asia of a new cyber security strategy and accompanying cyber security agency. The strategy intends to assist both commercial and public institutions and to replace a system of government institutions with distinct safety operations, including national information networks and vital infrastructure. It is a sensitive time for Pakistan, which has lately accused India of spying on Prime Minister Imran Khan with the Israeli malware Pegasus — and which calls cyber assaults on any Pakistani institution an attack upon national sovereignty.[185] The new cyber security policy for Pakistan would involve a

[181] Ibid.

[182] Ibid.

[183] Jacques S. Gansler and Hans Binnendijk, *Information Assurance: Trends in Vulnerabilities, Threats, and Technologies* (Washington, D.C: National Defense University (NDU), 2004).

[184] Ibid.

[185] William H. Dutton et al., "Cyber Security Capacity: Does It Matter?," *SSRN Electronic Journal* 9 (2019), doi:10.2139/ssrn.2938078.

new management and institutional structure for a 'safe cyber environment' together with the Computer Emergency Response Teams (CERTs) and national security operations centres (SOCs). The strategy asks for new channels for the sharing of knowledge, development of skills, training and public awareness initiatives. "Awareness of security is crucial. The dangers associated with interrelated systems and the function they play in guaranteeing safety have to be informed. Once this basis is built, it will be easier and more effective to implement technology and methods to support it."[186]

Its execution is the biggest obstacle for the policy. In conjunction with an action plan for the achievement of the policy objectives, the national cyber security policy is supplemented by a strategy paper. The strategy paper would contain prioritising the activities, deadlines, roles and duties of the entities in charge of achieving the goals set out in the policy. A dual civil-military agency institutional structure must be developed by the government. This would be raised to execute the above policy goals and to safeguard national cyber protection in government, trade and military areas.

The policy serves as the foundation for a complete digital ecosystem with supporting frameworks and components to ensure that digital services, applications and digital infrastructures are safe, dependable and standardised. This policy will push the basic need for excellent delivery of their goods and services in the local IT business. This gives local and international entrepreneurs and companies a chance to deliver key skills, services and solutions and offers local businesses a chance to compete and thrive internationally.[187]

It would also promote online companies that enable digital payments to operate smoothly both in Pakistan and abroad. In addition, it is imperative to strengthen national cyber security capacity by creating essential and coordinated mechanisms, implementing security standards and regulations in the context of a policy and legislative framework to mitigate cyber threats in

[186] Emma Woollacott, "Pakistan government approves new cybersecurity policy, cybercrime agency," *Daily Swing*, August 9, 2021, https://portswigger.net/daily-swig/pakistan-government-approves-new-cybersecurity-policy-cybercrime-agency.

[187] Amel Attatfa, Karen Renaud, and Stefano D. Paoli, "Cyber Diplomacy: A Systematic Literature Review," *Procedia Computer Science* 176 (2020), doi:10.1016/j.procs.2020.08.007.

the country today and to increase national cyber security perspectives. Cyber-Governance Policy Committee was established by the Government of Pakistan (CGPC)[188]. In accordance with the evolving cyber trends and technical advances of the relevant organisation, in conjunction with all stakeholders and after every 3 years and as needed, the national cyber security policy 2021 is subject to inclusive review.

Conclusion

Cyber attacks are a serious and rising concern, and Pakistan's efforts to combat them have so far fallen short. In Pakistan, there is still no cohesive cyber command or national cyber policy established to counter Pakistan's regional cyber challenges. While Pakistan has established a cyber security auditing and assessment laboratory recently, it remains in its formation stages. Increased tools and research capabilities are also available to help defend Pakistan's cyber-space, confidential data, and local economies from cyber attacks while limiting illegal access. In particular, the initiative by the recently formed National Center for Cyber Security to increase the number of indigenous cyber security practitioners trained in the public sector. Holding this course Pakistan should emphasize that its own cyber security sector is being built indigenously so that its civilian and military infrastructure will benefit from the long term in the near future. Therefore, while Pakistan is currently restricted in its ability to conduct a robust offensive operation within the area of cyber war, such moves will help laid the groundwork for more.

[188] Basit Shahzad, "National cybersecurity policy and 5th generation war," *Pakistan Observer*, September 3, 2021, https://pakobserver.net/national-cybersecurity-policy-and-5th-generation-war-by-dr-basit-shahzad/.

FINDINGS

1. The researcher find out that It is a malevolent act intended to destroy data, steal data, or otherwise disrupt digital life. Viruses, data breaches, Denial of Service (DoS) assaults, and other attack vectors are among the cyber-threats. An information technology asset, computer network, intellectual property, or any other type of sensitive data may be the target of a cyber assault. Trusted people inside a company can pose a cyber danger, as unidentified parties in faraway areas.
2. Cyber security is a fast-moving industry, as hackers and security providers compete to outwit each other in order to gain an advantage. Every day, new threats – and new strategies to resist them – arise. Cybercriminals have additional chances as the Internet of Things (IoT) expands. Other than computers, phones and servers, the Internet of Things refers to any physical item that can connect to the internet and share data. As the cyber security business continues to grow, cloud vulnerability is expected to continue to be a major trend. Again, the fast and broad adoption of remote working during the pandemic has raised the need for cloud-based services and infrastructure, with security issues for companies as a result. Humans cannot manage the enormous amount of cyber security threats alone. Desperate to improve their security architecture, companies are increasingly turning to artificial intelligence and machine learning.
3. Pakistan's information technology capabilities to deal with future security issues in banking and finance, health and education, national databases, defence and nuclear technologies was examined in length by the researcher. Digital currency's economic disruption is likely to be a big concern in the near future. Also, cyber bullying and online harassment are on the rise. By identifying and classifying problems early, Pakistan may better anticipate challenges. National danger perception mechanisms that can act as early warning systems must be developed in Pakistan. Pakistan is bordered by a hostile country that is a technological leader. "Indian Chronicles" by EU dis info Lab documents India's misinformation effort against Pakistan. Even with all the cyber difficulties Pakistan has, there is still plenty of opportunity to overcome them.
4. It's easy for hackers to misuse and disrupt the use of cyber space since it's increasing

due to the increased use of IT and telecom. Hackers' attack area has also increased to the point that they may now shutdown networks at their discretion. The banking, power grid, transportation and military command and control systems of a country might all be paralysed, as an example.

5. The researcher pointed out Pakistan's cyber-security system's weaknesses. They do not have a full understanding of the intricacy of cyber-attacks. It's a tragedy that Pakistan doesn't have a competent cyber security system. National cyber security strategies, according to the International Telecommunication Union (ITU), are crucial initial steps in dealing with cyber-security problems. Another crucial component of a solid cyber-security system is capacity-building in the domain of cyber security, although efforts in this area are still in their infancy. The policy's execution poses the greatest obstacle. As part of a national cyber security policy, there is a strategy document that includes an action plan to fulfill the policy's objectives.
6. This implies that Pakistan is very vulnerable to cyber-attacks and does not have a proper reaction system in place in order to counter them. In light of the growing risks to national security, which have been exacerbated by the COVID-19 epidemic, Pakistan must address its policy deficiencies in cyber security and its readiness. It may be expensive to postpone the development of cyber-security infrastructure. Cyber intrusions must be neutralised, and Pakistan's cyber security laws must be updated to reflect the evolving cyber threat environment. To guarantee coordination between government, military, and intelligence entities, a "National Cyber Security Agency" should be created. Critical infrastructures should be assessed for cyber risks, and security levels should be established. I think it's most necessary to look at present digital laws, especially PECA from a wider perspective so that it can better address cyberspace-related issues. If Pakistan ignores, delays, or does not invest in a comprehensive and active cyber defence, it will be at its own danger.
7. Prioritizing cyber security isn't the only issue. The difficulty is in comprehending it. Currently, very few people in our government understand the problem's sensitivity and true scope. Pakistan must understand and prioritise cyber security on a national scale. We must learn from these international crises and incidents - we are vulnerable, and the worst part is that we are doing nothing to address it.

8. All of this reflects poor management of Pakistan's cyberspace, a lack of relevant institutions, a lack of security debates, and the exclusion of the general public from security issues. These obstacles will continue to stymie Pakistan's progress toward becoming a digitally advanced country.

CONCLUSION

In cyberspace the globe has seen an incredible expansion. ICT's effect covers all sectors of the company. Cyberspace is an activator for every other area and unprotected cyberspace in current times might present a threat to the economic and security of national security of any nation. There are several types of cyber risks that must be addressed nationally and at departmental level. In the worst-case situation, cyber assaults may threaten the territorial sovereignty of the country by interfering, creating panic or unintended war, with government decision making processes. The Pakistani government is still in a position to pursue a cyber assault policy. The creation of a complete cyber policy has only been made formally since 2003, and so yet, practical execution has not been implemented. Currently, cyberspace is not only being misused by cyber criminals but also being utilised as a safety and strength tool for recruiting, retrieving, and mobilising cyber-terrorism networks. The analysis reveals that Pakistan is growing increasingly exposed to the present and emerging cyber threats every day. As the DG ISPR recently raises this issue in a seminar, he urges media workers and journalists to counter the anti-state storey spread on the Internet platform, known as fifth generation and hyber-based war which is already being impose. The governments are not sounding the targets for cyber attacks and the issue is being addressed in many instances. That is obvious, and Pakistan has to start and secure the cyber area as soon as it can. The war bells have already been burned.

The development of technology has posed a number of new dangers and difficulties to national security as hostile States and even non-state actors are continuously engaged in violating the cyberspace of government institutions and telecommunications corporations. Developing countries such as Pakistan have to deal with serious cyber concerns immediately. Citizen infringement, hacking of government web pages, entering government officials' personal WhatsApp accounts, evading financial institutions' cybersecurity, efficient use by terrorist organisations, and the international malicious cyber-campaigns of hostile countries such as India are a grave warning to policymakers to develop a new system. In order to improve coordination between civil and defence organisations, State must also create the National Cyber Coordination Center to strengthen its professional ability in the sector. Thus, improved collaboration amongst law enforcement agencies would mean that cyber security policies are strictly being implemented, enhancing Pakistan's cyber security picture.

It is hard to predict the impacts, influences, and scales of cyber dimensions between military and political conflicts. There are a plethora of techniques, procedures and methods are followed by the attackers or hackers. Internet is above all, open to attack. In addition to this, it has amplified capacity. So, the triumphs of cyber attack are going to convert into ground victories.

In the current scenario, the grounds for battles and wars have changed. The old fields of war like sea, land, and air are not remaining influential and prominent because of modification in war fares. The new battlefield, cyber space has discovered or invented. Now the digital world decides the defeat and triumph of rival parties whether in politics, business, and individual conflicts. It is beyond the boundaries of geography and reach of conventional or customary means like Geneva Convention. It is a real game changer not only for a region, but worldwide. This completely changes the policies, challenges, threats, and dynamics of war; therefore, the enemy is unpredictable due cyber warfare.

Because of strong return on investments in cyber tactics both non-state actors and state actors have enjoyed. The investments range from careful positioning designs propaganda to adversary of crucial infrastructure.

Internet evolves every area of life. The changes are not only positive, but also negative like Cyber Warfare and Cyber threats. Technologies and tactics of cyber have preferred the information technology of vigorous nations; however, for weak group, internet is remarkable and wonderful tool to strike on stronger traditional opponents. The complex, asymmetric, and continuous growth of Cyber Attacks leads to mass destruction and terrorism. Furthermore, cyber defense is necessary for the national security; therefore the planners should address the identification, retribution, review, investigation, and prosecution, etc.

Due to the current situation, the cyber arm race has begun between the states worldwide. Mostly, cyber attacks are among states not individuals. Every cyber-espionage has considered as cyber warfare which is not correct. Cyber warfare is something very big than the spying and stealing of data. Although, every government has been trying to spy and steal digital data in the globe. The cyber attack is very severe and causes destruction and devastation. So, they are considered as physical attacks. It is also predicted that cyber attacks will be used as low intensity skirmishes among states in the world in future to cause chaos and confusion rather than destruction.

A tremendous growth and development has witnessed all across the world in the field of Cyber Space. ICT's influence applies to all fields of industry. It plays a dominant role for all realms, and unregulated cyber space in current scenario can pose a threat to economy and protection of the national security of the country. National level has to handle more types of cyber threats in comparison with departmental level. In this current tough situation, by interfering with government decision making processes, resulting panic or unintentional war, these attacks impacts the country's territorial integrity and sovereignty. Pakistani government has strength, capabilities, and inertia to establish and implement strategies to cope with Cyber Attacks. The paper work has been done to establish a robust strategy for Cyber Attacks since 2003; however, there have been no real implementations so far. Not only cyber criminals exploit the cyber space, but it has become a strongest tool for terrorists to accomplish their agendas all across the world. They use internet and technology for communication, psychological warfare, data collection, and mobilization networks. The researcher has further enlightened the condition of Pakistan which is going worst day by day due to the diversity of the Cyber Attacks. DG ISPR has argued in a seminar in front of media staff and journalists to counter anti-state narrative spread on the internet forum, which is regarded as the fifth generation warfare and hybrid war that is already being imposed on Pakistan; therefore, Pakistan is making a soft target for these attacks. The statement clear cut expresses the current situation and future threats to Pakistan. Pakistan should have focus to secure cyber space as soon as possible.

RECOMMENDATIONS

Need of inter-state opportunities

There is a need of inter-state opportunities to recognize or exchange practices at regional level. So, government should focus on the collaboration and cooperation to fail the attacks of enemies.

Innovation in Policies

Government should implement the policies regarding cyber security in true meanings. There is also a need of innovation in the policies and legislature regarding cyber threat, cyber warfare, and cyber security.

Awareness in Public

There is also a need to aware public about this new kind of warfare to minimize its disastrous effects. Such as fifth generation warfare implemented and sponsored by India in the Baluchistan and other parts of Pakistan highly impacted its national security.

Separate Policy for State Bank

There should be separate policies for the sensitive units, such as State Bank of Pakistan and airports against cyber threats.

Computer Ethics and Cyber Warfare

Pakistan should introduce and promote it in the curriculum of universities to aware people about cyber warfare because there is no book which covers "Computer Ethics and Cyber warfare" subject.

National Security Policy in Broad Terms

A broad and detailed national cyber security is defined as the procedures to resolve cyber security concerns, is the first important move for the government to legislate. It is important to broaden the reach of the cyber crime bill and be part of cyber security agenda. So, it is possible to recognize the example of India's national security policy 2013 as a guideline model for developing a comprehensive policy.

Establishment of National Cyber-Command

In order to deal with the problem of cyber warfare, which is considered to a part of fifth generation warfare, the establishment of a national level cyber command is very necessary. The clear example is USSTRATCOM; the national cyber command in

Pakistan can be set up to operate under the national Security Council to take on board all concerned leaders when planning defensive and offensive capabilities for this warfare. The FIA's new NR3C will only continue to counter mild cybercrime.

Regulation of Pakistan's Cyber-Space

The current government has also failed to enforce the legislation for the cyber space which is important for Pakistan's national security. Due to the blasphemy, the government has banned the social media in recent past; however, it's not the permanent solution. The security has only achieved through development of a systematic mechanism with the help of IT industry and LEA to globally govern the cyber space with ICAN norms. The records of both devices mobile and computers should secure and maintained properly. They have to ban the illegal use of IP's, pirated softwares, and VPN's.

Capacity Building

In order to cope with modifications in the tactics of Cyber Crime, Pakistan should enhance the capabilities, capacities, and powers of Law Enforcement Agencies. The current situation has been creating troubles; therefore, the staff of Law Enforcement Agencies should be trained adequately and prepared to cope with Cyber Crime. In relation to intimidation, terrorism, economic embezzlement, and other fields of cyber, the powers should be divided into various areas of operation.

Public Awareness Campaigns

The governments, NGOs, and INGO's should arrange seminars, workshops, and conferences to aware public. The campaigns and advertisements are one of the best tools to aware public; moreover, public has no idea about the pros and cons of internet, these campaigns helps them to take benefit from internet rather than wastage of time and exposes the propagandas related to cyber space. Hundreds of individuals are scammed via the internet every day. Furthermore, specific marketing and promotional strategies should be introduced to teach general public about the tips and tricks to safe themselves from cyber threats. They should aware public both at academic and national level to overcome the cyber threats as soon as possible and safe the public from rumors and scams.

In the context of South Asian Association for Regional Cooperation (SAARC); there is no cooperation, coordination, and collaboration have been seen in the region of South Asia. The organization can play a vital role to combat cyber threats by collaboration and coordination.[189]

Cybercrime Response Mechanism

Stakeholders should

- Support and improve government capacities by increasing the technological capacity of law enforcement authorities to address cybercrimes.
- Establish contact and coordination for information and collaboration with other domestic and foreign cybercrime agencies.
- Strengthening processes and procedures and incorporating cyber safety into susceptible networks of public and commercial service.
- GLOBAL COOPERATION AND COLLABORATIONS
- Work with all international partners such as ITU IMPACT etc. The Ministry of IT & Telecom in collaboration with the Central Entity.
- Maintains a constant presence and professional contribution from Pakistan, including the ICANN, the GAC, the ITU and the APT, and other similar UN and Non UN agency organisations.
- Association of all national, regional and international bodies to coordinate and cooperate in creating cyber-situational awareness.

Cyber Policy

All segmented efforts should be combined under the umbrella of Cyber policy and all initiatives must be overseen and executed by Ministry of IT and communication.[190] The policy should focus on following:-

(1) Establish National Cyber Authority and all organization working in various setups like NR3C and NTISB, etc. be placed under this authority with ministry of IT as coordinating ministry,

(2) Formulate a comprehensive and fully integrated policy on Cyber technology education, keeping in view the following parameters:-

(a) In the long run, our education system should produce sufficient expertise for various segments of cyber Operations.

[189] Ibid.

[190] Sultan Ullah et al., "Pakistan and cyber crimes: Problems and preventions," *2015 First International Conference on Anti-Cybercrime (ICACC)*, 2015, doi:10.1109/anti-cybercrime.2015.7351951.

(b) Provide awareness and know-how on various aspects of cyber technologies.

(c) Adequate quality control measures must be instituted to provide standardized and quality IT related education to our youth.

(d) Advanced education programmes in selected subjects relating to cyber Operations should be planned in IT universities in the country.

(e) Initiate the process for enhanced and quality research work in our universities and IT institutes.

(3) The emerging cyber threats to the business sector, commerce, industry and banking should be highlighted along with need to develop viable safeguards and reasonable redundancy in our systems.

(4) All essential elements of the state, including media be integrated to create awareness while countering enemy propagandas with an aim to project and support our national objectives.

(5) Cyber policy should promote safe computing environments and lead towards enhanced e-government and e-commerce functions by highlighting need for and ensuring development of adequate redundancy and safeguard to counter jamming of links and to neutralize the effects of physical attacks for destruction of cyber hubs.

(6) The Policy should ensure that all elements of national power be judiciously utilized to develop a viable cyber operations capability to guarantee safety and redundancy of own strategic information and IT based systems against cyber attacks in the short term. Also a credible deterrence through offensive cyber operations capability in the midterm.

(7) Actively pursue acquisition and transfer of advanced Technologies (both hardware and software).

(8) Actively pursue creation of an integrated Cyber protection programme by the Islamic World and friendly states.

(9) Propose establishment of international safeguard regimes against cyber threat.

Short Term Measures at National Level or State Level

Attainment of Cyber Operations capability should be added in our list of national objectives on the strategic lines and contemplated through action plans in 2 to 3 years' time span:

(a) **Awareness and Training of Personnel**

Policy and law makers should be made aware of the threats posed by Cyber Operations and the benefits of using Cyber Operations to own advantage. Those who use and manage IT systems should be aware of threats attached as human element is biggest vulnerability in cyber domain, hence it is essential to create awareness at all levels by imparting professional training and special seminars and workshops.

(b) **Legal Framework**

Following needs to be done at the earliest:-

i. Laws to be promulgated to provide safeguards to vital information and important national information systems.

ii. Laws on cyber crimes and national information infrastructure protection be promulgated to meet the new challenges and to maintain supremacy of law in the country.

iii. To regulate cyber activities and ensure that unsafe practices do not result in compromising our vital national assets.

iv. Regulate IT education in the country, for standardization and quality control of the entire system.

v. Laws on E-Government and E-Commerce be promulgated to properly regulate these activities and provide sound basis for establishment of E-business in the country.

vi. To built mechanism for regular audit of all government networks, computer and communication systems for ensuring implementation of standard safe computing practices.

(c) **Human Resource Development**

The disciplines of Cyber Operations be introduced in selected IT Universities to broaden the level of understanding of the graduates and creating a pool of qualified personnel in the following fields:-

i. Various forms of cyber Operations.

ii. Quality control in network deployment and administration.

iii. Hardware and software testing against Chipping and Back Door(s) or Trap Door(s) etc.

(d) **Security of Cyber Systems**

Security of important cyber systems be enhanced by use of encryption technology and security software, i.e. Antivirus programmes, hardware and software Firewalls and Intrusion Detection Systems. Security analysis and scanning of vital systems should be carried out regularly and their logs be maintained.

(e) **Accountability of Manufacturers / Suppliers**

At present, security features in Internet Browsers, E-mail Clients, Instant Messengers and other software used in almost every PC in the World are deliberately disabled so that the communications could be read by intruders without difficulty. There is a need to make manufactures and suppliers contractually responsible to conform to an ‘Open Standard’ which allows implementing additional security applications developed by the Government and / or third parties to restore the level of security. This can be ensured by developing capability to inspect hardware and software against such mal-practices.

(f) **Local E-Mail Services**

Local E-mail servers are urgently required to ensure security of E-mails amongst government departments and public and private organizations. Hence, an E-mail server facility, on the lines of Hotmail and Yahoo needs to be created, through joint venture with the private sector. Presently no E-mail or electronic communications is safe from prying eyes of hackers.

(g) **Security software / techniques**

Development of security software / techniques, i.e. encryption software, firewalls and Cyber Warfare tools be emphasized to the national Information Technology developers and efforts be made to develop these technologies indigenously. Talented youth in the Information Technology sector within the country or abroad should be motivated for developing Cyber Warfare capability, thus creating an Information Technology pool.[191]

(h) **Building Parallel Virtual Machines**

To break or decode encrypted message, large amount of computing power is required. Though supercomputers may not be available to Pakistan, a very large cluster of high performance commercially available computers (Servers and Workstations) can be tied together to build 'Parallel Virtual Machines' that can provide the required computing power.

(i) **Prioritize the Cyber Sphere**

Critical information systems are the ones which are vital to our national security. These include classified military networks and critical communication links, economic and financial networks. Cyber sphere must be clearly prioritized at the national level by including all all elements of national power through a well defined and properly coordinated action plan.

(j) **Standardization of Cyber Systems**

The present trend of haphazard induction of systems in the government departments and the Army is counterproductive and wastage of financial resources. Hence a well defined policy be chalked out to standardize and streamline acquisition and development vital cyber related systems for all elements of national power.

Mid Term Measures at Domestic Level

Measures considered essential to be undertaken in midterm (4 to 7 years period) are as under:-

[191] Jannat A. Kalyar, "Pakistan's cybersecurity regime," *DAWN*, March 2, 2020, https://www.dawn.com/news/1537766.

a) **National Research Institute**

To keep pace with rapidly developing IT and related fields, a national research organization should be created. The said organization beheaded by a single competent executive authority, focusing on development of cyber operations tools and related necessities.

b) **Develop Encryption Indigenously**

We must develop a reliable encryption system to fulfill our needs in military, diplomatic, financial, economic and other important spheres. The expertise gained by different R&D setups must be fully exploited and developed at the national level by inducting more human and financial resources.

1. **International Collaboration**

The government's efforts be made to persuade friendly states to cooperate at bilateral level in the field of cyber Operations.

ii. **Long Term Measures**

The measures recommended below need to be implemented in 7 to 10 years time frame:-

1. **Lead and Magnetic Shielding**

Physical protection of the vital Information technology systems will greatly reduce the risk of cyber attacks. In order to evade emission capture, EMP attacks and other such like Cyber threats, lead and magnetic shielding of vital buildings and centers should be undertaken in a phased plan. This important aspect is kept in view while planning and developing new setups of vital national importance.

2. **Indigenous Production**

Imported computer and communications systems remain susceptible to foreign intrusion, as it is difficult to identify planted but dormant loopholes. Hence, there is a need to undertake following measures:-

a. Undertake standardization of own equipment.

b. Develop a strong industrial base for indigenous manufacture of essential equipment.

c. Develop facilities to manufacture computer hardware and software in the country. Joint ventures with friendly countries may be sought for this purpose.

3. **Satellite Capability**

Own communications and military satellites be launched to achieve and enhance strategic communications, satellite imagery, Psychology Operations and intelligence gathering capability, facilitating Cyber warfare.[192]

b. Organizational Setups

Ministry of IT is the lead organization dealing with cyber issues, however it is suggested that dedicated setup may be necessary to deal with this emerging issue. Few suggestions in this regards are as under:-

(1) **National Cyber Authority**

A potent organization under the patronage of the Prime Minister at National level with representatives from all concerned departments / organizations and Joint Staff Headquarters should be established. It should be legislated as the highest national policy making body on Cyber Operations and it should be made responsible for promulgating and controlling all Cyber Operations related policies in the country. It should be interfaced with CCNS by presence of science & IT minister in the committee as shown in annexure B.

(2) **National Cyber Security Cell**

The National Cyber Security Cell be formed immediately, comprising IT experts from government departments, media, finance and private sector IT companies / software houses. It should act as a bridge between public and private sector enterprises and give action plans in line with envisaged tasks to include:-

(a) **Identify Vulnerabilities of Critical Infrastructure Assets and Shared Dependences**

It should focus on the following:-

i. Nature and extent of vulnerabilities of our critical infrastructure in both peace and war.

[192] Rubab Syed, Ahmed A. Khaver, and Muhammad Yasin, "Cyber Security: Where Does Pakistan Stand?," *Sustainable Development Policy Institute (SDPI)*, February 2019, https://www.think-asia.org/bitstream/handle/11540/9714/Cyber-security-where-does-pakistan-stand%28W-167%29.pdf?sequence=1.

ii. Set goals for the security of government and other important computer systems to develop reliable and secure Information Technology related infrastructure in next five to ten years period.

iii. Address the weaknesses in cyber systems of government offices, organizations and network systems by ensuring each ministry, department and organization to work in unison.

iv. Encourage participation of private institutions and stakeholders for achieving greater cyber security for critical systems through unified approach.

(b) **Protection of Sensitive Infrastructure**

The Cell should recommend measures for protection of sensitive computer systems and lay down priorities for taking protective measures.

(c) **Assist in Making Laws and Policies**

The Cell should formulate recommendations to assist the government in formulating laws and policies to combat Cyber Crimes / Warfare.

(d) **Share Threat Warnings**

It should provide a unified systems for improved Information sharing from federal government down to each major network and systems, including private sector. It should also help in removing barriers to information sharing amongst various departments and organisations.[193]

(e) **Role of Enhancing Research and Development**

The Cell should recommend research requirements and priorities ensuring that our Cyber security technology stay abreast with changes in the threat and in overall development of technology.

(3) **Establishment of Computer Emergency Response Team (CERT) at National Level**

Computer Emergency Response Team at National level should be able to isolate and minimize damage and restore required capabilities quickly. It should provide plans for limiting an attack when it is under way. Also build recovery plans to ensure survivability and continuation of essential systems and services.

[193] Ibid.

(4) Risk Management

Risk management due to resource restrictions is required for the management of occurrences and problems. A risk-based strategy is to be established and realised by demanding and encouraging organisations as part of their business risk management activities to set risk criteria, risk appetites and risk tolerances for themselves. Furthermore, all entities and organisations themselves will have to maintain risk mitigation strategies.

The notable risks and challenges of cyber security might include Internet of Things, Ransomware, AI (Artificial Intelligence), server less applications, Critical National Infrastructure, Sophisticated Phishing Campaigns, Strategic Use of Information, Cloud Computing, Science and cyber security, and hacker-for-hire services and skills shortages.

Recommendation for Future Research Work

The researcher can contribute the details of types of cyber attacks launched on Pakistan and the inconvenience faced by Pakistan due to the attacks; furthermore, the researcher further contribute in analyzing the effectiveness of the policies of Pakistan to counter each kind of cyber attack and the ratio of cyber attacks on commercial, defense, and economic sector of Pakistan.

BIBLIOGRAPHY

Books

Andress, Jason, and Steve Winterfeld. *Cyber warfare : techniques, tactics and tools for security practitioners*, 2nd ed. Rockland: Syngress, 2014.

Buzan, Barry, Ole Waever, and Jaap D. Wilde. *Security: A New Framework for Analysis*. Colorado: Lynne Rienner Publishers, 1998.

Carr, Jeffrey. *Inside Cyber Warfare: Mapping the Cyber Underworld*, 2nd ed. Sebastopol: O'Reilly Media, 2011.

Cheng, Dean. *Cyber Dragon: Inside China's Information Warfare and Cyber Operations*. Santa Barbara: Greenwood, 2016.

Clarke, Richard A., and Robert K. Knake. *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats*. London: Penguin Books, 2019.

Dep Chief of Staff for Intelligence. *Cyber Operations and Cyber Terrorism, Handbook Number 1.02*. Leavenworth: US Army Training and Doctrine Command, 2005. https://www.hsdl.org/?view&did=465926.

Futter, Andrew. *Hacking the Bomb: Cyber Threats and Nuclear Weapons*. Washington: Georgetown University Press, 2018.

Gansler, Jacques S., and Hans Binnendijk. *Information Assurance: Trends in Vulnerabilities, Threats, and Technologies*. Washington, D.C: National Defense University (NDU), 2004.

Jajodia, Sushil, Paulo Shakarian, V.S. Subrahmanian, Vipin Swarup, and Cliff Wang. *Cyber Warfare: Building the Scientific Foundation*. Basingstoke: Springer, 2015.

Lee, Donna, and Paul Sharp. *The New Public Diplomacy: Soft Power in International Relations*. Edited by Jan Melissen. London: Palgrave Macmillan, 2005.

Libicki, Martin C. *Conquest in Cyberspace: National Security and Information Warfare*. Cambridge: Cambridge University Press, 2007.

Lin, Herbert, and Amy Zegart. *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations*. Washington: Brookings Institution Press, 2019.

Schreier, Fred. *On Cyberwarfare*. Geneva: Geneva Centre for the Democratic Control of Armed Forces, 2015.

Shakarian, Paulo, Jana Shakarian, and Andrew Ruef. *Introduction to Cyber-Warfare: A Multidisciplinary Approach*, 1st ed. London: Newnes, 2013.

Singh, Mithilesh K. *Cyber War And Terrorism*. New Dehli: Prashant Publishing House, 2009.

Springer, Paul J., editor. *Encyclopedia of Cyber Warfare*. Santa Barbara: ABC-CLIO, 2017.

Trim, Peter R. *Cyber Security Culture: Counteracting Cyber Threats Through Organizational Learning and Training*, 1st ed. London: Routledge, 2013.

Weimann, Gabriel, and Bruce Hoffman. *Terror on the Internet: The New Arena, the New Challenges*. Washington, DC: US Institute of Peace Press, 2006.

Yamin, Tughral. *Cyberspace CBMs Between Pakistan and India*. New Mexico: Cooperative Monitoring Center Sandia National Laboratories, 2013.

Yamin, Tughral. *The Evolution of Nuclear Deterrence in South Asia*. Islamabad: The Army Press, 2014.

Zetter, Kim. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York: Broadway Books, 2014.

Blogs

Aziz, Farieha. "Pakistan's Cybercrime Law: Boon or Bane? | Heinrich Böll Stiftung." *Heinrich-Böll-Stiftung* (blog). February 14, 2018. https://www.boell.de/en/2018/02/07/pakistans-cybercrime-law-boon-or-bane.

Butt, Abdullah R., and Amna Tauhidi. "Cyber Vulnerabilities of Pakistan." *CASS - Centre for Aerospace and Security Studies* (blog). February 2020. https://casstt.com/post/cyber-vulnerabilities-of-pakistan/147.

Center for Strategic and International Studies. "Significant Cyber Incidents | Center for Strategic and International Studies." *Center for Strategic and International Studies* | (blog). 2021. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

Gabbatt, Adam. "Adobe Warns 2.9 Million Customers of Data Breach After Cyber-attack (Update5)." *DataBreaches.net* (blog). October 3, 2013. https://www.databreaches.net/about/.

Groot, Juliana D. "The History of Data Breaches." *Digital Guardian* (blog). December 1, 2020. https://digitalguardian.com/blog/history-data-breaches.

Haworth, Jessica. "Data breaches are costing more than ever, as organizations take longer to detect attacks, apply patches – report." *The Daily Swig* (blog). July 28, 2021. https://portswigger.net/daily-swig/cyber-attacks#top.

Logsign Team. "What Are Real Time Security Threats?" *Logsign: Next-Gen SIEM, SOAR and Value Added Services* (blog). January 10, 2021. https://www.logsign.com/blog/what-are-real-time-security-threats/.

Masterson, Julia. "Timeline of Nuclear Diplomacy With Iran." *Arms Control Association | The Authoritative Source on Arms Control Since 1971* (blog). July 2021. https://www.armscontrol.org/factsheets/Timeline-of-Nuclear-Diplomacy-With-Iran.

Munro, André. "John J. Mearsheimer." *Encyclopedia Britannica* (blog). December 2020. https://www.britannica.com/biography/John-Mearsheimer.

Outpost24. "TOP 10 of the World's Largest Cyberattacks, and How to Prevent Them | Outpost 24 Blog." *Full Stack Risk Based Vulnerability Management Platform | Outpost 24* (blog). December 3, 2018. https://outpost24.com/blog/top-10-of-the-world-biggest-cyberattacks.

Rosenthal, Bill. *The Three Elements of Cyber Security*. Logical Operations, 2016. https://logicaloperations.com/insights/blog/446/the-three-elements-of-cyber-security/.

Rungta, Krishna. "25 Best Ethical Hacking Tools & Software for Hackers (2021)." *Meet Guru99 - Free Training Tutorials & Video for IT Courses* (blog). 2021. https://www.guru99.com/learn-everything-about-ethical-hacking-tools-and-skills.html.

Taylor, Hugh. "What Are Cyber Threats and What to Do About Them." *The Missing Report* (blog). June 16, 2021. https://preyproject.com/blog/en/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them/.

United Nations High Commissioner for Refugees. "Freedom on the Net 2016 - Pakistan." *Refworld* (blog). November 14, 2016. https://www.refworld.org/docid/5834007d6.html.

Broadcast

Rehman, Laiq U. "Security Agencies Foil Indian Cyber Attacks Against Govt, Defence Officials: ISPR." Podcast audio. August 12, 2020. https://arynews.tv/indian-cyber-attacks-defence-ispr/.

Research Journals/Periodicals

Alnagrat, Ahmed, Shakirat H. Sulyman, and Nur Adlya B. Muktar. "An Overview of Contemporary Cyberspace Activities and the Challenging Cyberspace Crimes/Threats." *Research Gate* 12, no. 3 (May 2014), 62-100. https://www.researchgate.net/publication/311953165_An_Overview_of_Contemporary_Cyberspace_Activities_and_the_Challenging_Cyberspace_Crimes Threats.

Attatfa, Amel, Karen Renaud, and Stefano D. Paoli. "Cyber Diplomacy: A Systematic Literature Review." *Procedia Computer Science* 176 (2020), 60-69. doi:10.1016/j.procs.2020.08.007.

Ayub Khan, Muhammad I. "Cyber-Warfare: Implications for the National Security of Pakistan." *NDU Journal 2019*, 2019, 117-132. https://ndu.edu.pk/ndu-journal/pub/06-Cyber-Warfare.pdf.

Awan, Jawad H., Shahzad Memon, Mahmood H. Shah, and Fawad H. Awan. "Security of eGovernment services and challenges in Pakistan." *2016 SAI Computing Conference (SAI)*, 2016, 1082-1085. doi:10.1109/sai.2016.7556112.

Baezner, Marie. "Hotspot Analysis: Regional rivalry between India Pakistan: tit-for-tat in cyberspace." *Center for Security Studies (CSS)* 1 (August 2018), 1-32. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2018-04.pdf.

Cardenas, Alvaro A., Saurabh Amin, and Shankar Sastry. "Secure Control: Towards Survivable Cyber-Physical Systems." *2008 The 28th International Conference on Distributed Computing Systems Workshops*, July 2008. doi:10.1109/icdcs.workshops.2008.40.

Dunn Cavelty, Myriam. "Cyber-Security and Threat Politics: US Efforts to Secure the Information Age." *Journal of Information Technology & Politics* 1, no. 4 (January 2008). https://www.researchgate.net/publication/277714726_Cyber-Security_and_Threat_Politics_US_Efforts_to_Secure_the_Information_Age.

Dutton, William H., Sadie Creese, Ruth Shillair, and Maria Bada. "Cyber Security Capacity: Does It Matter?" *SSRN Electronic Journal* 9 (2019), 280-306. doi:10.2139/ssrn.2938078.

Gandhi, Robin, Anup Sharma, William Mahoney, William Sousan, Qiuming Zhu, and Phillip Laplante. "Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political." *IEEE Technology and Society Magazine* 30, no. 1 (2011), 28-38. doi:10.1109/mts.2011.940293.

Jang-Jaccard, Julian, and Surya Nepal. "A survey of emerging threats in cybersecurity." *Journal of Computer and System Sciences* 80, no. 5 (2014), 973-993. doi:10.1016/j.jcss.2014.02.005.

Kanwal, Gurmeet. "Strategic Stability in South Asia: An Indian?s Perspective." *Institute for Defence Studies and Analyses (IDSA)*, June 2010. doi:10.2172/1367405.

https://www.idsa.in/idsacomments/IndiasColdStartDoctrineandStrategicStability_gkanwal_010610.

Kaponig, Hermann. "Austria's National Cyber Security and Defense Policy: Challenges and the Way Forward." *Connections: The Quarterly Journal* 19, no. 1 (2020), 21-37. doi:10.11610/connections.19.1.03.

Khan, Aarish U. "The Terrorist Threat and the Policy Response in Pakistan." *Stockholm International Peace Research Institute SIPRI* , no. 11 (September 2005). https://www.files.ethz.ch/isn/13595/Policypaper11.pdf.

Khan, Khurshid. "Understanding information warfare and its relevance to Pakistan." *Institute of Strategic Studies Islamabad*, 2011. http://www.issi.org.pk/wp-content/uploads/2014/06/1379480610_58047454.pdf.

Kundi, Ghulam M., Allah Nawaz, and Robina Akhtar. "Digital Revolution, Cyber-Crimes And Cyber Legislation: A Challenge To Governments In Developing Countries." *Cyber Crime and the Victimization of Women* 4, no. 4 (February 2014), 2225-0506. https://www.researchgate.net/publication/283316038_Digital_Revolution_Cyber-Crimes_And_Cyber_Legislation_A_Challenge_To_Governments_In_Developing_Countries.

Mohiuddin, Zibber. "A PAPER PRESENTED ON: CYBER LAWS IN PAKISTAN; A SITUATIONAL ANALYSIS AND WAY FORWARD." *Ericsson Pakistan*

(Pvt)., 2006. https://nanopdf.com/download/cyber-laws-in-pakistan-supreme-court-of-pakistan_pdf.

Mukhtar, Mudassir, Waseem Ishaque, and Muhammad S. Malik. "Natioanl Security Paradigm of Pakistan-Retrospective Analysis." *NDU Journal2019*, 2019, 187-202. https://ndu.edu.pk/ndu-journal/pub/11-National-Security-Paradigm.pdf.

Naseer, Rizwan, Musarat Amin, and Kinza Shaheen. "Cyber Security Challenges in South Asia and Room for Cyber Diplomacy." *NDU Journal*, 2020, 97-114. https://ndu.edu.pk/ndu-journal/articles/ndujournal2020/07-CYBER-SECURITY-CHALLENGES-IN-SOUTH-ASIA-AND-ROOM-FOR-CYBER-DIPLOMACY.pdf.

Patel, Asmaa. "Fifth-Generation Warfare and the Definitions of Peace." *The Journal of Intelligence, Conflict, and Warfare* 2, no. 2 (2019), 12. doi:10.21810/jicw.v2i2.1061.

Pillai, Beena G., and Madhurya J. A. "A Decentralized Data Privacy for Mobile Payment using Blockchain Technology." *International Journal of Recent Technology and Engineering (IJRTE)* 8, no. 6 (March 2020), 2277 - 3878. doi:10.35940/ijrte.2277-3878.

Rafiq, Aamna. "Challenges of Securitising Cyberspace in Pakistan." *Institute of Strategic Studies Islamabad* 39, no. 1 (2019). https://prdb.pk/article/challenges-of-securitising-cyberspace-in-pakistan-1538.

Rasool, Sadia. "Cybersecurity threat in Pakistan: causes Challenges and way forward." *INTERNATIONAL SCIENTIFIC ONLINE JOURNAL*, no. 12 (August 2015), 21-34.

http://sociobrains.com/website/w1465/file/repository/21_34_Sadia_Rasool_Cyber_security_threat_in_Pakistan_causes_challenges_and_way_forward.pdf.

Robinson, Michael, Kevin Jones, and Helge Janicke. "Cyber warfare: Issues and challenges." *Computers & Security* 49 (March 2015), 70-94. doi:10.1016/j.cose.2014.11.007.

Sadiq, Muhammad M., and Rasa Daugėlienė. "ASSESSMENT AND ENHANCEMENT OF CYBERSECURITY RISKS IN PAKISTAN." *Institute of Strategic Studies Islamabad ISSI*, December 2019. https://www.researchgate.net/publication/339051655_ASSESSMENT_AND_ENHANCEMENT_OF_CYBER_SECURITY_RISKS_IN_PAKISTAN.

Sciarrone, MarieO' N. "Cyber Warfare: The New Front." *George W Bush Institute*, no. 6 (Spring 2017). https://www.bushcenter.org/catalyst/modern-military/sciarrone-cyber-warfware.html.

Shad, Muhammad R. "Cyber Threat Landscape and Readiness Challenge of Pakistan." *Institute of Strategic Studies Islamabad ISSI,* April 2019. http://issi.org.pk/cyber-threat-landscape-and-readiness-challenge-of-pakistan/.

Shukla, Ashish, and Yaqoob U. Hassan. "PAKISTAN NEWS DIGEST A Selected Summary of News, Views and Trends from Pakistani Media." *New Media and Mass Communication*, July 2016, 16-31.

Syed, Rubab, Ahmed A. Khaver, and Muhammad Yasin. "Cyber Security: Where Does Pakistan Stand?" *Sustainable Development Policy Institute (SDPI),* February 2019. https://www.think-asia.org/bitstream/handle/11540/9714/Cyber-security-where-does-pakistan-stand%28W-167%29.pdf?sequence=1.

Tauhidi, Amna, and Aneeqa Safdar. "Is Pakistan’s Cyber Security Strong Enough to Protect the Country?" *Center for Aerospace and Security Studies*, 2021. https://casstt.com/post/is-pakistan-s-cyber-security-strong-enough-to-protect-the-country/358/j.ctvrnfqsx.8.

Trappe, Wade, and Jeremy Straub. "Journal of Cybersecurity and Privacy: A New Open Access Journal." *Journal of Cybersecurity and Privacy* 1, no. 1 (2018), 1-3. doi:10.3390/jcp1010001.

Ullah, Sultan, Muhammad Amir, Mudasser Khan, Hamid Asmat, and Kamran Habib. "Pakistan and cyber crimes: Problems and preventions." *2015 First International Conference on Anti-Cybercrime (ICACC)*, 2015. doi:10.1109/anti-cybercrime.2015.7351951.

Yamin, Tughral. "Cyberspace Management in Pakistan." *Governance and Management Review* 3, no. 1 (January 2018), 46-61. http://pu.edu.pk/images/journal/IAS/PDF/4-v3_1_18.pdf.

Government Publications

Defense Intelligence Agency. *Statement for the Record: Worldwide Threat Assessment*. USA: Defense Intelligence Agency, 2021. https://www.dia.mil/News/Speeches-and-Testimonies/Article-View/Article/2590462/statement-for-the-record-worldwide-threat-assessment/.

Federal Investigation Agency. *National Response Centre For Cyber Crime*. Islamabad: Federal Investigation Agency, 2016. https://www.nr3c.gov.pk/about_us.html.

M Akerboom, E. S. *Jihadists and the Internet 2009 update*. Netherlands: National Coordinator for Counterterrorism (NCTb), 2010. https://fas.org/irp/world/netherlands/jihadists.pdf.

Rab, Malahat. *PTA Blocks Access to Anti Islamic Video in Pakistan*. Pakistan: Pakistan Telecommunication Authority, 2012. https://pta.gov.pk/index.php/en/media-center/single-media/-pta-blocks-access-to-anti-islamic-video-in-pakistan.

SYED, MUSHAHID H. *[AS INTRODUCED IN THE SENATE] A BILL to provide for the establishment of a National Cyber Security Council*. National Cyber Security Council, 2014. https://www.senate.gov.pk/uploads/documents/1397624997_197.pdf.

Newspapers and Magazines

Ahmed, Fasih. "UAVs'Potent Force Multiplier." *Hindustan Times*, March 18, 2006. https://www.researchsnipers.com/cyber-attack-threats-increases-in-pakistan/.

Ashraf, Mubeen. "Cyber threats to Digital Pakistan." *THE NATION* (Lahore), December 31, 2019. https://nation.com.pk/31-Dec-2019/cyber-threats-to-digital-pakistan.

Bajpai, Ravi D., and Swati Parashar. "India in the 'Asian century': Thinking like a hegemon?" *DOC Research Institute – Dialogue of Civilizations* (Berlin), July 4, 2019. https://doc-research.org/2019/07/india-in-the-asian-century-thinking-like-a-hegemon/.

Baloch, Farooq, and Iftikhar Firdous. "Pakistani banks hit by biggest cyber attack in country's history." *SAMMA*, November 6, 2018.

Baloch, Farooq. "Hackers and cybersecurity." *The Express Tribune*, January 12, 2015. https://tribune.com.pk/story/820463/hackers-and-cyber-security.

https://www.samaa.tv/news/2018/11/pakistani-banks-hit-by-biggest-cyber-attack-in-countrys-history/.

Barrett, Brian. "Hack Brief: Marriott Got Hacked. Yes, Again." *WIRED* (New York), March 31, 2020. https://www.wired.com/story/marriott-hacked-yes-again-2020/.

BBC. "Credit card details on 20 million South Koreans stolen." *BBC*, January 20, 2014. https://www.bbc.com/news/technology-25808189.

BBC. "Russia gang hacks 1.2 billion usernames and passwords." *BBC News*, August 6, 2014. https://www.bbc.com/news/technology-28654613.

Business Recorder. "All set to implement 'Cyber Security Policy' by next year." *Business Recorder* (Karachi), September 17, 2021. https://www.brecorder.com/news/40120703.

Cadwalladr, Carole, and Emma G. Harrison. "Revealed: 50 million facebook profiles harvested for Cambridge Analytica in major data breach." *The Cambridge Analytica Files*, March 17, 2018. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

Coble, Sarah. "Hacker Sells Access to Pakistani Airlines' Network." *Info-security Magazine* (Virginia), November 10, 2020. https://www.infosecurity-magazine.com/news/hacker-sells-access-to-pakistani/.

Craig, Anthony, and Brandon Valeriano. "Realism and Cyber Conflict: Security in the Digital Age." E-International Relations. Last modified February 3, 2018. https://www.e-ir.info/2018/02/03/realism-and-cyber-conflict-security-in-the-digital-age/.

Cyber Defense Agency. "India is quietly preparing a cyber warfare unit to fight a new kind of enemy." *The Economic Times*, October 19, 2017. https://economictimes.indiatimes.com/news/defence/india-is-quietly-preparing-a-cyber-warfare-unit-to-fight-a-new-kind-of-enemy/articleshow/61141277.cms?from=mdr.

Davies, Vikki. "New cybersecurity policy for Pakistan." *Cyber*, August 8, 2021. https://cybermagazine.com/cyber-security/new-cybersecurity-policy-pakistan.

DAWN. "Electronic Transactions Ordinance promulgated." *DAWN* (Islamabad), September 12, 2012. https://www.dawn.com/news/56846/electronic-transactions-ordinance-promulgated.

DAWN. "Pakistan being subjected to 5th-generation warfare in 'massive way' but we are aware of threats: DG ISPR." *DAWN*, December 3, 2020. https://www.dawn.com/news/1593804.

Dunya News. "Card data of 20,000 Pakistani bank users sold on dark web: report." *Dunya News* (Karachi), November 6, 2018. https://dunyanews.tv/en/Crime/465384-Card-data-Pakistani-bank-users-sold-dark-web-report.

Finkle, Jim, and Dhanya Skariachan. "Target cyber breach hits 40 million payment cards at holiday peak." *Reuters* (Botson), December 19, 2013. https://www.reuters.com/article/us-target-breach-idUSBRE9BH1GX20131219.

Forrest, Conner. "NotPetya ransomware outbreak cost Merck more than $300M per quarter." *Teach Republic*, October 30, 2017.

https://www.techrepublic.com/article/notpetya-ransomware-outbreak-cost-merck-more-than-300m-per-quarter/.

Fruhlinger, Josh. "What is a cyber attack? Recent examples show disturbing trends." *chief security officers (CSO)*, February 27, 2020. Accessed April 10, 2020. https://www.csoonline.com/article/3237324/what-is-a-cyber-attack-recent-examples-show-disturbing-trends.html.

Hashim, Asad. "Pakistan: Thousands protest blasphemy acquittal, ignore PM's call." *Aljazeera* (Islamabad), November 1, 2018. https://www.aljazeera.com/news/2018/11/1/pakistan-thousands-protest-blasphemy-acquittal-ignore-pms-call.

Hassan, Raja T. "Cybersecurity Threats: Policy gaps, challenges and way forward." *Daily Times*, February 7, 2019. https://dailytimes.com.pk/352011/cybersecurity-threats-policy-gaps-challenges-and-way-forward/.

International Institutions and Global Governance Program. "Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms." *Council Foreign Relations*, February 23, 2018. https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms.

Kalyar, Jannat A. "Pakistan's cybersecurity regime." *DAWN*, March 2, 2020. https://www.dawn.com/news/1537766.

PEMRA. "PEMRA grants non-commercial FM Radio licence to NUMS." *Digital Association Press of Pakistan* (Islamabad), December 9, 2020.

https://www.app.com.pk/national/pemra-grants-non-commercial-fm-radio-licence-to-nums/.

Sajid, Islamuddin. "Pakistan says probing pro-India malware 'attacks'." *Politics, Asia Pecific* (Islamabad), February 25, 2021. https://www.aa.com.tr/en/asia-pacific/pakistan-says-probing-pro-india-malware-attacks/2156362.

Shah, Shafaat U. "Fifth Generation Warfare and the Challenges for Pakistan2019." *Pakistan Politico*, January 15, 2019. https://pakistanpolitico.com/fifth-generation-warfare-and-the-challenges-for-pakistan/.

Shahzad, Basit. "National cybersecurity policy and 5th generation war." *Pakistan Observer* (Islamabad), September 3, 2021. https://pakobserver.net/national-cybersecurity-policy-and-5th-generation-war-by-dr-basit-shahzad/.

Tauhidi, Amna. "Is Pakistan's cyber security strong enough to protect the country?" *Global Village Space*, May 1, 2021. https://www.globalvillagespace.com/is-pakistans-cyber-security-strong-enough-to-protect-the-country/.

Khan, M. I. "Pakistan gunmen kill 45 on Karachi Ismaili Shia bus." *BBC* (Islamabad), May 13, 2015. https://www.bbc.com/news/world-asia-32717321.

Khan, Mehwish. "7-Point Action Plan Proposed for Cyber Secure Pakistan." *ProPakistani* (Islamabad), 2013. https://propakistani.pk/2013/07/09/7-point-action-plan-proposed-for-cyber-secure-pakistan/.

Malik, Rehman. "Cyber security challenges and solutions for banks, national institutions — II." *The International News*, December 16, 2018.

https://www.thenews.com.pk/print/406447-cyber-security-challenges-and-solutions-for-banks-national-institutions-ii.

McMillan, Robert. "Siemens: Stuxnet worm hit industrial systems." *Computerworld*, September 14, 2010. https://www.computerworld.com/article/2515570/siemens--stuxnet-worm-hit-industrial-systems.html.

Perlroth, Nicole. "Yahoo Says Hackers Stole Data on 500 Million Users in 2014." *The New York Times* (San Francisco), September 22, 2016. https://www.nytimes.com/2016/09/23/technology/yahoo-hackers.html.

Safdar, Aneeqa. "The Emerging Threat of Indian Cyber Warfare Against Pakistan." *Daily Times*, August 28, 2020. https://dailytimes.com.pk/660092/the-emerging-threat-of-indian-cyber-warfare-against-pakistan/.

Siddiqui, Naveed. "Ministry of Foreign Affairs Website Hacked, Inaccessible in Several Countries." *DAWN* (Islamabad), February 16, 2019. https://www.dawn.com/news/1464217.

Snowden, Edward. "UK hacked routers to monitor Pakistan communications data: Snowden." *The Express Tribune* (Islamabad), October 6, 2015. https://tribune.com.pk/story/968194/uk-hacked-routers-to-monitor-pakistan-communications-data-snowden.

Woollacott, Emma. "Pakistan government approves new cybersecurity policy, cybercrime agency." *Daily Swing*, August 9, 2021. https://portswigger.net/daily-swig/pakistan-government-approves-new-cybersecurity-policy-cybercrime-agency.

Yusufzai, Amin. "Pakistan Ranks 67th in Index Measuring Commitment to Cyber Security." *ProPakistan*, 2017. https://propakistani.pk/2017/07/18/pakistan-ranks-67th-index-measuring-commitment-cyber-security/.

Zetter, Kim. "That Insane, $81M Bangladesh Bank Heist? Here's What We Know." *WIRED* (New York), May 17, 2016. Accessed October 17, 2020. https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/.

Research Reports

Bourne, Vanson. *Critical Infrastructure Readiness Report Holding the Line Against Cyberthreats*. Santa Clara, California: The Aspen Institute Homeland Security Program and Intel Security in advance, 2015. https://www.thehaguesecuritydelta.com/media/com_hsd/report/43/document/Critical-Infrastructure-Readiness-Report---Holding-the-Line-against-Cyberthreats.pdf.

Center for Global & Strategic Studies, and National Security Division, government of Pakistan. *Cyber Secure Pakistan Policy Framework*. Islamabad: Center for Global & Strategic Studies (CGSS), 2018. https://cgss.com.pk/publication/Publications/pdf/Event-Report-Cyber-Security.pdf.

Check Point Research. *2021 Cyber Attack Trends Mid-Year Report | Check Point Software*. US: Check Point Software Technologies LTD, 2021. https://pages.checkpoint.com/cyber-attack-2021-trends.html?utm_term=cyber-hub.

Committee on Developing a Cybersecurity Primer: Leveraging Two Decades of National Academies Work, Computer Science and Telecommunications Board, Division on Engineering and Physical Sciences, and National Research Council. *At the Nexus of Cybersecurity and Public Policy Some Basic Concepts and Issues (2014)*. Washington, DC: National Academy Press, 2014. https://www.nap.edu/catalog/18749/at-the-nexus-of-cybersecurity-and-public-policy-some-basic.

ENISA. *ENISA Threat Landscape Report 2016*. European Union Agency for Network and Information Security, 2017. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016/at_download/fullReport.

Fenz, Stefan. *Cyberspace Security: A definition and a description of remaining problems*. Information Society & E-Government, 2005. https://www.univie.ac.at/frisch/isegov/aushaengUniWien/CyberpaceSecurity_Fenz.pdf.

Haque, Jahanzaib. *Pakistan's Internet Landscape*. Islamabad: Bytes for All, Pakistan, 2013. https://www.academia.edu/9731697/Pakistans_Internet_Landscape.

Martin, Ciaran. *The Cyber Threat to UK Business 2017-2018 Report*. UK: National Cyber Security Center, 2018. https://www.ncsc.gov.uk/information/the-cyber-threat-to-uk-business-2017-2018-report.

Moteff, John, and Paul Parfomak. *Critical Infrastructure and Key Assets: Definition and Identification*. USA: Resources, Science, and Industry Division, CRS Report for Congress, 2004. https://sgp.fas.org/crs/RL32631.pdf.

OSAC. *Pakistan 2020 Crime & Safety Report: Islamabad*. Islamabad: OSAC, 2020. https://www.osac.gov/Content/Report/f36dd7e9-8cf3-489c-b9b4-187819994ff8.

Tertiary Sources

Australian Computer Society (ACS). "Cybersecurity - Threats, Challenges, Opportunities." ACS - The Professional Association for Australia's ICT Sector. Last modified November 2016. https://www.acs.org.au/insightsandpublications/reports-publications/cybersecurity-threats-challenges-opportunities.html.

Cabinet Division. "E-MAIL & INTERNET POLICY FORTHE FEDERAL GOVERNMENT." Cabinet Division. Accessed August 8, 2020. https://cabinet.gov.pk/SiteImage/Policy/internet-and-emails-policy.pdf.

KPMG. "Dealing with cyber threat is a complex challenge." KPMG. Last modified March 1, 2017. https://home.kpmg/qm/en/home/about.html.

Wikipedia, the Free Encyclopedia. "PlayStation 3." In *Wikipedia, the Free Encyclopedia*. 2001. Accessed March 7, 2020. https://en.wikipedia.org/wiki/PlayStation_3.