KINNAIRD COLLEGE FOR WOMEN

HYBRID WARFARE: CYBER PROXIES AND INDIRECT APPROACH BETWEEN INDIA AND PAKISTAN (2014-2021)

AYESHA BABAR

SAADIA BABAR

F19BAIR003

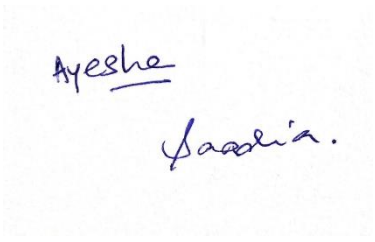
F19BAIR031

DEPARTMENT OF INTERNATIONAL RELATIONS

KINNAIRD COLLEGE FOR WOMEN

LAHORE, PAKISTAN

2019-2023



HYBRID WARFARE: CYBER PROXIES AND INDIRECT APPROACH BETWEEN INDIA AND PAKISTAN (2014-2021)

A THESIS SUBMITTED TO

KINNAIRD COLLEGE FOR WOMEN

IN FULFILMENT OF THE REQUIREMENTS

FOR THE DEGREE OF

BACHELORS HONORS

IN

INTERNATIONAL RELATIONS

BY

AYESHA BABAR

SAADIA BABAR

DEPARTMENT OF INTERNATIONAL RELATIONS

KINNAIRD COLLEGE FOR WOMEN, LAHORE

2019-2023

RESEARCH COMPLETION CERTIFICATE

It is certified that Ms. Ayesha Babar and Ms. Saadia Babar, of BA/BSc (session 2019 – 2023), Department of International Relations have carried out research work entitled **Hybrid Warfare: Cyber Proxies and Indirect Approach between India and Pakistan (2014-2021)** under my supervision.

It is assured that research work is original and has not yet been published anywhere else.

"All changes suggested by examiners during defense are incorporated in this final copy".

Signatures of Supervisor

Designation

Dated: May 18th, 2023

Signatures

Head of Department

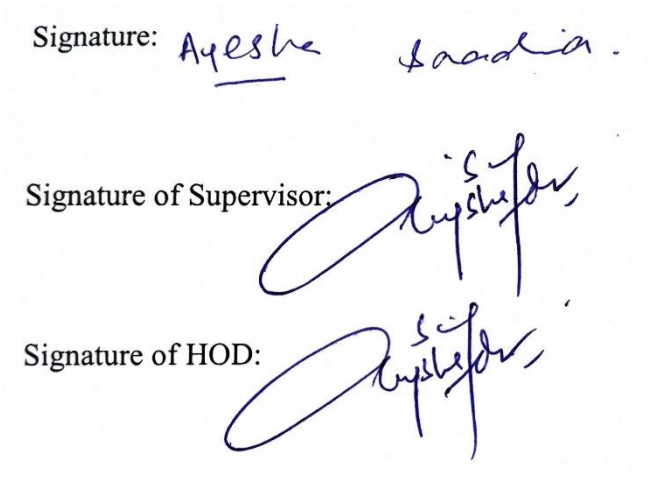
ANTI-PLAGIARISM DECLARATION

We certify that this is our own research work. The work has not, in whole or in part, been presented elsewhere for assessment. Where material has been used from other sources, it has been properly acknowledged. The similarity index of the research report is 11%. If this statement is untrue and we are found guilty of plagiarism, the punitive actions against us should be taken as per Kinnaird Anti Plagiarism Policy.

Names of the students: Ayesha Babar and Saadia Babar

Registration No: F19BAIR003 & F19BAIR031

Program: BA IR



ACKNOWLEDGMENTS

We would like to extend our deepest gratitude to the Principal Kinnaird College, Prof. Dr. Rukhsana David and Vice-Principal Kinnaird College, Prof. Dr. Nikhat Khan for providing us the opportunity to conduct our research, and for all the resources and support they provided. We are also extremely indebted to our research supervisor, Dr. Ayisha Safdar, for providing her unwavering support, guidance, and valuable feedback which has played an instrumental role in the success of this thesis research. We extend our sincere thanks to the instructors at the International Relations Department for their valuable insights, support and encouragement. Lastly, we are deeply thankful to our mother for supporting us throughout the process. The journey would not have been possible without her love and support.

Signatures

Ayesha Babar

F19BAIR003

Saadia Babar

F19BAIR031

ABSTRACT

The rapid advancements in the field of information technology alongside the information revolution has put states in the midst of a complex cybersecurity landscape in which all states are increasing and advancing their cybersecurity infrastructure to protect themselves from cyberattacks which pose a potential threat to their critical information infrastructure. The study of cyberspace and cyberattacks is therefore critical in current times because this domain is emerging as the arena for advanced geopolitical competition due to the nature of threat –cyber threats cannot be seen and are harder to detect, cyberattacks are transnational and sometimes transcontinental, and can be one of the tool for coercive diplomacy. When discussing geopolitical competition and tensions, South Asian region is of particular significance due to the relations of two nuclear-powers, India and Pakistan. Cyberspace offers these two countries a new domain for competition and both countries have formulate their respective National Security Policies in the face of emerging cyber threats from each other. This thesis evaluates the cybersecurity landscape of India and Pakistan with regards to threats and perceptions. It then discusses the policy responses of both countries and the nature of advancements in the domain cybersecurity –offensive or defensive, while highlighting the role of cyber proxies as an instrument of hybrid warfare. The research utilises Indirect Approach by Basil Liddell Hart as cyber threats cannot be seen and are hard to detect which puts the emery state at a vulnerable position. The research concludes at several recommendations for Pakistan to develop a comprehensive security framework.

TABLE OF CONTENTS

RESEARCH COMPLETION CERTIFICATE ii
ANTI-PLAGIARISM DECLARATION iii
ACKNOWLEDGMENTS iv
ABSTRACT v
TABLE OF CONTENTS vi
LIST OF FIGURES ix
LIST OF ABBREVIATIONS x
CHAPTER 1 1
1.1 Introduction 1
1.2 Significance of the Study 3
1.3 Purpose and Design of the Study 3
1.3.1 Aims and Objectives of the Study 3
1.3.2 Research Questions 4
1.4 Nature of the Study 4
1.5 Literature Review 4
CHAPTER 2 7
HYBRID WARFARE AND INDIRECT APPROACH: CONCEPT, ORIGIN AND MAIN POSTULATES 7
2.1 Introduction 7
2.2 Origin of Indirect Approach 7
2.3 Conceptualizing Strategy 10
2.4 The Indirect Approach 11
2.5 Eight Axioms of the Indirect Approach 12
2.6 Psychology of the Enemy 17
2.7 Linking Indirect Approach and Hybrid Warfare 18
CHAPTER 3 22
CYBER SECURITY LANDSCAPE OF INDIA AND PAKISTAN: EVALUATING THREATS AND PREPAREDNESS 22
3.1 Introduction 22
3.2 Cyberspace and Cyber Threat: Conceptual Understanding 23
3.3 Understanding Cyber Proxies 23

3.3 International Law governing Cyberspace 25
3.3.1 Developments in the Past Decade in International Law governing Cyberspace 28
3.4 Cyber Threat Landscape of India and Pakistan 31
3.5 Policy Responses: Evaluating National Cyber Security Policies and Cyber Governance of Pakistan 32
3.6 Policy Responses: Evaluating National Cyber Security Policies and Cyber Governance of India 34
3.7 The Challenge of Cyber Threat Readiness: Gauging Preparedness of India and Pakistan 37
CHAPTER 4 40
NATURE OF CYBER WARFARE BETWEEN INDIA AND PAKISTAN: OFFSENSIVE OR DEFENSIVE? 40
4.1 Introduction 40
4.2 Cyber Security Threat Landscape of South Asia 40
4.3 Nature of India's Cyberwarfare: Offensive or Defensive? 42
4.4 Composition of India's Cybersecurity Domain 42
4.5 India's Cyberspace Policies and Legal Frameworks 43
4.6 Nature of Cyberattacks by India 44
4.7 Nature of Pakistan's Cyberwarfare: Offensive or Defensive? 45
4.8 Composition of Pakistan's Cybersecurity Domain 46
4.9 Pakistan's Cyberspace Policies and Legal Frameworks 46
4.10 Nature of Cyberattacks by Pakistan 47
CHAPTER 5 50
INFLUENCE OPERATIONS AS INSTRUMENTS OF HYBRID WARFARE BETWEEN INDIA-PAKISTAN & SECURITY IMPLICATIONS 50
5.1 Introduction 50
5.2 Understanding Influence Operations: An Instrument of Hybrid Warfare? 51
5.3 India's Influence Operations against Pakistan: Deconstructing the Indian Modus Operandi 51
5.3.1 International Defamation: The 'Indian Chronicles' Influence Operation against Pakistan 52
5.3.2 Political Instability: Indian Propaganda Campaign in Balochistan and Against State Institutions 53
5.3.3 Economic Slowdown: The FATF Grey List 54
5.4 Indian Perspective 55
5.4.1 The Cyber Tit-for-Tat between India and Pakistan 56

5.4.2 Cyber Terrorism 57
5.4.3 The Threat of Disinformation and Propaganda 57
5.5 Security Implications: The Future of Strategic Stability in South Asia Amidst Cyber Threats 58
CHAPTER 6 61
RECOMMENDATIONS FOR PAKISTAN: STEPS TOWARDS DEVELOPING COMPREHENSIVE CYBERSECURITY FRAMEWORK 61
6.1 Introduction 61
6.2.1 Creation of a Cyber Policy Centre 62
6.2.2 Establishment of National Cyber Security Authority (NCSA) 62
6.2.3 Creation of Strategic Cyber Security Guideline 63
6.2.4 Cyber Diplomacy 64
6.2.5 Confidence Building Measures (CBMs) 65
CHAPTER 7 68
CONCLUSION 68
REFERENCES 73
SIMILARITY INDEX REPORT 81

LIST OF FIGURES

Figure 2.1	Liddell Heart's Indirect Approach
Figure 2.2	Operation Overload 1944
Figure 2.3	Map of Second Punic War 218 BCE Displaying Strategic Route of Hannibal's Forces
Figure 2.4	The Hybrid Warfare Concept
Figure 3.1	The Beneficiary-Proxy Relationship as Conceptualised by Tim Maurer
Figure 3.2	Cyber Security Composition
Figure 3.3	Spectrum of Traditional and Irregular Warfare
Figure 3.4	Tiers of Cyber Environment
Figure 3.5	The Current Cyber Security Landscape of Pakistan
Figure 3.6	India's Cyber Legislation Timeline
Figure 3.7	India's Cyber Security Institutional Landscape
Figure 5.1	Doval Doctrine: India's offensive Hybrid Warfare Strategy against Pakistan
Figure 5.2	Chronology of India-Pakistan's Cyber Tit-for-Tat since 2014
Figure 6. 1	Cybersecurity Guideline Response Framework

LIST OF ABBREVIATIONS

ATM	Automated Teller Machine
ANI	Asian News International
APT	Advanced Persistent Threat
BLA	Baloch Liberation Army
BMD	Ballistic Missile Defence
CCDCOE	Cooperative Cyber Defence Center of Excellence
CBM	Confidence Building Measure
CERT	Computer Emergency Response Team
CERT-IN	Computer Emergency Response Team India
CCRA	Common Criteria Recognition Arrangements
CGPC	Cyber Governance Policy Committee
DoT	Department of Technology
DeitY	Department of Electronics and Information Technology
DoP	Department of Posts
EU	European Union
FATF	Financial Action Task Force
GGE	Group of Governmental Experts
GSI	Global Security Index
HEC	Higher Education Commission
IAEA	International Atomic Energy Commission
ICT	Information and Communication Technology
IT	Internet Technology
ITU	International Telecommunication Union
IISS	International Institute of Strategic Studies
ISPR	Inter-Service Public Relations
ISR	Intelligence Surveillance Reconnaissance

JeM	Jaish-e-Muhammad
LeT	Lashkar-e-Taiba
LoC	Line of Control
NATO	North Atlantic Treaty Organization
NCCS	National Center for Cyber Security
NCSA	National Cyber Security Authority
NCSC	National Cyber Security Coordinator
NCSP	National Cyber Security Policy
NSA	National Security Advisor
NCIIPC	National Critical Information Infrastructure Protection Centre
NCCS	National Center of Cyber Security
NCII	National Critical Information Infrastructures
NR3C	National Response Center for Cyber Crime
MLAT	Mutual Legal Assistance Treaties
Pak-CERT	Pakistan Computer Emergency Response Team
PTA	Pakistan Telecommunication Authority
PLI	Postal Life Insurance
RPLI	Rural Postal Life Insurance
SBP	State Bank of Pakistan
UNGGE	United Nations Group of Governmental Experts

CHAPTER 1

1.1 Introduction

Asia is the largest continent out of all the world's seven continents and has wide-ranging natural resources, physical landscapes, and political units. The seven countries which make up the South Asian region include Pakistan, India, Bangladesh, Nepal, Bhutan, Sri Lanka, and Afghanistan. South Asia is extremely vital for trade routes and water resources but region's lack of integration, border issues, poverty, terrorism, and lack of multilateral trade makes this region a complex one. The relations of two nuclear-powers, India and Pakistan, and their dispute on the territory of Kashmir has given birth to some of the major security issues in South Asia. Therefore, the dichotomy of mismatched opportunities and capacities, security and insecurities, connections and disconnections has led South Asia to be an unstable region.

At the beginning of the 21st century, information, and communication technology (ICT) witnessed a revolution wherein everyone, including states, non-state actors and individuals increasingly shifted to internet and technology. While the hyper-reliance on ICT has generated interconnectivity, this reliance has also brought numerous challenges, vulnerabilities, and threats such as cyber-threats, cyber wars, cyber proxies, and influence operations. Cyber-attacks and cyber proxies have the potential to generate conflicts which can have implications for the national security of the state as state-backed hackers usually steal sensitive data of rival states and engage in misinformation campaigns. A similar atmosphere of threat has also emerged in the South Asian security landscape between India and Pakistan.

Pakistan's cyber threat landscape is characterized by its increased dependence upon the ICT infrastructures which increases the degree of vulnerability for the national security. The annual 2020 report of Global Security Index (GSI) ranked Pakistan at 79th out of 193 countries in terms of policies and commitment to cybersecurity whereas India was ranked at 10th. Insufficient legal and technical measures, coupled with internal and external security challenges, make Pakistan vulnerable to various cyber threats. India's cyber threat landscape is also characterized by cyberwars which break out every now and then. Contrary to India's image as a cyber-power, it does lack security frameworks due to lack of cybersecurity experts in the country. Apart from

internal security challenges, the country's national security also becomes vulnerable because India's rising status puts the sensitive systems at a constant threat of penetration. While domestic agencies may have discovered some of the intrusions, many other intrusions have been discovered by external agencies which point at country's capacity building to be done in its security infrastructure. However, since 2014, Nardenra Modi regime's rise to power, India has adopted more offensive approach towards Pakistan due to its superiority and advancements in the cyber domain. With conventional means of warfare, non-conventional warfare has also been equal importance. This can be witnessed in the post-Pulwama incident in 2019 wherein along with the heightened tensions on the disputed region of Kashmir, a massive surge in cyber-attacks from India, and in return Pakistan, also surfaced and a mode of hybrid warfare was created.

The Indirect Approach best captures the concept of cyber warfare and cyber threats especially between India and Pakistan. The Indirect Approach is a strategy formulated by British military strategist Basil Liddell Hart. According to the Indirect Approach, Liddell Hart emphasises that the means of war must be applied in a way to exploit the movement of the enemy, leaving them unprepared. In this indirect fashion, the enemy is taken by the element of surprise which allows the opportunity to exploit the enemy's before their recovery and achieve maximal gains. The Indirect Approach is then linked with the hybrid warfare theory as the elements of Liddell Hart's approach of deploying conventional and unconventional methods of warfare together is captured in the hybrid warfare theory. Frank Hoffman, a former United States Senior Director of Naval Capabilities and Readiness, was the first person to propose the concept of "hybrid warfare" as he envisioned the rise of hybrid warfare in 2005. The hybrid warfare theory proposes that while regular means of warfare have been deployed by states, the states may in future lead to a combined regular and an irregular method of warfare. Hoffman's idea of irregular warfare was the use of cyber threats such as influence operations, mass propaganda, foreign electoral intrusion, and fake news by the states. According to him, the converging modes of both regular and irregular warfare will fuse together into the variant of hybrid warfare wherein the threat to those targeted as well as its implications will be increased.

Pakistan and India are no exceptions when it comes to troubled bilateral relations due to cyber intrusions and cyber-attacks. While no major cyberwar has been declared, both the countries are regularly involved in small-scale cyber-attacks and cyber intrusions by the means of cyber-proxies

and with the intention of either defacing governmental websites or media houses or stealing any data that might be helpful in generating an incentive against the other state. Therefore, this study utilises the Indirect Approach to understand the indirect method of warfare, cyber-proxies and influence operations being employed within South Asia between the dynamic of the two highly securitized arch-rivals, Pakistan and India.

1.2 Significance of the Study

This study is a contemporary and emerging study that adds information to the existing literature via bridging research gaps and contextualizing the study in South Asian perspective. As the domain of cybersecurity has become increasingly complex bearing far-reaching implications, the study aims to analyse one of the most important dimension in this regard which is cyber security. By analysing the role of cyber-proxies in the highly securitized India-Pakistan relationship, it attempts to provide an understanding of the emerging cyber security threats which cyber proxies pose to the two countries and subsequently to the South Asian region as a whole. With this understanding, the study seeks to impart an insight for the prevention of emerging threats from cyber-proxies between India and Pakistan and the steps Pakistan can take in the face of emerging cyber security threats.

1.3 Purpose and Design of the Study

1.3.1 Aims and Objectives of the Study

The study aims at understanding the security implications that cyber-proxies constitute in India and Pakistan's relationship.

It, therefore, seeks to understand:

- The main postulates of Basil Liddell Hart's Indirect Approach.
- The individual security infrastructure of India and Pakistan and the importance of cyber-proxies in it.
- The nature of cyberwarfare (offensive or defensive) adopted by India and Pakistan.

- The emerging role cyber-proxies and influence operation in the balance of power between India and Pakistan and its security implications.
- Recommendations for Pakistan in the face of emerging cyber threats.

1.3.2 Research Questions

The study is guided by the following research questions:

- What is the Indirect Approach by Basil Liddell Hart and how can it be utilized to examine the emerging security threats from cyber-proxies between India and Pakistan?
- What is the individual security infrastructure of India and Pakistan and what role do cyber-proxies play in it?
- What is the nature of cyber-warfare adopted in the security profiles of India and Pakistan?
- How are cyber proxies and influence-operations being deployed as an instrument of hybrid warfare between India and Pakistan and what are the security implications?
- What are the steps Pakistan can take in the face of emerging cyber threats?

1.4 Nature of the Study

In this study, a case oriented qualitative research design is selected for analysing the emerging role of cyber-proxies in the India-Pakistan relationship. The case study application generates a qualitative analysis to understand the security implications of cyber-proxies specifically on India, Pakistan, and the region. The study also utilizes correlational research to understand the causal relationship between cyber-proxies and security. Additionally, the study is descriptive as it utilizes primary and secondary data for the analysis of characteristics of cyber-proxies in the security profiles of India and Pakistan.

1.5 Literature Review

Time Maurer in his book Cyber Mercenaries: The State, Hackers, and Power has explored the secretive state-proxy relationships and the common challenge it poses for global security and the state itself as the cyberspace becomes the new arena of geopolitics. Maurer's argument hinges on the idea that states use proxies to project power, maintain deniability, escape from the developing cyberspace international laws, and avoid direct conflict. Therefore, understanding the state-proxy relationship is important to understand so states can better their defence in the face of undetectable and continuously refining tactics. He presents his own typology of organization of state-proxy

relation whereby states either 1) delegate authority 2) orchestrate the relationship or 3) sanction even proxy's malicious behaviour. He analyses them in cases of United Sates, Iran, and Russia respectively while concluding that the US model of having a tight grip on their proxies ensure best state security out of all models. For international security, he suggests his DIM(LE) model of diplomacy, information, military, economic, and law enforcement instruments to influence a state's relationship to their proxy (Maurer, 2017).

Ben Buchanan in his book The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations characterizes the cybersecurity dilemma and its application whilst arguing for the failure of traditional security-dilemma mitigation techniques in the cyberspace. Buchanan's three pillars of cybersecurity dilemma is constituted by 1) state's pre-emptive action in cyberspace to gain advantage 2) sophisticated states have defensive reasons for such attacks 3) all attacks and intrusions are seen threatening to a state. He uses network intrusions to explain his model ultimately arguing that obscurity pertaining to capabilities and intents of other states makes the cybersecurity dilemma worse. Therefore, traditional security-dilemma mitigation techniques like offence-defence balance are virtually ineffective due to the heavy shift of balance in favour of offensiveness. Buchanan however does offer his own mitigating practices for the cybersecurity dilemma which include greater information sharing among states and more bilateral and multilateral trust (Buchanan, 2017).

Jamie Collier in his article Proxy Actors in the Cyber Domain finds the appeal of cyber proxy actors to individual states and helps in categorizing non-state actors involved in the cyberspace and available to the state. The analysis generated hinges upon the idea that states own deficiencies primarily compel them to work with available actors from the private sector, hacker groups, civil and volunteer militias and organised crime groups. It is found out that even with state deficiencies, states still have more leverage on the degree of their involvement with these actors. Collier also finds that trends to opt for proxies are likely going to rise in the future as well as other non-state actors to emerge since entry to the cyberspace has insignificant barriers, making the state stand at the centre of complex strategic decision-making (Collier, 2017).

Authors Borghard & Lonergan's primarily thesis in their article Can States Calculate the Risks of Using Cyber Proxies is that states face two fundamental national security dilemmas by employing cyber proxies that are the Promethean dilemma and dilemma of inadvertent crisis escalation. The

former is a dilemma whereby the proxies may use the same tools against the patron state and the later dilemma is a scenario whereby cyber proxies may expand their mandate also threatening the state. As the authors identify future trends of state employment of cyber proxies, it is suggested that states mitigate these twin dilemmas by incentivizing cyber proxies with benefits of reciprocity such as with economically motivated actors or providing less capabilities to politically motivated actors in order to reduce risks (Borghard & Lonergan, 2016).

Rebecca A. Keller in her article Influence Operations and the Internet: A 21st Century Issue traces the history of influence operations and describes two main types of influence operation which state actors may employ to achieve and maintain information superiority, and these two types of information operations include psychological operations and military deception. She then highlights the impacts of influence operations and explains how cyber advancements allow individuals to reach a global audience but simultaneously it also puts states at a vulnerable position of cyber-attacks to which states have to tackle immediately. She concludes her article by presenting an overview of challenges to effective information operations. (Keller, 2010).

Christopher Whyte in his article Cyber Conflict or Democracy "Hacked"? How Cyber Operations Enhance Information Warfare study and evaluate the effect of cyber information operations on democracies. He presents the view that in the sophisticated digital age, cyber operations puts the democratic functionality of a state in a vulnerable position as there may arise multifaceted unprecedented challenges which may subvert the traditional mechanisms of a democracy. To support his arguments and to illustrate the concept of democracy hacking, he presents a case study of 2016 US Presidential Elections wherein Russian and Russian affiliated hackers gained access to private information and stole wide range of private information which was then distributed among sources through social media to exacerbate political and social divisions within the country to harm the specific political targets of the election campaign. He draws the conclusion that these challenges and threats might increase in future, therefore, states must develop technologies and policies to tackle and to quickly react to these threats (Whyte, 2020).

CHAPTER 2

HYBRID WARFARE AND INDIRECT APPROACH: CONCEPT, ORIGIN AND MAIN POSTULATES

2.1 Introduction

Hybrid warfare, hybrid threats and cyber proxies have increasingly placed themselves at the heart of policies and strategies of the twenty first century style warfare due to the rapid development in the digital realm that has further highlighted the grey areas that exist in the international relations. This digital warfare differs itself from the traditional warfare in intensity and degree as it allows to undermine enemy's political system, communities, social cohesion and strategies, at a low cost, by empowering virtual tools that help in achieving the aims of a war without launching an attack –such as through data breaches, hacking, cyber proxies, influence operations, information and disinformation campaigns, war propaganda. This twenty first century style warfare is related to, and best captured in the concept and idea proposed by Liddell Hart, known as the Indirect Approach.

Basil Henry Liddell Hart is one of the most widely read British military strategist and historian of the modern time due to his comprehensive strategy that he proposed highlighting the use of technology ultimately formulating an integrated vision and strategy of warfare that is just not only applicable by military forces, but also by governments to achieve political aims, and by non-state actors in current times to disrupt databases and communities of the enemy country through cyber operations. Liddell Hart's strategy of Indirect Approach comes as a response to misinterpretation of Clausewitzian military thought and the advancements in technology that defined the destruction brought by the First World War and Second World War that demanded a new integrated strategy.

2.2 Origin of Indirect Approach

The origins of Liddell Hart's Indirect Approach can be traced from two perspectives namely the theoretical perspective and the empirical perspective. If we trace it from a theoretical perspective,

Liddell Hart's Indirect Approach comes a response to political and military leaders who he thinks misunderstood and misinterpreted the military strategy of a 19th century military strategist, Carl Von Clausewitz. However, from an empirical perspective, Liddell Hart's approach comes from the experiences of the First and Second World War such as the trench stalemate in the First World War alongside the ariel and mechanized battles against Adolf Hitler. After the World War I, Liddell Hart wrote in detail about the infantry tactics and called them as the "Man in Dark Formula" which he later described in his monumental essay "Man in Dark" that was published in June 1920. The formula was used to describe and visualize combined armed maneuvers utilizing mobile-platoon sized units and to drive attention to the potential of mechanized warfare to achieve a strategic advantage over the enemy. His goal was to avoid the bloodshed during wars and the destructive frontal assaults and instead achieve victory and success through maneuvers via platoon-sized mobile units.

Furthermore, Hart researched deeply on the infiltration tactics and strategic levels of wars and in 1929, he wrote about these in his book named "The Decisive Wars of History" in which he combined and recommended tactical infiltration and strategies alongside the deployment of an indirect approach. The main idea that he propagated for in his work was to delay the battle until the morale of enemy was weakened and to attack the enemy where they least expect it. The psychological dislocation is thus an important tool to achieve a strategic victory in an indirect manner. Liddell Hart also called the strategy of psychological dislocation as strategic penetration.

Moreover, Liddell Hart argues that the misapplication and poor understanding of Clausewitzian strategy led to bloodbaths in the World Wars, which ultimately called into question a new advanced military strategy answering how military force and strategies can be applied to achieve political aims, while also challenging the implication and results of old military strategies.

In addition, the increasing importance of airpower and sea power alongside the introduction and use of mechanized land forces called for a new or revised interpretation of Clausewitz. During the Great War, Germany had been choked by sea power and those who were looking after air forces during the interwar period also greatly failed to recognize the shift in technology that was occurring during that period. In addition, those who had airpower now had the power to strike at enemy's economy and communities without even launching an attack on the ground, all because of the advancements in technology. Similarly, the introduction of new mechanized vehicles and

strategies which led to a mechanized warfare, also led states to collapse the enemy without any direct attack such as by disrupting their control system, launching influence operations or by cutting supply lines. Each of these strategies are now collectively represented in Basil Liddell Hart's Indirect Approach.

Furthermore, the concept of mechanized warfare was not only merely a speculation. It can be witnessed that in the beginning of Second World War, Germany used the strategy of 'Blitzkrieg' or 'Lightening Warfare' which was carried out by a small number of mechanized units with support of Germany's airpower which led it to get control over Poland and France in an effective manner with relatively less bloodshed. In addition, Allied powers also pulled an air operation through communication networks to invade Continental Europe in order to hinder Germany and its ability to launch a counterattack.

In its main essence, the advancement of technology and mechanized warfare alongside new air, sea and land developments expanded the range of options to attack and also stakeholders that were attacked. This implies that these advancements had an effect on the formulation of military aims which could be seen as: increased direct attack against civilian objectives and new ways of crippling enemy's economy and military without launching a direct attack on their ground. At the end, Liddell Hart says that "the sum effect of the advent of this multiplied mobility, both on ground and on air, was to increase the power and importance of strategy relative to tactics which required fresh strategic thinking".

While these first hand experiences of the Great War provided a theoretical and intellectual analysis and roots for the strategies of the Indirect Approach, Liddell Hart's approach is also based on a much larger body of historical analysis, dating back to ancient strategies of warfare. To formulate strategy, Basil Liddell Hart, as a military strategist, has examined wars from the fifth century B.C to the middle of the twentieth century which include "Greek Wars, Roman Wars, Medieval Wars, Napoleonic Wars, and the two World Wars". Each of these wars have served as a case study which Liddell Hart has examined to analyze how wars have been successfully waged in the history. In addition to this, Liddell Hart as a military strategist also examined long periods of history and the period between major wars, alongside surveying a big range of military history which is then ultimately presented in his book known as Strategy. In this essence, Liddell Hart while describing his approach and philosophy with regards to the nature of war studies mentions, "It is not the realm

of human pursuit suited to abstract mathematical theorizing, but rather an endeavor dominated by understanding the importance of psychology and the human experience".

2.3 Conceptualizing Strategy

The word strategy is derived from two Greek words stratëgos (leader or general) and stratëgia (leadership or general-ship). Historically, the term and the study of term itself has been associated with the study of military strategies. In modern strategic studies, Carl von Clausewitz, a German Major-General has defined strategy as "the art of employment of battles as a means to gain objectives of war". In defining strategy, Liddell Hart stands against Carl von Clausewitz in how he attempts to define strategy. According to Liddell Hart, this definition is flawed in two ways. Firstly, "it intrudes on the sphere of policy, or the higher conduct of war, which must necessarily be the responsibility of the government and not the military leaders it employs as its agents in the executive control of operations". Secondly, "the definition unnecessarily stress the importance of engaging the enemy as the only means to achieve a strategic end, which leads to a profound heresy, that all efforts in the war should focus on setting up and fighting a decisive battle". Put simply, according to Liddell Hart, the definition proposed by Clausewitz placed heavy emphasis on battles and that they are the only means to fulfill military means to gain strategic end. In an attempt to understand strategy, Liddell Hart aligns himself with the Chinese military strategist who proposed the strategy and art of war in terms of subduing the enemy with less resources involved and by deception and surprise.

Furthermore, in an attempt to define strategy, Liddell Hart had aligned himself with a German General, Helmuth von Moltke the Younger who has defined strategy as "the practical adaptation of the means placed at a General's disposal to the attainment of the objective in view". Liddell Hart himself adopted a wider approach and defined strategy as "the art of distributing and applying military means to fulfil the ends of policy." According to him, the aim of the war should be "to coordinate and direct all the resources of a nation, or bands of nations, towards the attainment of the political objective of war –the goal defined by fundamental policy." He believed that strategy should aim to achieve objectives with the least amount of resources utilized and casualties possible. For a strategy to be successful, it is vital that the calculation of the outcome of war is sound and that resources are in coordination with the means and ends. He also emphasized the importance of

flexibility and adaptability in strategy, as well as the need to constantly reassess and adjust plans based on changing circumstances. Overall, Liddell Hart's definition of strategy focuses on the connection between military means and political ends, and the importance of achieving those ends efficiently and effectively.

In addition, what sets Liddell Hart apart from previous military strategists is the belief and the application of grand strategy. Liddell Hart believed that grand strategy is the highest level of strategy, which deals with the coordination and direction of all resources of a nation, or a group of nations, towards the attainment of the political objectives of the state. He argued that grand strategy requires a long-term perspective and a deep understanding of the political, social, and economic factors that shape the international environment. Moreover, he stressed that grand strategy should aim to achieve victory by indirect means, such as psychological, economic, and political pressure, rather than by direct military confrontation. According to Liddell Hart, the art of Grand Strategy is to secure the ends of policy with the least possible cost and risk, and to avoid the exhaustion of the nation's resources and willpower. For him, the grand strategy should be utilized to achieve the political objectives of the nation which is also the function of strategy during the war, therefore war and grand strategy are inseparable as grand strategy guides the actions of a state during the war and serves as the conduct of war.

2.4 The Indirect Approach

Liddell Hart's Indirect Approach is a strategic concept that emphasizes the use of surprise, deception, and psychological pressure to overcome the enemy's resistance with the least amount of force possible. He believed that the direct approach, which involves attacking the enemy head-on, is often costly and ineffective, and can lead to prolonged and bloody wars. In contrast, the indirect approach, that he offered, seeks to bypass the enemy's main strength, attack its weak points, and create confusion and disorganization among its forces. By doing so, the indirect approach can disrupt the enemy's plans and morale, and force it to make mistakes and expose its vulnerabilities. Liddell Hart argued that the Indirect Approach requires a deep understanding of the enemy's psychology, culture, and strategy, as well as the ability to anticipate its reactions and exploit its weaknesses. According to him, two things were essential to gain a strategic edge, and often win, against enemy. These two things included: dislocation and exploitation, which are also

explained by him in his eight axioms of the Indirect Approach that define the mindset one should have before and during launching an undetected attack on the enemy so that the enemy can be strategically dislocated and exploited at an early stage. In other words, one should concentrate strength where enemy has the least strength to cause an asymmetric matchup to dislocate and disperse the enemy from the places where he is least concentrated, as according to him, the true objective of war is calculated dispersion instead of concentration of force at one place.

Liddell Hart's Indirect Approach

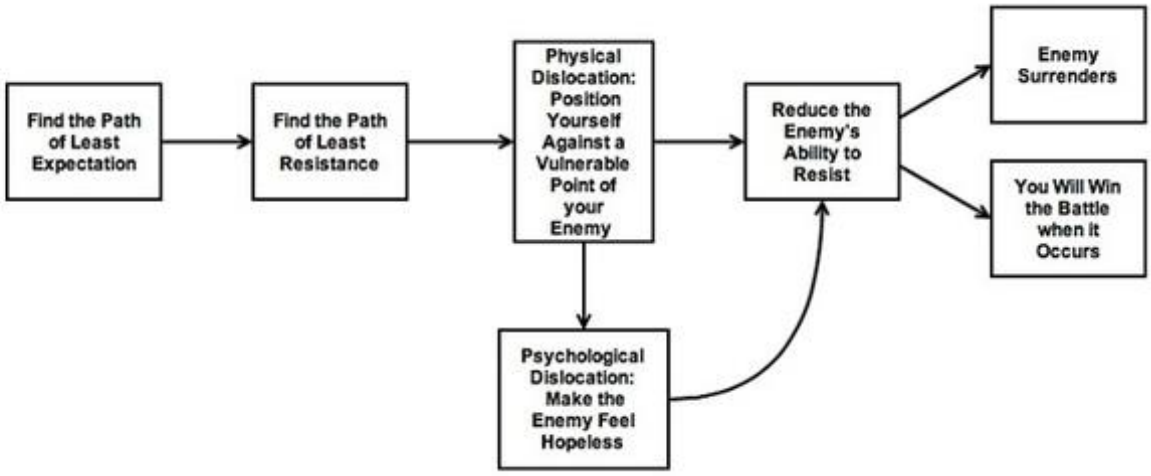


Figure 2.1

2.5 Eight Axioms of the Indirect Approach

Basil Liddell Hart has presented eight axioms, six positive and two negative, that serve as a checklist in the application of his Indirect Approach and provide framework for the tactical execution of the indirect strategy. In his words, these eight axioms are:

1. Adjust your end to your means

2. Keep your object always in mind

3. Choose the line (or course) of least expectation

4. Exploit the line of least resistance

5. Take a line of operation which offers alternative objectives

6. Ensure that both plan and dispositions are flexible – adaptable to circumstances

7. Do not throw your weight into a stroke whilst your opponent is on guard

8. Do not renew an attack along the same line (or in the same form) after it has once failed (Liddell Hart, 1967)

The first axiom represents the idea that for indirect approach to be successful, or for that matter, for any military strategy to be successful, it is essential that the political ends must be in line with the military means. This implies that states should consider and evaluate their military capability and the political objectives of the war should not exceed the military capabilities of the state because military might serve as a tool to achieve political objectives. Furthermore, he propagated the idea of "limited aim" which is a wise idea essentially because one should adjust ends as per means and avoid unnecessary use of resources where there is a little chance of winning. Liddell Hart's goal of minimum bloodshed during war and a successful war strategy would fail if any of these axiom is not implemented as mentioned by him.

The second axiom related to objective of the war is another significant idea presented by Liddell Hart under his indirect approach. According to Hart, there is a difference between political means and military objectives during a war and these two should be dealt distinctively while the confusion around the word "objective" should be eliminated as the political and military objectives should be signified differently. In doing so, Hart offers an alternative and suggests that the word "objective" should be used to define the policy goals of a state during war while the word "military aim" should be used to define the military goals and the way forces will achieve a certain policy goal. In addition, he emphasizes on the significance of aligning political ends with military means as the attainment of political objectives ultimately rely on the application of the military force. He adds that keeping an objective in mind helps driving the military force successfully and comprehensively rather than military activity becoming an end in itself. Moreover, according to Liddell Hart, it is also significant to ask that which particular mean is required to achieve the desire objective as military means is not always the end to achieve a goal. One should always maintain a clear eye on his objective and deploy a combination of means to subdue the enemy.

The third and fourth axiom are targeted at dislocating the enemy through two ways which include physical and psychological dislocation. This implies that when an enemy is targeted at the line of or course of least expectation, their physical and psychological balance pushes off which fundamentally gives the enemy a sense of being trapped. An applicable example of this

strategy is the Operation Overload or the Battle of Normandy 1944 wherein the allied forces launched a successful surprise invasion on the German occupied Western Europe as the invasion was planned and carried out at an unexpected time and at an unexpected location.

Operation Overload 1944

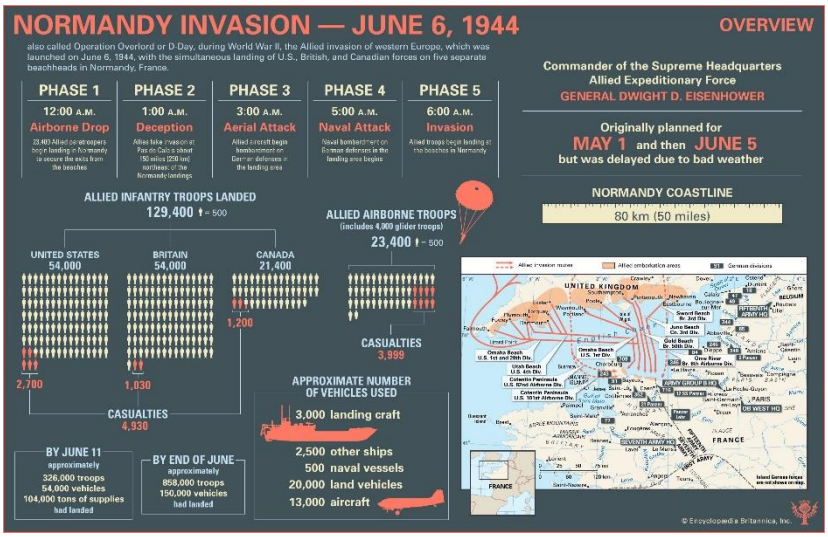


Figure 2.2

The psychological dislocation may also begin with physical maneuvers first, however, it is also essential to define both physical and psychological dislocation here. According to Liddell Hart, physical dislocation include "(a) upsets the enemy's disposition and, by compelling a sudden 'change of front', dislocates the distribution and organization of his forces; (b) separate his forces; (c) endangers his supplies; (d) menaces the route or routs by which he could retreat in case of need and reestablish himself in his base or homeland". On the other hand, Liddell Hart defines psychological dislocation as "it is the impression that the physical dislocation makes on the minds of the commanders and is strongest when sudden or when there appears no way to counter the dislocation. Psychological dislocation fundamentally comes from the sense of being trapped. To strike such an indirect attack on the enemy, Hart suggests that one should put himself in the shoes of his enemy and think like him while striking him at the least expected point.

The fourth axiom about the line of least resistance is also a similar concept and is equivalent to the idea of line of least expectation. Hart defines these two ideas as the "two sides of the same coin" and says that the indirect approach can be fully deployed and be successful when these two are combined and enemy is dislocated. This implies that to strike on enemy's least line of resistance

is to attack on enemy's weak flank rather than attempting to strike on its head. He noted that "In strategy, the longest way round is often shortest way home." This means that the enemy should be attacked through a difficult route such as forests, swaps, mountains and other hazardous terrains, as compared to taking a plain and easily predicted route. An applicable example of this strategy is the Second Punic War and the battle against the Roman in 218 B.C.E. Hannibal of Carthage, who is known for carrying out striking and legendary attacks against formidable forces, staged an attack against the forces of Roman by taking a difficult route. He knew that the usual route leading to the Roman forces was long and was familiar to them so he took a route which was marsh but short and caught the forces of adversary in surprise. Moreover, he also deployed 40,000 troops of Alps and elephants combined to serve as tanks to smash the enemy lines. The strategy caught the Roman forces off-guard and trapped them in an enveloped form. The strategy of Hannibal of striking the enemy at the line of least resistance is still considered as one of the historic maneuvers in the history of military. Liddell Hart therefore propagated for the idea of attacking enemy at the line of least resistance to launch a successful invasion with less waste of one's resources.

Figure 1 Map of Second Punic War displaying strategic route of Hannibal's forces

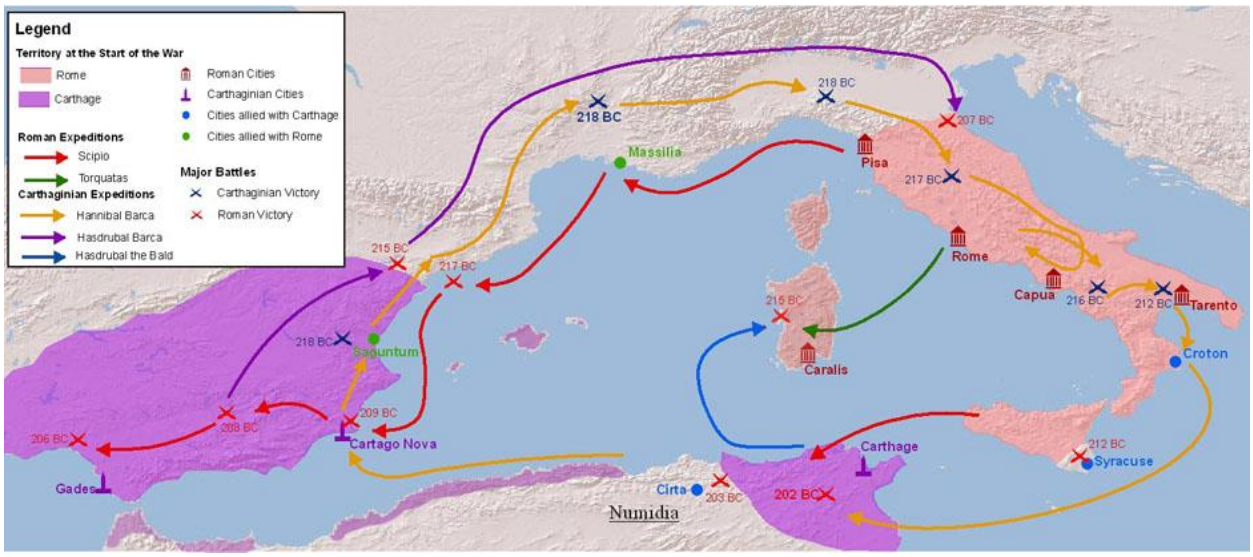


Figure 2.3

Moreover, it is also essential that the enemy should be distracted before launching such an attack in order to hinder his "freedom of action". According to Liddell Hart, alternate distribution of forces may be more helpful in launching an attack on enemy's least line of resistance rather than the concentration of forces at one place, and give that this strategy offers an access to achieving political objective, it should be deployed wherever possible.

This leads to the fifth axiom which deals with having multiple objectives. The strategy of having multiple or alternative objectives is to put the opponent at a place of confusion. Liddell Hart refers to this situation at putting enemy on the "horns of a dilemma" where he will be confused about which place to protect and defend, and how and where to distribute forces so all objectives can be possibly secured. This situation of dilemma puts the enemy at a position where his primary focus is divided at various different places which in turn leads the opponent to achieve his principle objective, or at the very least, makes the objective easier to achieve. Additionally, having multiple objectives, that are all in line with the political objectives, naturally helps in dispersing the forces of the enemy and prevents the concentration of forces. In his book Strategy, Liddell Hart wrote that, "an army should always be so distributed that its parts can aid each other and combine to produce the maximum possible concentration of forces at one place, while minimum force necessary is used elsewhere to prepare the success of the concentration." Hart's principle of dispersing and dividing the forces aims at establishing a culture of military strategy which offers flexibility instead of rigidity when laying down the strategy for war.

The sixth axiom is yet another significant strategy laid down by Liddell Hart. He suggests that a plan should always "foresee and provide for a next step in case of failure or success, or partial success". In doing so, Hart says that indeed the result of course of actions in any war is uncertain as any conflict can quickly be shifted and turned as per the strategic realities. This means that planning for all sorts of eventualities is essential so that the indirect approach can be implemented in more than one direction and wherever possible.

Finally, the last two axioms are what Liddell Hart calls the "negative lessons" or the results of practices out of the application of the indirect approach in the military history. While the first six axioms deal with what to do and provide guideline on that, the last two axioms deal with what not to do and what to avoid while planning a strategy for war.

Axiom seventh reminds that for an attack to be successful, it is essential that the enemy is paralyzed first in a sense that dislocation should occur first and then an attack to blow the enemy away should be launched. This serves as a reminder to not launch a direct attack on the head of the enemy but rather launch an attack on the weakest side of the enemy. A direct strike is where the enemy is most expecting an attack and is prepared to launch a response, whereas, an indirect attack is an attack where the enemy is least expecting and is least prepared to provide resistance.

The last and eight axiom says that if an attack has failed at a certain place, it is very unlikely that it will be successful in the next attempt on same place. Liddell Hart reminds the commanders that it is foolish to launch a strike on the same place thinking that the pervious strike would have weakened the enemy, however, it is most likely that the previous strike would have given the enemy an insight on how to deploy better forces at that place in case of another attack along the lines of the previous attack. It reinforces to the commanders to not commit a failure again and waste the resources and lives of soldiers. Instead, commanders should be reminded me axiom sixth of being flexible and dispose the plans that do not yield the desire results instead of deploying the same failed plan again.

2.6 Psychology of the Enemy

While highlighting the maneuver and surprise strategy under the Indirect Approach, Liddell Hart pointed out that the psychology of the enemy is a crucial factor in warfare and that understanding it is essential for achieving victory. Hart argues that psychological dislocation, or the sense of being trapped, can be a powerful tool for dislocating the enemy's morale and disrupting the strategy, as he also define in his third and fourth axiom of the Indirect Approach. Liddell Hart's Indirect Approach emphasizes the use of surprise, deception, and psychological pressure to create confusion and disorganization among the enemy's forces by attacking an area where they least expect it –the line of least expectation or resistance. By exploiting the enemy's fears, doubts, and weaknesses, the indirect approach can induce paralysis and force the enemy to make mistakes, which can be exploited to achieve victory with minimal bloodshed.

However, Liddell Hart was not the first one to propose and advocate for the idea of psychological pressure, deception and surprise. In 400BC, a Chinese military general and a strategist, Sun Tzu, wrote about the idea of conquering enemy's resistance without fighting through the supreme art of war which is deception. In his book 'The Art of War', Sun Tzu proposed main arguments about generals who were successful in subduing the enemy as they avoided to attack the enemy on head and rather attacked on their least line of expectation –an idea further developed by Basil Liddell Hart. Sun Tzu's strategy of war to appear weak when you are strong and to appear strong when you are weak. This is also the basis of deceiving the enemy. According to him, all wars are based on deception. This implies that attack the enemy where he is weak and avoid where he is strong,

appear close when you are far and appear far when you are close, and attack the enemy not on his head but on his weakest wing (Giles, 1910). The baseline of Sun Tzu's art of war was surprise and deception as according to him, attacking the enemy where he is mot fortified is never a good option, however, one should attack where he is least fortified. Another significant idea that he advocated was to capture the enemy instead of destroying him and subdue the enemy without fighting. According to him, if one is able to carry out this strategy, he has achieved the supreme art of war.

Liddell Hart was also known to the art of war strategy proposed by the Chinese military general. His explanation of the Indirect Approach and understanding the psychology of the enemy comes from the understanding of Sun Tzu's art of deception. Liddell Hart extensively studied all the military campaigns that followed Sun Tzu's art of war and attacked the enemy on the line of least expectation and were generally successful and also the campaigns that deployed Clausewitz's strategy of hitting the enemy on head and were generally unsuccessful with heavy loses. He then proposed his Indirect Approach which offers an insight to subduing the enemy with surprise but in modern ways –such as the use of technology.

Liddell Hart's strategy of understanding the psychology of the enemy highlights the importance of understanding the psychological dimension of warfare and the need to use it to gain an advantage over the enemy as dislocation is essential tool to exploit the enemy. Furthermore, the reason why Liddell Hart has laid significance on understanding and manipulating the psychology of the enemy is because launching an attack on the enemy requires a mindset of strategies and solutions, and the thinking of the leader is as important as the tools of attack. To strategically manipulate and dislocate the enemy, psychological dislocation is essential so that there is minimum to no bloodshed yet the results of the attack are yielded.

2.7 Linking Indirect Approach and Hybrid Warfare

The concept of hybrid warfare gained popularity in the early 2000s as a concept to define new ways of warfare that combined both conventional and unconventional means of warfare. Contemporary scholarship on the concept of hybrid warfare lacks a proper definition and the concept remains contested for not having a universally agreed definition as critics argue that the

concept is merely a buzzword and does not bring much conceptual clarity. Nevertheless, the remaining scholarship on the concept has been able to provide significant contribution in terms of providing insights to the upcoming security and defense challenges.

Put simply, hybrid warfare refers to the method of warfare that deploys a fusion of both regular and irregular means of warfare that are blended together to destroy the enemy in all capacities. There are a variety of terms that are used synonymous to hybrid warfare. These include: Grey Wars, Asymmetric Warfare, Sixth Generation Warfare, Next-Generation Warfare, New Warfare, Contactless Warfare, Ambiguous Warfare and Full Spectrum Conflict (Fridman, 2018).

There are two distinct and defining characteristics of hybrid warfare. Firstly, the risk and cost of a hybrid warfare is less than that of a conventional warfare where forces and tanks are deployed on ground directly, however the damage that hybrid warfare leaves is real and impactful. As the Chinese ancient military strategist Sun Tzu suggested, “The supreme art of war is to subdue the enemy without fighting.” Secondly, hybrid warfare is marked by ambiguity due to the hybrid actors that create a lot of vagueness and complicate the response by the targeted state. In other words, the grey areas in international relations is highlighted because the targeted state will either not be able to detect the attack or will not be able to detect the origin or the sponsor of the attack. This method and strategy of warfare is best captured in the Indirect Approach of Basil H. Liddell Hart who has highlighted the role of indirect attacks such as technology and information warfare in subduing the enemy without engaging in an on-ground conflict. With regard to the strategy explained in the Indirect Approach, Michael Howard regards Liddell Hart as “the man who, more

The Hybrid Warfare Concept

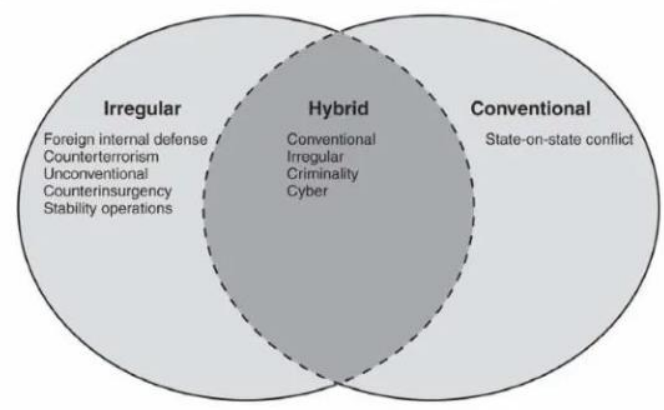


Figure 2.4 (US Government Accountability Office, 2010).

than any other in his century, has shown us how to think clearly and sanely about war" (Howard, 1966).

2.8 Indirect Approach and the Case Study of Pakistan and India

Basil Liddell Hart's Indirect Approach encapsulates the strategy of launching an indirect and hidden attack that would subdue the enemy and yield the same result as the conventional warfare but with minimum to low bloodshed. The reason why this strategy remains relevant in the recent times and remains applicable is because of the advancements in technology and cyberspace which provides the states with a new arena of competition wherein not only the nuclear capabilities will increase security challenges but the cybersecurity and cyber threat capabilities will also increase security challenges between states in the region. Therefore, states are looking for ways to enhance their cyberspace capabilities to only protect their critical information infrastructure but also to attack on the critical information infrastructure of the enemy state if required.

South Asia is already a volatile region due to border issues, poverty, terrorism and nuclear challenges and the increase reliance on cyberspace and information technology has further increased challenges for countries in the region. Pakistan and India have both been in a geopolitical competition since their inception and this can be seen in terms of their spending on military, acquiring nuclear weapons and now developing cybersecurity policies while referring it as an essential part of the national security. This implies that both states have attached significance to the cybersecurity and attack on critical information infrastructure would be considered as an attempt to damage and steal the data of the country.

The significance attached to cyberspace shows that this domain is emerging as a crucial domain for states to protect their crucial data, therefore, an indirect attack on their data in the form of cyber proxies and influence operations, will be taken as a matter of extreme significance. In this scenario, Liddell Hart's Indirect Approach remains relevant because the significance attached to cyberspace give states a strategic chance to attack the data of the enemy state and this indirect attack would not only be aimed at attacking the critical information infrastructure but it will also weaken the enemy as the attack will be on the line of least expectation and the line of least resistance –as explained by Basil Liddell Hart in his right axioms of the Indirect Approach.

Considering the significance of cybersecurity, both Pakistan and India have formulated policies and strategies to respond in case of any cyber-attack and both states have been engaged in acquiring advanced cyberspace technologies to protect their own critical information infrastructure and to show the cyberspace might to the other country. However, there has been no large scale cyberwar between Pakistan and India, yet the cyberspace domain remains a heated area due to the cyber threats that are not visible and often harder to detect.

In conclusion, it can be said that the concept of strategy is one of the most debated concepts in the analysis of war and peace. In a variety of ways, Liddell Hart was merely reevaluating and reapplying the ancient strategies that had already been deployed through the lens of advancements in technology under his indirect approach. Glimpse of Liddell Hart's strategic vision can also be seen in the centuries earlier writings and approaches of writers ranging from Helmuth von Moltke the Elder to Carl von Clausewitz to Flavius Belisarius. In its main essence then, Liddell Hart has advocated for maneuver and surprise to achieve the larger goal aimed at the destruction of the enemy. A British military historian, Michael Howard agrees to the idea that Liddell Hart's analysis of the fail strategies of the World War I paved the way for new strategic thinking in the interwar period and it was his idea of threatening alternate objectives, axiom fifth, that ultimately led German forces to spread and set up victory for the Allied powers.

Liddell Hart essential sheds light on the misinterpretation of the Calusewitzian strategy by the military commanders in the World War I which led to massive bloodshed. He emphasizes on the idea of dislocating the enemy first through physical and psychological dislocation and then launching a strike on the enemy so that the enemy is in a confused and weak state of mind and is not able to catchup with the new strategic development. In addition, Hart pays a large amount of attention to the technological advancements of the 20^{th} century and says that the developments in technology has played as essential role in further dislocating the enemy and his forces. His eight axioms serve as a checklist to ensure that the indirect approach is implemented successfully in order to achieve the political objectives of the war.

CHAPTER 3

CYBER SECURITY LANDSCAPE OF INDIA AND PAKISTAN: EVALUATING THREATS AND PREPAREDNESS

3.1 Introduction

Since the mid-1990s, internet and technology have become a part and parcel of the landscape of all countries forming a fundamental dependency over ITC infrastructure. More constructively, the advent of internet and technology has transformed the entire sphere of individual life revolutionising personal social life and work to even governance and politics. However, more destructively, it has exposed an array of stakeholders to threats beyond their scope and ranging in varying severity levels. From hacking and data breaches to espionage and cyberwarfare, all actors from individuals to corporations and governments are exposed to the same vulnerabilities since they use the same data transmission pipelines.

Therefore, as governments and international community progress at an excruciatingly slow pace while devising parameters and norms for this emerging challenge and considering that cyber attacks are motivated by multitude of motivations ranging from economic to political, there is an increasing need for states to ensure their preparedness and readiness against cyber threats aimed at them. Pakistan and India both have imparted inadequate importance to the cyber-security at official level, although both states receive wide-ranging threats to their critical infrastructure. Both states have devised respective cyber-security policies but they remain unmaterialized due to the non-realisation of importance of countermeasures, mobilisation and awareness of state citizenry as well as scanty technical infrastructure and cyber-experts to rely on.

In answering the second research question on individual security infrastructure of India and Pakistan and the role of cyber proxies in it, this chapter will be guided by the following questions. Firstly, what are the different cyber threats which compose the cyber threat landscape of India and Pakistan and what role do cyber proxies play in it? Secondly, what policy responses have been given by the officials in India and Pakistan so far to address the threats identified? Thirdly, how

have the policy responses aided or not aided in preparedness of India and Pakistan against cyber threats?

3.2 Cyberspace and Cyber Threat: Conceptual Understanding

Before delving deep into the cyber landscape, it is important to understand what essential elements constitute the cyber landscape of a country. This includes understanding what constitutes cyberspace, cyber threat and distinguishing it from a cyber-attack, knowledge of critical infrastructure and then cybersecurity itself. The term cyber refers to communication through an electronic medium such as a text message or an email, while cyberspace inculcates within its scope a sizeable community of people which interact via electronic mediums with each other from their respective locations. A cyber threat constitutes of cyber-attacks which disrupt or derail the critical infrastructure of any country and cyber exploitation by which misinformation and influence operations are carried out. Critical infrastructure constitute such vital infrastructure of state which is interlinked and thereby interdependent in provision of resources to its citizenry. This includes communication and transportation services, banking and financial architecture, and energy infrastructure. Cybersecurity of a state should therefore take into account the securitisation of cyberspace from all cyberthreats in order to protect critical infrastructure.

3.3 Understanding Cyber Proxies

One notably emerging threat to cyberspace is that of cyber proxies due to the fact that it imparts states with "plausible deniability" of their malicious cyber activities to extend their foreign policy and national objectives. Although, the term cyber proxies in international relations literature has been used in varying contexts. Even the high-profile United Nations Group of Governmental Experts (UNGGE) in their 2013 and 2015 landmark documents did not define the term cyber proxies, but went out to outline state obligations under international law regarding cyber proxies. One notable conceptual understanding of the term cyber proxies, however, can be derived from the work of Tim Maurer who in his work "Proxies and Cyberspace" built on the etymology of the word proxy as well as the work of Andrew Mumford to define cyber proxies. Accordingly, cyber proxies can then be understood as "proxies" working for a "beneficiary" or "Actor A working for Actor B." Maurer illustrates this further in a table (below) wherein subcategory (I) denotes a state being the proxy for another state and subcategory (II) denotes a non-state actor being the proxy for the state. Collectively, the two subcategories (I) and (II) represent the literature on private

mercenaries groups and state-sponsored terrorism towards an Actor C which is assumed to be another state but can also be a non-state actor. Finally, subcategory (III) and (IV) denote non-state actors using the state as the proxy such as in the case of weak states co-opted with organised non-state actors and non-state actors using other non-state actors such as a third party being hired by a non-state actor to conduct malicious activity.

The beneficiary-proxy relationship as conceptualised by Tim Maurer

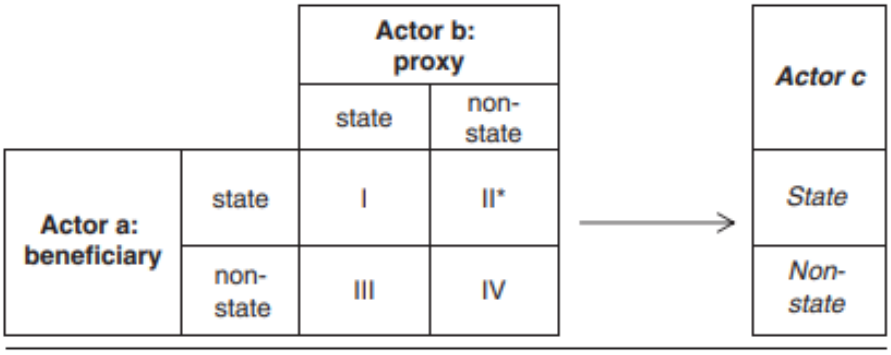


Figure 3.1

Cyber proxies are entities that carry out cyber operations either on behalf of or in collaboration with nation states. They can be either lone hackers hired for specific operations or organized groups of hackers. Some experts suggest that these companies should be categorized as cyber proxies, as targets often perceive them as such (Maurer, 2017). This trend is concerning, as it increases the likelihood of cyberattacks. Although cyberattacks have not yet reached their full potential, they are often viewed as less deadly than conventional weapons, making them more likely to be used. Additionally, they are relatively inexpensive to deploy, with the latest system vulnerabilities and tools readily available. Hackers can be hired by the hour, which means even the poorest states can launch highly sophisticated cyberattacks against their rivals. Attackers can also exploit the same vulnerabilities to launch simultaneous mass attacks on multiple targets, which would be difficult outside a full-scale war.

The use of cyber proxies is an attractive option for countries wherein countries are incentivized to tap into valuable cyber skills and resources that they may not have in their own security infrastructure. Additionally, cyber proxies operate in gray areas imparting them “plausible deniability” and allowing governments to distance themselves from controversial cyber operations. This also allows states to keep their own cyber capabilities private, providing a

strategic advantage. However, working with proxies also presents significant risks, including the possibility of the proxy turning against its state sponsor or the "Promithean Dilemma" as well as the risk of inadvertently escalating crises by utilising proxies (Borghard & Lonergan, 2016).

A review of literature suggest cyber warfare is increasingly becoming a part of regular public discourse a major concern for states and militaries around the world. Christopher Whyte in his article Cyber Conflict or Democracy "Hacked"? How Cyber Operations Enhance Information Warfare evaluate the effect of cyber information operations on democracies. He presents the view that in the sophisticated digital age, cyber operations puts the democratic functionality of a state in a vulnerable position as there may arise multifaceted unprecedented challenges which may subvert the traditional mechanisms of a democracy. He draws the conclusion that these challenges and threats might increase in future, therefore, states must develop policies to quickly tackle these threats (Whyte, 2020).

Muhammad Riaz Shad in his article Cyber Threat Landscape and Readiness Challenges of Pakistan explores how technology can both be an opportunity and a challenge for states. He presents the view that Pakistan is increasingly growing in the sector of information technology but lacks a comprehensive framework and cyber readiness. He supports his arguments by evaluating Pakistan's cyber readiness in the light of criteria provided by the United Nations and concludes on a recommendation that Pakistan needs to urgently develop a framework for cyber readiness and should undertake discourse such as cyber awareness (Shad M. R., 2019).

Shuchita Thapar in her article mapping the Cyber Policy Landscape: India explores the country's focus on cyber security at various levels including government institutions, civil society organizations, think tanks and academia. She also analyses the participation of stake-holders at all levels and concludes on mapping future opportunities, means and sites for engagement for the country (Thapar, 2016).

3.3 International Law governing Cyberspace

In the year 1834, first cyberattack occurred when the French telegraph was hacked by a pair of thieves to steal money. This was followed by another monumental cyberattack, nearly a century and half later, by Robert Tappan Morris in 1988 wherein he executed denial of service attack by infiltrating and hacking a computer that belonged to the Massachusetts Institute of Technology

and unleashed a “worm” in the network which managed to spread like wildfire within twenty four hours across all 6,000 computers that were connected to the fledging entity –now known as the internet. This incident marked a turning point in the history of computing and cybersecurity. The technological advancements although progressed in the 1980s and the early 1990s, cyberspace gained momentum and became a vital medium of discussion in warfare, businesses and technology in the early 2000s when the prevalence of broadband internet access became more common (Cherry & Pascucci, 2023). This advancement facilitated the technological progress and allowed the speedy transmission and sharing of vast amount of data. However, the laws, regulations and legislations concerning cyberspace have been far behind and have failed to keep up with the pace of technological advancements. The developments that have been made in the international law regarding cybercrime and cyberattacks cannot be denied as they serve as the monumental documents in the development of legislations in the cyber domain. The early 2000s saw several notable conventions. These include: Convention on Cybercrime 2001 –also known as the Budapest Convention, Additional Protocol to the Convention on Cybercrime concerning the Criminalisation of Acts of a Racist or Xenophobic Nature Committed through Computer Systems 2003, Convention on the Protection of Child against Sexual Exploitation and Sexual Abuse 2007, and a relatively recent Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence 2022.

Cybersecurity Composition

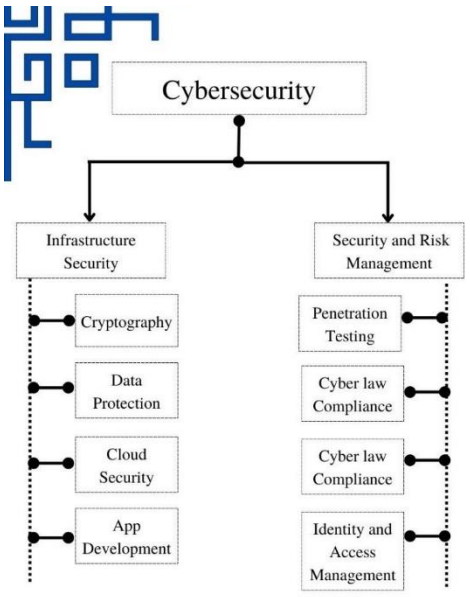


Figure 3.2

The Convention on Cybercrime 2001 or the Budapest Convention is a monumental convention because this was the first international agreement that was aimed at minimizing crimes taking place in the cyber domain and to harmonize national laws towards enhanced investigation techniques and cyber cooperation or cyber diplomacy between states for an increased international cooperation. The Additional Protocol to the Convention on Cybercrime concerning the Criminalisation of Acts of a Racist or Xenophobic Nature Committed through Computer Systems 2003 as aimed at obligating the states parties that have ratified the Budapest Convention to enact laws that criminalize xenophobic remarks and comments on the internet or expressed otherwise online. Similarly, another notable convention is the Convention on the Protection of Child against Sexual Exploitation and Sexual Abuse 2007 which is aimed at prohibiting the use of internet and technology to distribute child pornography, to access and view child pornography and to solicit children into activities of sexual nature. The Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence 2022 is aimed at enhancing cooperation between state parties to the Budapest Convention on disclosure of electronic evidence and domain names, and provides legal basis for the electronic evidence to be shared and used in the criminal proceedings.

Although there has been progress in formulating of conventions regarding international law governing cyber space, there is still a big question that remains largely answered –the scope, manner and extent to which the international law governing cyberspace is applied to the cyber and online actions of states. The reason why this ambiguity exists is because often states do not choose to align with a certain clear position as it would limit their actions and freedom, and sometimes states the states have yet not formally adopted a clear national position on cyber space. Moreover, another reason for this ambiguity is because states often deliberately choose to be unclear about their actions in the cyber space to further add complications and to further make actions difficult to detect in order to refrain from the legal actions yet achieving their national security interests (Cherry & Pascucci, 2023). However, despite these ambiguities, there have still been some developments in the past decade that have clarified the application of international law in cyber space –to some extent –and these developments are discussed below.

Spectrum of Traditional and Irregular Warfare

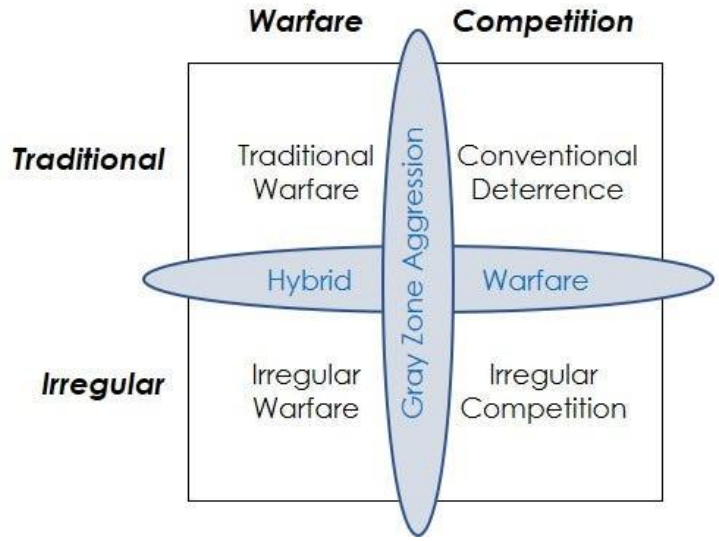


Figure 3.3

3.3.1 Developments in the Past Decade in International Law governing Cyberspace

The United Nations Group of Governmental Experts (GGE) (that are appointed to study particular issues that are of concern and significance) on Development in the Field of Information and Telecommunications in the Context of International Security, in the year 2012, concluded that "State sovereignty and the international norms and the principles that flow from sovereignty apply to the state conduct in cyber space and the states must meet their international obligations regarding internationally wrongful acts attributable to them."

Including this meeting, there have been five other meetings since 2004 of the Group of Experts on matters pertaining to cyber space. Of all the six meetings, there have been reports produced on three meetings that include meetings of the year 2010, 2013 and 2015. Furthermore, the meeting of the experts also clarified that "states have jurisdiction over cyber infrastructure that is located within its territory" (GGE, 2013). While the report was able to clarify the sovereignty and jurisdiction of states over cyber space and cyber infrastructure, it still failed at clarifying the role of sovereignty in making or not making states take certain actions.

Till 2012, the international community was able to formulate general agreements in international law that applied to actions in cyberspace, however, the public clear position of states with regards to international law and actions in cyberspace remained largely ambiguous. To cater to the issue of ambiguous public positions of states, a group of experts was convened from the Cooperative Cyber Defence Centre of Excellence (CCDCOE) of the North Atlantic Treaty Organization (NATO). The group of twenty scholars of international law produced the Tallinn Manual on the International Law Applicable to Cyber Warfare or the Tallinn Manual 1.0. The manual was produced on the efforts of experts over the span of three years. Tallinn Manual 1.0 is a notable document in the application of international law governing cyber space because the manual laid down 95 rules that were formulated considering the existing international customary and conventional laws that essentially dealt with how these laws and regimes are applied to the actions of states during cyber warfare. Therefore, the Tallinn Manual 1.0 serves as a notable standpoint to understand the application of international law in cyber space.

In 2015, another meeting of the United Nations Group of Governmental Experts (GGE) took place which produced the report affirming conclusions of the 2012 GGE report. Furthermore, the report concluded that the United Nations Charter and its articles related to sovereignty and jurisdiction also applies to the actions of states in the cyberspace and that they shall be held accountable for their internationally wrongful actions in the cyberspace. In addition to this, the report also mentioned states in the international community to remain consistent in their application of the United Nations Charter and take a clear position that aligns with state sovereignty related norms and principles in the cyberspace. Most significantly, the report also recognised the cooperation of international states and that the cooperation is necessary to promote a peaceful, stable, secure, accessible and an open cyber environment amongst states.

In 2017, another meeting of a large number of experts of the Cooperative Cyber Defence Centre of Excellence (CCDCOE) of the North Atlantic Treaty Organization (NATO) was convened that resulted in creating a Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. The reason why Tallinn Manual 2.0, containing 154 rules, is significance in the development of international law governing cyber space is because the manual increases the scope of states actions in cyber space and the cyber activities during peacetime should also abide by the international law

and state sovereignty. Furthermore, the manual stated that any breach in sovereignty through the cyber space would result in the breach of an international obligation upon a state.

One of the recent development in international law governing cyber space and its application was the United Nations General Assembly report in 2021 which is called "The Official Compendium of the Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communication Technologies by States Submitted by Participating Governmental Experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security". The report essentially dealt with urging states to take a view on international law governing cyber space and submit it to promote responsible behaviour of states, confidence building and capacity-building in order to promote cooperation, effective implementation of international laws and to minimize the existing potential cyber threats.

States in the international relations are continuously deploying and employing their cyber skills and are continuously making an attempt to equip themselves better in the cyberspace, however, the next decade will witness the development of opinio juris and practices of states with respect to international law governing cyberspace. Furthermore, there is still an array of questions that need to be clearly answered and clarified such as weather the concept of sovereignty constitutes as the rule of international law or the principle, weather a cyberattack on the information and financial systems of a country constitutes as deployment of force or prohibited intervention, can data and network systems be given the status of protected objects, prohibited interventions constitute information and disinformation campaigns to what extent, and weather the cyberspace allows collective measures by states and would they be considered lawful under the international law (Cherry & Pascucci, 2023). The Tallinn Manual 3.0 is already in process by a group of experts which would broader the understanding of applicability of international law in cyberspace, however, the next decade is likely to being more answers and clarity to these questions, policies and international law governing cyberspace.

Tiers of Cyber Environment

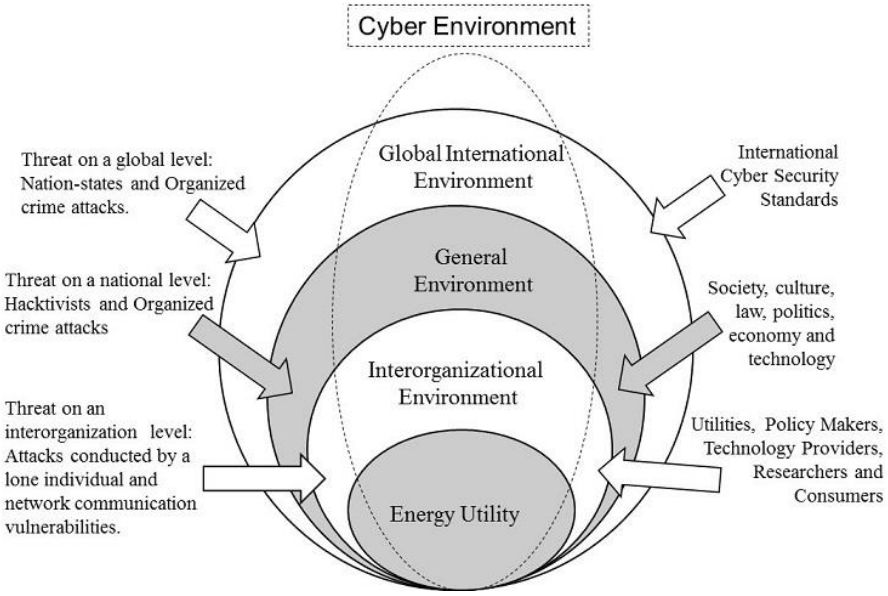


Figure 3.4

3.4 Cyber Threat Landscape of India and Pakistan

Pakistan is a state which faces a hostile socio-political environment both externally and internally. Pakistan's cyber threat landscape is characterized by its increased dependence upon the information and communication technology (ICT) infrastructures and upon the government to provide protection against cyber threats. These conditions increase the degree of vulnerability for national security and puts Pakistan at a disadvantage due to lack of reliable cybersecurity systems, immediate response and a comprehensive framework. The annual 2017 report of Global Security Index (GSI) ranked Pakistan at 67th out of 193 countries in terms of policies and commitment to cybersecurity (Global Security Index, 2017). This is due to insufficient legal and technical measures, poor state affairs and the inadequate cooperation and capacity building to upgrade cybersecurity. These factors, coupled with internal and external security challenges, make Pakistan a target of four various cyber threats which include: cyberterrorism, cyberwarfare, hacking, and organized and serious crimes.

India's cyber threat landscape is also characterized by cyberwars which break out every now and then. Contrary to India's image as a cyber-power, it does lack security frameworks due to lack of cybersecurity experts in the country. Presence of hackers and pirated software have made the country a hotbed of cyberwarfare, website defacement and hacking. Apart from internal security challenges, the country's national security also becomes vulnerable because India's rising status puts the sensitive networks and systems to a constant threat of penetration. While domestic agencies may have discovered some of the intrusions, many other intrusions have been discovered by external agencies which point at country's long distance yet to be covered in the security network.

3.5 Policy Responses: Evaluating National Cyber Security Policies and Cyber Governance of Pakistan

Until only recently, the policy responses from Pakistani policymakers towards cyber threats consisted only of legislations and guidelines with limited domestic scope such as The Prevention of Electronic Crimes Act 2016 and State Bank of Pakistan's Guidelines on IT. Under this Act, unauthorized access to information systems, critical infrastructure, and data are punishable offenses as well as fraudulent electronic activities, malicious codes, tampering communication and on an individual level the harm in terms of offenses to a person's modesty, hate speech, cyber stalking and glorification of offenses are also punishable (Prevention of Electronic Crimes Act, 2016, 2016).

Moreover, the Government of Pakistan recognized the importance of addressing Cyber Security Challenges and responded by creating the National Center for Cyber Security (NCCS) in 2018. The NCCS is solely focused on combating cyber-crimes through both theoretical and practical applications. Additionally, the NCCS has actively been working on various initiatives such as cyber reconnaissance, cybercrime investigation, block chain security, digital forensics, intrusion detection systems and malware analysis (Niaz, 2022).

Despite the wide-ranging threats discussed in the above section, the agenda lacked priority and interest of Pakistani policymakers in the security discourse. However, for the first time, a comprehensive document elevating the issue to the national security level has been materialized as Pakistan's National Cyber Security Policy (NSCP) in 2021. The policy is ambitious as it

addresses the emerging needs of counter-measures by aiming to protect critical information infrastructure, mobilise and inform the citizenry on cyberspace, and increase technification and capacity building by research and development opportunities as well as public-private partnerships.

The policy highlights 17 policy deliverables out of which 16 are directly connected to the cyber security of the country. They span around establishing effective cyber security governance in Pakistan, active defence of the country, increasing the resilience of national critical infrastructure and government's information systems, protecting its internet based activities, research and development, capacity building, awareness, fostering public-private partnerships, global collaborations and increasing Pakistan's ICT ranking are among the policy deliverables (National Cyber Security Policy, 2021, 2021).

The current cyber security landscape of Pakistan

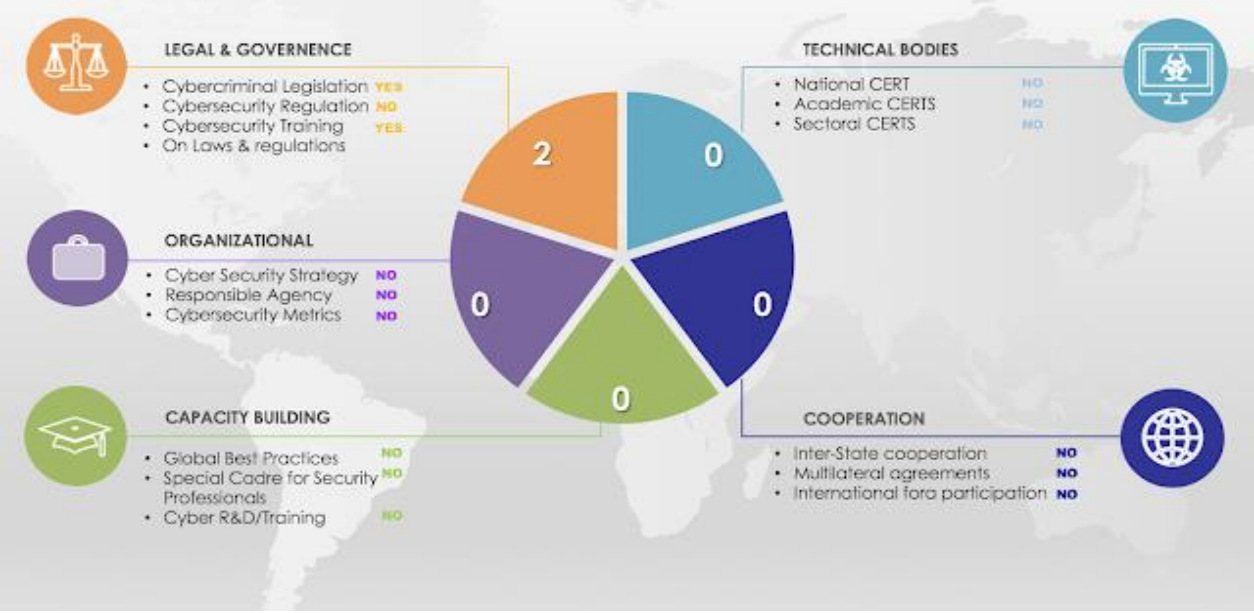


Figure 3.5 (ITU, 2019).

Most notably, the policy highlights the institutionalized approach the country has finally taken to address its looming cyber security concerns. Under the policy deliverable of effective cyber governance, the policy has constituted the Cyber Governance Policy Committee (CGPC) which will be responsible for the implementation and the oversight of the strategic cyber security issues of national concern. For this, the country has adapted from the best practises followed

internationally such as having cyber security governance under dedicated and exclusive national cyber security framework. However, Pakistan needs more institutional synergy between the already established 2018 National Center for Cyber Security (NCCS) and the newly constituted Cyber Governance Policy Committee (CGPC) under this policy in order to realize its policy deliverables and have robust and effective implementation of the policy.

3.6 Policy Responses: Evaluating National Cyber Security Policies and Cyber Governance of India

Indian National Security Council and policymakers have in contrast viewed cybersecurity as a national security agenda since 2002, engaging in international dialogues, establishing ministries from state to national level on the issue while also issuing consistent domestic legislations and guidelines. The country was also one of the first countries to have established its Computer Emergency Response Team (CERT) and has passed a number of legislations since 2000 regarding the various scopes of cyber activities, a timeline of which can be seen below.

India's Cyber Legislation Timeline

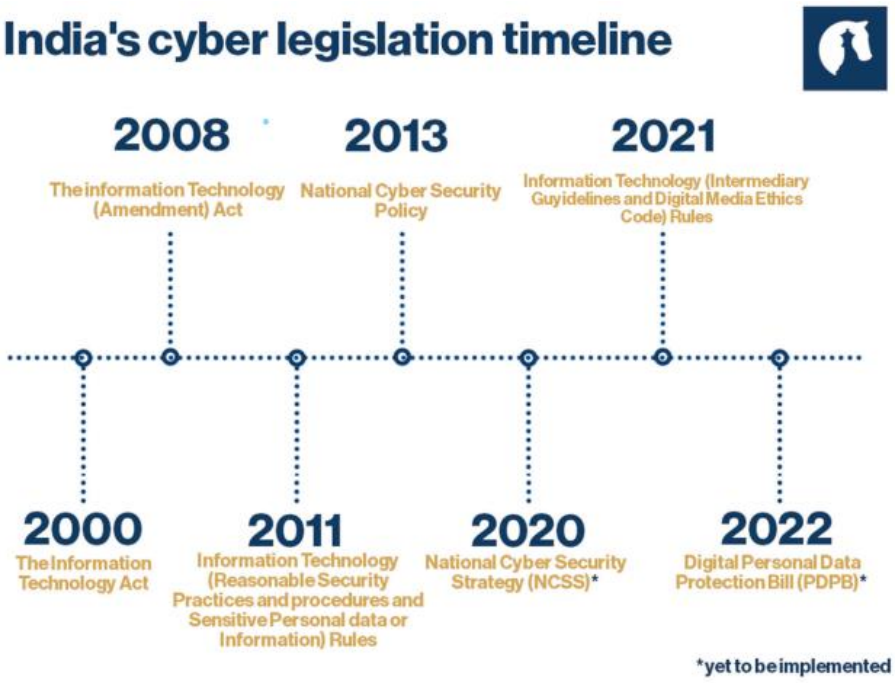


Figure 3.6

However, Indian National Cyber Security Policy as a comprehensive intra state document to address cyberthreats was materialized in 2013 as a framework that was put in place to effectively handle cyber security concerns within the country. The Indian NSCP also aims to inculcate countermeasures in cyberspace by utilising CERT for early warning, protecting all e-governance websites and critical infrastructure. It also aims to mobilise the citizenry by creating what it calls "a culture of cybersecurity understanding", and also aims to strengthen capacity and technification by building a network of 500,000 experts.

In 2015, the government of India further recognizing the importance of cyber security and established the National Cyber Security Coordinator (NCSC) position within the National Security Council Secretariat to coordinate efforts between different government departments and agencies. Although the NCSC reported directly to the Indian National Security Advisor (NSA) and was intended to handle technical, security, and legal aspects, there was no specific cyber security institution that has been realized as of yet. Therefore, the biggest challenge in the absence of an exclusive cyber security institution and just a post within the secretariat came with bureaucratic conflicts which hindered the NCSC's ability to carry out their duties (Patil, 2022). The only institution which focuses on a tangent of cyber threats to India is the National Critical Information Infrastructure Protection Center (NCIIPC) established in 2014 to protect against the threat of cyber attacks on national critical infrastructure and to give strategic leadership to the government in its response to cyber security threats against the national critical infrastructure.

Moreover, the government of India securitises against varying cyber threats through four different ministries. The Ministry of Electronics and IT collects, protects and manages the unique identity details of the Indian citizens. The Ministry of Finance has monumentally established the Reserve Bank Information Technology in 2017 in order to protect digital payments from cyber security threats. The Ministry of Home Affairs set up the Indian Cyber Crime Coordination Center in 2018 which works in collaboration with the law enforcement agencies in order to tackle cyber threats in the country as well will form Mutual Legal Assistance Treaties (MLAT) with other countries. Finally, the Ministry of Defence has constituted the Defence Cyber Agency of India in 2019 (Press Information Bureau, 2019). It is responsible for offensive cyber operations which have been noted with the recent targeting of Chinese and Pakistani networks.

Summing up the cyber governance of both countries, it can be said that both of their respective cyber security policies are ambitious. Although, it is important to note that both face significant implementation challenge as policy making and policy implementing gap is too wide. The most unrealistic objective of Pakistan's NSCP is to establish a centralised federal body with standardised norms relating to cybersecurity which shall look into all cyberthreats ranging from individual to governmental level. Not only is its scope too wide-ranging, but the current lack of consensus on budget allocations indicate that establishing this body would be a contentious and stretching objective. Indian policy too lack operationalization despite bold claims of capacity building, and is even ambiguous on the protection of civil and human rights during the process.

India's Cyber Security Institutional Landscape

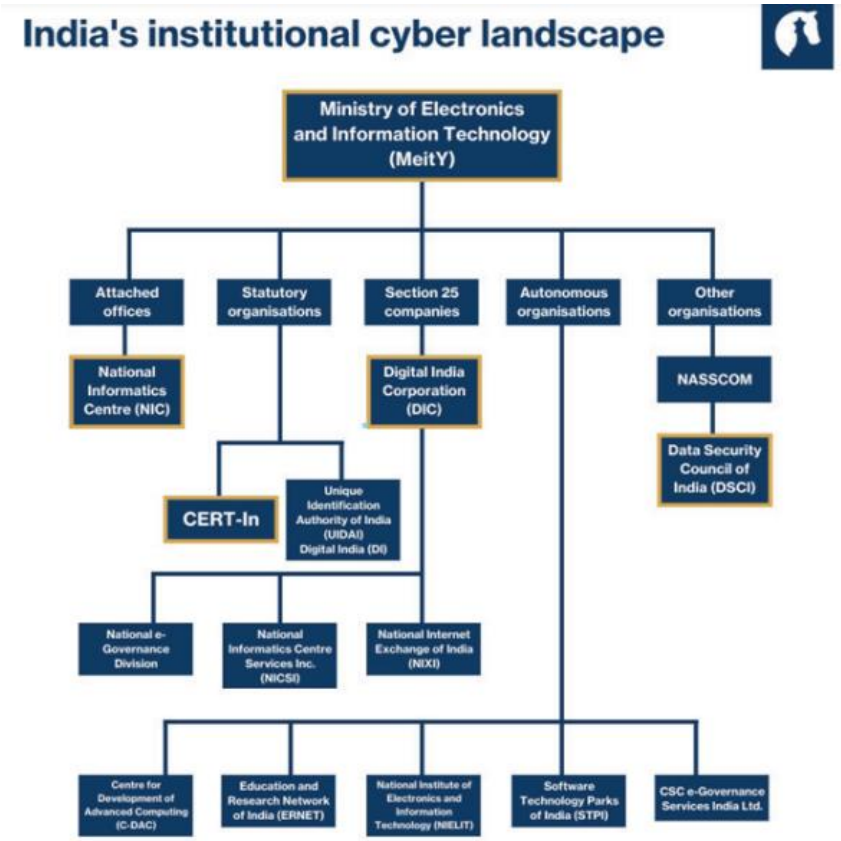


Figure 3.7

3.7 The Challenge of Cyber Threat Readiness: Gauging Preparedness of India and Pakistan

In order to gauge preparedness against cyber threats, the UN specialised agency, the International Telecommunication Union (ITU) has proposed a set of criteria: legislative, organisational, technical, international cooperation and capacity building. It further scores the performance of countries according to a metric signifying the accomplishment of these criteria with performance indicators like leading, maturing or initiating state. From 2017 to 2021, the rankings depict India's rank shifting from 23rd (maturing) to 10th (leading). While Pakistan's rank has downgraded from 66th to 79th place, it is still characterised as a maturing state on the index. The report therefore is vital to understand the importance of policy implementation and capacity building to address the challenge of readiness.

While the previous section has highlighted policy responses, it is imperative to also analyse Pakistan's capacity and readiness in terms of other criteria set by the ITU. In technical and capacity-building domain, Pakistan face considerable setback. The country has three prominent organisations present: the PAK-CERT, PISA-CERT and the National Center of Cyber Security (NCCS), yet all of them lack international standardisation and certification which hampers state to produce internationally recognized experts and technicians. In organisational domain, an offshoot of FIA, the National Response Unit on Cyber Crime manages all the cyberthreats while facing defunct resources to address such issues. In the NSCP 2021, however, a new centralised federal body to address such issues have been proposed yet funding remain its biggest pressure point. Finally, on international cooperation, Pakistan has been a part of number of multilateral forums on cybersecurity such as ITU-IMPACT and Asia Pacific Security Incident Response Coordination Working Group APSIRS-WG.

As for Indian preparedness, the country has in its technical domain one of the world's first and standardised CERT operating since 2000. In organisational terms, it has a set of governmental ministries, agencies and departments dedicated to cybersecurity but more importantly an already centralised federal body called the National Critical Information Infrastructure Protection Centre (NCIIPC). Finally, unlike Pakistan, the country has both multilateral and bilateral international cooperation, a number of dialogues initiated by itself, and cooperative CERT with other leading counties' CERTs.

3.8 The Indirect Approach and the Evolving Cyber Culture in South Asia

There are primarily three arguments as to why the indirect approach with respect to cyber proxies and cyber attacks is applicable to South Asia. In a context where the cyber culture of the region is evolving with internet users in both India and Pakistan growing exponentially from 14% in 2014 to 43% in 2020 for India and from 10% in 2014 to 25% in 2020 for Pakistan respectively, cyberspace presents itself with multiple opportunities to extend national objectives short of war, unconventionally, and through indirect means (World Bank, 2020). The three arguments for the indirect approach in case of India and Pakistan are therefore as follows:

i) The non-escalatory potential: Achievement of national objectives short of war
ii) Creating 'plausible deniability: Achievement of national objectives without facing meaningful consequences by the international community
iii) The offense-defense advantage: Achievement of national objectives through offensive cyber activities in the larger strategic context

Firstly, the non-escalatory potential that cyberspace holds comparative to the conventional means of conflict, amidst a nuclear South Asia where the strategic balance is delicate is important to note. Engaging in cyber operations through an indirect approach imparts actors with broader range of options to engage in low-intensity conflict. This is because cyber attacks lack the physical violence component of a conventional conflict as well as are ambiguous which is instrumental in not triggering the 'red line' of another country whilst simultaneously being in conflict with them. As per Erica Lonergan they "can create breathing room for crises to resolve short of war" (Gambrill & Schroeder, 2022).

Secondly, the indirect approach imparts "plausible deniability" to actors in South Asia i.e. India and Pakistan to extend their foreign policy aims and national objectives through cyber attacks and cyber proxies without facing any meaningful consequences for their illegal actions. The biggest argument for utilizing cyber proxies is to extend propaganda, disinformation, and influence populations of the other country by eroding trust in the government in the digital age. It is important to note that under international law, a state that has been the victim of a proxy attack cannot use force in self-defense against another state unless the link to the proxy is proven. As Kurt Sanger in an article on Atlantic Council puts it, that proving the aggressor state's link to the proxy "could

make future operations ineffective, compromise sources that produced the information, or risk leaving its accusation unsubstantiated" (Gambrill & Schroeder, 2022).

Finally, there is an argument of the offense-defense balance in the wider strategic context of South Asia. Using the indirect approach and cyber space as an arena of strategic competition, there is an assumption that the offense has an advantage of the defense. Since defense in cyber space is difficult due to the ambiguity and difficulty in setting appropriate red lines, the arena of cyber space is then reduced to risk tolerance and risk mitigation at best in terms of defense. Therefore, offensive operations and offense would have an advantage over the defense.

In conclusion, the revolution of the internet and technology in the contemporary world has created both opportunities and challenges for countries. The fast-paced communications pose significant challenges ranging from cyberterrorism to cyberwarfare, to hacking to website defacement. Pakistan faces massive external security threats and these threats put the country in a more vulnerable position because Pakistan lacks comprehensive cyber policies and reliable cyber systems. The policies formulated by Pakistan have had a domestic cope only until the 2021 National Cyber Security Policy. Similarly, Pakistan also down ranked in the UNITU and the insufficient legal and technical measures, poor state affairs and inadequate cooperation and capacity building to upgrade cybersecurity expose Pakistan to various cyber threats. India, on the other hand, has been involved in cyber security dialogues since 2002 and was also the first in the region to establish a CERT and its preparedness and the technical domain is also one of the fast-evolving domain. Finally, it also has bilateral and multilateral cooperation ties with a number of other countries related to CERT.

CHAPTER 4

NATURE OF CYBER WARFARE BETWEEN INDIA AND PAKISTAN: OFFSENSIVE OR DEFENSIVE?

4.1 Introduction

In the era of technological advancement, cyber space is known as the battlefield of the modern twenty-first century security landscape in which due to the rapid and drastic revolutionisation of digital networks, information technology, internet and cyberspace, states now engage in hybrid warfare to unleash and declare their dominance in the digital realm. The rapid speed of technological advancements has led cyber space to be an evolving (and a relatively newer) threat and a new domain of national security concern for states around the globe. With the rapid developments in technology also comes a variety of threats for states and Pakistan is no exception to it. Under the nuclear deterrence and strategic stability between two nuclear armed rivals, India and Pakistan, the cyber threats and cyber arms have become a more prudent in the South Asian region.

The introduction and use of cyber threats and cyber proxies in the South Asian region has further added a security concern between the two nuclear armed rivals in the region as the historical enmity has already between a cause of great concern in terms of traditional threats. Both countries are getting equipped with the newest technology and have designed multiple cyber operations to gain different outcomes and to declare digital dominance, which is likely to get worse with time. Therefore, there is an urgent need to study this dimension of security between India and Pakistan, which is being done in this research, and to timely evaluate the impact cyberwarfare can potentially have on the South Asian region.

4.2 Cyber Security Threat Landscape of South Asia

The volatile region of South Asia has experienced almost all sorts of security threats ranging from terrorism, suicide bombings, inter-state wars, civil wars, critical political and socio-economic

issues, environmental degradation, and lack of access to clean drinking water and water conflicts, amongst others. Apart from these, there has been a rise of another security dimension since the dawn of twenty first century. This new security dimension is the cyberspace that has brought a variety of challenges to states around the world and thus, South Asian states are no alien so the phenomenon. The rapid technological advancement and developments in the cyber domain has equally affected the countries in the South Asian region thereby opening a new battlefield for the states of this region that they now have to defend and protect from potential cyber threats. The cyber security threat landscape of South Asia is characterized by cyber threats which include cyber proxies, influence operations, information and misinformation campaigns, cyber bullying, cyber vandalism, data breaches and hacks and espionage.

The limited awareness on cyber security and cyber threat in South Asian countries has led to a greater number of security concerns for these countries and has predominantly marked and identified these countries as "sitting targets" for espionage operations carried out by various countries across the globe (Patney, 2015). Even though the number of population in the South Asian region is high and is considered as the populous region, the penetration of cyber threat awareness and information on ways to counter is very less known in these countries. In addition, the countries in South Asia also lack a strong infrastructure to protect their national critical information and most of the country's ICT infrastructures are at a budding stage.

The cyber security landscape of the South Asian region then becomes crucial when looking at India and Pakistan as the region is termed as a nuclear flashpoint because of the historical enmity between the two states and the unresolved issue of Kashmir that has remained as a major cause of tensions between the two. It is contented that the cyber domain has the potential to be a next flashpoint between the two nuclear armed rivals, leading to further tensions and strategic instability in the region (Baker, 2013). Due to the rapid advancements in technology and cyberspace, the communication between India and Pakistan has also been revolutionized. However, more significantly, it has also led to the rise and penetration of non-state actors in the cyber domain that pose and launch cyber-attacks on state that are often difficult to detect, thus highlighting the existence of grey area in the cyber domain.

4.3 Nature of India's Cyberwarfare: Offensive or Defensive?

India is one of the leading developing countries amongst other South Asian countries that has a much advanced and developed institutional and organizational framework with regards to technology, legal measures, policy frameworks, and cybersecurity architecture which comprises of multiple agencies and ministries working together to achieve a comprehensive cybersecurity approach. Owing to its large amount of population, India has the one of largest number of mobile phone users and internet subscribers in the Asian region, as per the Internet World Stats. Furthermore, due to the advancements in the technological sector, the country's Internet Technology (IT) sector and IT industry is considered as the crown jewel of the country, generating employment and creating huge shares and profits for the IT companies across the country (Patney, 2015). Since the IT sector contributes in a large amount to the economy, the Government of India has taken necessary steps to make technology and internet available in all parts of the country. These include steps such as e-government services, mobile banking services and online banking. Each year, the country produces a large number of IT professionals, however, the number of IT experts are relatively low and their expertise remain untapped.

4.4 Composition of India's Cybersecurity Domain

There are three government ministries, in India, that are involved in dealing issues related to cybersecurity. These ministries include Ministry of Defence, Ministry of Home Affairs and Ministry of Communications and Information Technology. However, the ICT sector in particular is governed by the Ministry of Communications and Information Technology which has three departments namely the Department of Technology (DoT), Department of Electronics and Information Technology (DeitY) and the Department of Posts (DoP). All three departments are designated with their respective tasks. The DoT aims to works towards providing high quality, secure and affordable telecommunication services all across the country as an attempt to accelerate the socio-economic development in an inclusive manner. On the other hand, DeitY aims to works towards the development of the IT sector, including human resource development, innovation, efficiency of digital space, security of cyber space alongside a multi-pronged approach that aims to empower citizens through e-governance. Lastly, the DoP also plays an essential role in country's

socio-economic development by offering schemes such as Small Savings Scheme, Rural Postal Life Insurance (RPLI) and Postal Life Insurance (PLI).

4.5 India's Cyberspace Policies and Legal Frameworks

In the face of growing cyber technologies and nuclear program, India has formulated several policies and legal frameworks to protect and regulate its critical infrastructure and the ICT sector. These policies and legal mechanisms include the 1997 Telecom Regulatory Act which was regulated to protect and manage the telecom services including the tariffs revision, the year 2000 Information Technology Act which aimed at guiding country's IT sector and was followed the IT Act of 2008 which observed several legal amendments in the previous act, the year 2013 National Cyber Security Policy (NCSP) which serves as country's strategy to protect and build a resilient cyberspace for its citizens, government activities, businesses and for the country, and lastly the year 2013 Guidelines for Securing National Critical Information Infrastructures (NCII) which was aimed at formulating guidelines to protect the critical information structures of the country such as telecommunication, transportation, defence, banking, energy, cyberspace etc.

In addition to these, in September 2013, the country also become an "authorizing nation" from a "consuming nation" with regards to IT products which is a milestone for the cyber security domain as the IT products, that have been verified and certified by India, can now be used without retesting by the member countries of the Common Criteria Recognition Arrangements (CCRA).

In addition to formulating several policies and legal framework, India has also designated various centres and agencies to protect the critical infrastructure, IT sector and the cyber domain of the country. These agencies include National Informatics Centre which works towards providing linkages between institutions all across the country and the e-governance programs, Standardisation Testing and Quality Certification Directorate which tests, check and provide quality assurance to all the electronics across country through a laboratories network that operates nationwide, Controller of Certifying Authorities that authorises electronic transactions and lastly the Computer Emergency Response Team India (CERT-IN) which prevents and detects crimes and incidents related to cyber domain. The Department of Electronics and Information Technology operates all of these agencies. Furthermore, in order to protect country's crucial defence networks,

Cyber Command is set up by the Indian Army which is also a major step taken by the country to protect itself in the face of cyber threats.

4.6 Nature of Cyberattacks by India

When it comes to cyberattack, despite various initiatives taken by the government to protect the critical information structure, the country continues to face cyber threats in the form of hacking, data breaches, malwares, digital espionage, web defacements, e-email spoofing, online surveillance and online financial frauds which largely put the country's cyber security at a risky position. The reason why India faces cyber-attacks is because of its rising status as a nuclear power, economic power and a technological giant alongside the lack of IT experts which leads to cyber expansion capabilities as an urgent step. The National Cyber Security Policy of 2013 identified that nearly 500,000 would be required by the year 2018 for the proper implementation of cyber security policies (Patney, 2015). However, in the face of growing threats, two large companies in India faced namely the Air India and the Mobikwik faced data breaches in 2021 alone.

Apart from Pakistan, the cyber threats faced by India emanate largely from a neighbouring country and a contested rising power in the region –China. After the Ladakh Crisis which took place between China and India on October 12, 2020, the Cybercrime Coordination Centre of India pushed for a ban of Chinese-linked mobile phone apps on the grounds of suspected stealing of user data via the backdoors. Four months later, India's capital Mumbai faced a malware attack targeting electricity supply systems of the city and the malware attack was suspected to be carried out by China, however it was not proved later.

Nonetheless, the physical standoff between China and India worsened the relations between the two but also showed how the physical deterioration of relations leads to a struggle for power and superiority in the cyber realm. This strategic placement of influence operations, malware attacks and data breaches is referred as the "newest form of aggression and deterrence" as the cyber-attacks gives country an option to attack the other country without launching a physical or nuclear attack yet yields the same strategic results.

When it comes to protecting its cyberspace in the region, especially from Chinese suspected attacks, India's approach is defensive in nature as China is one of the highly advanced countries

in terms of technology and a few of world's biggest tech firms also belong to China such as Alibaba, Baidu, Xiaomi and Tencent, which means that China is a lot advanced than India when it comes to protecting cyber space and cyber experts in country. Similarly, to deter potential threats, India has also taken steps in the domain of cyber-diplomacy such as bilateral information sharing and protective agreements with the UK, the US, Israel, Japan and Australia.

However, when it comes to Pakistan in the region, the nature and the approach of cyberwarfare by India is offensive in nature and this is because of several reasons combined. Firstly, the historical enmity between the two nuclear armed rivals on the unresolved issue of Kashmir has led cyber space to be a new battleground for the India-Pakistan rivalry. Secondly, the technological sector and the cyber space policies and the legal framework of India is more advanced and comprehensive than Pakistan which further gives India an edge to launch a cyber-attack and to show technological superiority.

In addition, the flourishing IT industry of India also gives India a technological edge over Pakistan. This can also be observed through the fact that India was ranked 10th on the Global Security index (GSI) in 2020 whereas Pakistan ranked 79th on the list. Thirdly, India has been paying more attention and investment to grow its cyber-security expertise which further serves as a security dilemma for Pakistan to protect its cyber-space and invest more in the ITC sector. While no large-scale cyber-attacks have been carried out between the two countries, small-scale cyber-attacks have taken place out of which web vandalism, influence operations and cyber-proxies are most common. According to a report of International Institute of Strategic Studies (IISS), "India has come cyber-intelligence and offensive cyber capabilities, but they are regionally focused, primarily on Pakistan" (IISS, 2021).

4.7 Nature of Pakistan's Cyberwarfare: Offensive or Defensive?

Pakistan is also one of the most populated country in the South Asian with a large amount of youth using internet, hinting at the digital transformation in the country, which many believe has the potential to flourish the IT sector of the country. Despite lacking preparedness in terms of cybersecurity, Pakistan has taken steps towards offering e-services to the citizens such as online banking, mobile wallets, and e-government services like salary distribution via Automated Teller

Machines (ATMs) which points towards country's effort towards digitalization. However, Pakistan continues to face several cyber threats as Pakistan is also a nuclear power in the region which essentially means that Pakistan's geopolitical region is contested in the region leading to an increased exposure towards cyber threats. In the face of these cyber threats, the country has made several efforts in terms of policies to detect the threats and protect the data and privacy of both the country and the citizens.

4.8 Composition of Pakistan's Cybersecurity Domain

Although Pakistan is yet to explore and implement its potential in the cyber realm, the country has still made large amount of efforts to protect its critical information infrastructure and have drafted several policies and frameworks that aim to deal with the looming cyber threats and to maintain data sovereignty of the country. In order to fight with the cyber-crime and cyber security challenges, the Government of Pakistan, in 2018, established a National Center for Cyber Security (NCCS) in a joint initiative with the Higher Education Commission (HEC), which works in areas including block-chain security, malware analysis, cyber-crime investigation, intrusion detection and digital forensics.

Since Pakistan's economic data remains at a higher risk of breach, the State Bank of Pakistan (SBP) has its own Cyber Security Department which has the responsibility to develop cyber security strategies and framework for cyber-risk management and to detect and respond effectively to cyber threats. In addition to this, the Federal Investigation Agency of Pakistan has also launched National Response Center for Cyber (NR3C) Crime which was transpired in 2007 to tackle with the issue of online abuse and online harassment which falls under the category of cyber-crime. The objectives of the NRC3 include digital crime investigation, cyber-crime training, investigation of high-tech crimes, information system security and research and development.

4.9 Pakistan's Cyberspace Policies and Legal Frameworks

Pakistan has drafted and passed several policies and ordinances with regards to cybersecurity. The two laws that have already been existing in the country with reference to cyber-crime include the

year 1996 Pakistan Telecommunication Reorganisation Act and the year 2002 Electronic Transaction Ordinance which established the National Center for Cyber Crime (NR3C). In 2007, the government passed the Prevention of Electronic Crimes Ordinance which was followed up by the 2009 Prevention of Electronic Crimes Ordinance both of which aims to take measures against electronic crimes and to punish those who misuse the networks through investigation and trail of offences. The electronic offences laid down by the ordinance include electronic fraud and forgery, malicious codes, cyber stalking, cyber terrorism, spamming and misuse of electronic devices, amongst other electronic crimes. In 2006, the Information and Technology Ministry also created Inter-Ministerial Committee for the Evaluation of Websites.

Another attempt to provide cyber security can be seen in the 2014 National Cyber Security Council Bill which was introduced in the Senate to provide framework for cybersecurity however, the Bill was not approved by the Ministry of Information Technology on the grounds of being not in align with the national security of the state. In 2016, Prevention of Electronic Crimes Act was passed which essentially lays down the punishment for cyber offenders and for any unauthorized act against the country's critical information infrastructure. Furthermore, the Act also proposed the creation of Pakistan Computer Emergency Response Team (Pak-CERT) which aims to prevent and detect data breaches. Furthermore, an eminent feature of Pakistan's attempt to provide security in the cyber realm is the Pakistan Telecommunication Authority (PTA) which allows policymakers to draft informed policies with regards to the rapid technological advancement and also regulated and filter mobile networks when required by the government. Lastly, in July 2021, Pakistan's first National Security was adopted which points to the country's effort in prioritising cyber security however it also highlights Pakistan's delay in prioritizing cyber security in its national security.

4.10 Nature of Cyberattacks by Pakistan

While Pakistan is making attempts to protect its critical information infrastructure and to provide cybersecurity, the ICT environment continues to face cyber threats. The threats faced by Pakistan in the cyber domain include online financial frauds and money laundering, debit and credit card frauds, web defacement, hacking, cyber bullying, cyber stalking, influence operations, cyber proxies, malware attacks, unauthorised intrusions and digital espionage. Pakistan's exposure to these growing cyber threats is due to the reason that the policies implemented in the cyber domain

lack governance and institutional frameworks and lack IT experts. Similarly, Pakistan also lack investment in the digital sector which has the potential to strengthen digital infrastructures and existing policies. In addition, the country also lacks a comprehensive legal framework to deal with the cyber-threats which further makes country prone to these attacks. Pakistan has also long been absent in prioritizing cyber security in its national policy which has significantly contributed to country's inability to meet the cybersecurity criteria and potential capacity building measures. Thus, the inadequate cyber security standards has led Pakistan to be vulnerable to data breaches, influence operations and cyber proxies.

In the face of these internal challenges of policy implementation and external cyber threats, the nature of cyberwarfare adopted by Pakistan is defensive in nature in a sense that the attacks launched by Pakistan in the cyber domain are mainly to deter the enemies and to protect its own critical information infrastructure in the light of looming cyber threats from a neighbouring country –India. In 2010, Pakistan's military and government agencies became a target of a suspected Indian launched attack named Operation Hangover.

Similarly, another attack was launched in the same year aimed at defaming the websites of Pakistan under an Indian suspected attack named Black Dragon Indian Hacker Squad (Chandio, 2015). Thus, India's superiority in the cyber realm poses a huge threat to the national security of Pakistan in the face of lack of adequate response measures by Pakistan. Due to lack of advance cyber space technology and comprehensive security policies, hacktivism is increasing day by day in Pakistan and adequate legal and governmental steps are required for proper implementation of the National Security Policy.

While summarising the chapter, it can be clearly seen that the cyber space has become an increasingly prominent domain globally in terms of practise, government and national policies, and literature. Countries all across the world are modernizing their cyber domain and prioritizing cyber security in their national security policies because cyber threats transcend traditional boundaries and therefor it is significant to have cyber threat laws and policies in the face of increased threats. Considering the rise of this non-traditional security threat, South Asian region then becomes essential to study because of the volatile nature of the region and the enmity that exists between the two nuclear armed rivals, India and Pakistan. India's nature of warfare is the regional centric in nature where it deploys defensive cyber warfare when it comes to China but

offensive cyber warfare when it comes to Pakistan in the region due to the lack of cyber security policies drafted by Pakistan and the lack of technological advancement which gives India a technological edge over Pakistan in the region. Similarly, Pakistan has also made efforts to develop framework and policies related to cyber security but lacks proper implementation and investment in the cyber domain due to which the policies have failed to yield the required security. Therefore, it is essential for authorities in Pakistan to draft a comprehensive cyber security plan and to invest in the digitalization of country to be able to timely detect and deter potential cyber security threats.

CHAPTER 5

INFLUENCE OPERATIONS AS INSTRUMENTS OF HYBRID WARFARE BETWEEN INDIA-PAKISTAN & SECURITY IMPLICATIONS

5.1 Introduction

In this milieu where the nature and character of warfare between the two archrivals India and Pakistan is significantly shifting, influence operations have emerged as prominent instruments of hybrid warfare between the two countries which carry significant security implications. The weaponization of the civilian domains via influence operations as well as targeting cognitive vulnerabilities of a government, fostering mistrust between the government and its citizenry, and influencing its political decision-making puts an entire country at risk. It is in this context that the strategic reality of the link between politics and warfare is realized. Hybrid warfare gives actors the space to one-up each other in a series of small bursts of intense conflicts, and actors compete to achieve desired political objectives through hybrid means of warfare. This chapter will discuss how India is utilizing influence operations with a three-pronged approach against Pakistan:

i. For the international defamation of Pakistan
ii. For fostering political instability within Pakistan
iii. For the economic slowdown of Pakistan

Moreover, it will also explain how Pakistan is similarly a rising cyber threat for India in three ways:

i. As a constant low-intensity threat in the mutual cyber tit-for-tat between the two countries
ii. As a source of cyber terrorism
iii. As a source of disinformation and propaganda

5.2 Understanding Influence Operations: An Instrument of Hybrid Warfare?

According to the US Department of Defense, influence operations can be defined as such "coordinated and synchronized application of national diplomatic, informational, military, economic, and other capabilities in peacetime, crisis, conflict, and post-conflict to foster attitudes, behaviors, or decisions by foreign target audience that furthers US interest" (Larson et. al, 2009). Influence operations can include the collection of tactical information about an adversary as well as the dissemination of propaganda in pursuit of a competitive advantage over an opponent.

Influence operations are instruments of hybrid warfare as they are often used as a tool in the interplay or fusion of conventional as well as unconventional instruments of power and tools of subversion (Bilal, 2021). Hybrid warfare entails the blending of instruments or tools in a synchronized manner to exploit the vulnerabilities of an antagonist and achieve synergistic effects. Influence operations can be used to influence the population of target countries through information operations, proxy groups, and other influence operations (Chivvis, 2017).

Moreover, the influence operations used in hybrid warfare comprise of a variety of activities and cover the use of different instruments to destabilize a society by influencing its decision-making (Marovic, 2019). Interference in electoral processes, such as through campaigning, media, and social networks, is a common tactic used to influence the outcome of an election in a direction that favors the adversary's political interests. The use of cyber technologies promotes greater asymmetric opportunities for influence, control, and undermining of one's adversary in hybrid warfare.

5.3 India's Influence Operations against Pakistan: Deconstructing the Indian Modus Operandi

There have been several reports and allegations of Indian influence operations against Pakistan most notably the report on Indian influence operation "Indian Chronicles" by EU DisinfoLab. These operations are typically aimed at influencing public opinion, destabilizing the Pakistani government, and promoting Indian interests in the region. Some of the tactics that have been

reported to be used in these operations include propaganda campaigns, disinformation and fake news dissemination, cyber-attacks, and support for separatist movements in Pakistan.

5.3.1 International Defamation: The 'Indian Chronicles' Influence Operation against Pakistan

In 2020, a European Union (EU) DisinfoLab report claimed that Indian-backed disinformation networks were active across the globe, including in Pakistan, and were spreading propaganda against Pakistan. The "Indian Chronicles", as it was termed, was a fifteen year influence operation that began in 2005 and is still ongoing is one of the most paramount influence operation carried out by India against Pakistan (Machado et. al, 2020). The EU DisinfoLab report uncovered a massive operation targeting international institutions and European Union Member States by a network of over 750 fake local media outlets, NGOs, and think tanks which were used to promote Indian interests and discredit Pakistan. These fake media outlets and NGOs were run by the Srivastava Group, a Delhi-based NGO, that created and coordinated them with the mission to discredit nations in conflict with India in Asia, particularly Pakistan, and to a lesser extent, even China. The report also revealed that the Indian press agency Asian News International (ANI) was the only press agency to extensively cover these fake media outlets.

It aimed to spread a pro-Indian narrative, discredit Pakistan and its interests, and promote the ruling Indian government's policies and agendas on an international level. The operation actively involved the creation and dissemination of misleading and false information on a wide range of issues, including Indian-Pakistani relations, Indian-Chinese border disputes, and the Kashmir conflict. Furthermore, the operation involved the conscious and strategic manufacturing of information and its dissemination to specific target audiences to shape or alter their opinions (Raashed, 2020). It targeted members of the European Parliament and the United Nations, among others, and spread over at least 116 countries.

In terms of its impact, the operation was successful in building a strong sense of constant official support of the EU to Indian interests. Additionally, the operation used a large number of fake media outlets, a big network of zombies and misappropriated accredited NGOs, impersonating renowned personalities to create fake profiles, and laundering content produced by fake media to real media to undermine Pakistan internationally. The Indian Chronicles operation which was therefore

aimed to consolidate the power and improve the perception of India internationally, damaged the reputation of Pakistan vis-à-vis India ultimately garnering India more support from international institutions such as the EU and the UN.

5.3.2 Political Instability: Indian Propaganda Campaign in Balochistan and Against State Institutions

The goal of fostering political instability within Pakistan is well contextualized within the Indian milieu through the Doval Doctrine. The Doval Doctrine is a hybrid warfare doctrine created by India to achieve national objectives while remaining under the so-called "nuclear umbrella". It involves the use of irregular forces and unconventional methods to target key vulnerabilities of opponents. The doctrine is named after India's current National Security Advisor, Ajit Doval, who is known for formulating and promoting the doctrine. As part of this doctrine's implementation, the Indian government has been accused of supporting proxy separatist groups like the Baloch Liberation Army (BLA) in Balochistan and conduct propaganda against state institutions (Raashed, 2020).

Doval Doctrine: India's offensive Hybrid Warfare Strategy against Pakistan

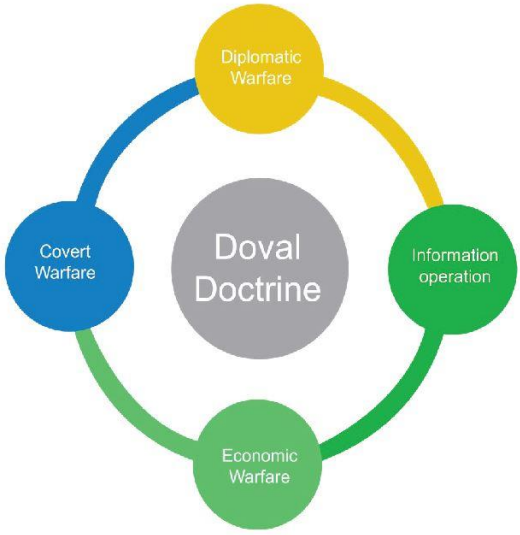


Figure 5.1

The use of information technology forms the dominant contour of this doctrine. It is a defensive offense doctrine that aims to prevent threats to India's national security. The Doval Doctrine is

considered a 'real and present danger' against Pakistan and has been followed by the BJP government in India (Shah, 2020). The doctrine puts a disproportionate pressure on the government to compensate for strategic weaknesses and neglects the traditional tools of diplomacy. Furthermore, the doctrine is characterized by a proactive approach to national security, where India aims to neutralize threats before they become a major issue, and is based on the principles of using threats as opportunities, pre-emption, and striking at the root of the problem. It is controversial and has been criticized for its aggressive posture, but has also been praised as a bold and effective approach towards securing India's national interests.

There have been reports of alleged Indian influence operations and propaganda campaigns in Balochistan, a restive Pakistani province where separatist movements have been active. The Pakistani leadership has been blamed for not taking enough action to protect Baloch rights, identity, and the province's demography (Shahi & Baloch, 2021). India has been accused of supporting these separatist elements as part of its efforts to exert influence in the region and has been exploiting this critical vulnerability of Pakistan. Additionally, there have been reports of Indian intelligence agencies conducting espionage and gathering information about the situation in Balochistan. In 2016, Indian Prime Minister Narendra Modi also referred to Balochistan in his Independence Day speech and denounced Pakistan for its alleged human rights abuses in Balochistan (Khan, 2021).

The Indian government on the other hand has denied allegations of interference in Balochistan and has accused Pakistan of sponsoring terrorism in India. India has not officially commented on the issue of Balochistan, but some sources suggest that India's objective is to undermine Pakistan's economy by disturbing peace in Balochistan and not allowing the development of the Gwadar port to safeguard its SLOC (Khan, 2021). The Director-General of Inter-Services Public Relations (ISPR) has also stated that the recent upsurge in violence in Pakistan is a direct consequence of Indian interferencee (Khetran, 2017).

5.3.3 Economic Slowdown: The FATF Grey List

India has been accused by Pakistan of playing a role in keeping it on the grey list of the Financial Action Task Force (FATF), a global intergovernmental organization that sets standards and promotes effective implementation of legal, regulatory and operational measures for combating

money laundering, terrorist financing, and other related threats to the integrity of the international financial system. A statement by the Pakistan's Foreign Office levied that India lobbied hard to keep Pakistan on the grey list and prevent it from being moved to the black list in a "malicious campaign". India has denied any wrongdoing and has maintained that it has been working towards ensuring greater compliance with the FATF recommendations.

Pakistan was on the FATF's grey list due to strategic deficiencies in its anti-money laundering and counter-terrorism financing regimes. Pakistan was first grey-listed by the FATF in 2008 for a brief period but quickly came out of it (DAWN, 2022). In June 2018, Pakistan was grey-listed again after the FATF found multiple strategic anti-money laundering and combating the financing of terrorism deficiencies and was not removed until 2022. According to several studies India has played a role in keeping Pakistan on the grey list of the Financial Action Task Force (FATF) (Kunwar, 2021; Parvaz, 2021). India has reportedly used the FATF for its political designs against Pakistan (Parvaz, 2021). The FATF is an important measure for India to put pressure on Pakistan to dismantle the infrastructure that supports cross-border attacks. However, Pakistan claims to be sincerely and constructively engaged with FATF during the implementation of the FATF Action Plan.

RSIL, a prominent legal think-tank in Pakistan, released a comprehensive report in June 2021 that analyzed Pakistan's progress in regards to FATF obligations. The report revealed that Pakistan's progress was not subjected to the same level of strict scrutiny as other countries such as Iceland, Bangladesh, and Bhutan, which had been removed from the grey list. The report specifically highlighted the leniency of FATF's evaluation to other countries compared to Pakistan's efforts in investigating and prosecuting terrorist financing and money laundering (Aziz & Iftikhar, 2021). Additionally, a 2021 research paper published by an independent think-tank, Tabadlab, reported that grey-listing spanning from 2008 to 2019, may have resulted in GDP losses worth $38 billion for Pakistan (Sardar, 2021).

5.4 Indian Perspective

Although there are no influence operations carried out by Pakistan against India in literature, also owing up to its relatively lesser capabilities and resources to carry one, there are still a number of Pakistan's actions in cyber space that have formed Indian concerns.

5.4.1 The Cyber Tit-for-Tat between India and Pakistan

In the early days, Pakistan constituted a major cyber threat to India through hacking and defacing of Indian websites. This was facilitated by the fact that many Indian websites were using outdated software and open-source programs, making them vulnerable to these attacks. During the Kargil conflict in 1999 between India and Pakistan, both Indian and Pakistani hackers engaged in retaliatory attacks, targeting mainly government websites. This trend of retaliatory cyber attacks and "tit-for-tat" has continued over the years, with the attacks becoming more sophisticated with modern cyber infrastructure.

The actors involved in this cyber tit-for-tat can be categorized into two groups: the hacktavists and patriot hackers which at both sides target government institutions and media, and the Advanced Persistent Threats (APTs) which are more advanced and sophisticated and target the military institution as well as diplomatic personnel (Baezner, 2018). The most consistent cyber attack techniques between the two countries is website defacement of government or media websites, spear phishing through which victims are lured into clicking malicious links and file attachments in order to steal data, and finally malware which is spread through applications in order to steal data and conduct espionage by accessing sensitive information. A chronology of this cyber tit-for-tat retaliation is given below where cyber space has materialized into an arena of retaliation from real world events such as skirmishes at the Line of Control (LoC), surgical strike operations, and national days.

Chronology of India-Pakistan Cyber Tit-for-Tat since 2014

26.01.2014	Pakistani hackers deface thousands of Indian websites on the Indian Republic Day (Khan, 2014).
26.11.2014	Indian hackers deface several Pakistani government websites on the anniversary of the Mumbai terrorist attacks (Web Desk, 2014a).
26.11.2015	Indian hackers target more than 200 Pakistani websites on the anniversary of the Mumbai terrorist attacks. Pakistani hackers retaliate by defacing the Indian Central Bank website.
06.01.2016	Terrorists attack an Indian Air Force base in Pathankot in northern India.
07.01.2016	Indian hackers retaliate for the terrorist attack in Pathankot with the defacement of Pakistani websites (RFSID, 2016).
03.03.2016	Pakistani authorities arrest an Indian individual suspected of espionage in Pakistan (Shukla, 2017).
15.08.2016	Indian hackers deface more than 50 Pakistani websites on Pakistan Independence Day (TNM Staff, 2016).
18.09.2016	A Pakistani militant group kills 19 individuals in an attack in Uri in Jammu.
23.09.2016	India retaliates for the attack in Uri with surgical strikes.
04.10.2016	Pakistani hackers retaliate for the surgical strikes with the defacement of thousands of Indian websites and Indian hackers claim to have access to Pakistani critical infrastructure networks.
10.04.2017	The Indian individual arrested in 2016 receives the death penalty in Pakistan.
10.04.2017	Indian hackers retaliate with the defacement of hundreds of Pakistani websites to protest against their compatriot's death penalty sentence (Trivedi, 2016).

Figure 5.2 (adapted from Baezner, 2018)

5.4.2 Cyber Terrorism

Cyber terrorism constitutes as another important issue in India's cybersecurity landscape vis-à-vis Pakistan. Groups like Jaish-e-Mohammed (JeM) and Lashkar-e-Tayyaba (LeT), who India accuses of being backed by Pakistan, have been utilising the cyber space especially the social media platforms to spread propaganda, recruit members, and radicalize people in India (Rao, 2016).

New concerns also emanate from the rising Daesh group (Islamic State) which has intensified this problem, as they are focusing on targeting and mobilizing individuals to carry out attacks on their own. Indian concerns are further cemented as Daesh managed to lure Indian youth through their propaganda to join their violent campaign in Iraq and Syria during their height from 2014 to 2017. This has resultantly caused a significant challenge for India's counter-terrorism efforts, as they work to counter extremist propaganda within the cyberspace.

5.4.3 The Threat of Disinformation and Propaganda

Another threat that India perceives from Pakistan in its cyber space is the issue of extremist propaganda. The issue of extremist propaganda is closely linked to the problem of fake news and disinformation campaigns, which have become increasingly prevalent due to the widespread use of social media.

In this regard, India perceives Pakistan as a particularly concerning source of disinformation as well as the extremist propaganda. In August 2019, following India's decision to withdraw the special status of Jammu and Kashmir (J&K), the Pakistani government used social media platforms to spread false information about India. This was done through the use of fake profiles, cyber trolls, journalists, and even Pakistani diplomats, with a focus on topics such as alleged human rights violations in Kashmir which went on to highlight hardships faced by Kashmiri citizens during the revocation of its special status. While the Indian government has made efforts to combat these disinformation campaigns, it has struggled to keep up with the rapidly evolving nature of the cyberspace and sees the issue as a rising concern.

5.5 Security Implications: The Future of Strategic Stability in South Asia Amidst Cyber Threats

For over seven decades, India and Pakistan have remained entrenched in a bitter and seemingly unending conflict, with no resolution in sight. The future of strategic stability in South Asia is therefore the top concern in a rapidly evolving cyber arena which gives both India and Pakistan the edge of plausible deniability and remaining ambiguous whilst simultaneously carrying out non-escalatory yet consistent attacks on each other's institutions, critical infrastructure, personnels, and entire populations.

In the realm of cyber technology, the interconnectedness of all devices poses a threat to all aspects of society. This domain is particularly susceptible to vulnerability as it encompasses and brings together multitude of actors such as governments and state institutions, non-state actors, and individuals. Of these, the military has a heightened interest in exploiting cyber space as it presents a challenge in terms of identifying the aggressor. Moreover, the cost of deploying cyber operations is minimal. Cyber technology has then ability to destabilize various aspects of society making it a highly vulnerable domain due to low cost of deployment and even a lower cost of responsibility.

Considering both the countries are nuclear powers and their respective nuclear plants and warheads are being modernized, one significant challenge is the digitalization of the command, control, communication, computing, and intelligence (C4I) structures of the two countries (Babar et al., 2021). Due to the underdeveloped nature of autonomous Intelligence Surveillance Reconnaissance (ISR), early-warning systems, and Ballistic Missile Defence (BMD) capabilities, there is a significant likelihood of false alarms from these systems. If a country's early-warning, ISR, and BMD sensors provide inaccurate information and false negatives are transmitted to it, it may be perceived as legitimate and prompt a pre-emptive or preventive use of nuclear weapons as a response. This could be extremely dangerous and off-tip the strategic balance.

Moreover, cyber threats such as spoofing can produce false positives on the early-warning satellites and radars which impacts their reliability in detection, or can alternatively produce false negatives which can cause blindness in intercepting enemy's warheads. Spoofing, in essence, interrupts the communication by posing as the original source of the communication. The caveat here is the discrepancy between the real threat and the perceived threat from an adversary.

Therefore, emerging cyber technologies present a challenge for the threat perception of India and Pakistan.

Apart from causing a great challenge for threat perception, cyber threats can also hamper the operations and delivery systems. As evident from the Stuxnet incident of attack on nuclear facility, such cyber technologies are available which can hijack critical infrastructure and cause disruption in the operations and delivery systems of missiles and warheads. In an event where command and control is attacked, the operations may seriously be hindered which could cause failed or inaccurate launch leading to destruction and even self-destruction. In such a scenario, the strategic stability is under threat as the deterrent value of nuclear heads is called to question as their operations can be rendered ineffective through cyber attacks.

Additionally, seeing the current trend of the cyber tit-for-tat between India and Pakistan, if the low-level attacks become too disruptive there is a chance of conventional conflict getting triggered which also brings the use of nuclear weapons in question. It is important to note that in times of heighted tensions, the two arch-rivals have utilised cyber attacks to achieve their national interest as was the case of post-Pulwana cyber attacks in 2019. These regular small scale cyber attacks such as website defacement and cyber espionage on personnels have a social impact where it creates distrust between the government and the citizens in terms of their security and data protection as well as create hindrances for the government. However, the effects of cyber attacks have largely been constrained and have not yet escalated to the conventional realm in fifteen years.

Finally, technological advancement invariably has an impact on military postures of countries. Given that the two countries are at loggerheads with each other since their inception with an important border dispute bittering the conflict between them, there is more of an incentive to adopt modern technologies for the purpose of warfare. The lack of clarity on their own respective nuclear doctrines further aggravates this problem (Topychkanov, 2022). Since nuclear policies should be dictated by constant consensus-based goals instead of technological advancements, newly emerging technologies should be integrated insofar as they run consistently with the goals. However, both countries lack this clarity and the issue is further compounded by their lack of transparency, disrupted communication, and absence of Confidence Building Measures (CBMs) with respect to each other which fogs such judgement at a policy level.

While a conflict based on cyber attacks, proxies and influence operations may not occur at this point, given the vast strategic tensions between the two countries on Kashmir border dispute and Indian Ocean, the possibility of such a conflict in the future can not be ruled out if the offense-defense balance tips. Additionally, although, it is premature to give a final verdict on the lasting impact of emerging cyber technologies on strategic stability in South Asia, it is crucial to emphasize that regardless of the extent of technological progress the human element must always retain control over strategic decision-making and command-and-control systems.

In conclusion, due to advancements in military and technology, the concept of mutually assured destruction has become less relevant. Instead, in the 21st century, a new form of warfare known as Hybrid Warfare has emerged. This type of warfare involves a multifaceted approach to harm the enemy in various ways, including economically, politically, diplomatically, ideologically, and more. India is currently engaged in information warfare against Pakistan as part of the Doval Doctrine. This strategy aims to use covert means to exploit Pakistan's economic, political, and security vulnerabilities, while also damaging its international reputation.

As the chances of traditional warfare decrease, India has turned to undercover information operations against Pakistan. Although the information weaponizing operation that was recently uncovered by the EU Disinfo Lab had been underway for fifteen years, it is still unclear how much covert activity has taken place under the Modi-Doval leadership. However, Indian motivations have been clear from NSA Doval's remarks, "Make the paradigm shift; go for high technology, and in response, prepare for intelligence driven operations [sic]" (Syed, 2019).

Similarly, Pakistan has used the cyber space against India to respond and retaliate to real events as is the case of their prolonged cyber tit-for-tat. Additionally, India also precieves the country as spreading cyber terrorism in the country and is particularly concerned about groups such as LeT, JeM and Daesh or the Islamic State. Finally, India also struggles to keep up with the evolving nature of disinformation and propaganda in the cyber space especially the one related to its national objectives carried out by Pakistan.

CHAPTER 6

RECOMMENDATIONS FOR PAKISTAN: STEPS TOWARDS DEVELOPING COMPREHENSIVE CYBERSECURITY FRAMEWORK

6.1 Introduction

In the wake of rapid technological advancements, countries around the world are prioritizing cyber security in their national policies as a strategic asset for their security and to protect their critical information infrastructure. As the concept of security and security-related threats are evolving from a traditional perspective to a combined traditional and non-traditional threat perceptive, as analysed by Liddell Hart in the Indirect Approach, it is essential for governments to revisit their national security policies and adapt new frameworks to cater to evolving cyber threats. A closer look at historical enmity between states like India and Pakistan highlights that cyber space has emerged a new layer of potential conflict apart from the layer of traditional conflicts and while there has been no major cyber conflict between the countries, the potential of cyberspace as a potential flashpoint cannot be disregarded as it has the potential to change the dynamic of conflict between India and Pakistan and for the South Asian region as a whole.

Due to a comparatively low cost of cyber conflicts, as compared to traditional military conflicts, cyber space and cyber conflicts even allows countries with a limited military capability to cause damage to the other country and to particularly damage their critical information infrastructure at a point in time when they are least expecting it –also known as the line of least resistance postulated by Liddell Hart in his eight axioms of the Indirect Approach. However, since cyberattacks are secretive in nature, it is essential for countries to be prepared for cyberattacks and have an effective degree of preparedness with regards to attacks on cyber security. A closer look at India and Pakistan's GSI standing reveals that India is relatively more advanced and prepared than Pakistan when it comes to a response mechanism for cyber-attack. Therefore, it is significant that policymakers in Pakistan prioritize cyber security and draft a comprehensive framework to detect and effectively respond to targeted cyber-attacks.

6.2 Recommendations

The discussion in previous chapters suggests that there is an urgent need for Pakistan to develop policy and security frameworks to ensure cyber security and the protection of critical information infrastructure alongside the proper implementation of the previously drafted policies. The following section aims to provide a list of recommendations and steps that Pakistan can take considering the country's vulnerability to cyber-attacks and influence operations.

6.2.1 Creation of a Cyber Policy Centre

Considering the amount of significance given by other countries in the region, for instance the coordination amongst several ministries and state agencies for cyber security by India, it becomes crucial that Pakistan also dedicates the same amount of significance and thought input to the cyber domain. For this purpose, a potential step that Pakistan can take is the formulation of cyber policy cell which would work in coordination with the Information and Technology Ministry of Pakistan and would operate at a national level to guide and scrutinize policies related to cyber security alongside providing strategic directions to institutions across country that are working in the cyber domain.

The cyber policy centre would be tasked to formulate a roadmap to increase and develop cyber capabilities, and an in-depth analysis of potential cyber threats and their manifestations. Although there are several think tanks in Pakistan that are working towards, and advocating initiatives in the cyber security domain, however a creation of a cyber policy centre can help in bringing together researchers, policymakers and leading software and IT experts for the purpose of establishing a comprehensive security and response framework in the face of increasing cyber threats. Furthermore, ministries such as Information and Technology Ministry of Pakistan and the Ministry of Science and Technology can work in coordination to achieve a multi-layered response approach towards implementation loopholes in the existing policies.

6.2.2 Establishment of National Cyber Security Authority (NCSA)

The establishment of a National Cyber Security Authority (NCSA) goes in tandem with the previous recommendation of creation of a Cyber Security Policy Centre. While the Cyber Security

Policy Centre will be tasked with analysing cyber-threats and loopholes in the existing policies, the establishment of a NCSA then becomes significant as it will be tasked with coordination and implementation of cyber security policies at all levels including organizational, provincial and national level. The NCSA will serve as a central body for the implementation of policies, therefore, its establishment is the need of the time. It is essential for policymakers to clarify the cyber security governance and operating framework for the effective implementation of policies and to achieve desirable results.

The coordination between Cyber Security Policy Centre and NCSA then become a crucial step in order to develop exclusive research in the cyber domain and provides avenue for inter-intuitional coordination for better synergy. It is highlight significant for Pakistan establish comprehensive mechanism to safeguard its cyber frontier, and to coordinate amongst several institutions and stakeholders, therefore, creation of an independent authority for cyber security governance becomes an essential step for Pakistan to take.

Cybersecurity Guideline Response Framework

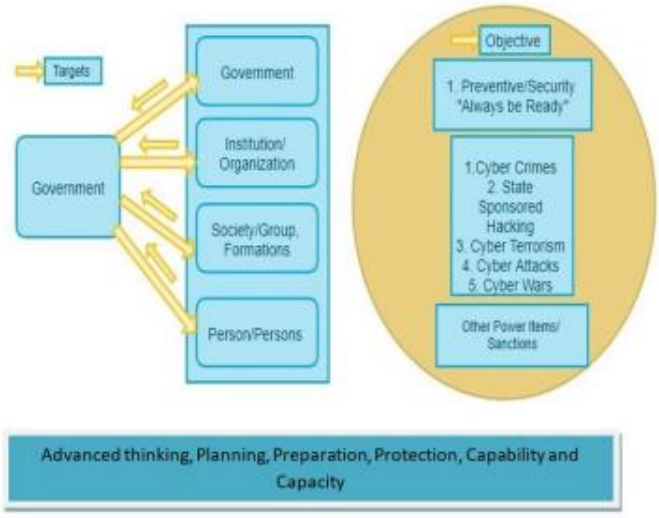


Figure 6.1

6.2.3 Creation of Strategic Cyber Security Guideline

The creation of a strategic cyber security guideline goes in accordance with the previous two recommendations as the creation of Cyber Policy Centre will assist in formulating policies and detecting potential cyber threats, whereas the NSCA will be tasked with the implementation of

those policies. The drafting of a strategic cyber security guideline then becomes essential in order to outline a national security vision and steps to take in case of a cyber-attack –action plan for a response.

The strategic cyber security guideline can serve as a strategy or a response framework in case of a cyber intrusion thereby contributing in the protection of cyber space. Furthermore, the strategic security guideline can also focus on improving the ability to detect cyber threats by improving a response framework, knowledge sharing, capacity building and international collaborations to increase development in the domain of cyber security. The goal of the guideline is to build resilience against wide range of cyber threats.

6.2.4 Cyber Diplomacy

Diplomacy has always served as a successful took to promote bilateral and peaceful relations between states. Cyber diplomacy is referred as the use of diplomatic tools by states to conduct peaceful relations in the cyberspace to achieve objectives in the complex and ever-evolving cyber domain through the use of shared protocols and accepted rules, and to minimize the potential of cyber aggression, data breaches, influence operations, cyber proxies, cyber espionage and other offensive cyber-crimes carried out by either state or non-state actors (Cyber Risk GmbH). A landmark step towards cyber diplomacy is the Paris Call for Trust and Security in Cyberspace which was signed in 2018 as a call for states and actors to come together and find middle grounds to uphold the norms of the cyberspace.

Keeping in mind the implications a potential cyber warfare between India and Pakistan can have on the South Asian region, it is highly significant that both of these states engage themselves in acts of cyber diplomacy over cyber aggression. To engage in cyber diplomacy, it is essential for India and Pakistan to comply responsibly with the cyber international norms and become part or signatories of the international treaties and conventions relating to cyber space such as the 2001 Budapest Convention on Cybercrime.

Another step can be the deployment of mutual trust and stability framework in the form of confidence building measures for crisis management, engagement, restraint and collaboration. For crisis management, functional cyber-crime response teams alongside multilateral cyber

adjudication and a cyber hotline can be developed. India and Pakistan already have a cyber hotline namely the Director-General of Military Operations (DGMO), established in 2018, which is linked with Secretariat Building in New Delhi to Prime Minister's Office in Islamabad. A similar initiative can be taken to establish a hotline between the Foreign Ministers of two countries for better communication and should be used regularly to examine the cyber space issues between the two countries.

For collaboration, both states can jointly conduct investigations in the cyber-crime incidents in compliance with the international practices regarding cyberspace and the international laws governing cyberspace. To help mitigate crises, both states can create a Joint Probing Committee of their respective trusted experts and officials to work towards mutually workable frameworks.

6.2.5 Confidence Building Measures (CBMs)

Confidence Building Measures (CBMs) have historically been used by India and Pakistan to reduce their traditional security challenges, however, when it comes to non-military security challenges, the CBMs between the two have not ventured beyond the Director-General of Military Operations (DGMO) and only basic information sharing which has led India and Pakistan to heavily rely on Track II assisted third-party diplomacy.

Unlike the traditional security threats, the non-traditional security threats present a unique set of challenges to both the states due to lack of an adequate mechanism to address the cyberspace challenges. Therefore, it is essential for India and Pakistan to engage in a bilateral cooperative framework for the purpose of solving the unique and unaddressed cyber challenges, and for risk reduction and risk aversion.

First step towards establishing a mutual trust and cooperation framework is to develop a joint-understanding approach based on joint technological and academic analysis of cyber concerns of both countries to bolster the understanding of shared concerns and to assess the gaps in the frameworks while offering risk assessment and combined training programs by the international stakeholders to enhance learning in the cyber domain. Therefore, academic discussion can serve as a potential first step towards the CBMs because it does not threaten any states national interest,

nor requires a lot of funding but still provides a platform to both countries to increase confidence and to learn about shared concerns.

The second step can be aimed at bringing the civilian nuclear enterprises together as nuclear domain is one of the hot topics between the two nuclear armed rivals. This medium can serve as a Track II diplomacy wherein the civilian nuclear enterprises from both sides will share their nuclear cyber-related incidents and concerns to address the existing deficiencies in the cybersecurity policies of both states.

Developing bilateral CBMs is thus an essential step that should be taken by both states in the face of ransomware attacks to understand and address cyber vulnerabilities, its fallouts on the human security aspects and to design information sharing mechanisms.

The third step should then be focused on creating a joint task force on cyber space with an institutional backing –such as it was done in the Indus Water Treaty backed by the Indus Water Commission which was signed between the countries to solve the issue of water distribution. The Commission was able to make both states agree that engaging in a joint initiative is beneficial for both states to address performance deficiencies and mutual vulnerabilities. Similarly, the joint task force on cyberspace would focus on cybersecurity vulnerabilities between India and Pakistan, threat assessment and response framework. In addition, compliance with the international security standards will be one of the crucial factors of the task force, however, moving towards this requires a deeper understanding of the cybersecurity concerns on both sides. Bilateral initiatives on cyberspace between India and Pakistan can be assisted by any international organization such as the International Atomic Energy Commission (IAEA).

Therefore, to build CBMs, the two countries can adopt the above suggested three-pronged approach which includes a joint understanding approach, Track II diplomacy and creating a joint task force as these measures can contribute towards a better understanding of cyber threat perceptions and hared cyber space concerns.

Concluding, it can be analysed that the digital revolution is transforming the world, and India and Pakistan are no exception. Both countries are rapidly embracing digitalization to stimulate economic growth, open new avenues for their citizens, and enhance their global standing. However, this trend also brings with it increased risk of cyber threats due to the vast amounts of

data stored digitally in both states. To protect against such risks, both India and Pakistan have to implement strong cybersecurity measures as well as work on preparedness and capabilities that can be used in case of a cyber-attacks.

Additionally, cyber intrusions have become increasingly sophisticated over time, allowing malicious actors to gain access to sensitive information or systems that could potentially be used against a country's citizens or national security interests. This has opened new pathways of escalation as well as new risks of miscalculation or misperception in international relations.

Therefore, it is essential that Pakistan and India continue exploring ways they can jointly address any cyber threats posed by one another while simultaneously taking steps independently through improved cybersecurity measures to ensure that any attempts at interference from either side will be thwarted before causing significant damage either economically or politically. Such efforts would go a long way towards mitigating future tensions between them while also providing an opportunity for collaboration instead of furthering hostilities down even more dangerous paths than those already taken historically.

CHAPTER 7

CONCLUSION

In the rapidly advancing and complex modern world, digital footprints of states are increasing at a fast pace with growing significance attached to cyberspace and cybersecurity. Cybersecurity refers to the protection of data, internet connected systems, electronic systems, programmes and critical information infrastructure from digital attacks –also called cyber-attacks. Cybersecurity is utilised by individuals or enterprises, inside or outside of an organization, to combat threats against data and network systems.

There are different types of cyber threats which include malware, spyware, ransomware, phishing and cyber-crime, amongst others. Whereas, different types of cyber-attacks include cyber proxies, influence operations, data breaches, identity based attacks, spoofing and password attacks, amongst others. On the other hand, there are also several different types of cybersecurity which constitute network security, mobile security, cloud security, application security, endpoint security and zero trust –all of which are aimed at building security walls around the data to protect the valuable asset of the organization.

The reason why the study of cyber space and cyber-attacks then becomes crucial to study and research upon is because it is an emerging domain with regards to security and states in the international arena are attaching significance to cyberspace and cyber security in their national security policies, strategies and frameworks. This is also because cyber threats are not visible as compared to conventional threats such as increase in arms and nuclear weapons. When the threats are visible to states, it is relatively easy for them to devise a plan of action or to acquire relatively similar capabilities to strengthen their own security.

However, the threats become more crucial for states when they are unable to see or detect the threats which in turns lead the states to be at an extremely vulnerable position as they are now unable to acquire similar capabilities as that of the adversary state. Therefore, the study of cyberspace and cyber-attack is gaining more popularity between the leaders and policy makers so that the state is equipped with sufficient capabilities and a response framework in case of an unwanted and undetected attack.

The phenomenon of undetected attack highlights the strategy proposed by the British military strategist, Basil Liddell Hart who formulated the Indirect Approach with the two core interconnected ideas: dislocation and exploitation. The Indirect Approach, in its main essence, highlights the significance of rapid technological advancements and how states can utilise those to strategically gain advantage over their adversary without fighting an on-ground battle and without causing maximum bloodshed which he witnessed in the two World Wars.

Hart offers an approach towards subduing the enemy with less tools utilised. This can be seen through conventional versus non-conventional types of threats, challenges and warfare. For instance, in a conventional warfare, states have to train their soldiers and invest and equip themselves in all forms of arsenals such as land, sea and air. This in turns leads to a lot of spending on the preparation of warfare and even during the warfare, a lot of bloodshed and casualties take place, which can have an impact on people and things even years after the war has ended.

After analysing these strategies and their results, Liddell Hart suggested the strategy of Indirect Approach which essentially allows the state to launch an attack without heavy military spending. This means that the significance of technological advancement is rapidly growing as technological advancement and advance cyberspace capabilities can allow states to subdue the enemy without an on-ground attack that would result into bloodshed. Furthermore, Liddell Hart also emphasizes on the importance of understanding the psychology of the enemy and dispersing your resources at several places to launch an attack on enemy's weakest area instead of attacking the powerful area. This implies that enemy's weakest line of resistance or line of least expectation should be attacked so that the enemy could be captured without wasting too many attempts.

The whole concept of an indirect attack therefore remains relevant in the recent times due to the advancements in information technology which allows the states to launch an undetectable attack on the adversary, however, at the same time, it also puts the states at a vulnerable position from a similar attack as these cyber-attacks cannot be seen visibly. Furthermore, this is a relative new domain of security for states that is currently evolving.

The issue then becomes relevant for South Asia because it is an already volatile region and the emergence of this new domain of security challenge between India and Pakistan not only puts the two adversaries at a point of competition, but also has consequences for the South Asian region as a whole as any conflict between these two nuclear-armed rivals could be costly for states in the

region. With regards to acquiring cyberspace capabilities, both India and Pakistan are working on formulating policies and response frameworks in the face of unwanted and ever-emerging cyber-attack. If we analyse the nature of these capabilities between the two states, the nature of India is offensive due to the technological edge that it has over Pakistan as India also stands higher than Pakistan in the Global Security Index. On the other hand, the nature of Pakistan is defensive in nature due to its lack of technological development, lack of internet experts and the lack of attention paid to the cyber domain. This can be seen through the time frame of the formulation of National Security Policies by bot states. India's security policy was formulated in 2013 whereas Pakistan's security policy was formulated in 2021.

However, despite the efforts made by both sides to be equipped in the face of cyber-threats, there is implementation gaps in the policies formulated by both countries. This is because the cyber domain is currently emerging and it would require time for states to be fully equipped in cyberspace. Although there has been no major cyberwar fought between India and Pakistan, both states have been engaged in cyber proxies and influence operations to cause political instability especially during the times of heightened tensions between the two countries where events in of the real would also prompt a response in the form of a cyber attack on each other.

Moreover, in case of India and Pakistan, both countries have incentives to adopt for indirect approach and engage in cyber warfare through proxies for three distinct reasons. Firstly, the potential of cyberspace to be used for non-escalatory conflict is significant in South Asia, where the balance of power between nuclear nations is delicate. Using cyber operations allows for a range of low-intensity conflict options. Secondly, this indirect approach grants actors like India and Pakistan "plausible deniability" to pursue their foreign policy and national objectives through cyber attacks without facing consequences. Thirdly, due to the difficulty of defending against cyber attacks, the offense holds an advantage in this arena of strategic competition, reducing defense to risk tolerance and mitigation.

The two countries also constitute as major cyber threats to one another. Pakistan's main concerns stem from the EU DisinfoLab's exposed wide network of influence operation known as "Indian Chronicles" which has considerably defamed the country's repute and image at an international stage. The carefully woven fifteen year long influence operation has exposed the length's India has gone to undermine Pakistan internationally. Another concern for Pakistan is Indian propaganda

against its state institutions and exploiting its critical vulnerability in Balochistan vis-à-vis information warfare which is comprehensively outlined as the dominant contour of the Doval Doctrine. Pakistan is also concerned about the impact of the international defamation campaign by India against the country that kept the country in the FATF grey list despite constructive engagement from Pakistan's end.

India on the other hand, while hasn't been a target of Pakistan's influence operations, it has faced regular cyber attacks from proxies such as hacktavists and patriot hackers of Pakistan as well as Advanced Persistent Threats (APTs). However, the country has also retaliated with the same which has led the entire phenomenon to be the one of cyber tit-for-tat between the two countries who are already at loggerheads of each other. An additional Indian concern emanating from cyber space is that of cyber terrorism from Pakistan which it accuses is spread through Pakistan-backed terrorist groups such as LeT and JeM which recruit and radicalize Indian citizens as well as spread propaganda. In the same line, another concern for India is the threat of disinformation and propaganda from Pakistan such as on the instance of the revocation of special status of Kashmir in the aftermath of which it alleges that Pakistan formed fake cyber trolls, journalists and even diplomats to condemn Indian aggression.

Ultimately, this raises the concern for the future of strategic stability in South Asia amidst a rapidly evolving cyberspace between the two nuclear-armed arch-rivals, India and Pakistan. The integration of cyber space with the nuclear and military component is relatively immature which is also the reason why its highly susceptible to vulnerabilities and can be exploited. Both threat perception and its response is seriously unreliable and destructive if early-warning systems as well as delivery mechanisms can be the target of cyber attacks.

This further brings into question the deterrent value of nuclear heads is called to question as their operations can be rendered ineffective through cyber attacks. Finally, the lack of clarity at the level of strategic decision-making regarding nuclear policies in terms of pursuing a policy based on technological advancements as compared to consistent and agreed goals further presents a pessimistic view of strategic stability in a hostile environment of disruptive communications, absence of transparency, accountability and CBMs between the two countries. While the incidents that constitute as cyber threats have not crossed a red line, are small-scale, and have not triggered a conflict between the two countries the possibility of it in the near future cannot be ruled out.

However, as mentioned earlier, international actions do not exist isolation. Every action that is taken by any states has consequences for others and in a region like South Asia, that is already volatile, a new form of security challenge and a new form of geopolitical competition cannot be accepted as any action that would be taken against other state will have consequences for those in the region. This implies that the cyberspace should not be utilised as an area of competition between India and Pakistan, however, both the states could engage in cyber diplomacy and confidence building measures to establish a mutual trust and cooperation framework to develop a joint-understanding approach based on joint technological and academic analysis of cyber concerns of both countries to bolster the understanding of shared concerns and to assess the gaps in the frameworks while offering risk assessment and combined training programs by the international stakeholders to enhance learning in the cyber domain.

REFERENCES

About NCCS. (n.d.). National Center for Cyber Security | Pakistan. https://www.nccs.pk/nccs/nccs-objectives

Aaj News. (2020). *IndianChronicles: 15-year-old disinformation operation against Pakistan exposed*. Aaj English TV. https://www.aajenglish.tv/news/30249246/

Asad, T. (2022). *Doval doctrine distorting Pakistan's image: An appraisal*. Hilal Publications. https://www.hilal.gov.pk/eng-article/detail/NjY2MQ==.html

Aziz, J., & Iftikhar, N. F. (2021). *Measuring Pakistan's technical compliance with the FATF recommendations*. RSIL. https://rsilpak.org/wp-content/uploads/2021/05/2021_FATF-technical-compliance_RSIL.pdf

Babar, S. I., Mirza, M. N., & Qaisrani, I. H. (2021). Evaluating the Nature of Cyber Warfare between Pakistan and India. *Webology*, *18*(6), 6973-6985. https://www.webology.org/data-cms/articles/20220827072604pmwebology%2018%20(6)%20-%20596.pdf

Baezner, M. (2018). *Regional rivalry between IndiaPakistan: tit-for-tat in cyberspace*. Center for Security Studies (CSS) ETH Zürich. https://www.researchgate.net/profile/Marie-Baezner/publication/326866504_Regional_rivalry_between_India-Pakistan_tit-for-tat_in_cyberspace/links/5b6985fd299bf14c6d950724/Regional-rivalry-between-India-Pakistan-tit-for-tat-in-cyberspace.pdf

Basil Liddell Hart and the art of peace. (2022, November 25). Engelsberg ideas. https://engelsbergideas.com/portraits/basil-liddell-hart-and-the-art-of-peace/

Baker, E. W. (2013). A Model for the Impact of Cybersecurity Infrastructure on Economic Development in Emerging Economies: Evaluating the Contrasting Cases of India and Pakistan. Taylor and Francis.

B. H. Liddell Hart, strategy (1954). (2016, January 19). Classics of Strategy and Diplomacy – Recovering the classic sources of strategic thinking. https://classicsofstrategy.com/2016/01/19/liddell-hart-strategy-1954/

Bilal, A. (2021). *Hybrid warfare – New threats, complexity, and 'Trust' as the antidote*. NATO Review. https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html

Borghard, E. D., & Lonergan, S. W. (2016). *Can States Calculate the Risks of Using Cyber Proxies?* Science Direct. https://www.sciencedirect.com/science/article/abs/pii/S0030438716300175?casa_token=daifvuBynDcAAAAA:EpTUs0ZsYQzrjfgel1VWWxC10T4hTNpUQK5cPXbEcL92gSLaErYkCTc5t9k5G87UBiJiQWRiWA

Chandio, K. 2015. Cyber security/warfare and Pakistan. Islamabad Policy Research Institute

Cherry, L. M., & Pascucci, P. P. (2023). *International law in cyberspace*. American Bar Association. https://www.americanbar.org/groups/law_national_security/publications/aba-standing-committee-on-law-and-national-security-60-th-anniversary-an-anthology/international-law-in-cyberspace/

Chivvis, C. S. (2017). *Understanding Russian "Hybrid Warfare" And What Can Be Done About it*. RAND Corporation. https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf

Cuffley, A. (2021). Building a bilateral framework for cybersecurity in South Asia. Stimson Center. https://www.stimson.org/2021/building-a-bilateral-framework-for-cybersecurity-in-south-asia/

Cybersecurity governance in South Asia: India and Pakistan. (n.d.). European Foundation for South Asian Studies | EFSAS. https://www.efsas.org/publications/articles-by-efsas/cybersecurity-governance-in-south-asia-india-and-pakistan/

Cyber space security in South Asia on 28th January 2021. (2021, December 8). Strategic Vision Institute -. https://thesvi.org/svi-webinar-panel-discussion-report-on-cyber-space-security-in-south-asia/

Danyk, Y., & Briggs, C. M. (2023). Modern Cognitive Operations and Hybrid Warfare. *Journal of Strategic Studies, 16*(1), 35-50. https://doi.org/10.5038/1944-0472.16.1.2032

DAWN. (2022). *There and back again: A timeline of Pakistan's journey out of the FATF 'grey list'*. https://www.dawn.com/news/1694958

Fridman, O. (2018). *Russian "Hybrid warfare": Resurgence and politicization*. Oxford University Press.

Gambrill, Y., & Eschroeder, E. (2022). *Assumptions and hypotheticals: First edition*. Atlantic Council. https://www.atlanticcouncil.org/commentary/article/cyber-strategy-assumptions-and-hypotheticals/#proxiesdebate

Government of India. (2013, July 02). National Cyber Security Policy 2013. India: Ministry of Communications and International Technology. Retrieved from https://www.meity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20%281%29.pdf

GGC, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. (2013, June). ODS. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/371/66/PDF/N1337166.pdf

Hart, S. B. (1967). Strategy. F.A. Praeger.

Helberg, J. (2022). *The wires of war: Technology and the global struggle for power*. Simon & Schuster.

IISS. (2021). Cyber Power—Tier Three: India. In Cyber Capabilities and National Power: A Net Assessment. International Institute for Strategic Studies. https://www.iiss.org/blogs/research-paper/2021/06/cyber-power---tier-three

Jnguyen. (2022, August 1). *What is cyber security?* Check Point Software. https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cybersecurity/

Khan, A. M. (2023, March 27). Cyber deterrence and confidence building between Pakistan and India. South Asian Voices. https://southasianvoices.org/cyber-deterrence-and-confidence-building-between-pakistan-and-india/

Khan, M. A. (2021). *Indian interference in Balochistan*. The Nation. https://www.nation.com.pk/08-Feb-2021/indian-interference-in-balochistan

Khetran, M. S. (2017). Indian Interference in Balochistan: Analysing the Evidence and Implications for Pakistan. *Strategic Studies*, *37*(3), 112-125. https://issi.org.pk/wp-content/uploads/2017/10/7-SS_Mir_sherbaz_Khetran_No-3_2017.pdf

Kunwar, N. (2021). *FATF and India's 'Role' in Pakistan's grey listing – OpEd*. Eurasia Review. https://www.eurasiareview.com/27072021-fatf-and-indias-role-in-pakistans-grey-listing-oped/

Larson, E. V., Darilek, R. E., Gibran, D., Nichiporuk, B., Richardson, A., Schwartz, L. H., & Thurston, C. Q. (2009). *Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities*. RAND Corporation. https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG654.pdf

Machado, G., Alaphilippe, A., Adamczyk, R., & Grégoire, A. (2021). *Indian chronicles: Deep dive into a 15-year operation targeting the EU and UN to serve Indian interests*. EU DisinfoLab. https://www.disinfo.eu/publications/indian-chronicles-deep-dive-into-a-15-year-operation-targeting-the-eu-and-un-to-serve-indian-interests

Marović, J. (2019). *Wars of ideas: Hybrid warfare, political interference, and disinformation*. Carnegie Europe. https://carnegieeurope.eu/2019/11/28/wars-of-ideas-hybrid-warfare-political-interference-and-disinformation-pub-80419

Maurer, T. (2016). 'Proxies' and cyberspace. *Journal of Conflict and Security Law*, *21*(3), 383-403. https://doi.org/10.1093/jcsl/krw015

Maurer, T. (2018). *Cyber mercenaries: The state, hackers, and power*. Cambridge University Press.

National Cyber Security Policy. (2021). Ministry of Information Technology & Telecommunication. https://moitt.gov.pk/SiteImage/Misc/files/National%20Cyber%20Security%20Policy%202021%20Final.pdf

National response centre for cyber crime. (n.d.). National Response Centre For Cyber Crime. https://nr3c.gov.pk/about_us.html

Niaz, M. T. (2022). *Pakistan's Cyber Security Governance: Challenges and Way Forward*. https://ndu.edu.pk/issra/insights/23/01-Insight-Cyber-Security.pdf

Parvaz, B. (2021). *Pakistan on FATF's grey-list: India's role*. Strafasia. https://strafasia.com/pakistan-on-fatfs-grey-list-indias-role/

Patil, S. (2022). *India's cyber security landscape*. SpringerLink. https://link.springer.com/chapter/10.1007/978-981-16-7593-5_6

Patney, A. M. (2015). *South Asian Cyber Security Environment: An Analytical Perspective | Asian defence review 2014-15*. KW Publishers Pvt.

Prevention of Electronic Crimes Act 2016. (2016). Government of Pakistan. https://na.gov.pk/uploads/documents/1470910659_707.pdf

Raashed, M. (2020). *The 'Indian chronicles': India's information Weaponisation against Pakistan*. Centre for Strategic and Contemporary

Research. https://cscr.pk/explore/themes/defense-security/the-indian-chronicles-indias-information-weaponisation-against-pakistan/

Rafiq, A. (2021). The National Cyber Security Policy of Pakistan 2021. Islamabad: Institute of Strategic Studies Islamabad.

R S., A A., & M Y. (n.d.). *Cyber Security: Where Does Pakistan Stand?* Sustainable Development Policy Institute | SDPI. https://www.think-asia.org/bitstream/handle/11540/9714/Cyber-security-where-does-pakistan-stand%28W-167%29.pdf?sequence=1

Sanaullah. (2019). Hybrid Warfare: A New Baseline of Instability in South Asia. *NDU Strategic Thought*, (1), 114-127.

Samuel, C. (2014). India's Cybersecurity - The Landscape. In Chinese Cybersecurity and Defense (pp. 101-127). John Wiley & Sons Co.

Sardar, N. (2021). *Bearing the Cost of Global Politics: The Impact of FATF Grey-Listing on Pakistan's Economy*. Tabadlab. https://www.tabadlab.com/wp-content/uploads/2021/02/Tabadlab-Working-Paper-07-Bearing-the-Cost-of-Global-Politics.pdf

Shad, M. R. (2019). Cyber Threat Landscape and Readiness Challenge of Pakistan. Journal of Strategic Studies, 1-19.

Shah, S. U. (2020). *Crack it to bust: Myths and realities of Doval doctrine*. Hilal Publications. https://hilal.gov.pk/eng-article/detail/NDcwNg==.html

Shahi, S. M., & Baloch, M. (2021). *Is Pakistan serious about peace talks in Balochistan?* The Diplomat. https://thediplomat.com/2021/07/is-pakistan-serious-about-peace-talks-in-balochistan/

Sir basil Liddell Hart. (n.d.). Encyclopedia Britannica. https://www.britannica.com/biography/Basil-Henry-Liddell-Hart

South Asia's digital opportunity: Accelerating growth, transforming lives. (2022, March 29). World Bank. https://www.worldbank.org/en/topic/digitaldevelopment/publication/south-asia-s-digital-opportunity-accelerating-growth-transforming-lives

State bank of Pakistan Cyber Security Department (CySD). (n.d.). State Bank of Pakistan. https://www.sbp.org.pk/departments/cysd.htm

Sunzi, & Sun, T. (1994). *The art of war*. Westview Press.

Syed, A. R. (2019). *Doval doctrine & covert operations*. Daily Times. https://dailytimes.com.pk/366415/doval-doctrine-covert-operations/

Thapar, S. (2016). Mapping the Cyber Policy Landscape: India. London: Global Partners Digital.

The new era of the proliferated proxy war. (2022, January 19). The Strategy Bridge. https://thestrategybridge.org/the-bridge/2017/11/16/the-new-era-of-the-proliferated-proxy-war

The Indirect Approach. (n.d.). Military history | Erenow. https://erenow.net/ww/strategy-a-history/12.php

The Prevention of Electronic Crimes Ordinance, 2009 ORDINANCE XIV OF 2009. (n.d.). https://nasirlawsite.com/laws/peco09.htm

Topychkanov, P. (2020). *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk South-Asian Perspectives*. Stockholm International Peace Research Institution.

U B. (2022, December 30). *Pakistan's Cyber Security Governance: Challenges And Way Forward*. Institute for Strategic Studies, Research and Analysis National Defence University. https://ndu.edu.pk/issra/insights/23/01-Insight-Cyber-Security.pdf

Union, International Telecommunication. (2021). Global Cybersecurity Index 2021. ITU Publications.

United Nations Institute for Disarmament Research. (2021, June). Cyber Policy Portal UNIDR. Retrieved from UNIDR: https://unidir.org/cpp/en/states/india

UN General Assembly. (2021, July 13). *Official Compendium of the Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information*

and Communication Technologies by States Submitted by Participating Governmental Experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. ODS. https://documents-dds-

Valori, G. E. (2019, November 7). Psychology and indirect strategy. Modern Diplomacy. https://www.google.com/amp/s/moderndiplomacy.eu/2019/11/01/psychology-and-indirect-strategy/amp/

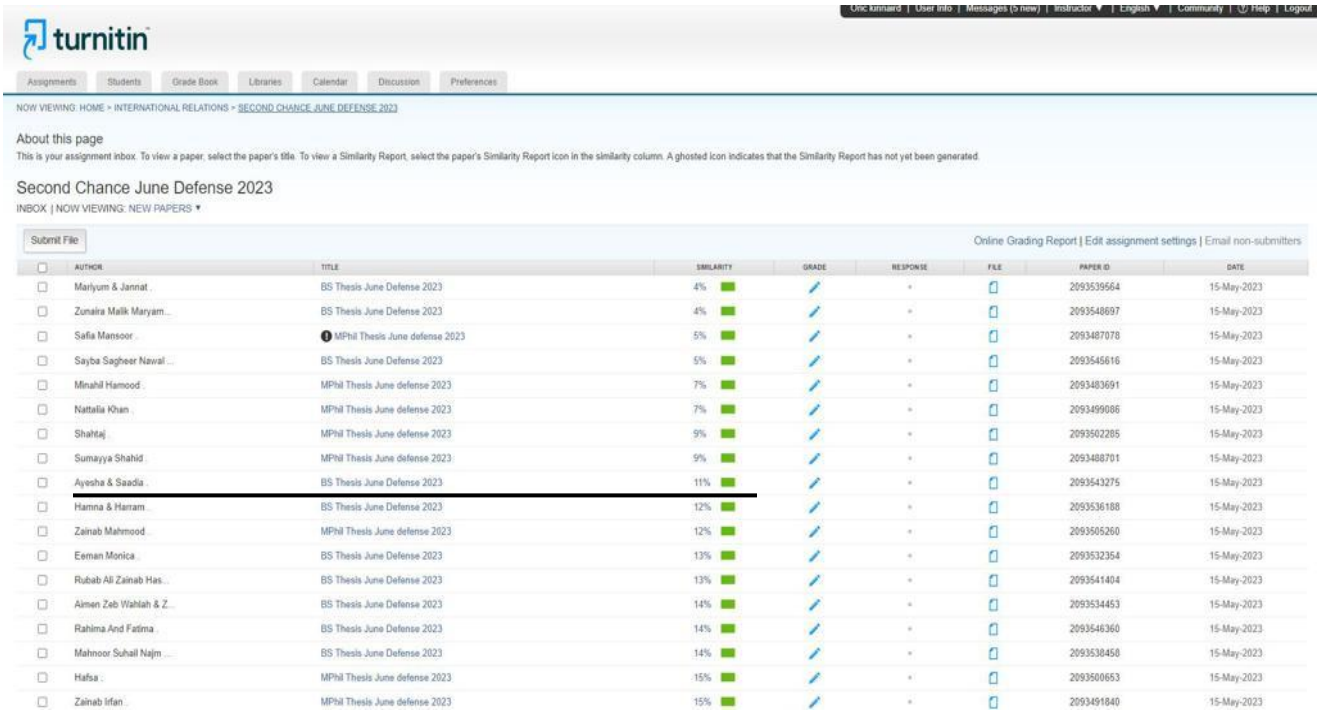
Yamin, T. (2014). Cyberspace CBMs between Pakistan and India. NUST Publishing. https://library.nust.edu.pk/wp-content/uploads/2022/04/Cyberspace-CBMs.pdf

What is cyber diplomacy? (n.d.). GmbH The EU Cyber Diplomacy Toolbox. https://www.cyber-diplomacy-toolbox.com/Cyber_Diplomacy.html

What is cybersecurity? Everything you need to know | TechTarget. (2022, September 26). SearchSecurity. https://www.techtarget.com/searchsecurity/definition/cybersecurity

Whyte, C. (2020). Cyber Conflict or Democracy "Hacked"? How Cyber Operations Enhance Warfare.

SIMILARITY INDEX REPORT



turnitin

Assignments | Students | Grade Book | Libraries | Calendar | Discussion | Preferences

NOW VIEWING: HOME > INTERNATIONAL RELATIONS > SECOND CHANCE JUNE DEFENSE 2023

About this page

This is your assignment inbox. To view a paper, select the paper's title. To view a Similarity Report, select the paper's Similarity Report icon in the similarity column. A ghosted icon indicates that the Similarity Report has not yet been generated.

Second Chance June Defense 2023

INBOX | NOW VIEWING: NEW PAPERS

Submit File

Online Grading Report | Edit assignment settings | Email non-submitters

AUTHOR	TITLE	SIMILARITY	GRADE	RESPONSE	FILE	PAPER ID	DATE
Mariyum & Jannat	BS Thesis June Defense 2023	4%				2093539564	15-May-2023
Zunaira Malik Maryam	BS Thesis June Defense 2023	4%				2093548697	15-May-2023
Safia Mansoor	MPhil Thesis June defense 2023	5%				2093487078	15-May-2023
Sayba Sagheer Nawal	BS Thesis June Defense 2023	5%				2093545616	15-May-2023
Minahil Hamood	MPhil Thesis June defense 2023	7%				2093483691	15-May-2023
Nattalia Khan	MPhil Thesis June defense 2023	7%				2093499086	15-May-2023
Shahtaj	MPhil Thesis June defense 2023	9%				2093502285	15-May-2023
Sumayya Shahid	MPhil Thesis June defense 2023	9%				2093488701	15-May-2023
Ayesha & Saadia	BS Thesis June Defense 2023	11%				2093543275	15-May-2023
Hamna & Harram	BS Thesis June Defense 2023	12%				2093536188	15-May-2023
Zainab Mahmood	MPhil Thesis June defense 2023	12%				2093505260	15-May-2023
Eeman Monica	BS Thesis June Defense 2023	13%				2093532354	15-May-2023
Rubab Ali Zainab Has	BS Thesis June Defense 2023	13%				2093541404	15-May-2023
Aimen Zeb Wahlah & Z	BS Thesis June Defense 2023	14%				2093534453	15-May-2023
Rahima And Fatima	BS Thesis June Defense 2023	14%				2093546360	15-May-2023
Mahnoor Suhail Najm	BS Thesis June Defense 2023	14%				2093538458	15-May-2023
Hafsa	MPhil Thesis June defense 2023	15%				2093500653	15-May-2023
Zainab Irfan	MPhil Thesis June defense 2023	15%				2093491840	15-May-2023