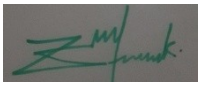
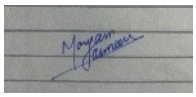
KINNAIRD COLLEGE FOR WOMEN

DETERRENCE STRATEGIES IN THE FIFTH DOMAIN: TRILATERAL CYBER NEXUS BETWEEN USA, CHINA AND RUSSIA

ZUNAIRA MALIK & MARYAM YASMEEN

F19BAIR018

W18BAIR022

DEPARTMENT OF INTERNATIONAL RELATIONS

KINNAIRD COLLEGE FOR WOMEN, LAHORE

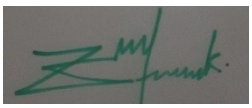
2019-2023

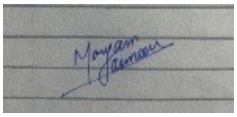
DETERRENCE STRATEGIES IN THE FIFTH DOMAIN: TRILATERAL CYBER NEXUS BETWEEN USA, CHINA AND RUSSIA

A THESIS/ DISSERTATION SUBMITTED TO KINNAIRD COLLEGE FOR WOMEN IN FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF BACHELORS IN INTERNATIONAL RELATIONS

BY

ZUNAIRA MALIK & MARYAM YASMEEN





DEPARTMENT OF INTERNATIONAL RELATIONS

KINNAIRD COLLEGE FOR WOMEN, LAHORE

2019-2023

RESEARCH COMPLETION CERTIFICATE

It is certified that Zunaira Malik & Maryam Yasmeen of BA/BSc (session 2019-2023 & 2018-2022 respectively), Department of International Relations have carried out research work entitled **"Deterrence in fifth domain: Trilateral Cyber Nexus between USA China and "** 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".

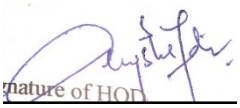


Signatures of Supervisor

Designation

Assistant Professor

Dated: 18th May, 2023



Signatures

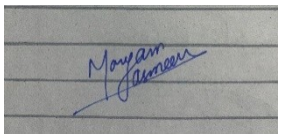
Head of Department

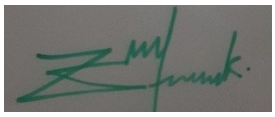
ANTI-PLAGIARISM DECLARATION

I/we certify that this is my/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 _4% _. If this statement is untrue and I am found guilty of plagiarism, the punitive actions against me should be taken as per Kinnaird Anti Plagiarism Policy.

Name/s of the student/s**: Zunaira Malik & Maryam Yasmeen**

Registration No: **F19BAIR018 and W18BAIR022**

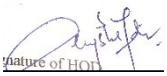




Signature:



Signature of Supervisor:

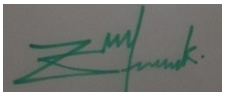


Signature of HOD

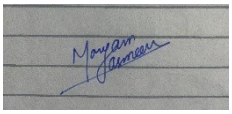
AKNOWLEDGEMENTS

We, Zunaira Malik & Maryam Yasmeen, first and foremost thank Allah almighty, without whom we could never have been able to carry out a task like this; he is the one who gave us the strength and courage to carry out our research responsibly. After him we thank our parents who believed in us and supported us throughout the process of conducting this research. A big hand behind our success goes to our supervisor ma'am Asia Mukhtar, without her guidance it would have been impossible to get this research done, her knowledge and skill enabled us to remain devoted and work hard for our research in a responsible manner. Lastly, we thank our teachers of the International Relations department, Dr. Ayisha Safdar, Dr. Qudisa Akram, and Miss Shireen Mushtaq who taught us throughout these years.

Signature:



Zunaira Malik
F19BAIR018



Maryam Yasmeen
W18BAIR022

ABSTRACT

The technologically revolutionized 21st century prompted a novel domain that was malleable, volatile yet porous serving as a realm of asymmetric warfare known as 'Fifth Domain' of strategy. This potential battle space incited strategic competition because of its dynamism, intractability and interconnectedness. This prompted the importance for states to protect their critical infrastructures and deter any prospective attacks especially for cyber-space giants like USA, China and Russia. The enigmatic nexus between Cyber deterrence and structural malleability of fifth domain as elucidated in cyber persistent engagement stability theory places the deterrence postures of three giants in paradox. The trilateral cyber deterrence junction between USA, China and Russia has spillover effects on international digital order. This have raised the importance of conducting research to delve into this paradoxical conundrum of cyber deterrence for this purpose descriptive yet correlational and analytical style of research methodology have been employed to probe into this matter. the second chapter, the genesis of cyber deterrence strategy has been articulated along with the conceptual growth of this phenomena. The dispersed evolution of cyber deterrence in practice have been narrated with a regional prism. In the third chapter, the theoretical lens of cyber persistent engagement stability theory has been used to recount on the cyber deterrence enigma both conceptually and pragmatically. However, this chapter also illustrated the gray areas in theory articulating the gaps that this theory entails while explaining the dilemma of cyber deterrence. This chapter shed light on how the loopholes that accompany the deterrence phenomena in fifth domain are reflected in futile efforts to execute this strategy. In the 4th chapter, the deterrence posture of USA has been elucidated with its development during different administrations, the Command-and-Control system used to execute the policy, the faces of United States cyber deterrence policy and many other factors has been analyzed. The deterrence posture of USA has been a reflective of offense-defense balance with its deterrence posture carrying no implied element in it. In the fifth chapter, the implied character of Russian and Chinese deterrence posture has been expounded which is in all but name. in

the 6th chapter the loopholes, challenges and gray areas in the deterrence postures of these three states projected at each other have been narrated after a comparative analysis of their deterrence postures. In 7th chapter, the implications of deterrence strategies of each of the individual state have been narrated with the impact of trilateral nexus on international order. It is concluded cyber deterrence is difficult to be executed but its relevance could still be traced in strategies of states. Maintaining deterrence stability is the biggest challenge in cyber space that states are trying to cope with.

Table of Contents

KINNAIRD COLLEGE FOR WOMEN ..... **i**

DISSERTATION APPROVAL CERTIFICATE ..... **i**

RESEARCH COMPLETION CERTIFICATE ..... **ii**

ANTI-PLAGIARISM DECLARATION ..... **iii**

AKNOWLEDGEMENTS ..... **iv**

ABSTRACT ..... **v**

LIST OF ABBREVIATIONS ..... **xiii**

LIST OF TABLES ..... **xv**

TABLE OF FIGURES ..... **xvi**

INTRODUCTION **1**

1.0 INTRODUCTION 1

1.1 SIGNIFICANCE OF STUDY 4

1.2. PURPOSE AND DESIGN OF THE STUDY 5

1.2.1 AIMS AND OBJECTIVES 5

1.2.2 RESEARCH QUESTIONS 5

1.3 NATURE OF STUDY 5

1.4 LITERATURE REVIEW 6

GENESIS OF DETERRENCE IN FIFTH DOMAIN: HISTORICAL EVOLUTION OF CYBER DTERERRENCE IN THEORY & PRACTISE **13**

2.0 CONTEXTUALIZING DETERRENCE IN THE FIFTH DOMAIN 13

2.1 CYBER DETERRENCE – DEFINITION, CHARACTERISTICS AND TYPES 15

2.1.1 DEFINITIONS 15

2.1.2 CHARACTERISTICS 18

2.1.3 TYPOLOGY OF CYBER DETERRENCE 20

2.2 PRE-REQUISITES/CONDITIONS OF CYBER-DETERRENCE STRATEGY.....23
2.2.1 PURPOSES OF CYBER DETERRENCE STRATEGY.....24
2.2.2 GENERIC MODEL OF CYBER DETERRENCE.....24
2.3 CHALLENGES TO CYBER DETERRENCE.....28
2.4 HISTORICAL EVOLUTION OF CYBER DETERRENCE: IN PRACTISE.....31
2.4.1 EVOLUTION OF DETERRENCE PHENOMENON: FROM CONVENTIONAL TO DETERRENCE IN FIFTH DOMAIN.....31
2.5 EVOLUTION OF CYBER DETERRENCE STRATEGY.....32
2.5.1 DEVELOPMENT AT INTERNATIONAL LEVEL: STRATEGIES OF USA/ CHINA/ RUSSIA.....33
2.5.2 DEVELOPMENT AT REGIONAL LEVEL.....34
2.6 FAILURES OF CYBER-DETERRENCE.....40
EMERGING CYBER PERSISTENCE STABILITY THEORY AND DILLEMA OF CYBER DTERRENCE.....42
3.0 CONCEPTUALIZING CYBER PERSISTENCE.....42
3.0.1 WHAT IS CYBER PERSISTENCE.....42
3.0.2 THE STRATEGIC ROOTS OF PERSISTENT ENGAGEMENT.....45
3.0.3 ESSENTIALS OF A SUCCESSFUL PERSISTENT ENGAGEMENT.....47
3.1 CYBER PERSSITENCE THEORY.....49
3.1.1 INTELLECTUAL ROOTS.....49
3.1.2 ASSUMPTIONS OF CYBER PERSISTENCE THEORY.....51
3.1.3 POLICY INSIGHTS FOR COHERENT CYBER STRATEGY IN CYBER PERSISTENCE THEORY.....53
3.1.4 PROPONENTS OF CYBER PERSISTENCE THEORY.....54

3.1.5 DEFINING PERSISTENT ENGAGEMENT AS PER CYBER PERSISTENT ENGAGEMENT THEORY....55
3.2 CONTEXTUALIZING CYBER DETERRENCE IN CYBER PERSISITENCE THEORY....55
3.3 DETERRENCE STABILITY IN CYBER PERSISTENCE THEORY: STABILITY INSTABILITY PARADOX....56
3.4 DETERRENCE TYPES AND CYBER PERSISTENCE THEORY....57
3.5 PROBLEMS WITH CYBER DETERRENCE....58
3.6 ALTERNATIVES TO CYBER DETERRENCE....60
3.7 CYBER PERSISTENT ENGAGMNET STABILITY THEORY AND CYBER DETERRENCE IN PARADOX: A CRITICAL APPRAISAL....64
3.7.1 RISKS ASSOCIATED WITH PERSISTENT ENGAGEMENT AND PERSISTENT ENGAGEMENT STABILITY THEORY....65
3.7.2 PUBLIC-PRIVATE DILEMMA AND CYBER PERSISTENT ENGAGEMENT STABILITY THEORY....66
3.7.3 TECHNICAL SHORTCOMINGS OF CYBER PERSISTENT THEORY....67
3.7.4 CYBER PERSISTENT ENGAGEMENT STABILITY THEORY AND PRACTICE: IN PARADOX....68
3.7.5 FEASIBILITY FOR SMALLER STATES: A US CENTRIC PERSPECTIVE OF THEORY....69
3.8 KEY FINDINGS....69
USA CYBER DETERRENCE STRATEGY....71
4.0 USA ROLE IN INTERNATIONAL DIGITAL ORDER: THE DECLINE OF DIGITAL PAX AMERICAN....71
4.1 US STRATEGIC SCHOLARSHIP: DEFINING CYBER DETERRENCE....72
4.3 EVOLUTION OF US CYBER DETERRENCE POLICY: IN PRACTICE....75

4.4 TYPES OF DETERRENCE POSTURE AND US STRATEGY.....83
4.5 US CYBER DETERRENCE STRATEGY.....87
4.5.1 THRESHOLD TO CYBER WAR: DRAWING RED LINES.....87
4.5.2 US COMMAND AND CONTROL SYSTEM AND CYBER DETERRENCE.....88
4.6 U.S. CYBER DETERRENCE POSTURE.....90
4.6.1 DEFENSIVE POSTURE.....90
4.6.2 OFFENSIVE POSTURE.....91
4.6.3 COMPONENTS OF US CYBER-DETERRENCE STRATEGY.....92
4.6.4 FACTORS OF CYBER DETERRENCE STRATEGY.....93
4.7 CYBER THREATS AND DETERRENCE STRATEGY.....93
4.7.1 DETERRING RUSSIAN CYBER THREAT.....93
4.7.2 DETERRING CHINA THREAT.....94
CHINA AND RUSSIA CYBER DETERRENCE STRATEGIES.....96
5.0 DETERRENCE IN CYBER SPACE: IMPERATIVES OF RUSSIA AND CHINA.....96
5.1 RUSSIAN PERSPECTIVE ON CYBER DETERRENCE.....97
5.2 CYBER DETERRENCE IN RUSSIAN STRATEGIC THOUGHT.....99
5.3 RUSSIAN CYBER DETERRENCE STRATEGY: IN PRACTICE.....101
5.4 RUSSIAN DETERRENCE POSTURE IN CYBER SPACE.....103
5.4.1 OFFENSIVE POSTURE: INFORMATION CONFRONTATION.....104
5.4.2 PRINCIPLES OF RUSSIAN INFORMATION CONFRONTATION.....104
5.4.3 DEFENSIVE POSTURE: INFORMATION SECURITY.....106
5.5 DETERRENCE IN CYBER SPACE: IMPERATIVES FROM CHINA.....108
5.5.1 DETERRENCE IN CHINESE STRATEGIC THINKING: DEFINITIONS AND COMPONENTS.....108

5.5.2 CHINESE CONCEPTION OF CYBER SPACE....110
5.6 CHINESE CYBER DTERRENCE POSTURE....112
5.7 CHINESE DETERRENCE POSTURE IN CYBER SPACE....114
5.8 RUSSIA-CHINA ALLAINCE IN CYBER SPACE....117
IMPLICATIONS OF CYBER DETERRENCE STRATEGIES OF USA RUSSIA ANS CHINA....120
6.1 INTERNATIONAL SYSTEM AND DETERRENCE STRATEGIES....120
6.1.1 A NEW COLD WAR?....120
6.1.2 GROWING CYBER LEGALISM....121
6.1.3 CHINA RUSSIA ALIGNMENT AND ITS IMPACTS ON TRILATERAL CYBER DETERRENCE DYNAMICS....122
6.1.4 PARTIAL PEACE RESTORATION....123
6.1.5 GROWING TREND OF ACTIVE CYBER DEFENSE STRATEGY IN CYBER SPACES....124
6.2 CONSEQUENCES OF CHINA, RUSSIA AND US CYBER DETERRENCE STRATEGY ON INTERNATIONAL DIGITAL ORDER....124
6.2.1 IMPLICATIONS OF US DETERRENCE STRATEGY....125
6.2.2 IMPLICATIONS OF RUSSIAN DETERRENCE STRATEGY....127
6.2.3 IMPLICATIONS OF CHINESE DETERRENCE STRATEGY....129
COMPARITIVE ANALYSIS OF CYBER DETERENCE STRATEGIES: A CRITICAL APPRAISAL....133
7.0 COMPARITIVE ANALYSIS OF CYBER DETERRENCE STRATEGIES OF USA/ RUSSIA AND CHINA....133
7.1 CRITICAL APPRAISAL OF CHINESE CYBER DETERRENCE STRATEGY....136
7.1.0 VULNERABLE SYSTEMS....136

7.1.1 DEFENSE OF FRAGMENTED NATURE.....137
7.1.2 CHINESE CYBER SPACE EXPLOITATION BY WEST.....138
7.1.3 NEGATIVE TRENDS.....138
7.2 CRITICAL APPRAISAL OF RUSSSIAN CYBER DETERRENCE STRATEGY.....139
7.2.1 OVER RELIANCE ON OFFENSIVE STYLE OF CYBER DETERRENCE.....139
7.2.2 LACK OF CYBER PORTFOLIO: DOCTRINAL DILEMMAS.....139
7.2.3 TECHNICAL COMPLEXITY AND FLAWS IN RUSSIAN CYBER-DETERRENCE STRATEGY: DOMESTIC CHALLENGES.....140
7.3 CRITICAL APPRAISAL OF US CYBER DETERRENCE STRATEGY.....141
7.3.1 ATTRIBUTION CHALLENGE.....141
7.3.2 PROBLEM IN DETERRING COUNTER VALUE AND COUNTER MILITARY ATTACKS.....142
7.3.3 TECHNICAL PROBLEMS.....142
7.3.4 PROBLEMS WITH DETERRENCE STRATEGIES OF NORM/ ENTANGLEMENT.....143
7.3.5 ISSUES WITH ACTIVE AND PERSISTENT CYBER ENGAGEMENT.....144
7.3.6 INFRASTRUCTURAL PROBLEMS.....144
7.3.7 POLITICAL COMPLEXITIES.....145
7.3.8 COUNTER MEASURES FROM ADVERSARIES AND CYBER DETERRENCE 146
7.3.9 CYBER VULNERABILITIES AND DETERRENCE STRATEGY.....147
CONCLUSION.....149
REFERENCES.....160

LIST OF ABBREVIATIONS

AMS	Academy of Military Science
APEC	Asia-Pacific Economic Cooperation
ASEAN	Association of Southeast Asian Nations
C2	Command and Control
CAN	Computer Network Attack
CISA	Cyber Security and Infrastructure Security Agency
CNE	Computer Network Exploitation
CND	Computer Network Defense
CIA	Central Intelligence Agency
CIWG	Critical Infrastructure Working Group
CMF	Combined Maritime Forces
DHS	Department of Home Security
DoD	Department of Defense
DOJ	Department of Justice
DPRK	Democratic People's Republic of Korea (North Korea)
EO	Executive Order
EU	European Union
FBI	Federal Bureau of Investigation
FED	Federal Reserve System
GGE	United Nations Group of Governmental Experts
ICS	Industrial Control Systems
ICT	Information and Communications Technology
IMF	International Monetary Fund
INFOOPS	Information Operations
IO	Information Operations
IW	Information Warfare
KSA	Kingdom of Saudi Arabia
MAD	Mutually Assured Destruction
NATO	North Atlantic Treaty Organization

NMS	National Military Strategy
NSA	National Security Agency
NSD	Network System Department
OMP	Office of Military and Political Affairs
OODA	Observation, Orientation, Decision, Action
OP	Operation Procedure
OSCE	Organization for Security and Co-operation in Europe
PCIs	Public Cyber Institutions
PDD	Presidential Decision Directive
PLA	People's Liberation Army
ROK	Republic of Korea (South Korea)
SIGNIT	Signals intelligence
SSD	Space System Department
SSF	Strategic Support Force
SCO	Shanghai Cooperation Organization
USSTARTCOM	US Strategic Command
USAID	United States Agency for International Development

LIST OF TABLES

2.1 Definitions of Cyber Deterrence……17

2.4 Kinds of Challenges to Cyber Deterrence…….30

2.5 Evolution of Cyber Deterrence Strategy……38

3.5 Hurdles in Execution of Persistent Engagement Strategy…….53

4.1 Development of Cyber Deterrence in Us Strategic Though…….74

4.2 Development of US Cyber Deterrence Strategy……81

4.5 Us Cyber C2 System and Functions of Vital Bodies……89

7.1 Comparative Analysis of Deterrence Postures ……134

TABLE OF FIGURES

2.2 Features of Cyber Deterrence Strategy …….20

2.3 3cs Of Cyber Deterrence Strategy ……25

3.1 Essential Components Of Persistent Engagement……44

3.2 Persistent Engagement Strategic Development……46

3.3 Components of Persistent Engagement Strategy……..49

3.4 Roots of Cyber Persistent Engagement Stability Theory……..51

3.6 Fait Accompli ……63

4.3 Typology of Us Cyber Deterrence Postures……..87

4.6 Components of USA Deterrence Strategy……92

5.1 Reasons for Russian Skepticism on Cyber Deterrence ……98

5.2 Factors in Russian Cyber Deterrence Understanding……101

5.3 Elements of Russian Cyber Deterrence Strategy……107

CHAPTER 1

INTRODUCTION

1.0 INTRODUCTION

The technologically revolutionized 21st century prompted a novel domain and a realm of asymmetric warfare known as the ‘Fifth Domain’ of strategy. Being antithetical to the strategic posture of the physical domain, this virtual space is contingent on the electromagnetic spectrum. Fifth domain is broadly characterized as a potential yet newest battle space that manifests itself as a multifaceted T-junction of IT system with cyber-geography. This domain which is labelled as a human brainchild, is malleable, volatile and porous. It is often featured as a ‘cross-domain’ rather than as an independent domain of warfare or strategic competition because of the spillover effect that it creates in physical domain with its strategic competition that takes place inside of the domain. Fifth domain is recognized as a warfare domain in core US military strategy in 2009 and later on become indicative with the establishment of USCYBERCOM (US cyber command) officially recognized by NATO in 2016. This novel battle space opens the doors of strategic competition in the fifth domain which is defined as exploitation rather than coercion of an adversary's critical infrastructure. Cyber-politics has introduced multiplicity, structural volatility, dodgy and erratic asymmetry with obscure actor identity in international strategic context. This non-traditional cyber space has epitomized and hyphenated the traditional concept of the Westphalian international system, in the cyber domain, notably **cyber-competition, cyber-war** and **cyber-deterrence**. Impeding an adversary from taking a punitive action in the cyber domain by maneuvering a Computer Network Attack (CAN) or Computer Network Exploitation (CNE) capabilities, is what is determined as Cyber Deterrence by the scholars. The malicious activity of adversary is deterred by defenders targeting the OODA loop of rival with the aim of maintaining the status-quo in this cross cutting yet elusive conception of deterrence which demands superlative intelligence and is resource intensive.

The typology of cyber deterrence could be crafted in these types of deterrence strategies notably deterrence by punishment

1. deterrence by denial
2. deterrence by association
3. deterrence by norms
4. deterrence by entanglement
5. deterrence by de-legitimization
6. deterrence by reputation.

Deterrence by punishment involves the launch of preemptive and retaliatory attack that could be both of cyber and kinetic nature for example STUXNET. Deterrence by Denial on the other hand is to fortify the robustness of one's own critical infrastructures thereby denying the access and intensifying the cost of attack for adversary. The parameters of effective cyber deterrence strategy is use of common lexicons or effective communication of deterrence declaration, gauging the proportionality of attack as mentioned in Tallin Manuel, cyber attribution, signaling the intention. The intricate cyber deterrence nexus that exists in between US-China-Russia is the most pertinent cyber trilateral deterrence in 21st century. This trilateral nexus of cyber deterrence is the true manifestation of deterrence by punishment as stated in words of the Chinese and US department of defense i.e., "Deterrence by cost imposition".

Cyber deterrence, although very novel, has a notable presence in states' cyber policies. The most influential works which triggered the debate of strategic competition and power projection in the fifth domain include, the 1993 article of John Arquilla and David Ronfeldt on Cyberwar as an imminent threat followed by the article of Richard Clarke and Robert Knake in 2010. The book 'Cyber-security Dilemma' written by Ben Buchanan also adds to literature. The most notable publications on Cyberspace deterrence include works by notable scholars such as Martin C. Libicki and Joseph Nye. Cyber deterrence as a term, was coined by James Der Derain in 1994 at the time of US army's 'Desert Hammer VI' war game exercise. When Iraqi communication networks were paralyzed by US Operation Desert Storm, it triggered scholastic debate on deterrence in cyberspace. Further actions of deterrence were

carried out afterwards. An example can be NATO-Georgia, when NATO failed to constrain Russian intrusions. This incident stands as an image of failure of 'extended cyber deterrence' on part of NATO-Georgia but as a success story for Russian 'Deterrence by Denial' strategy. Another example of 'Deterrence by Punishment' Strategy was OP1 and OP2 campaigns by Russia and China respectively, to collect US classified, secret information. 'Deterrence by De-legitimization' is another characteristic cyber-strategy. 'Five Eye Alliance' called out in 2017, Not Petya Russian Campaign, and the 2018 deployment of TRITON by Russia, are a few examples. This malware was used by Russians for causing blackouts in Ukraine in 2016 as well. In 2020 US Cyber National Mission Force, to gauge the Russians in cyber web, used twitter for advertising adversarial malware samples to subdue the asymmetric information superiority which Russians claim. In 2021, US blamed China for launching APT10, APT40 campaign as a part of its 'deterrence by de-legitimization strategy'. US have also adopted the policy of Cross-domain deterrence that is to gain asymmetric advantage in cyber domain by tactics in physical domain. Extradition of Yanjun Xu in 2018 and arrest of Russian businessman Vladislav Klyushin in 2021. The 'trilateral nexus of cyber deterrence' was declared in 2015 in response to Chinese cyber espionage on companies' sanctions and in 2016 against Russia for intruding in US elections. Chinese deterrence posture is of exfiltration and that of Russian is through interference. Power projection in the fifth domain opens the door for states which constantly involve themselves.

The power projection in fifth domain with Russia-China-US deterring each other could be contemplated with 'Cyber persistence theory'. This theory was proposed by Michael P. Fischer Keller, Emily O. Goldman or Richard J. Harknett in a book called "Cyber Persistence Theory: Redefining National Security in Cyberspace". Characterized as the "domain of interconnectedness" this theory recognizes persistence of strategic competition in cyberspace and identifies the probability of cyber warfare as scarce. Reconfiguration of cyber security in one's strategic advantage could be possible by the strategy of '*cyber fait accompli*' that is to deny the access of adversary to critical infrastructure through D and D strategy. This concept is compatible with the rationale of 'deterrence by denial' strategy. Exploitation of Russian vulnerabilities by USCYBERCOM, in order to deny them access to US midterm election

infrastructure, is an example. But this theory fails to contemplate typologies of cyber deterrence that exist in the 21st century.

1.1 SIGNIFICANCE OF STUDY

With the diffusion of technology, both use and abuse of digital spaces has proliferated. The mischievous maneuvering of fifth domain have resulted in national security squabbles difficult to comprehend. Amid this time of prevailing uncertainty & intractability of digital spaces have enhanced the significance of deterring these attacks on national security infrastructure and also the need to study this phenomenon. The states reliance on digital systems and strategic competition in fifth domain have compel them to prioritize the security of their critical infrastructures. All of the major powers including USA, China, Russia have framed cyber deterrent postures to protect their digital systems from adventurism even though their policies lack credibility and are facing multiple structural, technical, infrastructural challenges. Conceptually and pragmatically cyber deterrence is ambiguous strategic concept that is also less talked about in cyber realm. This research work highlights and addresses these grey areas. The first research gap that this research study fills includes the once over explanation of offensive and defensive cyber strategies of USA, China and Russia with respect to deterrence phenomenon. This research study will also explore the typologies of cyber deterrence strategies pursued by each state with the incoherence in their cyber deterrence perspectives. This study will provide a better and critical contemplation of power projection in the fifth domain under the lens of 'cyber persistence theory', which is a novel paradigm to gauge strategic competition in cyber discourse. This study will also explore how cyber persistence being the only theoretical paradigm that talks about the elusive or volatile nature of cyber deterrence phenomena but how it fails to look into the typology of deterrence strategies that states are pursuing in the cyber domain. The future researchers will not only get an analytical account of US, Russian and Chinese deterrence perspectives but this research work will also create an understanding on the correlation of USA, China and Russia cyber strategies. Another significant point of this research study is that it will look into the implications that these cyber strategies that are meant for power projection and deterrence are having on security architecture of cyber domain.

1.2. PURPOSE AND DESIGN OF THE STUDY

1.2.1 AIMS AND OBJECTIVES

- To explore the historicity of cyber deterrence as a phenomenon in the fifth domain.
- To testify cyber deterrence under the lens of 'Cyber Persistence Theory' and critically interpret the shortfalls of this theory with cyber deterrence contextualization.
- To examine the deterrence imperatives and strategies of Russia, China and USA in the fifth domain.
- To analyze the trilateral nexus in between deterrence strategies of USA, China, and Russia by drawing a comparison of their cyber deterrence perspectives.
- To assess the impact of cyber deterrence strategies pursued by states on global cyber security.

1.2.2 RESEARCH QUESTIONS

1. What is the outlook and historicity of cyber deterrence phenomenon in the strategic calculus of fifth domain in 21st century?
2. How Cyber Persistence theory disseminate the paradox of cyber deterrence in 21st century. Give critical appraisal of cyber persistent engagement stability theory?
3. How the offensive and defensive cyber strategies of USA, China and Russia frame their cyber deterrence imperatives?
4. In what way cyber deterrence strategies of USA, China and Russia are impacting the global cyber security?

1.3 NATURE OF STUDY

In this research work mixed research design will be used with primarily qualitative nature of study. The type of research used to explain volatility of deterrence strategies in fifth domain will be analytical with respect to the cyber persistence theory in order to elucidate the complex phenomena of cyber deterrence, and to provide a critical appraisal to theory of cyber persistence. For the deterrence strategies and perceptive of each state explanatory or descriptive method will be used. Correlational research approach will be used to elaborate on the trilateral nexus in between deterrence strategies of USA, China and Russia. The data

collected involves articles, books, reports and research papers, all the leading and well reputed pieces of literature. Both primary and secondary sources of data collection are employed to provide empirical grounds to the arguments presented in this research work. This study will explore the association in between deterrence strategies of US, Russia, China in an explanatory fashion.

1.4 LITERATURE REVIEW

Based on neo-realist framework, this article very compellingly explores the great power competition in cyberspace in 21-century. The writer, Francis C. Domingo, explains the emergence of cyberspace as a new front of security in international system and thus explains the competitive behavior of states in increasing their capabilities for warfare to conquer this domain. According to the writer, cyberspace is the new battlespace of strategic competition and the ground zero for next global arms race. The article is centered around the perpetual cyber competition between US and China, both racing for military developments in cyberspace. Presenting evidence from respective states' policy documents and reported cyberattacks and cyber military units, the author hypothesizes three key implications from his study i.e., the proliferation of cyberspace, the competition to dominate the cyberspace and the escalation of kinetic cyberattacks to achieve these resolutions (Domingo, 2016).

The concept of cyberspace as an independent domain has been in vogue for the last two decades. Considerable political and economic activity has been generated in this domain. Extensive intelligence operations have also been carried out within this space. But the idea of recognizing it as the fifth domain of war is relatively newly found. In the article 'Cyberspace – The Fifth Operational Domain', the author Larry D. Welch, a USAF retired general, explores the very idea with respect military involvement in cyberspace. The author analyzes cyberspace as the fifth operational domain and compares it with other operating domains – land, sea, air and space. Strategies involved in the cyberspace range from passive and active defense to exploitation to attack and deterrence. The article further explores the idea of building cyber forces since successful military operations now depend upon cyber advancement and operations (Welch, 2011).

In his report ‘Cyber Security: Understanding the Fifth Domain’, Kan Casapoglu characterizes cyberspace as being different to the physical dimensions of traditional security of international system. The writer recognizes as a novel space for political, military, economic and social interactions, and as the fifth domain based on electromagnetic spectrums. The writer focuses on how this difference lies in the fact that cyberspace is a man-made domain and a space with low costs. This has led it to become an ‘informational-zed battlespace’ with network-centric warfare concepts. But applying core international relations concepts of power, capacity, offense-defense and deterrence in the cyberspace is not easy (Kan Casapoglu, 2017).

Exploring the cyber debate of ‘strategic campaigns vs intelligence operations’, this article is written to coincide various works by various authors, under the theoretical perspective of Cyber Persistence theory. The article examines this cyber behavior and interaction dynamics between states provided that those interactions are heightened but fall short of a war. The core idea of the article is to unhinge strategy as the face of coercion and war. The authors have orchestrated two alternative approaches for the explanation of persistence theory in cyberspace i.e., by presenting cyber activity as a strategic competition and as an intelligence contest between states. The article maintains that though, both the approaches share a common ground and can be bridged in order to form a cyber policy but it is the former approach which lies more in sync with the original theoretical contours. The article consists of three sections. Firstly, it outlines key features of both the variables. Secondly, it finds a common grounds for the debate and thirdly, it argues in the favor of strategic competition being the best explanation as to why cyber activity falls short of armed conflict (Fischerkeller & Harknett, 2020).

Writer Mattas Hjlem assesses the use of cyber strategies and operations as a modern manifestation of political warfare. Orbiting his research around Russia and US, Hjlem explores the reasons behind conflict in the digital domain i.e., the cyberspace also known as the fifth domain of warfare. The author has used Principle-Agent theory to explain this interaction between the very two leading actors within cyberspace. According to the author, lower internal cyber capability, low costs and the ability to evade accountability are the three

major driving forces of such cyber operations. Hjelm persists that cyberspace that enabled a new set of effects with strategies being utilized to project power but below the threshold of war. Cyber offense, digital proxies and cyber deterrence all are multiple facets. Such cyber proxies escalate the foreseeable challenges (Hjelm, 2021).

The idea of cyber persistence as a strategic competition was proposed back in 2020 in an article, while the theory itself was documented as a book in 2022. The book 'Cyber Persistence theory: Redefining national security in Cyberspace' introduces new logic and lexicon to the cyber activity in International Relations. The book tries to differentiate strategy in various security paradigms: strategy as a tool of coercion in nuclear and conventional domain and strategy as a tool of competition, persistence and bargain in cyber domain. The concept of cyber *fait accompli* is also introduced in the book. Explored in detail with the case study of US, the book refers to redefining US cyberspace policy by adding the cyber *fait accompli*, to deny its adversary access to its critical infrastructure, via strategies such as D & D in cyberspace. To attain an alternative to cyberwar, this is a leverage and the central question of 21st century (Fischerkeller, Goldman & Harknett, 2022).

Establishing the importance of cyberspace in the 21st century along the basis of airpower doctrine of 20th century, the writers Zoe Hawkins and Liam Nevill, explore the transposition of power and strategy from traditional mediums to the digital domain. Cyberspace is identified as a new front and a new domain which paints the modern conflict and contemporary and future warfare. It defines its significance in the role played by various states in the cyberspace via multiple strategies. One of the evolving strategies is the one of cyber deterrence. The authors maintain that cyber deterrence is the new common theme of retaliation in found in national cyber policies. US International Strategy for Cyberspace adopted the policy of deterrence in the digital domain in 2011. UK adopted the cyber deterrence doctrine in 2015 and Australia made its mention in 2016. The article is written with specific perspective to Australian national cyber deterrence, but it does explore the fact that this trend to 'deter or defeat enemies in cyberspace' is global. The trend has advanced offensive and defensive capabilities of states in cyberspace. It has also helped in bolstering defense and confidence building in the new digital domain (Hawkins & Nevill, 2016).

Christopher Fitzgerald Wrenn writes in his research paper ‘Strategic Cyber Deterrence’, about the importance of developing a theory for cyber deterrence. The Cyber wars of 2007 and 2008 between Russia and Estonia, and Russian and Georgia, respectively, has led to the reflection of cyber domain being increasingly vulnerable. State and Non-state actors alike, are increasing their cyber capabilities and therefore, according to the writer, a deterrence theory applicable to cyber war is now the need of the day. The author addresses the importance of using already existing deterrence theories within cyber domain by assessing them through various cyber cases. The author has utilized the two cyber cases …. to form four hypotheses structured around the triadic components of basic deterrence. Wrenn concludes in his research that he finds deterrence by cooperation to be best suited in cyber cases. The writer has thus, presented in his paper a ‘theory of strategic cyber deterrence’ based upon denial and punishment and cooperation. He also concludes that cyber deterrence unlike basic deterrence is more conditional given the constant expansion and contraction of cyber vulnerabilities (Wrenn, 2012).

Researching on the possibility of ‘Deterrence in the Cyber Realm’, the writer Nadia Kostyuk explores the working of cyber deterrence in her article. The article is written as an entry for the journal of ‘International Studies Quarterly’ and argues upon the ineffectiveness of cyber deterrence upon the basis of already established scholarly works. The article tries to distinguish the cyber deterrence ability in public and private cyber capacity. Instead of addressing cyber operations, the writer has tried to fill the research gap of deterrence ability of cyber institutions of states. It maintains that the deterrence ability of public cyber-institutions (PCIs) is as proactive to a country’s cyber offensive and defensive capability and can be used for national cyber deterrence posture. This deterrent capability is however, limited and scarce. These cyber institutions are used by weak states to project their power and strength which in reality decrease their overall cyber capacity. The writer has provided empirical evidence of plausibility of cyber-institutional deterrent ability by using election interference campaigns as example case studies (Kostyuk, 2021).

Illustrating the failure of deterrence in three recent examples, Dr Joe Burton has very comprehensively raised questions of the nature of deterrence amidst contemporary globalized

security threats. Security threats from state and non-state actors spark the complexity of deterrence which according to the writer is ‘equally apparent in cyber domain.’ In his paper ‘Cyber Deterrence: A Comprehensive Approach’, the author has entailed upon the issue of expanding cyber threats within international system, but with little official progression made in deterrence against these cyber threats. The author has tackled the two very important questions in his paper i.e., whether cyber deterrence is possible and whether it can be sustained. Different approaches of cyber deterrence have also been discussed in the second section of this paper. According to Burton, these questions are significant in both academia and policy making. The author concludes that the concept of deterrence should be stretched beyond the binary Cold War conceptions to stem a broader cyber deterrence strategy (Burton, 2018).

Lt. Col. Michael J. Philbin in his Strategy Research Project for the American War College expresses his opinions on ‘cyber deterrence’ by calling it ‘an old concept in a new domain.’ According to the author, cyberspace is categorized as the newest domain within US military and one question that remains unanswered is whether deterrence is possible in this new space. In his paper, the author has outlined the concept of deterrence as an old phenomenon of prevalence in physical domains i.e., land, air, sea and space. Cyberspace is a new domain with its monetary cost of cyber operations and ill-defined nature of permissible behavior, but according to the author, these attributes do not fundamentally change the nature of deterrence in cyberspace. The author suggests the importance of cyberworld for domestic defense and concludes that for cyber deterrence to be successful in this increasing cyber oriented world, the US government must develop, invest and lead in cyber domain (Philbin, 2013).

In the book ‘The Fifth Domain’, the authors Richard Clarke and Robert Knake explore cyberspace as the fifth domain of war. Written with perspective to US cyber security and cyber experts, the book makes use of impactful cyber events such as that of Stuxnet and EternalBlue and hypothesizes the next big war as a cyber war. Therefore, according to the two authors, there is a need to change the balance of power in the cyber domain. The writers reiterate the need to be more ‘resilient’ within cyberspace, by transitioning from offensive to defensive, from being an attacker to a defender. Thus, ‘cyber resilience’ should be

incorporated as an approach to US cyber policy. The book mentions future predicaments and the role of new technologies such as Machine Learning, Artificial intelligence, 5G and Internal control systems in changing the cyber world, and thus the essentiality of cyber deterrence, cyber containment and cyber threat intelligence to be used as national strategies, is suggested in this aspect. The authors have also provided a 'DevSecOps' model to be applied in cyberspace, for cyber deterrence and cyberattack mitigation (Clarke & Knake, 2019).

In the research paper, 'From Offense Dominance to Deterrence', Tianjiao Jiang explores the evolving position of Chinese strategic thinking within cyberspace. From early 1990s to 2000s, the Chinese strategies on cyberwar have been well-publicized as launching of large scale cyberattacks against its opponents, particularly US. The writer builds his case upon this discretion and sketches a historical evolution of Chinese cyber strategic thinking, which according to the writer has evolved over the past decades. From offensive dominance based on 'ideology of offense' in 1990s and PLA's primary approach of 'informationisation leaping forward' to questioning the effectiveness of these cyberattacks in 2008 and building a consensus on developing a cyber deterrence strategy in 2015, Chinese official documents reflect a dynamic shift of its strategic thinking. The author has presented this hypothesis with specific scenarios to cyberwar fallacies between US and China, maintaining a stance that China has opted this strategy of deterrence in cyberspace as a reaction to increasing cyber deterrence by the US (Jiang, 2019).

In the research paper 'The future of Political warfare: Russia, The West, and the coming age of global digital competition', the writers comprehensively explore Russia's stance on political warfare against the Western democracies. Russian strategy has evolved from overt to covert influence activities, which include asymmetric and information tactics such as disinformation campaigns and cyberattacks. The new tools being utilized include AI, automation and machine learning in the information sphere. The authors have maintained the research's focus on the threat that the democracies of the west face from authoritarian states like Russia and China. The paper outlines the current state of play of this political warfare

from a digital perspective and identifies emerging threats in the face of cyber activities (Polyakova & Boyer, 2018).

Russia's cyber strategic thinking is explored in much in detail in a report by NATO Strategic Communications Center of Excellence. The report centers around the Russian cyber conception and its approach of 'information confrontation' which makes use of offensive operations in cyberspace or information sphere. The report analyzes Russian activities in this sphere and the tactics used to attain the end strategic objective of 'information superiority'. Russia actively uses cyber strategy alongside military and non-military means to attain its strategic objectives. Based upon Russian thinktanks and official policy documents, the report clarifies the Russian doctrine for information space which is constant and extends from information protection to information confrontation. The tactics utilized by Russia in this information environment involve electronic warfare, kinetic action and psychological and influence operations, all three used for physical and cognitive attacks in order to gain 'information superiority.' The report further suggests some recommendations for the Alliance to develop its defense against Russian cyber activities (CCDCOE, 2021).

CHAPTER NO. 2

GENESIS OF DETERRENCE IN FIFTH DOMAIN: HISTORICAL EVOLUTION OF CYBER DTERERRENCE IN THEORY & PRACTISE

Deterrence as a practice and a theory is now experiencing a renaissance. It is suggested to be in its 'fourth wave' with deterrence as a phenomenon flourishing in theoretical, empirical and policy domains with its applicability to state and non-state security concerns including the matters of cyber insecurity, which arise in the face of proliferation of armed technology in cyber space. Contextualization of deterrence in the fifth domain therefore, stems on the security dilemma and stability-instability paradox to pave way for deterrence policy and strategies, which find their ground in agreed strategic competition and cyber persistence engagement in the face of cyber nexus between major powers, thus leading to a whole new phenomenon of 'Cyber Deterrence.' In the first section of this chapter deterrence as a phenomenon has been contextualized. The definition of cyber deterrence has been established and its types discussed. In the second section the prerequisites of the strategy along with the challenges that cyber deterrence faces conceptually has been penned down. In the latter half the scattered has been assembled from regional and global perspective.

2.0 CONTEXTUALIZING DETERRENCE IN THE FIFTH DOMAIN

Categorized as the **fifth domain of strategy**, cyber domain is a digital space contingent as a multifaceted T-junction of cyber geography and IT system. It is a novel space for political, economic, social and military interactions – a space thus, malleable, porous and quite volatile, paving way for cyber security and insecurity, the defined paradox. Now visualized as the new realm of strategic competition with a strategic posture quite antithetical to that of physical domain, the cyberspace thus, manifests itself as harboring the potential of becoming the newest battel space for the quest of international cyber security within global system. The space offers several opportunities and possibilities for cyber security threats and counter threats in the face of 'cyber persistence engagement' and 'cyber persistent competition', which ultimately shapes the strategic environment of the cyber space. Presently, the space

needs to be monitored relentlessly given the adaptation into a constantly changing threat environment with deterrence stemming as a major phenomenon (Iasiello, 2018).

Deterrence in the fifth domain mainly relies upon the **strategic environment of the fifth domain** i.e., cyber domain. Cyber domain which is characterized by its complex infrastructure constituting of computers, telecommunication systems, fiber optic cables, cyber personas, information and digital data, all waived together into an interconnected and resilient yet a vulnerable technological network system acting as the warehouse as well as a gateway to **sensitive and strategic information**. Within this domain, data is stored, exchanged and modified and replaced, as well as attacked, hindered and manipulated. Within this domain take place interactions between state and non-state actors – the nature of these interactions varying from peaceful and cooperative to conflictual and competitive, thus encouraging a strategic environment of persistent opportunism for states to access and leverage the data while simultaneously seeking to secure one's own data flow from being attacked by other actors.

This combination of cyber space interconnectedness represents it as a terrain of ever-changing operational reality with imperatives for states to seek and secure and advance their interests in, through and from cyber space (Fischerkeller & Harknett, 2019). This task is often practiced in the face of derivative cyber operations undertaken by the states to wage strategic campaigns against the respective adversary's political, economic and security interests without ever physically crossing the territories and borders. Such operations wield below the threshold of armed conflicts, and thus often require deterrence as the being norm strategy, hence demonstrating the capability, resolve, and persistence of the states in the cyber space. This makes the strategic campaigns in cyber space low-cost in comparison to other domains of strategy and therefore also leads to expansive cyber strategic competition being less expensive and cost effective and thus, quite wide spread with the space probating and threatening equally, the international public security as well as national security of the nation-states. Deterrence in the cyber domain hence is a way to safeguard one's state in this cyber strategic competition.

Like cyber domain which epitomizes and mirrors the traditional narrative of politics, competition, security and war within the cyber space; cyber deterrence simply is the virtual encapsulating of the deterrence in Westphalian International Relations. It is the threat of use of force in the virtual space. It is the usual act of dissuasion and preemption against one's enemy but in cyberspace.

2.1 CYBER DETERRENCE – DEFINITION, CHARACTERISTICS AND TYPES

The question of cyber space being a space for persistent competition and engagement has been around since several decades, but the notion of practice of deterrence in the very space is comparatively novel. In the contemporary world, serving as a contentious reality while plaguing the prevalent system of international security, cyber deterrence is the phenomenon conceptualized as the use of 'deterrence strategies' in the fifth domain, mainly as a way to fit the growing strategic environment of the cyber space.

2.1.1 DEFINITIONS

Deterrence can be defined as a preventive strategy aimed at preventing any course of coercive engagement with a potential aggressor, by instilling in him the fear of consequences outweighing the perceived benefits. Deterrence is regarded as the backbone of any military strategy and policy within all three domains of traditional warfare. The use of such deterrence strategy within the vast cyber expanse is what generally called as cyber deterrence or deterrence in the fifth domain.

Firstly according to **Lawrence Freedman**, deterrence is 'the attempt to manipulate behaviors of others through conditional threats.' Within cyber domain thus, the use of cyber and hybrid threats as a reaction to any action is what deterrence constitutes of. The question nonetheless that arises with the idea of cyber deterrence is not 'what' but much related to 'how' and 'whether.' It is a question which has governed the minds of scholars for decades, and thus leading the way to a whole new discourse and scholarship pathway within cyber space.

Cyber deterrence has been defined in different ways by various scholars of International Relations with its definition changing and evolving over time by being conceptually stretched

into different rhetorical functions (Smeet, 2016). It remains however, a concept related to quintessential anchoring for cyber political debates to illustrate the use of offensive use of military operation within cyber space (Soesanto &Smeets, 2020). Secondly according to **Patrick Morgan**, deterrence can be defined as a strategy of delineating the course of action an adversary might contemplate to carry out, via having the costs of consequences undermine the national security benefits the adversary is aiming to achieve (Morgan, P). Thirdly on co-relating the two concepts of nuclear deterrence and cyber deterrence, according to **Dr. Ratazzi and Dr. Jabbour**, 'cyber deterrence is the threat of mutually assured self-destruction of assets and approaches in cyberspace as a way to manipulate the enemy's cost benefit equation.'

Fourthly according to the author **Emilio Iasiello**, a working definition of cyber deterrence by any scholar may probably identify cyber deterrence 'as a strategy sought by the defending states, targeted at the hostile state, in order to maintain the status quo by signaling the intentions to deter any sort of hostile activity' (Iasiello, 2018). This definition provides a baseline understanding of fifth domain deterrence as being a practice with the main aim to avoid engaging in cyber destructive activity and to influence the decision-making apparatus of the adversary by a promise of an equal if not greater reprisal. Fifthly providing a complete, cohesive and a coherent definition of cyber deterrence however can be challenging as according to the author **Dorothy Denning**, deterrence in no other domain has been addressed across its entirety. Instead, the attention is directed towards particular weapons and activity, provided that that there is no concept of "land deterrence", "air deterrence", "sea deterrence" or "space deterrence" unlike in cyber discourse where the idea of "cyber deterrence" exists.

Sixthly **William Kaufman's** definition of deterrence can also be used to understand the phenomenon of deterrence in the fifth domain. According to Kaufman, there are two components of deterrence: the expressed intention to defend an attack and the capability to actually achieve that defense by inflicting upon the attacker, the cost of the offense and its unintended consequences (Kaufman). By the extension of this definition, it is assumed that, for a state to make its deterrence strategy possible, it needs to have two basic attributes and

abilities: the ability to frustrate the attacks and the ability of threat of retaliation i.e., the ability of denial and punishment, respectively.

Deterrence in fifth domain is about how technologies in this silicon and digital age could play their part in deterring the adversary by evincing four essential components that includes strategic advantage to offensive deterrence posture, ability to maneuver strategic environment in one's benefit, imposition of cost on adversary and denial to one's own system. Also, another important requisite of successful deterrence policy in fifth domain is deterrence declaration and its communication with the adversary. In the cyber domain however the objective of deterrence strategy is to defend the critical infrastructures from any adventurism and hostility.

Following is the compilation of all definitions given by scholars to explain the complex topic of cyber deterrence

2.1 DEFINITIONS OF CYBER DETERRENCE

Scholar	**Deterrence in fifth domain**
Lawrence Freedman	Through conditional threats the attempt to manipulate other behaviors.
Patrick Morgan	Delineating a cyber course of action for adversary to contemplate.
Dr. Ratazzi & Dr. Jabbour	Cyber deterrence is the threat of mutually assured self-destruction of assets and approaches in cyberspace as a way to manipulate the enemy's cost benefit equation.
Emilio Iasiello	A strategy sought by defending state against an adversary with the aim of maintaining status quo.
Dorothy Denning	Rarely is the chance that deterrence in fifth domain operates in its entirety in one domain as it is a function of cross domain

	penetration of deterrence declaration.
William Kaufman	It is the expressed intention to defend an attack and the capability to actually achieve that defense by inflicting a cost on attacker.

Source: drawn by author, data source: (Smeets, 2016 & Iasiello, 2018)

2.1.2 CHARACTERISTICS

Cyber deterrence or deterrence in the fifth domain, is a difficult practice to execute, particularly by denying or punishing and therefore requires certain characteristics in order to be practiced to the best of its abilities. A cyber deterrence strategy must constrain the action of adversary to an acceptable level while also bearing an acceptable cost that accompany with it. However, a holistic cyber deterrence strategy that could constrain the actions of all actors and that does not mean that traditional cyber defenses should be put in place to counter non sophisticated cyber attacks as the sophisticated attacks only could be countered by deterrent policy. Also, for the cyber deterrence to function effectively it is an essential requisite that the adversary and opponent must be rational actor. The adversary must fear that its malicious acts could invite unprecedent retaliation difficult for it to bear. Also, it is an important requirement that the adversary must have something to lose (Willner,2017). The cyber deterrence strategy must have some credibility and if it gets triggered there must be consequences that opponent must bear. An example of such state is North Korea who have considerable little to lose as there are only targets. There are three levels according to which the success of cyber deterrence strategy could be assessed. At first it must stop an attack from happening, after an attack happened the attacker must be punished and sometimes before the launch of attack the offender is punished. The cyber retaliation must not be merited because in that case it might affect the deterrence credibility.

Three Cs are often laid down as the foundation of an effective deterrence strategy i.e., **capability, credibility** and **communication**. State's cyber capability is the ability or technical capacity to implement deterrence measures. It is in building a strong cyber military workforce for operating in highly defensive networks is one major characteristic of cyber

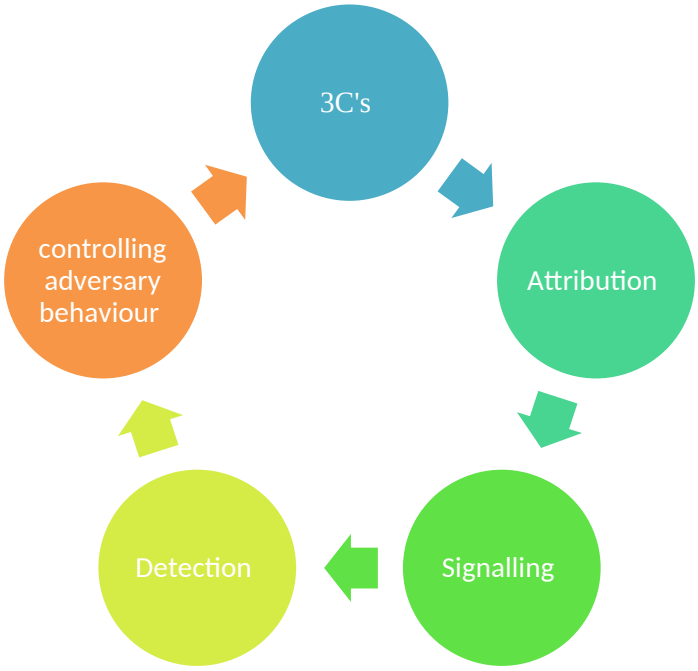
deterrence strategy. In 2010 for instance, Mike McConnell of NSA described the need to develop and increase early-warning systems to monitor cyberspace, identify any intrusions and to locate the sources of attacks. Credibility of cyber deterrence is the will to implement deterrence measures by manipulating the potential hostile behavior of any state via issuing a timely, credible and appropriate threat of equal retaliation. The success of credible cyber deterrence depends upon the communication of such threats, which is a two-way understanding and perception for successful cost-benefit calculations on both sides (Taddeo, 2018).

Another most important feature is that of **attribution**, particularly with respect to the adversary in order to effectively draw the redlines and cyber thresholds, as well as influence the cyber posture and apparatus of the adversary. For effective attribution and credible cyber power thus, the ability of **detection** and **retaliation** is important in addition to the abilities of geo-location, intelligence analysis and impact assessment.

Other established parameters include good sense of **signaling** and **proportionality**, both of which are necessary for the operational success of deterrence in the fifth domain. At the very base, lies the conception of deterrence as **a strategy of discouragement** i.e., in order to deter the enemy from taking an action it otherwise might take via instilling doubt and fear of the consequences in the face of a full retaliation, which will out-weigh the benefits. Cyber deterrence is an extension of such traditional deterrence – the concept of impeding the adversary from undertaking punitive actions within cyber domain via Computer Network Attacks (CAN) and Computer Network Exploitation (Brantly,2018).

Thus, essential are these characteristics without which, the adversary won't be able to receive the defender's intent which will lead to the risk of misunderstanding therefore increasing the risk of escalation towards state-on-state confrontation. Also, sometimes the diversity of actors demands a differential response from the defender. Sophisticated attacks must be met differently.

2.2 FEATURES OF CYBER DETERRENCE STRATEGY



Source: Drawn by researchers, Data Source: (Brantly, 2018).

2.1.3 TYPOLOGY OF CYBER DETERRENCE

Deterrence by default can be restrictive or absolute, general or immediate, direct or extended and even an act of Compellence. Within typology, there exist different types of deterrence strategies in cyber space i.e., by punishment and denial, as well as by de-legitimization, entanglement and reputation.

1. **DETERRENCE BY PUNISHMENT**

The strategy of punishment as a form of deterrence involves the notion of massive retaliation for ensure a Mutually Assured Destruction (MAD). The 'punishment' acts as a clause to intimidate the attacker via a promise of second kinetic strikes and economic sanctions. Within cyber space, deterrence by punishment assumes the form of retaliatory cyber strikes as well as pre-emptive strikes in the digital space, against any incoming cyberattack or cyber operations. Cyber deterrence by punishment aims at persuading the adversary a credibly threatening reaction to its coercive action. However there has been an issue when it comes to executing deterrence by punishment as it involves taking punitive actions that could result in escalation. The tensions in between states also increase because of assertive policies that

comes with the assertive actions undertaken to deter cyber-attacks by adversaries. Sometimes this strategy serves the purpose of self-dampening mechanism. The only factor that could fix this dilemma is the element of attribution where targeting only that party that involve in malicious activity should be targeted. However sometimes the element of time and technical difficulties that comes with attribution should be considered that is only a deal of a cyber power. Meanwhile there are number of other factors that need to be considered when it comes to deterrence by punishment. This involves the elements is to communicate the level of threshold, drawing distinction in between what is difficult and impossible (Cullen, 2019).

2. DETERRENCE BY DENIAL

Denial is the inherent part of any deterrence strategy. It is an approach which is less conflict driven and an approach which seeks to convince the offensive actor that the incoming attack will become futile and cease to bring it the benefits it seeks. Within cyber space, deterrence by denial is regarded as a traditional defensive tactic, discouraging the attacks via robust, costly, and proactive defenses. For effective Deterrence by denial strategy in the fifth domain, governmental sponsored large, focused and up to date security systems and networks are required, as well as trusted security practices and hardware and software components, the costs of which are significantly high. Resilience is one main important component of deterrence by denial strategy. To sum up deterrence by denial is all about resilient building tactics. The cost assessment of deterrence by denial tactic iterates it to be of low cost. In the paradigm of national security, it often fits well and is suitable. However, the cyber spaces and fifth domain is unpredictable and complex to an extent where unilateral denial is almost impossible. The deterrence by denial is often focused on systematic vulnerabilities. Sometimes the nature of attacks on system also needs to be determined in order to protect the system. Also there is a need to highlight the fact that sometimes the denial strategy is the focus on bolstering defense by inward capability building after shock (Monaghan, 2022).

3. DETERRENCE BY DE-LEGITIMIZATION

Also known as naming and shaming, deterrence by delegitimization deals with governmental deliberations in formulating rules and norms for state behavior in cyber space. With a threefold aim and process, deterrence by delegitimization focuses on shrinking the battlespaces by creating a general principle of restraint and raising the costs of bad behavior. This narrative has been around for many decades but only a handful of times it has been pursued by state governments. A few examples include the delegitimization of Not Petya campaign by Russian military campaign. The Chinese ministry of state security was also called out for delegitimization for its APT10 and APT40 campaigns in 2018 and 2021. In this strategy the policy of tailored and extended deterrence also comes in play. It also involves targeting the adversary offensive campaigns by means of establishing acceptable and non-acceptable attitudes and thereby concentrating attention on marginal gains. It also increases the leverage and bar of credibility. The deterrence surface area is also increased. an example of this strategy is the reassurance missions of united states of America in Europe which are considered to be legitimate. This also serve the purpose of complicating adversary OODA loop (Monaghan, 2022).

4. DETERRENCE BY ENTANGLEMENT

Prominently articulated by Joseph Nye in his paper 'Deterrence and Discussion in Cyberspace', the strategy of deterrence by entanglement rests upon the debate of how state-to-state interdependencies facilitate and mitigate interstate conflicts (Nye, 2017). Within cyber space, deterrence via entanglement aims at imposing serious costs on the attacker and as well as on the victim in order to enhance the benefits of disincentives and minimizing the risk seeking by an adversary. Unlike the conventional deterrence practice, deterrence by entanglement focuses on creating a world with barriers not raised with hard sovereignty over cyber space, but a world in which barriers are lowered (Nye, 2017).

5. DETERRENCE BY REPUTATION

Deterrence by reputation rests on the idea that 'a country's image is one of the things worth fighting for, for action and expectations other countries carry about its behavior (Schelling, 1996). It is a well-established strategy of traditional deterrence but within cyber space

context, this strategy hasn't been explored much. It revolves around the idea of a state resolving any crisis by deterring up to the mark of its reputation and self-image. For example, U.S. STUXNET cyber campaign against Iran in 2009, to hinder its nuclear facility clearly sent a message of its reputation being in possession of sophisticated intelligence agencies. Russian deterrence by reputation strategy signals its asymmetric superiority in information warfare (Nye, 2017).

Many scholars regard the phenomenon of fifth-domain deterrence as an ambiguous phenomenon with its conceptional lines being stretched while incorporating no real and authentic examples as a proof of the existence and possibility of this phenomenon. Today it persists as a quintessential anchoring concept in political and security debates with states engaging in cyber threats and counter-threats over the course of last three to four decades. Cyber deterrence thus, as a phenomenon has evolved and developed as an extension of conventional deterrence from the late 20th century till present day 21st century. It is of much importance to trace out this historical evolution as well as keep in account the different challenges and limitations the practice of deterrence faces in this new domain of strategy i.e., the fifth domain or cyber domain.

2.2 PRE-REQUISITES/CONDITIONS OF CYBER-DETERRENCE STRATEGY

Because of the problems of global reach, scattered nature and computer networks interconnectedness as Zhang Xin wrote, it is getting difficult to execute cyber deterrence strategies. Meanwhile with the network system's vulnerability increasing there is a dire need for a coherent and well-articulated cyber deterrence strategy. In order to frame a well preached on strategy certain requisites need to be catered. A coherent cyber deterrence strategy doesn't mean that it should deter all kinds of attacks but to deter attacks on major scales so as to constrain the strategic goals that each adversary intends to achieve with cyber-attack. The first step in framing of cyber deterrence strategy demands a will power on part of the decision makers and credible signaling.

2.2.1 PURPOSES OF CYBER DETERRENCE STRATEGY

There are multiple purposes apart from deterring adversary from attacking and launching an assault on one's system for which states wage cyber deterrence strategy. There are as follows

i. The prime purpose of cyber deterrence strategy is to cast punishment on adversary.
ii. It also includes taking the adversary decision making apparatus in one own influence so as to diminish any chances of rewards that an adversary could expect from cyber-attacks.
iii. Imposing limitation on the benefit an offender could attain from an attack.
iv. The massive retaliation could be faced by the offender in case of launching an attack would be playing part in deterring it.
v. Moreover, another purpose of cyber deterrence strategy is to convince the attacker that because of one's own resilient critical infrastructure, it will not be gaining any award.

Mean that states try to achieve from cyber deterrence strategies is to convince the offender that more benefit could be achieved by not opting for revisionist policies. The purpose of cyber deterrence should be that it must deter all sort of private and public actors of the adversary state (Kuglar, 2009).

2.2.2 GENERIC MODEL OF CYBER DETERRENCE

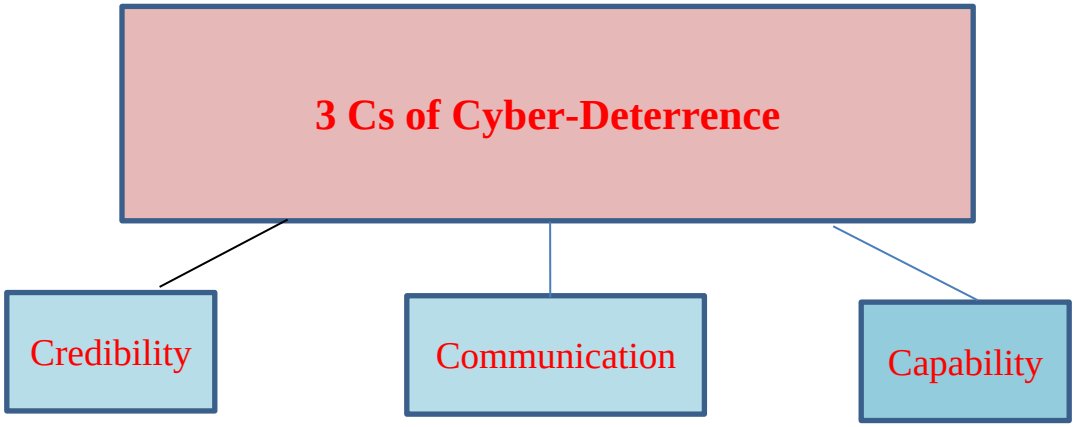
Cyber deterrence strategy demands that deterrence objectives should be specified, adversary's capability analysis, identification of desired effects that the actor is intending to achieve, development of course of action, plan and capabilities and the execution of plan.

1. 3CS OF CYBER DETERRENCE

The spatial factor in cyber deterrence strategies demand them to be of full-spectrum nature. As "black energy malwares" could be used not only by states but also non-state actors and any individual. As cyber-attacks range from small attacks leading to computer network systems exploitation and penetration to capable of creating an impact of cyber Pearl harbor. Thus full spectrum cyber deterrence is in demand. The character of cyber deterrence demands that it must entail the character of general deterrence refereeing to the whole international

community and even tailored one (Jensen, 2012). The 3Cs of cyber deterrence involves credibility, capabilities and conveying the threat. Cyber deterrence strategy coherence demands that a declaratory policy depicting the resilience and credibility of one's own critical infrastructure should be crafted to deter the adversary and this credibility of cyber deterrence declaratory policy comes with the situational awareness, well-coordinated command and control system, increased capability of cyber space by developing counter-cyber offensive weapons to inflict cost of retaliation on the adversary (Kugler, 2009). This is to counter the increased vulnerability of cyber-spaces whose vulnerability also increase with the enhanced digital capacity of a state as Henry Kissinger put it.

2.3 3Cs of CYBER DETERRENCE STRATEGY



Source: Drawn by researchers, Data Source: (Kauglar, 2009).

2. DECLARATION OF THRESHOLDS

A coherent cyber deterrence strategy demands that a convincing explanation must be given about setting thresholds which must be indicative of how serious the decision makers are on cyber offense launched by adversary. This threshold must also entail that what kind of decisive action could be invited on a potential act of war and no doubt should be left in the mind of adversary's policy circles. A tailored yet overwhelming and proportional violation should be called for om breach of red line and threshold (Kuglar,2009). The threshold must be credibly signaled by defender so as the adversary could not misinterpret the intentions as in cyber spaces because of ambiguous reputation of states being status quo- and revisionist

powers. In order to avoid vague signaling two paths could be followed one of general and other one of tailored signaling. Moreover another condition aligned with threshold declaration is attribution of the offender which must not be dubious. Otherwise it could make retaliation costly thereby impacting cost benefit analysis. (Taddeo, 2018). States need to avoid drawing fuzzy lines which must identify in between run of the mill sort of cyber-attacks and the significant one's calling retaliation for the latter one's (Willner, 2017).

3. NEED OF CYBER NORMS

Regulative norms shape the prescription of acceptable cyber behavior. The need of cyber norms in digital spaces could be endorsed on account that those norms could curtail; the ambitious policies of the offenders. These norms even are undeveloped but include imposing control on acquisition of cyber weapons by revisionist states and non-state actors and no first use of cyber offense policy. The prime purpose of these cyber norms is to initiate international opprobrium thus fostering cyber deterrence. Setting allows threshold is another essential requisite of coherent cyber deterrence strategy. according to the Ann Florini norm development theory the cyber space norms are at the first stage of norm emergence and then will be followed by norm cascade and internationalization of norms. The international organizations like UN. NATO, EU and ICANN could provide platform for evolution (Thayer,2015).

4. DOCTRINAL GUIDE OF CYBER DETERRENCE STRATEGY

There are multiple types of cyber deterrence doctrines that includes general and targeted capability doctrines aiming to achieve a mastery in retaliatory attack over general and some specific targets. The date highways are being exploited in assured disruption doctrines thereby disrupting the IT services of the adversary. Forced transparency aim to frame covert operations and doctrines of digital media control intending on spinning narratives thus influencing the cognitive milieu of adversary. An ideal cyber deterrence document must cater the uncertainty aligned with the offender identity, avoidance of unintended escalations, pseudonymity and heterogeneity being character of the digital spaces, building sophisticated network systems. There are four characteristics of cyber deterrence such as scholars consider

the cyber strategies to be vital one for the nations that are less tech dependent and smaller or middle powers. Moreover sometimes the attribution is a choice of the nations as sometimes they don't want themselves to be identified. The contents of cyber deterrence doctrines include posture of force, procedures of command and control, escalation rhetoric as there exist myriads of strategic options in digital spaces. The doctrines of cyber deterrence differ from that of nuclear deterrence one's as in these doctrines the problems of attributions are being fixed by conducting false flag operations to indicate that defender have full capability to organize a massive retaliation. Moreover the strategy of soil erosion that includes the exhibition of both considerable intensity to that of capable of launching small scale skirmishes. Moreover, the cyber deterrence strategies must also cater force postures including sub conflict capabilities (Martellini, 2013).

5. RESILIENT CYBER OFFENSIVE/ DEFENSE CAPABILITIES

States must readily prepare to develop cyber forensics to locate the offender. This ability of attribution which has been a constant hurdle in cyber space could be fixed by developing forensics on model of nuclear and biological weapons. Inter department and agency collaboration is in need in order to develop such technologies that could bolster cyber defenses and make deterrence postures functional. This should be made part of defense and intelligence advanced research projects. The cyber defense could be improved by fixing the computer network vulnerabilities which could be done consolidation of government internet connections. The nature of such initiatives must cater public private and bilateral-multilateral divide. Cyber privateering strategy which involves bolstering defense of allies and partners should be made part of initiatives to develop offensive and defensive capabilities. Conducting cyber offensive operations should also be part of the effort.

6. FUNCTIONAL COMMAND AND CONTROL SYSTEM

Cyber deterrence strategies demand effective and functional command and control systems to avoid accidental escalation. This system must also be capable enough to analyze the intentions of the expected offender. This could be done by employing simulation exercises. This command and control system requires close coordination in between the intelligence

agencies homeland security and national security agencies. Deterrence and denial units need to have close cooperation or coordination with national level security institutions. Both bilateral and multilateral cooperation is in need with allies is in need because of increased vulnerability in case of retaliation. The command-and-control system must also be aware of the global situation which needs to be holistic as it should cover the potential adversaries and their identification, their assets and capabilities analysis coupled with motives and value structures of one's own system (Kuglar,2009).

It has been established that for a state to forge cyber deterrence posture, it must have the capabilities to pose threat on adversary and there must be credible implementation of deterrence declaration being established. The compliance with international cyber norms that establishes the standard of acceptable and non-acceptable behavior is an essential requisite for the strategy. Also, a doctrine stating guidelines for the execution of strategy is an important element of deterrence strategy. However, deterrence in fifth domain face multiple challenges because of incompatibly of the strategy with the strategic environment in cyber space. The challenges faced by cyber deterrence have been explained below.

2.3 CHALLENGES TO CYBER DETERRENCE

The digital age is inherently in paradox with deterrence phenomena. The interconnectedness could lead to ambiguity in target identification leading to third party being dragged.

- **CONCEPTUAL CHALLENGES**

Cyber deterrence is a complex phenomenon where states with more capability are more at risk. It is often difficult to deter the actors with weaker information system. The credibility question on deterrence mechanism is another problem where retaliatory attack could result in escalation making the defender more vulnerable and thereby limiting the willingness of launching a counter offensive attack that is important for deterrence reliability. A conceptual difficulty in cyber deterrence is that it gets difficult to convey the threat. Sometimes the anonymity of the challenger could pose another hurdle (Lupovici, 2011). Because of multiple actors like private audience/ non-state actors and organizational actors operating in digital space it gets difficult to holistically encapsulate all of the motives and intentions whereby

each adversary demands a different response for its behavior. Moreover, the net assessment of offensive -defensive capabilities of the challenger often gets difficult to make. The most common challenges in deterring the challenger with cyber offense is that it could disrupt the cohesion of allies and while maintaining full spectrum deterrence and that of extended one it often gets difficult to protect third parties from the menace. Imposing a control on escalation and because of the shifting red lines it also gets difficult to avoid escalation.

- **TECHNICAL CHALLENGES**

It is characteristics of cyber deterrence that one deterrence declaratory policy could not be sufficient for deterring all kinds of attacks like cyber thefts, espionages and attacks as sometimes the challenger use proxies to launch attack which take years and sometimes more to punish them. Moreover, the cyber-attack sometimes gets difficult to trace because of the third and second order effect that it produces. The alignment of thresholds for attacks from private actors with that of usage by states of that hardware need to be carefully articulated in deterrence strategies. For example, attack by Mirai malware could be done at any level. One of the biggest technical challenges with deterrence by punishment is that it requires continuous and coherent intelligence preparation of battlefield. The range and time factor in punishing the offender must also be catered. A sustained intelligence is required with weapons system that must be aimed at specific target. Moreover, the basic requirement to maintain the critical infrastructures that are also complex in deterrence by denial phenomena is ante-impetus reducing the probability of penetration (Brantly,2018).

- **PRAGMATIC CHALLENGES**

The influx of actors in digital space makes the attribution of attacker and offender considerably complex. States often put blame on rogue actors for malicious activities. In cyber space the either/or frame of attribution does not work and identification demands time. Moreover signaling in cyber deterrence holds multiple grey areas as states prefer to keep their capabilities confidential. Moreover, each cyber weapons have multiple uses and even private sector hardware could be used for covert operations. The chances of outstripping the defense by offense with signaling is also great. From the magnitude of the result caused by the attack

the necessity and jus ad bellum principle of retaliation could be sufficed. The time and scale of retaliation must also be catered (Jensen,2012).

2.4 KINDS OF CHALLENGES TO CYBER DETERRENCE

CATEGORY	CHALLENGES
Conceptual Challenges	1. Sometimes state with more credibility is more at risk 2. Accidental Escalation 3. Difficulty in conveyance of retaliation threat 4. Difficulty in comprehending the challenger intentions and motives
Technical Challenges	1. One deterrence declaration is not sufficient for different kinds of threats 2. Private sector dilemma 3. Maintenance of Continued Surveillance 4. Factor of second and third order effect
Pragmatic Challenges	1. Actors Pluralism in cyber space 2. Strategic advantage to cyber offense 3. Difficulty in maintaining the time and spatial factor 4. Difficulty in attacker attribution

Source: Drawn by researchers, Data Source: (Jensen, 2012)

2.4 HISTORICAL EVOLUTION OF CYBER DETERRENCE: IN PRACTISE

2.4.1 EVOLUTION OF DETERRENCE PHENOMENON: FROM CONVENTIONAL TO DETERRENCE IN FIFTH DOMAIN

The importance of deterrence lies in its variability of a strong defense which can rebuff an offense by inflicting in return massive retaliatory damage. Deterrence thus, by its virtue is the concept dealing with the threat of use of military force in order to impose insufferable costs on the adversary by using the intended instruments of bargaining and coercion i.e., a mix of defensive and offensive capabilities in addition to the capacity of influencing the motivations and psychology of the potential attacker. It is a phenomenon carried into account if an opponent takes up an unacceptable action. The threat extended usually categorizes as credible and calculated with potential gains outweighing the possible harms i.e., deterrence as a strategic campaign short of an armed attack. This makes deterrence a more nuanced approached in military and nuclear calculations, with its yet further anchoring in political calculations amidst the Cold War period. Today, deterrence as an anchor falls within cyber domain as well, and thus it can be witnessed it circumscribes all the five domains of strategy i.e., from conventional domains to nuclear to the cyber domain. In order to understand the strategic environment of deterrence in cyberspace it is necessary to understand the historical development of deterrent strategy being shaped in and through from conventional to nuclear to cyber area.

Throughout history, threatening of use of military force has been utilized during **conventional strategy** and traditional warfare. However, alongside the changing international system has changed the context of this deterrence phenomenon. This change is reflected in the number of adversaries and capabilities of the states i.e., from single peer adversary to several different opponents, each with distinctive and increased military capabilities as well as increased tolerance for risks. This was particularly prevalent in the 20 century which witnessed an extension of deterrence strategy into a deterrence theory, within the confinements of **nuclear frontier**, paving way for nuclear deterrence. The strategic engagement and competition between United States and Soviet Union which hovered in the

backdrop of most of the 20th century during the Cold War era, is the classic example of deterrence engagement. After the first use of nuclear weapons in 1945, as in the words of Bernard Brodie, 'the chief purpose of our military has been to win wars, its purpose now must be to avert them' and thus evolved deterrence as strand of larger defense strategies by US and USSR, as a result of which it was being deployed as an offensive-defensive strategy in controlling nuclear escalation (Kuglar, 2009).

In the contemporary global system, this practice of threat of use of force further extends well into the fifth domain i.e., cyber domain. Along the course of its development as a practice, deterrence therefore stretches from conventional domains of warfare i.e., land, sea, and air to the fifth domain of strategy, giving rise to the concept of cyber deterrence or **deterrence in the fifth domain**. Adding to the purpose of military is thus another duty i.e., the effective prevention of cyber space.

With its conception in the 1990s, cyber deterrence as a strategy was nurtured by the US Department of Defense as a war game exercise when during operation 'Desert Storm', the Iraqi communication networks were paralyzed. This triggered the scholastic debate on deterrence within cyberspace. The term was later introduced in 1994 by James Der Derain. Numerous examples can be found in the following years particularly in the first decade of the 21st century. From **Denial-of-service campaign** in 2007 to Russian **'extended cyber deterrence'** in Georgia and all the way to the **STUXNET campaign,** cyber deterrence has gained exponential attention within global security. In 2014, NATO is seen as to be maintaining an ambiguous deterrence strategy for cyber space.

The years from 2013 to 2016 are regarded as the golden age of cyberwar scholarship with official cyber deterrence strategies and policies being adopted by states. It is in these years that a tri-lateral cyber competition and a deterrent nexus between U.S., China and Russia has been witnessed.

2.5 EVOLUTION OF CYBER DETERRENCE STRATEGY

Deterring a full-blown cyber conflict in this digital age is the main concern of major powers including USA, China and Russia who want to leave no stone unturned in a bid to protect their

critical infrastructures including computer network systems. The major powers have not only identified their cyber threats but also adversaries which is reflective of the intense strategic competition that exists in cyber realm. A trilateral nexus of cyber deterrence has been established in between USA, China and Russia because of the China and Russian realignment. Following it has been explained that how deterrence as a strategic phenomenon evolved over the course of time in different states and regions of the world. However, the evolution of cyber deterrence phenomena has not been consistent and coherent. It has evolved in different regions of the world differently with states incorporating this element in their strategies.

2.5.1 DEVELOPMENT AT INTERNATIONAL LEVEL: STRATEGIES OF USA/ CHINA/ RUSSIA

- **UNITED STATES OF AMERICA:** The cyber pearl harbor threats in 1990s provoke the debates on cyber deterrence. In **US Clinton** administration 1996 executive order started the debate on denying access to critical infrastructures. Then in Bush 2002 NSS deterrence was being mentioned but not in cyber space. In White House National security strategy to secure Cyber space deterrence principle was articulated mentioning that US retaliation in case of cyber-attack would not be limited to criminalization of offenses. In 2005 cyber assurance support was being touched with 2006 Quadrennial defense review calling for maintenance of deterrence posture by DoD. 2006 NSS of USA asked for building a tailored deterrence posture against disruptive threats such as cyber one's. In the year 2007 National Military strategy to secure cyber space asks for capability building in bolstering attribution abilities. It was part of US entanglement strategy that Chinese did not use cyber-attack means on US power grid because they feared that cost might exceed the benefit. In Obama era however cyber deterrence was being mentioned multiple times in 2010 NSS and 2011 NMS. More consistently cyber space deterrence was being mentioned in Joint doctrines of JP 3-14 of space and cyber operations call for bolstering cyber defense (Trujillo, 2014). It was 2014-2015 realized that the passivity of USA deterrence posture in USCYBERCOM need to be revised. USA as part of deterrence by

punishment and cross domain deterrence imposed economic sanction on Russia because of the cyber offense being committed in elections.

- **IN RUSSIAN CYBER STARTEGY:** In 2011 a malware was inserted in US infrastructure to deter US by reminding them of the vulnerability in their system. The Russian cyber offense on Ukrainian power grid was part of their deterrence by punishment strategy. In 2016 the Russian disruptions in presidential campaign is often dubbed as part of deterrence by punishment strategy in order to respond to the 2011 Hillary Clinton propaganda campaign against Russian elections (Nye,2017). Russia in doctrines like Gerasimov and in statement given by Deputy PM in 2013 Russia is in constant war with West in cyber space for which it needs to pursue strategy of concealment and deception. in order to manipulate the cognitive thinking of adversary it has used strategy of cumulative deterrence since 2016 as seen in attacks Estonia in 2004, Georgian war 2008, Crimean conquest in 2014 and US elections attack in 2016. It was in National security strategy 2021 they mentioned this strategy (Kari,2022).
- **IN CHINESE CYBER STRATEGY:** In Chinese strategic thinking in order to execute plan of weishe a terminology used for both deterrence and compellence offensive posture is important. This strategic thinking prevails till 2008 from 1990s. It was year 2008 that serve as hinge point for shift in strategic thinking where they started using terminologies like MAD and first strike advantage for cyber deterrence. In year 2015 they made cyber deterrence crucial part of their strategy In 2014 China as part of deterrence by punishment strategy boycott the bilateral cyber committee. (Jiang, 2019).

2.5.2 DEVELOPMENT AT REGIONAL LEVEL

- **EUROPEAN UNION AND NATO** The Ghost RAT attacks in 2010 provoked EU members to collectivize efforts in order to deter belligerent adversaries from attacking for which they adopted Capability development plan which in 2013 turn into EU cyber security strategy focusing on capability building. It is an established fact that the deterrence dynamics of EU strategy is complex and the reason for that is the

horizontal and vertical interconnectedness that exists in cyber domain. There although exists a robust system of agencies and bodies assigned with the tasks of securing the critical infrastructures and denying the attack on systems These bodies involve the ENISA, EDA & CERTS. The conciliation of policies is the amin target of this policy where EU intends to maintain a system of secure cyber spaces. (Nye, 2017). The ultimate factor that decides the fate of EU strategy is the factor of international friction that exist in between three main pillars namely USA, Russia and China. However, the EU policy still lags in the matter when it comes to denying the access to state and sophisticated actors of the system. The point worth noting here is the fact that the first policy of EU in cyber domain in 201 was triggered by the malicious. The creation of synergetic initiatives in between members states, the comprehensive policy adoptions, increasing the resilience of cyber defenses. This was all part of EU Cyber security strategy EUCSS was part of its policy. Attacks on its system by the foreign belligerent powers and parties. In 2016 NATO and EU joined hands and joined declaration was issued which also led to 2017 Permanent Structured cooperation by member states of contributing armed forces. When it comes to NATO strategy the major breakthrough took place in 2010 strategic concept titled ss “Active engagement and defense that aimed at deterring pernicious threats and sophisticated attacks. this notion also exists in NATO strategic thinking that cyber-attacks are matter of National security. Also, NATO intends to detect and deter cyber-attacks while also attaining the capacity to recover from them. It was after 2007 cyber-attacks that triggered response leading to conference of Bucharest 2008 such as CDMA/RRTs of NATO to build resilient critical infrastructures.it was in 2009 that harmonization of denial capabilities building was done under NATO defense Planning procedure known as NDPP. The bodies responsible for deterring attacks on NATO member states involve North Atlantic Council NAC, Cyber defense Committee CDS, Cyber defense management board and NATO Incident Response Capability NCIRC. In 2010 under “deterrence and defense” section of NATO strategic concept that crafted centralized cyber response system using both offensive and defensive capabilities to frame deterrence posture in cyber space. Under this

concept which entail 10-year plan leading to establishment of multiple agencies like NCI/NCIP/MNCDE from 2013 till 2015 leading to cyber space declaration as military domain (Manjikian, 2021). However when it comes to NATO-EU cooperation in field of cyber deterrence the 2018 Brussels Summit plays an important role where it was decided that strong cyber defense plays an important role in bolstering deterrence.

- **IN MIDDLE EASTERN STATES CYBER STRATEGY:** In the year 1997, Tahlia agency was established in Israel to reduce vulnerability in state cyber space. in the year 2007 Operation Orchard against air defense system of Syria was an approach to deny the penetration into state critical infrastructure. The use of Stuxnet against Iran in 2010 was an example of offensive posture in Israel strategy. In the 2015 NSS of Israel a strategy of commutative deterrence strategy (Gori,2022). When in 2015 C41 directorate and Unit 8200 were merged that assisted in Israel becoming second largest cyber power announced in 2017. As a model of deterrence by punishment Israel use both kinetic and non-kinetic means such as IDF in order to brag on its overwhelming military power in cyber space launched an attack on Hamas in 2019. The 2020 blackout in Natanz in Iran was an example of Israel use of offensive power. Israel is also waging low intensity conflicts with its key enemies Hamas Syria to maintain deterrence such as May 2021 attacks where Hamas operative buildings were destroyed. (Ibrahim, 2022). Iran holds a capacity to maintain a minimum deterrence posture against Saudi Arabia as it was deflected in 2012 when Shamon virus was used to trigger disruption in Saudi workstations. Iran cyber deterrence strategy is of both offensive and defensive nature. Iran recently has entered into an alliance with Russia to bolster its cyber defense. In KSA there has been islamization of cyber security mechanisms since 2007. The Shamoon virus attack in 2012 was an awakening call for Saudi government to build resilient cyber infrastructure that could deny and deter the non-state and state level threats but 2014-2015 Cyber emotions attack on infrastructures provoked the vulnerabilities. Iran on the other hand in order to develop a Cyber Shi'ite Crecent and use of proxies in order to conduct more destructive yet sophisticated attacks being a second-tier cyber power. The National level passive

defense organization is responsible for using power to coerce and deter enemy and it was established in 2003 and hosted conferences like “cyber-Hezbollah “in 2010 establishing and cyber defense headquarters and cyber army in 2012 to conduct attacks such as in 2017 attack on KSA petrochemical industry.

- **IN EAST ASIAN STATES CYBER STRATEGY:** With the increase in cyber-attacks from 2013-2018 as reported by NCIT in Japan especially major attacks like against Tokyo Olympics Committee. Now Japan has crafted some discursive mechanism of denying the access to critical infrastructure as mentioned in National security strategy 2013. North Korea strategy is of cumulative cyber deterrence by launching cyber offense like 2009 attack on ROK national defense ministry to 2013 Dark Seoul attacks and 2014 attack on ROK nuclear power plant. It was in year 2011 that National Cyber security plan in ROK used terminology of deterrence in cyber context. However, it was further advanced and crafted in 2019 National Cyber Security strategy.
- **IN SOUTH ASIAN STATES CYBER STRATEGY:** In 2019 after Pakistan was ranked at 75th place in global cyber security index and attacks as reported by ISPR in 2020, Amnesty International Report that India is involved in attacks against Pakistan such as Pegasus Spyware against Pakistan that led to Pakistan declaring its first cyber deterrence posture in Pakistan national cyber security strategy 2021 with Pakistan CI/CII being the red lines and thresholds with attack on them considered to be attack on Pakistan national sovereignty (Moiz,2023). In India there has been considerable growth witnessed in the information and technological sector. In order to create the effective cyber deterrent, it was one of the few countries who resorted to legal measures. The first Information and technology act was passed in 2000 in line with UN model law on electronic commerce. The key elements on which Indian cyber deterrence strategy rely involves punishment given on documents tampering, hacking as offense, illegal digital certificates distribution. The financial and technical systems have also been improved considerably. India started developing its cyber deterrence posture after National Cyber security strategy in 2013 which did not comprehensively articulate cyber deterrence policy but in 2017 in Joint Indian Armed forces doctrine

they called for TRIAD in cyber space and building credible deterrence through launching punitive attacks and offensive posture. In 2019 and 2020 national cyber security strategies were restructured (Kumar, 2019). Apart from India and Pakistan another important state that started framing its strategy to counter attacks on national infrastructures was that of Bangladesh. It came after the attack on national bank in 2016. The main strategy to counter and deter cyber-attacks in country especially of criminal nature was mentioned in the National Cyber security strategy of 2014. Its prime focus was on strengthening the legislative system for which it was established that the ITU toolkit and Convention on Cyber-crime would be consulted. Also, the technical and procedural measures would be adopted to further strengthen the system. The institutions responsible for framing the strategy in Bangladesh involves the APT Cyber security forum and direct coordination with prime minister office.

2.5 EVOLUTION OF CYBER DETERRENCE STRATEGY

State/ Region	Evolution of cyber deterrence in strategic thought
USA	- In 1990s cyber pearl harbor threat triggered debate of deterring it. - In 1996, Clinton administration issued executive order to deny access of adversary. - Bush mentioned deterrence in 2002 National security strategy. - 2006 Quadrennial Defense review asked for maintenance of deterrence posture - 2007 National military strategy to secure cyber spaces asked for bolstering defense resilience. - In Obama administration the cyber deterrence was mentioned in 2010 NSS, NMS 2011 and joint doctrine of JP 3-14 of space and cyberoperations - In Trump era the USCYBERCOM was relegated with this responsibility.
RUSSIA	- Russia has always opted for deterrence by cost imposition and punishment option. - Cumulative deterrence strategy was used in 2004 attacks on Estonia and war with Georgia in cyber realm.

	- 2011 attack on US infrastructure. - Cyber deterrence was mentioned in doctrine of Gerasimov and statements given by Putin in 2013. - In 2021 NSS Russians mentioned cyber deterrence under information security category
CHINA	- In China cyber strategy the word Weishe was used for cyber deterrence from 1990s- 2008 - From 2008 they started considering options of first strike capability and MAD in cyber realm for deterring attacks - 2015 cyber deterrence was made crucial part of strategy
EAST ASIA	- In Japan the debate of cyber deterrence by denial started in 2013 after attacks on Olympics committee that lasted till 2018. Deterrence by denial posture was adopted in NSS 2013 t - North Korea has adopted strategy of cumulative deterrence posture since 2009 - 2011 in RoK National cyber security plan that cyber deterrence was mentioned which was repeated in 2021 cyber deterrence strategy
MIDDLE EAST	- 2010 establishment of Tahlia agency in Israel - Series of operations such as 2007 Operation Orchard in Syria and 2010 Stuxnet attack part of cumulative strategy - It was officially adopted in 2015 NSS. - Low intensity attacks such as 2020 Natanz blackout are examples. - Commutative cyber deterrence posture was adopted in 2021 - Saudi Arabia has adopted defensive posture such as 2007 Cyber security measures - Iran has adopted an offensive posture of cyber deterrence against KSA and Shamon virus attacks are example a passive defense organization have also been established
SOUTH ASIA	- It was in 2019 that Indian Pegasus Spyware that triggered Pakistan policy circles. - 2021 Pakistan gave its first cyber deterrence posture in cyber security strategy - From 2013 India started building resilient technologies in cyber space, and

	first information an technology act was passed in 2000, TRIA cyber deterrence policy and deterrence by de-legitimization was adopted in 2017 Joint Indian armed forces doctrine - Cyber deterrence triad existed in strategy of India till 2017 which led to restructuring of cyber strategies in 2021 - In Bangladesh in 2014 NSS cyber deterrence was mentioned after attack on national bank
EU/NATO	- It was in 2007 that during Bucharest conference it was decided under NATO RRT/CDMA that defensive lines must be made resilient - 2010 Ghost Rat attack provoke the debate of cyber deterrence in EU - 2010 capability development plan was adopted in EU cyber strategy. - In NATO 2010 strategic concept the section of cyber deterrence was reserved. - 2013 cyber security strategy of EU - In 2016 EU/NATO joined hands

Source: Drawn by Researchers, Data Source: (Kumar, 2019)

2.6 FAILURES OF CYBER-DETERRENCE

In 2007 because of difficulties in locating attacks like Titan Rain and denial of service attacks on Russia the attribution problems in cyber deterrence strategy emerged. The attribution problems are so deep rooted that Russians were blame for theft of 76 million addresses while in reality it was being launched by US citizen residing in Moscow. Moreover, the attribution of Sony pictures attack to North Korea was also called into question. The instances when cyber deterrence failed involve 2007 denial of service attacks on Estonia, 2008 Russian attack on Georgian critical infrastructures, Stuxnet attack and Iranian retaliatory attacks in 2012 and 2013 on US financial institutions (Nye,2017). The Petya and Not Petya attacks in 2015 and 2016 at global scale was example of deterrence failure at global scale. The second order effects were witnessed in 2018 (Tolga,2018).

The states who frame their deterrence postures in cyber space often do so with the aim of protecting their critical infrastructures from any kind of adventurism. At the tactical level for deterrence strategy to become successful the element of pre-emption and retaliation must be

there. Retaliation must be used an option if the adversary could not stop from provoking the system and exploiting the vulnerabilities. Also, a deterrence strategy must carry the ability to differentiate between serious and minor cyber-attacks because in cyber spaces the malicious activities are considered to be part of daily activities. Threshold must be put in place that could only be violated in case of existential threat posed by the opponent towards critical national infrastructures. The public private dilemma must be dealt with effectively in cyber spaces. The strategy must also have an element where it should be flexible and adaptable but not static. The defending state must have this ability to respond affectively, timely and accurately so that the credibility of deterrence declaration must be attained. The repeatability of the action must also be maintained. However, it is being highlighted that for cyber deterrence to function effectively a stable persistent engagement must be retained as to fill the gaps that exist in cyber deterrence strategy as sometime sit faces the constrain from the system and could not function effectively and accurately that is the requirement of it. The following chapter analyze the cyber deterrence strategy from cyber persistent engagement stability theory perspective.

CHAPTER 3

EMERGING CYBER PERSISTENCE STABILITY THEORY AND DILLEMA OF CYBER DTERRENCE

Deterrence is a strategy that has been exercised in the fifth domain by all of the three major powers namely USA, China and Russia. However, it tends to be a contested strategy and phenomena that demands greater intellectual scrutiny, resilient systems, balance of offensive and defensive strategic postures and a lot more. For deterrence as a strategy to be exercised in the fifth domain within contemporary security environment is a daunting task as sometimes it stands in sheer contrast to the strategic environment in cyber spaces. New theories and concepts therefore, are being introduced to explain the growing strategic environment of Cybered Westphalian Age and to explain the complex concepts and volatile strategies like that of deterrence. Cyber persistent theory is the approach that carefully analyze the strategic environment that persists making it difficult for the strategies like deterrence to function that operates well in traditional domains of strategy otherwise. This chapter at first explains the concept of cyber deterrence and then describes the assumptions of cyber persistent theory. Cyber persistent theory focuses on the ambiguous and gray aspect of cyber deterrence strategy and enlist the factors that makes it difficult for this strategy to functions well in cyber spaces. This chapter comprehensively delves into these details and also critically analyze the points where cyber persistent engagement theory lags in comprehending the concept of cyber deterrence.

3.0 CONCEPTUALIZING CYBER PERSISTENCE

3.0.1 WHAT IS CYBER PERSISTENCE

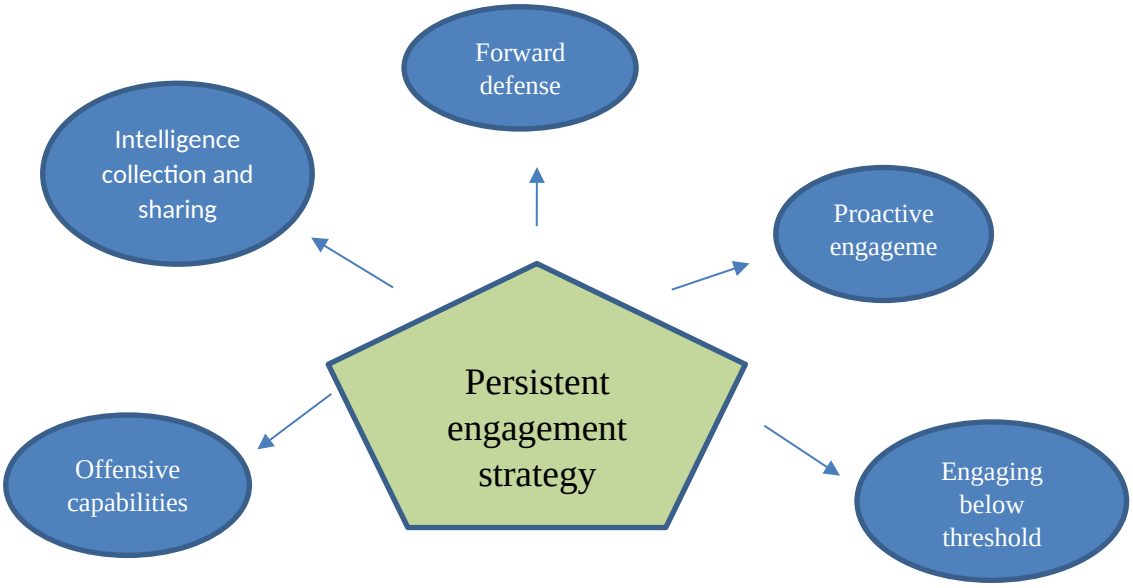
For countering adversary's gains in cyber space amid strategic competition without even resorting to war is what cyber persistent strategy is for. Persistent cyber engagement is proactive, yet the continuous strategic posture states opt for in order to limit the access of their adversaries to the gains an idea also known as tactical bargaining. It is because of the interconnectedness of the cyber chains that states often remain in continuous contact with each other making persistent strategic posture a liability. Persistent strategic posture is often

adopted to maintain a tactical advantage over adversary by means of resilience and engaging in continuous strategic competition (Fischer Keller and Harknett 2019). It is also a feature of persistent engagement that it calls for moving close to the adversary's infrastructure in order not only to maintain a 'forward defense' posture but also whose ultimate aim is to compel the adversary for changing its strategic posture from offensive to that of defensive with minimum chances of attack. The origin of this strategy could be traced to strategic guidance in 2018 issued by White House and from Department of Defense in US. With that its origin could be traced to 2018 National Security Strategy (Fischer Keller and Harknett 2019). Another strategic advantage that this persistent engagement provide is that it makes adversary futile moreover it renders the adversary's defensive posture more costly yet ineffective. The ultimate objective is to maintain the environment of cyber deterrence by means of both offensive and defensive strategic postures. The idea of persistent engagement is the fusion of cyber deterrence and active defense. This is a concept of proactive cyber deterrence. Involves the persistent projection of power by one party with another one in order to mold its behavior to acceptable international standards while staying below the cyber threshold level and not to escalate the matter (Kello,2017). ere are multiple factors that play their part in persistent engagement of one party towards another. This involves the party A constantly involved in the collection of intelligence about the opponent techniques and system resilience. It not only involves element of proactively engage with the adversary but meanwhile updating the resilience of one's own system so that adversary would be deterred to escalate the matter into war. As this is the strategy that demands extending the influence to adversary cyber kill chains and area of influence so a close collaboration and interests allegiance with the third parties and that of allies is also an important step. But meanwhile this is the strategy that asks for a lot of financial cots and sometimes it is dangerous as it could invite backlash from the third parties who then become collateral damage in this game. Also, it carries a lot of risks as assessment of opponent's systems could likely go wrong leading the situation to escalate into cyber conflict and sometimes war. There are five principal standards that a state needs to pursue for the effective implementation of strategy. The assessment of the risk is the first step that states need to take. This assessment involves scrutiny into the adversary's motive, capabilities and assets. The complete knowledge of adversary system and its sophistication is

essential to avoid any escalation of the matter into full blown conflict. The kind of threat being faced by state that could be a state actor, non-state actor or even private organization. Also, next step is intelligence sharing and collaboration with third parties and lastly it is the use of that collected information and intelligence and launching an action (Benton, 2020). The cyber spaces were technically enabled as they shape the behaviors of actors and operations in the domain. There exists intense interconnectedness and inter-dependence of cyber spaces that overlaps each other and run parallel meanwhile the systems of states become vulnerable to exploitation that could only be fixed if states could operate and function persistently. It serves as strategic imperative. Also, in cyber spaces the functionality of one strategy is extremely difficult to pertains for a longer period of time based on the changing nature of operational dynamics. In that case persistent engagement is the only viable option. the only alternative option in case of non-compliance with persistent engagement is the use of offensive capabilities that make conflict more likely however cyber persistent in the very theory of it will likely reduce the likelihood of cyber war. An analogy however is used by the pessimists when it comes to cyber persistent theory that state that persistently engaging with adversary is like running a motorcycle over Grand Canyon. And it could likely invite the opponents to attack more. However, the scholars have come to the conclusion that cyber persistence works well in time of peace (Healey & Caudill 2020).

Following are the essential elements of cyber persistent engagement are mentioned

3.1 ESSENTIAL COMPONENETS OF PERSISTENT ENAGEGMNET



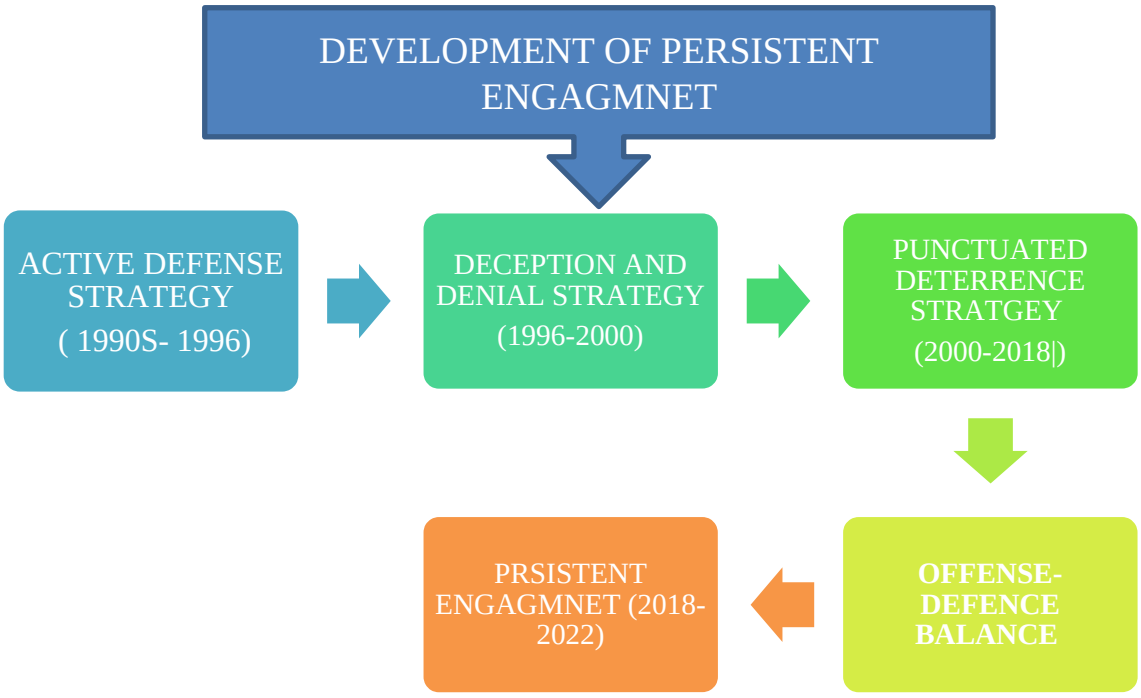
Source: Drawn by Researchers, Data Source: (Healey & Caudill 2020).

3.0.2 THE STRATEGIC ROOTS OF PERSISTENT ENGAGEMENT

The overtly complex strategic environment of cyber space which demands cross-domain cyber engagement for maintaining cyber deterrence and extremely resource intensive offensive cyber operations the maintenance of proactive deterrence posture is the only possible solution. Adopting offensive posture in order to project deterrence is considerably a nuisance as Lindsay and Gartzke noted. Moreover, for successful cyber deterrence projection the engagement of private sector is also important because of fragmented defense being the character of cyber space. in cyber space for the maintenance deterrence the offense-persistent not dominant posture is need of hour. It was Scoot Jasper who illustrated the need for imposing active defense mechanisms if a state specifically US wants to gain a share of power in cyber space. once threshold is being maintained the states need to carry persistent efforts at low baseline. The strategic roots of this approach could be approached back to era of 1990s when active defense was put into effect along with deterrence strategies. Then back in 1996 the face of strategy changed with the active defense in the pretext of deception and denial strategy whose basic notion was establish normative grounds for the engagement and the part was played by defense science board summer study. But hallmark shift took place in 2000 when the CND cyber responses previously relying on the reaction principle shifted towards Defensive cyber operation response actions whose primary purposes are to introduce changes in adversary infrastructure (Healey, 2019). This vision was officially inscribed in USCYBERCOM vision 2018. The aim of this strategy is to ultimately shape the interactive environment of cyber space by means of persistent engagement. Cyber deterrence as Dorothy Deaning also noted, is a failed strategy when it comes to complete prevention of malicious activities for which persistent engagement is the option. Kello gave a policy option of punctuated deterrence of communicating red lines when it is meant to deter an attack having cumulative impact (Hoffman, 2019). This game started when in 2018 in order to deter attacks from Russian Internet troll agency the US forces persistently constraint offense by positioning an attack on energy infrastructures an declaring the intentions. But the consciousness of USA forces is reflected in their establishment of National Security

presidential memorandum and presidential policy directive 20 for synchronization of activities. But some critics claim this engagement to be of collateral damage and equally destabilizing. But meanwhile some scholars such as Nakasone claim this to be of most decisive policy option a state could look into (Devanny, 2021). The strategic roots of this strategic roots of this policy could be traced back to 2011 International cyber space strategy which asked for expanding influence in terms of alliance formation. This was implemented from 2011 till 2015 in case of Chinese malicious activities against permanent management office/ US navy, Russian exploitation of Ukrainian networks and Iran attack on Qatar and KSA facilities. Controlling escalation by means of normative deterrence was maid the character of 2015 Cyber strategy of US (Schneider, 2019). The following is the illustration of cyber persistent engagement strategy evolution

3.2 PERSSIETENT ENGAGEMNET STRATEGIC DEVELOPMENT



Source: Drawn by researchers, Data source: (Schneider, 2019)

3.0.3 ESSENTIALS OF A SUCCESSFUL PERSISTENT ENGAGEMENT

The perspective that cyber persistent strategists hold about cyber space includes the acceptance of malleability, interconnectedness and absence of sovereignty. The persistent engagement demands the acceptance of cyber space violability to exploitation. For persistent engagement the states need to build automated infrastructure that could identify the malicious activities, protect critical infrastructures and nip the cyber offense in the bud. It also involves capacitating the OAAs in order to provide timely yet temporary response to any malicious activity on part of adversary. The functional impairment of adversary servers involved in projecting offense against one's own critical infrastructure is what strategists demand from persistent engagement. The purpose of all this is to retain and maintain a share of power in cyber space which could deter the adversary from launching an armed offense and thereby advancing the aligned interests (Fischerkeller & Harknett, 2017). In order to forge a successful cyber persistent engagement with adversary, a state needs sturdy yet sustained civil-military leadership, confidence of local and international allies/ partners engaging in that environment, robust critical infrastructure for intra-agency interaction, declaration and signaling to the adversaries and lastly well-equipped and trained militia.

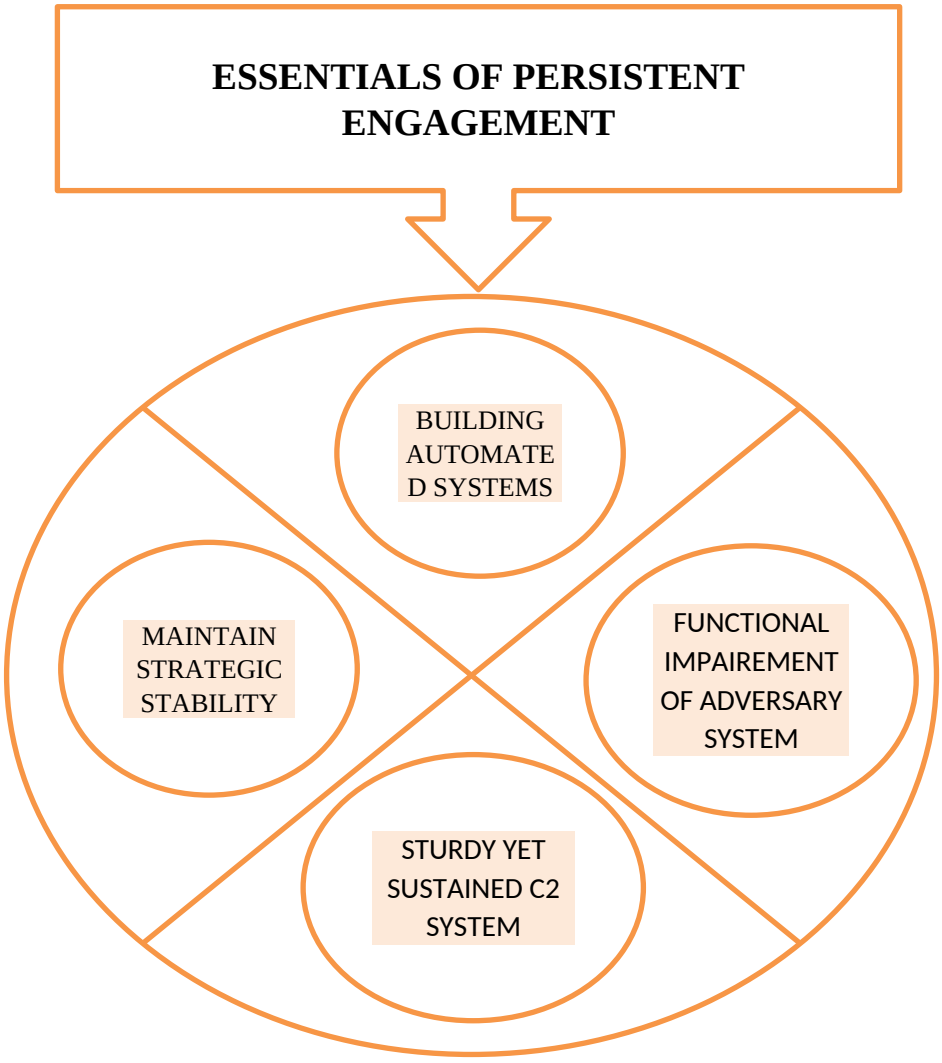
Another important requisite for successful persistent engagement is the synchronization of all facets of cyber policy including diplomatic, military and information one. For waging successful strategy, the strategists must be careful enough to differentiate in between red vs blue and gray spaces which is possible only with confidence that allies could entrust the state with otherwise it could possibly result in their antagonization and unlikely friction. The risk factors associated with this strategy is that if triggered during times of geopolitical rifts it could escalate into a war so preferable implementation of this strategy should be in peace time (Caudill & Healey, 2020). Maintaining strategic stability of cyber space is the ultimate aim in this strategy. The continuous belligerent contact of two adversaries could result in escalation a parallel of which could be traced in cold war times in words of Joe Nye.

This also demands the presence of diplomatic hotlines, deterrence declaration. The on net risks involve the possible friction in case adversary start capacitating itself against the constant engagement which will drain one' own funds. The normative grounds in this case

will be established by means of tactic bargaining and tit for tat effect. With the lack of strategic depths and demilitarized zones, the states need to be over conscious about escalation that could result if states caught in goldilocks phenomena. For as happened in case of Iran Shammon attack because of persistent malware threats from Saudi and Qatar forces. So self-balancing effect accepted from cyber persistent engagement is often exaggerated (Healey, J. 2019).

The following is the illustration of essential elements required for framing a coherent cyber persistent engagement stability theory.

3.3 COMPONENETS OF PERSISTENT ENGAGAMNET STRATEGY



Source: Drawn by Researchers, Data source: (Healey, J. 2019).

3.1 CYBER PERSSITENCE THEORY

3.1.1 INTELLECTUAL ROOTS

Cyber persistent theory is also known as cyber persistent stability theory. There are multiple theories where the roots of persistent engagement could be looked for. The madman theory

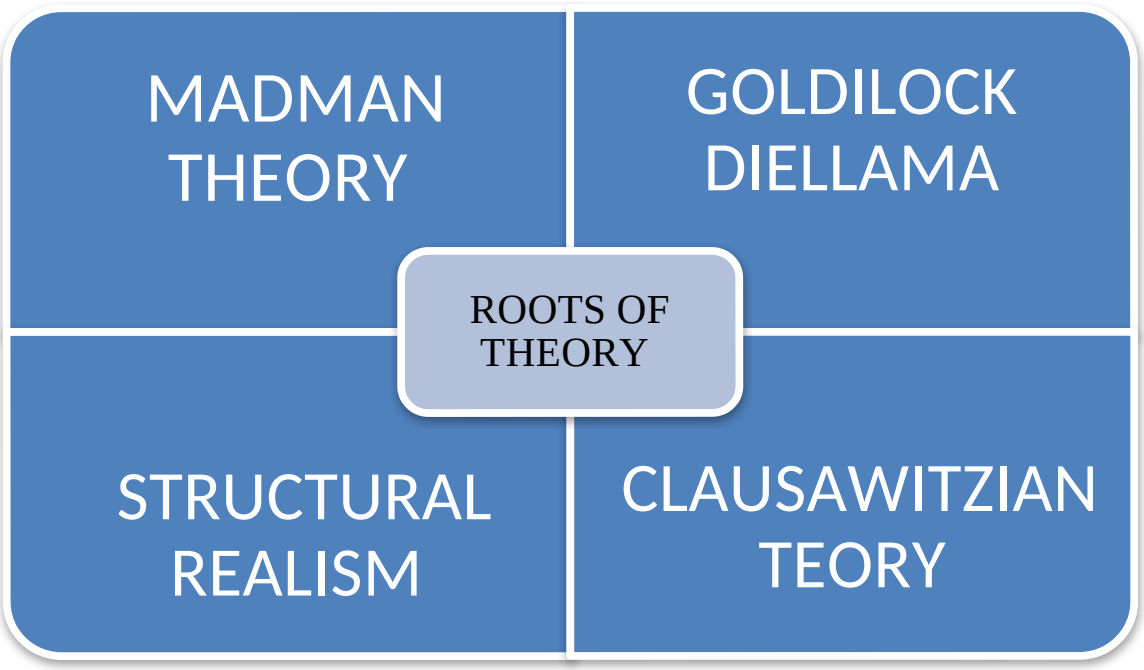
reflects on the mindset of the individual carrying away with the process persistent engagement. It basically reflects the antithetical nature of persistent engagement with the leaders' irrational attitudes that deviated from rational approaches like that of signaling what needs to be catered. Credibility is the basic requisite of persistent engagement which madman theory declare being absent in the attitudes of the irrational decision makers. The scholastic perceptive of cyber persistent theory could be traced to the works of Healey that persistent engagement is meant for limiting the process of escalation of small skirmishes into full blown conflict and to maintain deterrence structure. Another important scholar who focusses on the persistent engagement of states is Nakasone who illustrated that states need to shift their defensive cyber forces into persistent one's. When it comes to cyber space the narratrixes are primarily comes from US literature (Devanny, 2021). Moreover, another intellectual dimension in which the concept of persistent engagement could be traced is based on the underlying objective this narrative project. It aims at maintaining strategic stability in the cyber domain under the umbrella of Cyber deterrence. This is done by not opting for dominant but persistent engagement in order to maintain an offensive-defensive balance and that is basic notion of Goldilocks dilemma (Baldwin, 2014). Another important root of could be traced to the article of Buchanan titled as "The Cyber security Dilemma: Hacking Trust and Fear between nations which didn't explicitly talk about persistent engagement but he noted the aspect of active defense to intrude into the network spaces of other states. He also mentioned in his article that in cyber space the states need to hold some offensive recognizance capabilities to dive into the in-depth of matter (Kello,2017).

Moreover, deeper analysis reveals that Clausawitzian theory that reinstate the notion that the purpose of defensive posture and active intrusion should be to bring a constructive change in the strategy of adversary and comply it according to one's own principles. Moreover, the conscious offensive capabilities could bring the attacker with strategic advantage (Ecke, 2018). Moreover, in structural realism the idea of persistent engagement could be traced as it focuses on the structural constraints the system imposes for its malleability. This part explained that how the conceptual grounds that provided foundation to the framing of

persistent engagement module in cyber space was paved by its roots to be found in other theoretical frameworks (Kello,2017).

The following is the illustration of cyber persistent engagement theory and its intellectual roots in other theoretical paradigms and models

3.4 ROOTS OF CYBER PERSSITENT ENGAGEMNET STABILITY THEORY



Source: Drawn by Researchers, Data Source (Kello,2017).

3.1.2 ASSUMPTIONS OF CYBER PERSISTENCE THEORY

Cyber persistent theory which centers its contention on the differential environment that exists in cyber space. Cyber persistent theory also places emphasis on the personality and behavior of state. Neo classical realism and classical realism offshoots could be traced in cyber persistence theory. Cyber persistence theory frames a course of action for states in cyber space if they want to achieve structural stability. Following are the assumptions that cyber persistence theory draw

1. The state behavior in cyber space should be continuous and proactive not discontinuous when it comes to breaching of other states networks and spaces.
2. States project their power in cyber space primarily to exploit the environment to gain power but not to introduce coercion.
3. Once a deterrence is achieved that the security of cyber spaces is maintained by means of strategy named as fait accomplice which if not properly executed could result in escalation into full blown cyber conflict.
4. Rather than launching the espionages and attacks on the critical infrastructure of other states the focus should be on persistent engagement or that of fait accomplice which could serve the purpose of deterring the adversary.
5. The constant dynamic of cyber spaces is the continuous competition that exist in cyber world.
6. The cyber engagement is predominantly indirect but scarce ratio of direct engagement is also there.
7. In cyber space the possibility of cross domain escalation is often rare and so is the war or possibility of armed conflicts.

The purpose of persistent engagement is to frame the environment in one's own favor and for drawing the balance of power in cyber domain. For this they are willingly capacitating themselves in a bid to build robust systems for persistent engagement. The environment as the persistent theory assumes in cyber space is of neither that of peace nor war. The unlimited spatial and time factor is there when it comes to persistent engagement. For example, French organizations threats spanning over years from Russian targeting agencies, from year 2009 till 2013 US authorities reported relentless targets from the East Asian states primarily China. The persistent engagement faced threats from advanced persistent threats that intrude in full spectrum with a specific mission to accomplish and is organized (Fischerkeller, Harknett & Goldman, 2022). The conception of CPT starts by establishing a structural perceptive of cyber space to be malleable, interconnected. The constant contact at which state are put into make their power share in domain to be vulnerable for them to constantly engage. This makes the strategy of cyber fait accomplice that depends on the unilateral targeting of the adversary

examples of which are the Russia and United states competition for gaining control over the resources. On the same pattern North Korea tried to capture control (Fischerkeller & Harknett, 2020).

3.1.3 POLICY INSIGHTS FOR COHERENT CYBER STRATEGY IN CYBER PERSISTENCE THEORY

Cyber persistent theory has highlighted there exists de facto norms in cyber space which need to be fixed. For this there are multiple means to prepare the normative ground of engagement by means of tactical bargaining that is establishing the rules of engagement by means of engaging in a strategic competition. Secondly this problem of defector rules could be fixed by states declaring their national interest and establish a threshold for engagement which will establish the fact that attack against that particular infrastructure will result in escalation of the conflict. Then by means of customary international law this problem could be fixed. Moreover, more sustainable pattern of engaging in cyber space is when state by means of active engagement protect its critical infrastructure. Moreover the security of one own system rests on the capabilities to exploit the structure of other state. The coherent strategy is the one that look for the excessive systematic vulnerabilities of the adversary and use it for gaining cumulative gains. It places emphasis on the operates for careful execution of policy or else the strategist will bear the burn of it. Cyber strategies should be continuous and rule based. It is not prospective action that brings stability or security but the cumulative action. The states often pursue attacks that remain below of the threshold established by states. For this a coherent strategy is the one that is synchronized. Active defense is possible only with some legal amendments in the system for example USCYBERCOM did. States in order to protect or deter the attack on their facilities should frame strategies with campaign mindset. The campaign should be focused on exploitation the cost benefit framework of other states (Fischerkeller, Harknett & Goldman, 2022).

3.5 HURDLES IN EXECUTION OF PERSISTENT ENGAGAMNET STRATEGY

HURDLES IN COHERENT POLICY	POLICY INSIGHT

Normative problems (de-facto rules)	**1.** States should establish customary international law by means of consistent practices. **2.** by means of tactical bargaining **3.** declaration of deterrence thresholds
Protection of critical infrastructure	1. pursuing policy of active engagement 2. policy of fait accomplice 3. policy of commutative action for bringing stability

Source: drawn by researchers, Data source**:** (Kello,2017).

3.1.4 PROPONENTS OF CYBER PERSISTENCE THEORY

The proponents of cyber persistence theory are Richard Harknett, Michael Fischerkeller and Emily O. Goldman who gave this theory in the book Cyber Persistence theory: Redefining National security in cyber space. In the institute of defense analyses Michael served as staff member for information and technology division. He provided intellectual support to Defense Secretary in US for about 20 years and also at joint chief of staffs and at multi-national force commanders. He wrote articles like “Deterrence is not a credible strategy for cyber space”. He holds this perspective that cyber operations should be waged with the intention of compelling an adversary to back off rather than escalating the situation. Moreover, he picked on the credibility of 2019 Atlantic papers which establish this notion that under nuclear deterrence states could use cyber tactics to fulfill their interest which is a naïve perspective (Fischerkeller, 2022). His profile at semantic scholar claim to place his works to be cited in 9 of highly influential works. Richard Harknett in 2017 was serving as US full bright scholar. He was the first one to serve at Cyber command. He wrote about 50 research articles on the fundamentals of cyberspace with the theme of cyber security, information warfare and cyber strategy. He also served at University of Cincinnati and Vienna diplomatic academy Austria. He is a neo-realist who primarily explored the problem of deterrence in cyber domain. Emily

Goldman holds expertise in subject matter of cyber persistence who served at NSA (Harknett &Smeets, 2020).

3.1.5 DEFINING PERSISTENT ENGAGEMENT AS PER CYBER PERSISTENT ENGAGEMENT THEORY

The persistent engagement in the cyber persistent engagement stability theory is defined as the constant engagement with the adversity that should be short of armed attack in order to control the adversary behavior not only strategically but also operationally and tactically. this theory also emphasized the fact that sometimes there are multiple parallel cyber engagements existing that stairs need to manage and communicate and it also involves aligning the adversary behavior with at the scores of acceptable attitudes and it is a strategy currently being scarce in the international digital order. A state also needs to keep its domestic laws and capabilities in align with the persistent engagement (Harknett &Smeets, 2020). For director cyber engagement both offensive and non-offensive capabilities could be put in place. for effective cyber persistent strategy to be executed the first criteria is the battle should be agreed on a number of standards and an agreement should be reached so as not to cross the threshold of cyberwar and turning the friction off strategy competition into a full-blown conflict. also, the competition should be agreed by setting the reward opportunities and communicating the intentions of the attacker with the diversity that it wants the other party to change its behavior but not to consider it as a threat to its infrastructure. the strategies of tactic coordination tactic bargaining and tactical aberration should be used.

3.2 CONTEXTUALIZING CYBER DETERRENCE IN CYBER PERSISITENCE THEORY

The debate of deterrence strategy is the debate with nuances of both policy and academia. Within the context of cyber persistence theory, deterrence as a policy in cyber space has been used as a commonplace for understanding, by being encompassed to be visualized as a component of national security (Freedman, 2008). The theory persists that dire need to view ‘strategy’ divorced from the presumption of being chained with the realm of coercion, militarized crisis and war in cyberspace (Harknett &Smeets, 2020). This is primarily reflected in the large part of state behavior, which dives not towards war and coercion in

cyberspace but falls short of an armed conflict. The apt strategic approach which can bring 'short of war' outcomes in, through and from cyber space, is thus the approach of deterrence.

Traditionally, the success rate of any deterrence tactic depends upon the conviction of the opponent on the assessment that an attack will not be a cost-effective option, given that the consequences will outweigh the potential gains as a result of persistent competition. This success depends upon multiple elements:

- the structure of the strategic environment i.e., whether conventional physical domain or cyber space
- effective communication between the adversary and deterring state
- credibility in the capability of using threat of retaliation
- credibility in the resolve to follow through on the threat (Harknett & Smeets, 2020)

3.3 DETERRENCE STABILITY IN CYBER PERSISTENCE THEORY: STABILITY INSTABILITY PARADOX

In cyber environment unlike that of the situation in case of nuclear deterrence. The stability instability rationale could be translated to the condition of cyber deterrence where states in order not to breach the upper tactical bound engage in persistent activity of competitive nature. The primary nature of this instability at lower level by persistent campaigns should be focused on the exploitation of vulnerabilities and malleable cyber nature not on escalating the small skirmishes into war which according to cyber persistence theory is limited. The interconnectedness of the strategic spaces and because of the lack of any strategic depth the states are bound not to resort into war for which the persistent engagement and policy of fait accomplice is the only option. The tendency of instability in cyber space is limited to the phenomena when the other state takes that competition as incentive to further engage in polishing its own infrastructure. The multiple destabilizing elements that could uplift the competition to level of war is when cycle of tit for tat fait accomplice starts. This will result in adventurous escalation and possibly of spiral competition. When states don't have an idea about their acceptable behaviors which should not trigger the threshold of other states. It creates a situation of disability and thereby escalating into full blown conflict. For not letting

the things at short end to take over the upper barriers established for armed conflict, the communication of deterrence capacities is important. Uncertainty and tactical misunderstanding could result in the conflict. Direct cyber-attacks responsible for altering balance of power and incapacitating the adversary infrastructure could likely disrupt the deterrence structure and attacks should remain limited enough so as not to trigger the threshold and this could be done by means of pervasive surveillance. In the pretext of prohibition of direct harmful tracks small skirmishes such as espionages, surveillance. Even those states who have the ability to carry sophisticated attacks avoid doing it because they must have the ability to deter the retaliation that comes with it. Moreover, states can turn their systems to be more robust by opting for deceptive means. Sophisticated computer network exploitation suggested by cyber persistence is also an option (Lindsay & Gartzke, 2016). There are number of elements an factors that could trigger deterrence stability and as clear the cyber conflict mentioned in the president engagement stability theory that involves that sometimes it becomes difficult for states to assess the imperatives of cyber strategic environment resulting in the catastrophic loss of their cyber warfare capabilities resulting in an asymmetry which is dangerous for them to carry on with the deterrence strategy. And sometimes the cyber powers are not capable enough to carry on an effective response. More ever the strategy of external facing that could give the adversary infrastructures in constant contact with risk would eventually result in adversary behavior by default setting the security environment of the cyber real and sometimes an imbalance of initiative is being created by students deliberately when they failed to set the conditions in their favor There are multiple factors that could result and the instability of the deterrence being established between parties that involves the poor assessment of strategic environment in cyber real by the attacker.

3.4 DETERRENCE TYPES AND CYBER PERSISTENCE THEORY

Even though the theory doesn't address the types of deterrence postures that a party could adopt in order to counter attacks. The deterrence by entanglement could be perceived in the strategy of tactic bargaining where a mutually agreed behavior is being adopted resulting in the shift from unilateral and independent decisions of the stairs in the cyber realm. It asks to

manage the complex cyber relations in between two states by signaling the intention of affinity and persistent engagement with the other party and sometimes and all at once tactic bargaining agreement could not be possible. It is a theory that also suggests a pathway of deterrence by norms development. The progress towards Opinio Juris. With the help of Tallinn Manual and the principle of countermeasures are the scores of acceptable and non-acceptable cyber behaviors or could be shaved that could deterred the adventurist policies by the rogue states. The international law on cyber spaces said the principle of sovereignty and nod interventionism as important and vital for the stability of the international digital order and there exist multiple interpretations by Japanese French New Zealand and UK authorities. The Tallinn Manual permits the use of retaliation in cyber defense and thereby allowing the establishment of cyber threshold. The extended cyber deterrence strategy has been promoted under this study which suggested that all stairs must not only respect and protect the norms at the international level but should advance and progress towards establishing a mutual understanding of acceptable and non-acceptable behaviors. For example, strategic rewards have been set up in the G7 agreements in order to do reward the acceptable behavior compliance by the powers and it is also being recognized that sometimes the informal alliances in between states are more effective than the institutional avenues being used to deter the aggressive activities in the cyber realm.

3.5 PROBLEMS WITH CYBER DETERRENCE

This ability to threaten and then carry out the threat in order to deter the execution of any offensive action by the adversary, is something essential to the very existence of deterrence. But it can be problematic as well provided that it is necessarily required in maintaining a balance. This balance lies in competition which falls short of a cyberwar, while deterrence actions in their full pursuit i.e., by denial and punishment, fail to achieve this aim. It is therefore necessary to identify various problems that exist within the phenomenon of cyber deterrence, problems that exists in the face of **offensive** use of cyber deterrence strategy which causes **cyber exploitation**.

According Thomas C. Schelling, a deterrence concept requires the presence of both **conflict** and **common interests**, between the two or more parties involved (Schelling, 1960). While

the presence of conflict is an obvious fact but that of common interest suggests the notion of deterrence as to be executed with the unraveling of a situation both sides wish to avoid in the long run. It is a strategy of halt and pause, even if it doesn't necessarily resolve the issue or crisis at hand. Thus, the element of common interest adds stability to the deterrence regime, otherwise which deterrence becomes unstable and prone to failure in due time. This applies deterrence in cyber space as well, which is generally considered a more volatile and more ambiguous phenomenon given the absence of sound, physical boundaries and unlimited access to cyber space within a limited budget. This ultimately brings the readers towards the various problems that lie alongside the execution of deterrence in the fifth domain.

According to Martin Libicki, the goal for cyber deterrence is to 'reduce the risks of cyber-attacks to an acceptable level at an unacceptable cost' (Libicki, 2009). This leads to an environment where the defending state uses the threat of offensive and potent retaliation in order to mitigate potential offensive action by another state. This strategy works as a defensive strategy with cyber deterrence measures taken as cyber defensive measures alongside the possibilities that these measures cannot be executed in a vacuum. But over time, the clause of cyber deterrence strikes as pre-emptive measures has seeped through, which essentially make the defensive strategy of deterrence as an offensive action.

Cyber persistent theory regards deterrence as a twofold phenomenon: **a prospective threat** and **an action** i.e., committed threat contingency to engage in response actions the costs of which will outweigh the benefits, followed by imposing those costs by executing the action. Latter step takes the theory of deterrence into practicality, by moving it into a condition beyond deterrence which involves fighting, blunting, contesting and countering via operations (Fischerkeller, 2022). The second step moves the deterrence into being an offensive defense, a problem carrying the tendency to plague the cyber deterrence discourse in the future. For example, U.S. in its 2011 Strategy for operating in cyberspace (DoD), justified the use of cyber deterrence measures as the pre-emptive measures to prevent any intrusions. This clause alongside the Presidential Policy Directive-20' suggests the isolated use of cyber deterrence actions as a way to curb and imminent threat i.e., a threat perception based on probability. This clause coupled with the 'presidential policy directive-20' has led

the state to engage in cyber deterrence as an offensive tool, without acquiring the president's approval.

In cyberspace, states are usually presented with a fluid opportunity laden environment to experiment, test, plan and achieve the gains without seizing territory or destroying any sources of power, thus having the options to choose to advance interests through alternative mechanisms to war. But, in terms of cyber persistence and cyber deterrence, it has been argued by the scholars that states face a structural imperative in initiating persistence and seizing and maintaining the initiative of security in and through cyberspace, that is to exploit adversary's vulnerabilities while simultaneously trying to reduce the potential of their own exploitation. Nearly all other international politics theories regard the assumption of 'internal balancing' that states engage in some degree of internal facing security activity but the novelty of Cyber Persistence Theory lies in its argument of a state's external facing measures that leverage cyber capabilities for unilateral exploitation, therefore making external balancing and **exploitation** the dominant state behavior in cyberspace.

According to Herb Lin, **cyber exploitation** is defined as a cyber offensive action conducted for the purpose of obtaining information', which involve actions such as military intelligence activities, maneuvering and information collection, for a state to carry exploitative behaviors in and through cyberspace. This leads to an environment of strategic competition with one state gaining advantage by making use of another state's cyberspace vulnerabilities, by targeting the physical, logical and cyber persona such as direct hacking, social engineering and water-holing.

3.6 ALTERNATIVES TO CYBER DETERRENCE

As discussed above, the success rate of deterrence as being a prospective threat, depends upon the committed contingency to engage in an action the outcomes of which will outweigh the benefits. But the problem with deterrence as viewed by the persistence theory is the one related to these costs, given that imposition of costs directly moves deterrence from being a prospective threat towards being an intended action. It moves the states into a situation beyond deterrence. Within cyber space, this can lead to a situation of offense and exploitation

which may not fall short of a cyber war. Cyber persistence theory hence, instead of creating new concepts of exploitative inter-state cyber behavior in cyberspace, manifests and leverages on the already developed tactics such as that of '**fait accompli**' to be utilized in cyber space.

According to Dan Altman, 'fait accompli is the limited and unilateral gain at an adversary's expense in an attempt to get away with that gain when the adversary chooses to relent instead of retaliation.' Alexander George defines fait accompli as 'the alteration of status quo in one's favor via a quick and decisive transformation of the conflictual situation in order avoid any unwanted retaliatory escalation.' Russian invasion of Crimean Peninsula in 2014 is one illustrative example of such a situation with coercive bargaining as the representation of failure of deterrence, and as a representation of fait accompli in terrestrial domain.

Regarded as the concept of 'agreed battle', fait accompli in its academic heyday is largely an empirically derived term with very less theoretical attention. In cyberspace discourse though, fait accompli has been elevated to describe the state behavior which theories like 'coercion' have failed to describe. When researching on terrestrial disputes, Dan Altman noted two kinds of crises i.e., crises as competitions in risk taking and crises as tactical cleverness with attempts to outmaneuver the enemy. Altman placed central emphasis on the concepts of coercion, signaling resolve, brinkmanship and escalation, as tactics displaying most state behaviors in crises as competition. Such concepts however, fail to explain the state behaviors in cyber space and cyber competition, particularly the behavior which falls short of militarized and armed conflicts. And thus, this where **cyber fait accompli** comes into discussion.

Within cyber space framework, Michael Fischerkeller on writing about **fait accompli and cyber persistence engagement**, defines it as the 'unilateral' gain where the gain is retained when the target is unaware and unwilling to respond. In such scenarios, the immediate unilateral gain in and through cyber space is usually the setting of favorable security conditions via technical, tactical, operational and strategical reconfiguration of cyber space (Fischerkeller, 2020).

The key term when describing the fait accompli tactic is that of 'unilateral' which means that it is a one-sided activity in which the defender is not a participant, which makes fait accompli an action rooted in exploitation, thus distinguishing it from coercion. The imperative here lies in the fact that making gains at the expense of an adversary is not the same as threatening to impose costs as in deterrence or coercion. The benefit of gain is instead utilized to serve as the foothold for strategic bargaining. Fait accompli thus is about seeking gains through exploitation. It is a concept which is rooted in seizing an opportunity of unilateral gains, both in terrestrial and cyber spaces. China's cyber-enabled illicit acquisition of key personnel data from US office of personal management is such an example. United States military Cyber Command's (USCYBERCOM) efforts to secure the 2018 US midterm election is also an example of fait accompli in cyber space.

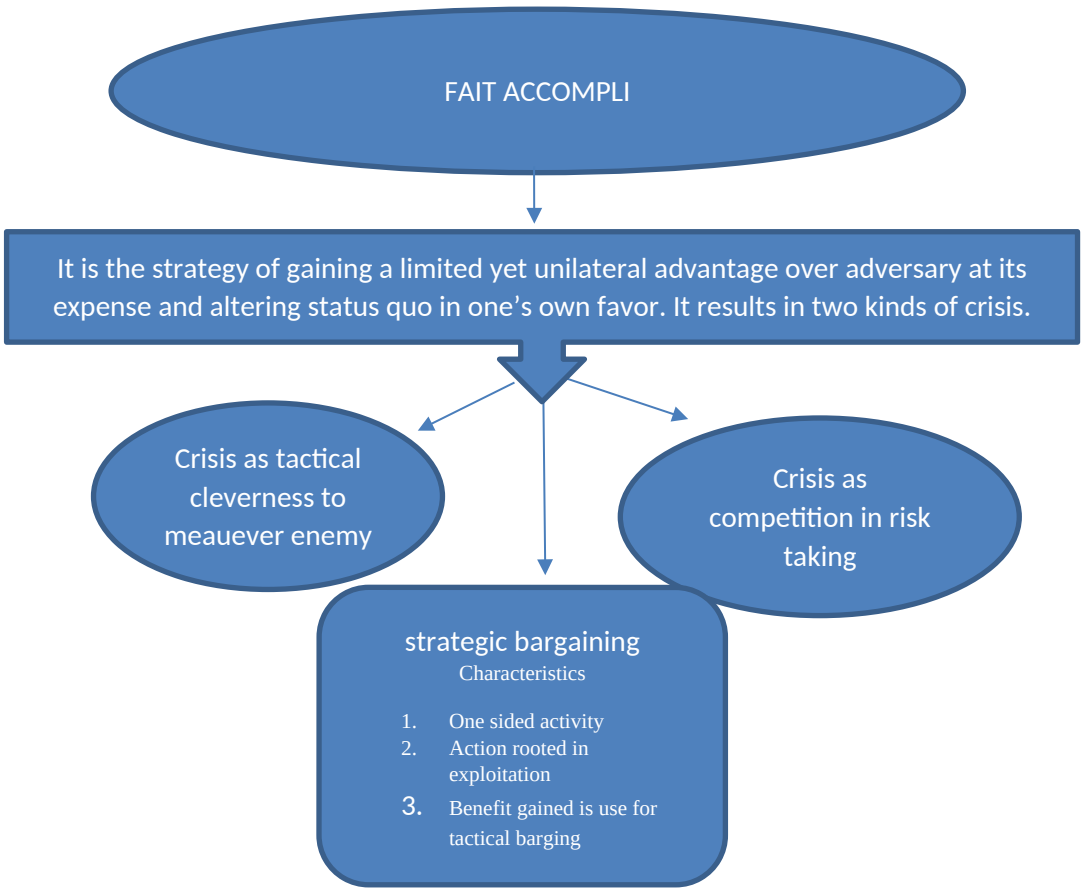
Cyber persistence theory explores this alternative better option of 'fait accompli', with its concept of **strategic bargaining**, which presents itself as a useful concept for describing and explaining state's primary and operational tactical behavior i.e., how the states persist in seizing and maintaining the initiatives to set conditions for security in addition to strategically bargain to change the status quo in international system.

Furthermore, the logic behind the strategic bargaining of fait accompli also lies along the hinges of **finding vulnerabilities** in red lines, which acts as the line of distinction between 'compliance' and 'violence' in a coercive action. In conventional crises, red lines are anchored on a disputed border, such as between India and Pakistan for which Kashmir border is the Red Line. Such an approach of fait accompli i.e., an agreed battle which falls short of an armed conflict, when states seek to compete and gain without actually provoking a direct war. Similarly in cyber space as well, the strategic logic behind the fait accompli hinges on finding vulnerabilities, which unlike the conventional domain lies not in coercive demand but within the very fabric of cyber space itself i.e., within the technological system which is vulnerable yet resilient offering an abundance of opportunities to exploit, all of which falls short of a cyber war. Moreover, like in conventional framework, fait accompli in cyberspace is also utilized as a way to strategically bargain in order to change the status quo. Unlike in conventional domain however, cyber fait accompli campaigns are unilateral and independent

actions and thus do not require strategic bargaining but unilateral pursuance of strategic competition. For instance, the unilateral aggressive campaign of cyber-enabled theft of crypto currency and financial institutions, pursued by North Korea from 2016 to 1019, to expand its nuclear weapons program and develop intercontinental ballistic missiles, is one evident example of cyber fait accompli.

The pursuit of fait accompli in cyber space thus, is more accurately a unilateral and an independent strategic choice in cyberspace rather than a mechanism for strategic bargaining. This is the stance which cyber persistence theory arguably persists on i.e., unlike in deterrence theory, cyber persistence theory recognizes that while strategic bargaining is competition but not all strategic competition is bargaining (Harknett, R). Fait accompli thus, is an alternative strategic approach than deterrence, open for all attackers and defenders to pursue bargaining and competition. It is also a more appropriate approach than coercion as it describes the behaviors of states in cyber space as unilateral actions in the pursuit of gains while in the avoidance armed conflict simultaneously.

3.6 FAIT ACCOMPLI



Source: Drawn by researchers, Data Source: (Fischerkeller, 2020).

3.7 CYBER PERSISTENT ENGAGMNET STABILITY THEORY AND CYBER DETERRENCE IN PARADOX: A CRITICAL APPRAISAL

Persistent engagement which is meant to maintain stability and that of cyber deterrence to be the security of cyber spaces are mutually exclusive. The continuous presence will make the over stability of the system to be in dilemma and of volatile nature. Moreover, the intrusion in other systems even that of allies is too idealistic to be seem acceptable. The persistent engagement aims for maintaining reducing friction by means of active defense but this could result in friction with the allies. Moreover, the primarily concentrating their narrative on the red and blue cyber spaces this theory ignores the vulnerability of gray spaces or private sector presence being prone to this constant maneuvering and thereby subjecting the whole system influx. And although how volatile of the situation could be in terms of cyber deterrence the states still need a threshold at upper tactical level for persistent engagement to carry o without any hostility. A close assessment of this phenomena reveals that it falls short of feedback loop being established. The impact of persistent engagement went down in loop because rather than constraining the activities of adversaries and deterring them it accidently invites for action even in conditions where it could inform of the possibility of action. It thus, produces a negative feedback loop which cyber persistence theory don't address. One risk factor that cyber persistence theory don't address is that lack of any communicative means in this strategy were signaling of intentions come only from the language of action or strategic activities in cyber domain.

Moreover, the cyber persistent theory ignores the fact that this strategy which demands intrusion into other spaces but also ask for the allies' trust is the most assertive of the strategies in nature that makes the execution process even more difficult. This strategy also demands full spectrum influence and triggering an impact on overall structure. The adversary indicatives to increase the robustness of the system could result in immense cost pressure (Whyte,2020).

3.7.1 RISKS ASSOCIATED WITH PERSISTENT ENGAGEMENT AND PERSISTENT ENGAGEMENT STABILITY THEORY

Cyber persistence theory present a strong case of staying in constant contact with the adversity to be a vital and important strategy in order to deter cyber conflict but the point is worth noting that it is not the only strategy for cyber deterrence to be effective but there are multiple risks associated with this strategy that are being ignored for example persistent engagement which is considered to be a vital board of US cyber deterrence strategy is not considered to be a risky one by the US cyber command. there are only two discs that are considered by the United States policymakers that this strategy would eventually lead militarization of the cyberspaces but other risks are being ignored. This strategy ignores the risk of collateral damage escalation and the constant instability in the international digital order and could invite negative feedback from the adversary thereby exasperating the conflict. This point was being raised by Max Smeets and Robert Jervis. There exist multiple feedback loops in cyber persistence strategy being recommended by the cyber persistent engagement stability theory that sports the stability element of this strategy under threat. the risks associated with this strategy includes the likelihood of friction possibility of tactic bargaining and reciprocity element. this could likely disrupt the reputation of the country as it stands in violation with the norms that exist in the international digital order. This strategy of persistent engagement demands the constant effort to impose a cost on adversity and to weaken its infrastructure which would result in friction if the adversary on the other side holds the capability to name with stand that persistent engagement. The adversary could come back with a newly devised aggressive forward defense strategy resulting in the degradation of own capabilities. Also, the element of tactic bargaining that persistent engagement stability theory suggests is extremely risky that sometimes the interactive process of constant engagement results in unacceptable attitudes and escalation of the conflict resulting in a tit for tat behavior. Also, this strategy demands a vivid signaling which is extremely difficult to carry on in cyber real and would be extremely expensive and difficult to carry on. sometimes this strategy needs tactics like hacking back that stands in contradiction to the commitment towards norms by the state for example as happened in the case of United States when they tried to hack the personal management office of China. Also, a point worth

noting here is that in cyber rearm there are no strategic depth sandy militarized zone to separate the third parties becoming prone to collateral damage. It could possibly invite negative attitude And sometimes the tactics put in place for surveillance could result And it could work only affectively if the adversary perceives at as a deterrence declaration And the noncompliance of norms is indicative of the fact that the cyber status quo would eventually by default fell into the trap of values and norms established by adversaries And it would only do their the cyber-attacks espionage is but not the other strategy is the hostile information exchange across the borders and existential threats to cyber regimes. This could provide an excuse to the adversaries that they are not following first strike but striking back policy as that happened in case of lack of restraint exhibited on part of United States towards Iran and Russia thereby resulting in Russia calling the 2016 attack a retaliation of US defaming strategy. This could introduce cognitive biases in the adversary decision making module as could provide the military adventurists with an excuse of war and conflict. Also, this strategy depends on the sensitive element of persistently engaging to a level where it could only mold the adversaries' behavior but not escalate friction into conflict which is pragmatically not possible. It is also a strategy that demands a shift in the mindset of not only decision makers within the state but also that of the adversary so that the war could be properly ended unacceptable behavior could be framed (Healy, 2019).

3.7.2 PUBLIC-PRIVATE DILEMMA AND CYBER PERSISTENT ENGAGEMENT STABILITY THEORY

This cyber persistent engagement stability theory does not address the element of private sector that is essential for effective execution of forward defense and tactics to install and anticipatory resilience. Also, it demands compliance of the private sector with the governmental incentives in order to secure their cyberspaces and sometimes the governments could learn from the persistent engagement of the private sector as that happened in the case of hard to forward strategy being adopted by US cyber command in 2018 congressional elections. this theory does not address the public private sector collaboration in order to wage persistent engagement with the adversity and to introduce a change in adversaries' behavior. For example, the take down of botnets such as 2013 citadel botnet, 2014 zero-access botnet

demands constant collaboration with the private sector. Moreover, the private sector should act in synergy with public sector for carrying out attribution and it could provide its technical expertise which is essential for effective execution of strategy. Moreover, the private companies supported the open Internet policies and it could hold the digital authoritarianism which is essential for the effective execution of persistent engagement (Monarez, 2021).

3.7.3 TECHNICAL SHORTCOMINGS OF CYBER PERSISTENT THEORY

The persistent engagement stability theory lacks technical intricacies involved in selective and persistent engagement with the adversary. these includes the difficulty in signaling and communicating the intentions of persistent engagement with the adversity in aerial where there exist a diversity of activities and actors and also the conscious effort to avoid the breach of sovereignty and digital spaces of foreign governments so as not to attract any negative feedback from third parties. Also, it ignores the fact that sometimes tools that could look for alternative routes to target the infrastructure and could avoid detection because of their sophistication making the space contraction essential for direct confrontation with adversary. Also, it is extremely difficult at the operational level to assess the motivations of the adversity and to shape its behavior because of the ambiguity that lies in the cyberspaces. Also, persistent engagement demands all of the governmental sectors to get involved in order to tame the adversaries' behavior which could provide at diversity with all-in-one opportunity to overcome the strategy. Also, this theory that does not address the possibility of adversary learning the strategies of attacker and persistent engager. sometimes the adversaries take this persistent engagement as an opportunity to carry out their reconnaissance and surveillance operations into the attacker's system and to frame their strategies and capabilities development accordingly. this could possibly invite again scared of cyber conflicts because of the misperceptions that could result from persistent engagement as the adversary could take it as an instant of cyber war being compelled and imposed on it. Also, the effective implementation of persistent engagement strategy demands signaling of the intention that if the adversary would comply with the behavior required by the attacker it could result in mitigation of the conflict. Also, the structural contradiction that cyber engagement persistently entails is so vivid that it carries a lot of technical intricacies. For instance, that

digital order at international level is interdependent open and intricately linked that makes any spotty persistently engaging with military cyber weapons considered to be responsible and could invite backlash. These goals of the strategy of persistent engagement could be considered mutually exclusive with the international level of interdependence that exist in between states and it does not consider the individual perspective and the privacy problems that comes with it (Whyte, 2020). Another technical difficulty that comes with the cyber persistent engagement is the paradox of escalation and stability in the digital order as it becomes extremely difficult to differentiate escalation and forward defense mechanism being used by states frame their strategies in order to frame their strategies. Also it becomes extremely difficult to agree on the terms of competition with the adversary. Sometimes the asymmetries in between adversaries create an imbalance leading to the intensification of competition and relative power shift in between them which would eventually create a security dilemma for the declining state and a war could be triggered. Sometimes miscommunication happens that the persistent engagement tactics being used by one party are considered to be escalatory by the other one and interpreted in wrong way resulting in accidental war and this happens when there is an incomplete information and signaling coupled with the lack of shared references (Harknett & Fischerkeller, 2019).

3.7.4 CYBER PERSISTENT ENGAGEMENT STABILITY THEORY AND PRACTICE: IN PARADOX

Does cyber persistent engagement stability theory often ignores the operational tactics that are in need in order to carry these forward defense strategies affectively. First of all, it demands a direct interference in the adversaries kill chains and do covertly manipulate their systems so as not to let them advance and develop their capabilities. these tactics involves the strategy is of erosion manipulation subversion overthrow. Sometimes the state others need to collaborate with the proxy actors in order to carry out covert operations which are essential for persistent engagement with the adversaries' cyber kill chains.

This theory does not address the element of providing military and Technical Support to these proxy actors and the consequential impact that it could pose on the stairs' infrastructure. Also the erosion tactics such as Stuxnet, NotPetya Attacks are difficult to comprehend as there are

multiple issues associated with these strategies. For example, the number one challenge that persistent engagement strategy carries which is being included ignored in the theory is sometimes the tactics used to attain a strategic value are not being fulfilled even in case of operational success for example the ransom attack on Iranian nuclear facilities by United States was not successful in hindering the Iran's progress towards access to nuclear capabilities even though it did achieve its operational value. Also, the tactics and weapons used by cyber operations are sometimes of temporary detrimental nature as they do not leave a permanent scar on the adversaries' infrastructure which is considered to be essential for shipping and compelling the adversity to device its behavior as per the intentions of the attacker (Maschmeyar, 2022).

3.7.5 FEASIBILITY FOR SMALLER STATES: A US CENTRIC PERSPECTIVE OF THEORY

For the persistent engagement the cyber capabilities are needed assuredly effective enough in order to reverse the balance of cost benefit for the rogue adversary in order to counter its malicious other activities that demands huge expenditures and loss of revenues for example CISA suffered the damage of about 1.9 million dollar Also for an effective cyber persistent engagement it is important to eliminate the elements anonymity and obfuscation of for effective signaling and resolve of the intentions which is far from the cyber capabilities that smaller states carry. A strong deterrence with cyber persistent engagement requires meaningful cost exceeding activation of the all sectors of government. Moreover, for persistent cyber engagement the transparency of the offensive operations must be insured which is essential for norm establishment and to agree the terms of competition which becomes impossible for the smaller states to manage (Bates, 2022). Moreover, the persistent engagement stability theories are written from the perspective of United States security intentions and strategic environment that exist in the territorial boundaries of interest rates of America.

3.8 KEY FINDINGS

The mutual exclusiveness of cyber persistent engagement stability theory is often reflected in matter getting escalated. Sometimes the friction resulted from persistently engaging with

adversary often doesn’t give the desired results of fixing the conflict as it is nevertheless aimed for. The number of reasons for the persistent engagement strategy which was aimed to be the tactic serving the purpose of constraining the adversary from taking punitive action falls short of its purpose and fails because of feedback loop created because of strategic incapability with cyber spaces structure. Also, this theory fails to put the public private diellama to fixture.

in the next chapter the cyber deterrence strategies of all of the states have been talked about in order to determine that the extent to which cyber persistent engagement stability theory highlights the gaps of cyber deterrence strategy have been exaggerated or states actually have to face these challenges.

CHAPTER 4

USA CYBER DETERRENCE STRATEGY

For decades, USA has enjoyed strategic prominence in fifth domain also known as digital pax Americana which is said to be in decline. It is because of this that USA is facing both sophisticated challenges to its critical systems. It has always tried to craft its deterrence strategy in cyber spaces not only to combat contemporary challenges but also future one's. This chapter delves into the details of how the concept of cyber deterrence evolved in the strategic thought of US cyber realm. Under different administrations, this chapter explores the development of cyber deterrence strategy. It then delves into the detail of other deterrence strategies and gives a tactical perspective.

4.0 USA ROLE IN INTERNATIONAL DIGITAL ORDER: THE DECLINE OF DIGITAL PAX AMERICAN

For long the USA dominated the domain of constructing the international order based on its dominant role in the UN IMF European Union and a number of other regional organizations but the Information technology diffusion cracked it all down. Behavior of number of actors in the international arena including India China and Russia that are framing their own rules by restricting the flow of data in their borders having their own perspective on the organization of the digital world order. This constrain the companies access to their systems with a pressure being received by the independent news websites and online activities on USA to take these powers on board as they are big markets. The new trends in the digital world order including the militarization of the cyber domain with the strategic advantage being given to the offensive capabilities and blurring of boundaries in between war and peace are no longer being managed by United States. Pre-emptive strikes are being given a strategic advantage with US also introducing it into its strategy. New technologies such as quantum communication technologies that could fix the attribution and defense problems in the cyber domain are being used by the agencies like National Security Agency in order to counter misinformation and to serve this purpose in 2015 a new directorate for digital innovation was being set up in CIA. US has this strategic advantage of being the home of Internet with all of

the data being processed by its intelligence agencies through the automated surveillance systems and by online analysis of data sustained in systems of applications like Facebook Google Microsoft Twitter. A number of information and communication technological hubs like Silicon Valley being located in the United States. But also, the US systems are equally porous/ vulnerable as reported by defense size board and the critical infrastructure is heavily dependent army on the computer and digital command or control system makes it military highly one rebel to cyber-attacks. Some other adversaries of use now using this domain too serve their national good and in order to exert force with the US power being in steady decline with the companies like Microsoft ones being termed as interdependent are now being used by the governments and big markets like China India and European Union to collect data (Segal, 2016).

4.1 US STRATEGIC SCHOLARSHIP: DEFINING CYBER DETERRENCE

The evolution of US strategic thought on cyber deterrence has carried the character of cyber activities at that time and cyber threats being faced by vulnerable critical infrastructures. Since 2003 major developments in cyber deterrence strategy took place where not only definition of deterrence renewed, governmental bodies created and strengthened, multi-sector cooperation and partnerships secured but also cooperation with allies increased. there have been three waves of cyber deterrence. The **first wave** of conceptual evolution in US circles this involves when Der Derain first published an article titled as “cyber deterrence” in Wired Magazine. Wheatley and Hayes were the most prominent scholars of that time who noticed that where nuclear deterrence inspired their understanding of cyber deterrence. The cyber deterrence strategy at those times carries these elements of clear deterrence declaration, with the will of deterring the adversary and also communicating this policy with rival. Timothy Thomas introduce the need of deterrence by means of cooperation with allies as viable option. He not only defined a potential adversary that should demand a deterrence policy and also noticed that unlike nuclear domain the adversaries at that time were primarily of decentralized nature. During the times of gang war in between Masters of Deception and that of legion of doom, cyber deterrence was perceived to be with criminology prism. Punishing

the cyber offenders who would have invited kinetic consequences because of their malicious cyber activities like FBI arrest of Kevin Matnick in 1995 was considered to be a viable deterrence strategy. US department of defense in times of information warfare equated cyber deterrence with the lens of increasing cyber defense resilience so that adversaries could be deterred. The US department of Defense when realized that defending critical infrastructures is not sufficient to deter adversary, they introduced the strategy of attacking rivals' OODA loop as important part of cyber deterrence strategy. The article published by John Arquilla and David Ronfeldt in RAND titled as "Cyber war is coming" changed the definition of adversary from state centric larger systems to that of non-state centric smaller systems also changing definition of cyber deterrence strategy. It was defined as a strategy of introducing depth oriented defensive schemes by utilizing the leak proof defense ability with the objective of deterring adversaries and also by launching an offensive yet disruptive incursive counter attacks. In the mid-1990s phycological & information warfare rather than cyber connotations were being attached with cyber deterrence strategy that happened after operation desert storm. In the desert Hammer VI war games exercises the term cyber deterrence was coined defined as "With the aim of asserting US military dominance in hyper digitalized context by media, technological and strategic exhibition and simulation of capabilities. The ***second wave of deterrence*** conceptualization started in the late 1990s RAND scholars played a significant role in high-lightening the gray areas in cyber deterrence strategies such as attribution problem, faulty assessment of cyber-attack proportionality, cyber asymmetry existing in between US and its allies. Richard Harknett, Gray Weatley & Richard highlighted the problem in US cyber cognitive circles where there was only the will of deterrence but not the strategic translation of that will. This era was marked by Roger Barnett when he stated the importance of communicating the will and policy of deterrence to the adversary by giving an indication of turning in worse off condition. In the **early phase of 21st century** a lot of attention was being paid to cyber war threat and deterrence strategy by scholars like Betz, Steven, Richard Clarke, Robert Knake who stated that how US physical cyber infrastructure was under threat because of the lack of capabilities to deter the adversary. With 480 publications in this domain, it was concluded that cyber deterrence is a strategy to use military means for cyber-attack deterrence but also vice versa. Use of traditional deterrence

tactics as Dorothy put it could be used to deter the attack and also by means of deterrence by punishment, denial, entanglement and delegitimization. Richard Harknett, Emily Goldman, Michael Fischerkeller by means of offensive and defensive persistence engagement USA would be able to deter its rivals and adversaries (Smeets & Soesanto, 2020). Recent developments in US cyber deterrence strategic thought included norm creation and setting as another mean of cyber deterrence strategy. James Lewis highlighted the importance of creating norm-based deterrence by standard setting of acceptable behavior (Lotrionate, 2014). Another important scholar names Geoffrey French emphasized the importance of tailored deterrence focused on deterring adversaries rather than detecting them he also recommended type of deterrence approach based on type of adversary and securitization of critical infrastructures started when USSTARTCOM was assigned with responsibilities of surveillance, reconnaissance by James Eliss. Martin Lbinki highlighted the decencies in US cyber deterrence strategy and recommended denial and deception approach for deterring adversaries.

4.1 DEVELOPMENT OF CYBER DETERRENCE IN US STRATGIC THOUGHT

WAVE	SCHOLARS	Notable Developments
First wave	1. Der Derain 2. Wheatley & Hayes 3. Timothy Thomas 4. Kevin Matnick 5. Hammer VI	- Nuclear deterrence understanding triggered debate of cyber deterrence - Facets of cyber deterrence strategy: deterrence declaration/communication/will of deterring were defined - Need of cyber deterrence was emphasized - Cyber deterrence was taken with defensive connotations - Both state and non-state threats were identified

Second Wave	1. Richard Harknett 2. Grey Weatley 3. Roger Barnett	- Gray areas in cyber deterrence strategy execution were identified - Fault lines in US cognitive set-up as there was will of deterring adversary but no proper execution of plan
Third Wave	1. Richard Clarke 2. Robert Knake 3. Emily Goldman 4. Michael Fischer Keller 5. James Lewis 6. Geoffrey French 7. Martin Lbinki	- Lack of USA capabilities to deter Cyber threat - Focus on creating norms - Tailored cyber deterrence was also recognized as mean of deterrence - Assigning responsibilities to important department with the task of framing and executing policies. These departments include USCYBERCOM & DoD

Source: Drawn by author, Data Source: (Smeets & Soesanto, 2020)

4.3 EVOLUTION OF US CYBER DETERRENCE POLICY: IN PRACTICE

Four major changes have been observed in US cyber deterrence strategy. The technological advancements that improved US attribution, retaliation and cost imposition capabilities resulted in shift of US deterrence strategy from defensive posture to that of offensive one. Because of proliferation and increased intensity of cyber threats being faced by US critical infrastructure a balance is being strike in between denial and punishment capabilities. For instance, in 2018 Russian attack was disrupted by close collaboration between DoD & DHS. Moreover, the attribution problems have been fixed by its replacement with culpability for example in 2017, Bossert stated by labelling actors as challengers US will constantly put in efforts to counter their behavior. This will deny them the benefit of anonymity. The US cyber deterrence strategy carries a multi sector engagement. With prime role being played by

USCYBERCOM in launching coercive means of deterrence but it also involves cooperation from departments like that of DoJ, DHS, FBI and state department thereby blurring lines with the goal of framing a holistic cyber deterrence approach (Wilner, 2019). The reliance of US policy makers of cyber deterrence strategy started in the mid-1990s. During Clinton and Bush administration there were considerably marked as the onset of US cyber deterrence strategy.

- **CLINTON ADMINISTRATION**

Clinton administration at first securitized the cyber threats by declaring them a national security problem. The national advisory council was created on national information infrastructure in 1993 by integrating the software/hardware domain where 1993 PDD introduced encryption technology that ask to maintain individual liberties by means of countering foreign intelligence threats to system and increasing resilience on protection of system in order to bolster defense. It was in 1996 that cyber threats to US critical infrastructures including financial and telecommunication system was identified and Infrastructure protection task force was created with a commission assigned on analyzing threat to private system. The president commission on critical infrastructure protection was established as a result of CIWG report that identified the asymmetry in between adversary and US cyber space capabilities. The National security strategies of 1995 and 1996 highlighted this risk when in 1997 a comprehensive policy was introduced in the documents titled as "Critical foundations protecting American infrastructures and report titled as towards Deterrence in cyber domain calling for stiffening ties with the allies in a bid to deter adversaries. Clinton assigned a commission on framing of cyber policy in order to protect the critical infrastructures that asked for revision of the technological systems and frame retaliation based on the attribution of attacker. Another document that signified the deterrence policy during administration was titled as 1997 report on "towards deterrence in cyber space "that whereby identified the flaws in defensive technologies highlighted the significance of adopting an offensive cyber deterrence posture. This policy has three strands of retaliation in response to over destructive adventurism, defensive capabilities to scrutinize the adversary infrastructure and that of the offensive capabilities. During Clinton administration it was emphasized in 1998 presidential decision directive (PDD/NSC-63) asking to improve the

resilience of critical infrastructures as mentioned in the national security strategies of year 1999 and 2000. As a result of espionage solar sunrise, the operation moon light maze was launched for surveillance and scrutiny in system (Boys, 2018). In 2000 under Richard Clarke supervision National plan for information system protection was devised that was based on the strands of preventing cyber-attacks while preparing for it, attribution of attacker and responding to it coupled with increasing resilience of the critical infrastructure (Wren, 2012). Another important step taken during his administration was where lead agencies were created for each sector of the companies in order to bolster cyber defense and deny access of adversaries coordinated by National Coordinator for Security, Infrastructure protection and counter terrorism. And to serve that purpose the sector specific information sharing and analysis centers were created to increase the capabilities of attack analysis and attribution (Rosenzweig, 2010).

- **BUSH ADMINISTRATION**

A comprehensive National strategy to secure cyber space document introduced a three-tier strategy of cyber deterrence including prevention of cyber-attacks, bolstering cyber define capabilities and reducing impact of cyber-attacks by not only assigning each state actor with certain responsibilities for reducing vulnerabilities but also combating all kinds of cyber threats by fostering multilateral collaborations and information sharing. This strategy had both elements of deterrence by denial and punishment where for the institutions like FBI, DHS DOJ were assigned to investigate and punish perpetuators by means of criminological deterrence, apprehension tactics. It also aimed at launching retaliatory attacks in response to any cyber adventurism. For denial tactics like creating awareness, reducing systematic vulnerabilities and capacity building was included (Wilner, 2018). A responsibility of concept framework drafting was assigned to DHS under presidential directive 7 2003 where first of its kind National Infrastructure protection plan was devised maintaining a balance between deterrence by punishment and denial in order to increase the risk of failure for the offender. All of this was result of Homeland security presidential directive thereby declaring cyber space as separate domain. Mandating DHS to ensure close coordination in between agencies at domestic and international level. Another important strategy was NS for physical

protection of critical infrastructures and key assists which resulted in adaptation of cyber space as military domain in 2004 National Military strategy**.** It was in the year 2006 when the military was mandated with the responsibility to create an environment thereby deterring the adversaries and laid the foundation of coordinating network operational response, kinetic response, information warfare to impose costs on adversaries (Wren, 2012). Another important step taken by Bush in this regard was adaptation of Comprehensive National Cyber Security Initiative asking for drafting a clear cyber deterrence strategy in 2008 and increasing cyber awareness (Rosenzweig, 2010).

- **OBAMA ADMINISTRATION**

It was in year 2009 that Obama completed the comprehensive National Cyber security Initiative review as per Cyber space policy review thereby introducing some changes. He tilted the shift of deterrence posture from defensive nature to tailored cyber offense. He expanded the role of US intelligence agencies in cyber deterrence assigning FBI with task of establishing national cyber investigation task force for attribution purposes by collaboration with NSA, CIA, DHS mandated with defense tasks of protecting governmental infrastructures through national cyber security center. The cyber offensive retaliation was considered to be job of homeland security and defense department with state secretaries. The goals of cyber deterrence strategy were iterated in 2009 resting on three poles of improving warning capabilities, assigning international partners and domestic agencies with some roles to play and crafting responses for different cyber threats. Creating a holistic and comprehensive cyber deterrence was Obama administration aim which was initially carried by Executive Branch Cyber security coordinator names as Howard Schmidt. In 2009 USCYBERCOM was established assigned with task of launching offensive and defensive strategies for protection of DoD computer network systems. Based on important cyber space documents of 2011 National security strategy and Quadrennial Defense Review includes declaring cyber space as operational military domain, launching 133 Cybercom cyber mission forces with aim of providing the military antics pf cyber deterrence with cyber space effect. More comprehensive deterrence posture was articulated in 2011 under DoD cyber policy report which stated that if denial does not work the US should resort to both kinetic and

non-kinetic military response. Issues and challenges to cyber deterrence strategy highlighted in this report involves acquiring escalation control capabilities by DoD, fixing attribution problem by means of cyber forensic investigation and communication of deterrence declaration with adversaries. 2013 marked the issuance of Resilient systems of military and advanced cyber threat by DoD task force which also included the possibility of nuclear retaliation in case of massive cyber-attack and asks to adopt offensive cyber capabilities leading to establishment of defense science board for crafting policy and strategic option in cyber deterrence realm. In 2015 DoD Cyber strategy prioritized offensive posture and deterrence by punishment over deterrence by denial by use of CMF teams. It was result of this that CMF teams were capacitated in 2016 and Joint force headquarters DoD information network were established. The main focus of DSB was highly sophisticated stat and non-state centric cyber offenders and challenging them with using both digital and non-digital warfighting capabilities. There were significant changes introduced that involved deterrence by cost imposition of diplomatic, political and economic costs on offender and also emphasize building cyber offensive capabilities by recognizing the asymmetry in capability. It also aimed to build second strike cyber resilient system. In order to counter cyber threats and recognize them Obama issues a presidential directive 13687 specifically targeting North Korea and EO 13694 declaring malicious threats as extraordinary liabilities on national security The EO 13757 against Russia and indictment of Chinese military hackers in 2014 under criminal charges were part of this process. A lot of punitive measures resulting in criminal prosecution of individuals from China in 2018, Iranian private and revolutionary guard cops and indictment of 13 Russians in charge of disrupting 2016 elections. The administration also focused on deterrence delegitimization means through putting cyber agenda in G20, UN, OSCE, APEC, ASEAN. International engagement was also considered to be part of strategy as embarked on ensuring safe and open cyber spaces as mentioned in International cyber-Strategy 2011 and international cyber space policy strategy in 2016 indictive of US priorities (Lilli, 2018). It also went on to establishing office of the coordinator of cyber issues resulting major breakthroughs such as US China agreement on economic cyber espionage etc.

- **TRUMP ADMINISTRATION**

The offensive posture of US cyber deterrence strategy continued to remain salient feature of policy and as CYBERCOM chief in 2017 iterated that offensive capabilities must be relegated down to tactical level. The establishment of CISA abbreviated as Cyber security and infrastructure security agency was part of Trump policy. The first step taken by Trump when he took office was to five CYBERCOM status of United Combatant command thereby loosening any restriction on utilization of cyber offensive capabilities. In order to deter any attack on critical infrastructures cyber deterrence was linked with intonement of nuclear deterrence in 2018 Nuclear Posture review. Following the policy of deterrence by cost imposition it was established in brief by state department titled as 'recommendations to the president on deterring adversaries and protecting American from cyber threats in order to revise the cyber deterrence strategy. The command vison for CYBERCOM in 2018 integrated cost imposition on adversary as part of cyber offense (Joe, 2022). Another important document that highlighted the cyber deterrence strategy importance was 2018 DoD cyber strategy as a complementary to National security strategy. It established the tactic of persistent engagement and active or forward defense by conducting preemptive attacks through lethal forces. The active cyber defense certainty act prohibiting access to any computer systems resulting backlash from companies like Google. US also aimed of establishing a Cyber deterrence initiative a collation of US and allies to deter any attack on critical infrastructures. It was in 2019 that Cyberspace Solarium commission was established that asks to deter attacks based shaping behaviors based on norm setting process, denying benefits and imposition of costs. It was also aimed in National Defense Authorization Act opt for an inter departmental and sector holistic approach to deter the enemies. As per the Presidential Memorandum on national security, hunt forward cyber operation as per offensive strategy were started and as result of this in 2021 as a report it was noticed that USCYBERCOM conducted about 2 dozen of such attacks (Ellis & Carmack 2021). The Stuxnet attacks, implantation on Russian energy infrastructures compelled restriction on Russian Internet research agency highlighted Trump assertiveness. Starting a technological

war and operation clean network program indicated the competition with China (Fidler, 2020).

- **BIDEN ADMINISTRATION**

Some clandestine attacks were launched during Biden administration in response to Solar winds intrusions and attacks from Russian territory thereby leading to shut down of ransom group of Russian origin named as REvil. Biden administration pointed out the adversaries namely China Russia and North Korea with China being the most persistent threat to US national security. The first National Cyber security strategy was issued under Biden administration on March 2, 2023 indicating the replacement of China with Russia or being the prime threat. It entails a coherent and holistic approach of both deterrence by denial and punishment and that of cooperation not only asked on defending critical infrastructure but also focused on increasing resilience through means of partnership with allies and launching preemptive measures for disrupting attacks.

4.2 DEVELOPMENT OF US CYBER DETERRENCE STARTEGY UNDER DIFFERENT ADMINISTRATIONS

Administration	Strategic Documents	Deterrence posture
Clinton Administration	1. PDD 1993 2. NSS 1995, 1996 3. 1997 report 4. PDD/NSC 63 5. 2020 NPISP	- Cyber spaces were securitized - National advisory Council was created 1993 - Encryption technology was introduced 1993 - 1996 threats to critical infrastructures were identified - 1997 report asked to maintain extended cyber deterrence with allies - 1997 report titled as “towards Deterrence in Cyber domain was

		published” - Shift from defensive to offensive posture took place after 1997 report - A commission was assigned to frame policy - The deterrence posture was based on three important elements involving 1. Massive retaliation 2. Building defensive capabilities 3. Building offensive capabilities 4. Attribution of cyber attacks - Agencies were created including National Coordinator for security Infrastructure protection and counter terrorism
Bush Administration	1. DHS PD -7 2003 2. 2004 NMS	- Bolstering cyber defensive capabilities - National infrastructure protection plan was crafted - Deterring the adversaries
Obama Administration	1. NCSI Review 2. 2011 National security strategy 3. 2011 Quadrennial Defense review 4. 2015 DoD Cyber strategy 1. Executive order 13757, EO 13694	- Shifted from defensive to tailored offense - Collaboration of FBI with NSA, CIA, DHS - Warning capabilities were improved along improved partnership with states - National cyber investigation task force was created - USCYBERCOM was established

		- Resilience of system increased - -Engagement on international platforms increased
Trump administration	- 2018 Command Vison of USCYBERCOM - 2018 DoD Cyber security strategy - 2019 National Defense Authorization act	- Offensive deterrence posture - Cyber security and Infrastructure Security agency - Lifted USCYBERCOM to status of United Combatant Command - Nuclear and Cyber deterrence were linked in nuclear posture review 2018 - Tactics of persistent engagement and Active Cyber defense were adopted
Biden Administration	1. NCS 2023	- Fusion of both defensive and offensive deterrence posture - A holistic Cyber deterrence strategy - Use of both deterrence by denial and punishment strategy

Source: Drawn by Author, Data source: (Rosenzweig, 2010).

4.4 TYPES OF DETERRENCE POSTURE AND US STRATEGY

- **DETERRENCE BY COST IMPOSITION:** United states has resorted to the strategy of deterring malicious cyber activities on critical infrastructures by means of holistically through diplomatic, economic, political, legal means is the imposition of cost on adversary. It was introduced in 2011 International strategy for Cyber space. US decision makers reported that in case of attack the response should not need to be only of cyber nature. These costs are of economic and legal nature as any attack intended on theft of economic secrets and intellectual property would be met with significant economic reproductions. The imposition of economic sanctions on North Korea and 2015 Presidential directive issued to imposed costs on the any entity

involved in disrupting American business and provoking a threat to national security are part of this policy of deterrence by cost imposition. Another important mean of cost imposition is the use of investigative techniques to probe into unauthorized attacks on US infrastructure through forensic and authorized surveillance means. Using the principles of federal prosecution by department of defense is part of this strategy. For this purpose six Chinese charged for economic espionage against individuals in US nuclear power plan were indicted. US has also launched the training partners for allies in this regard to implement Budapest Convention on cyber-crime in order to deter the attacks by means of cybercrime law's enactment and capacity building of agencies. In order to ensure a time sensitive response a 24/7 High Tech Crime is on readiness. The Cyberspace Solarium Commission in its report gave prime importance to the imposition of costs on adversaries. According to the CYBER COMMAND vison 2018, the cost was imposed on Russian internet agency (Dykstra, & Met, 2022).

- **DETERRENCE BY DENIAL:** Centered around the principal of reducing benefits for adversary and increasing costs, the early cyber deterrence strategy in US was pre dominated by defensive posture of increasing resilience. There are two strands of deterrence by denial strategy as it not only involves bolstering one's own system but also that of physically impeding the adversary of capacity to attacks. In US strategy deterrence by denial took place by means of introducing disruptions in adversary's critical infrastructure/ command and control system but also an increase in cost of attack for adversary. This was indoctrinated in US strategy 2018 DoD vison of defending forward. But denial of access to one's system could also be done by cross domain means involving economic, diplomatic and other means or tactics. One of the most obvious strands in US strategy is that of increasing systematic resilience for example when the CISA warned of the systematic flaws that demand renewal. The denial of access to the most sophisticated attacks was inscribed in 2015 and 2018 DoD cyber strategy. The hunt and defend forward operations by USCYBERCOM such as 2020 join operation of Estonian defense forces with USCYBERCOM and that of

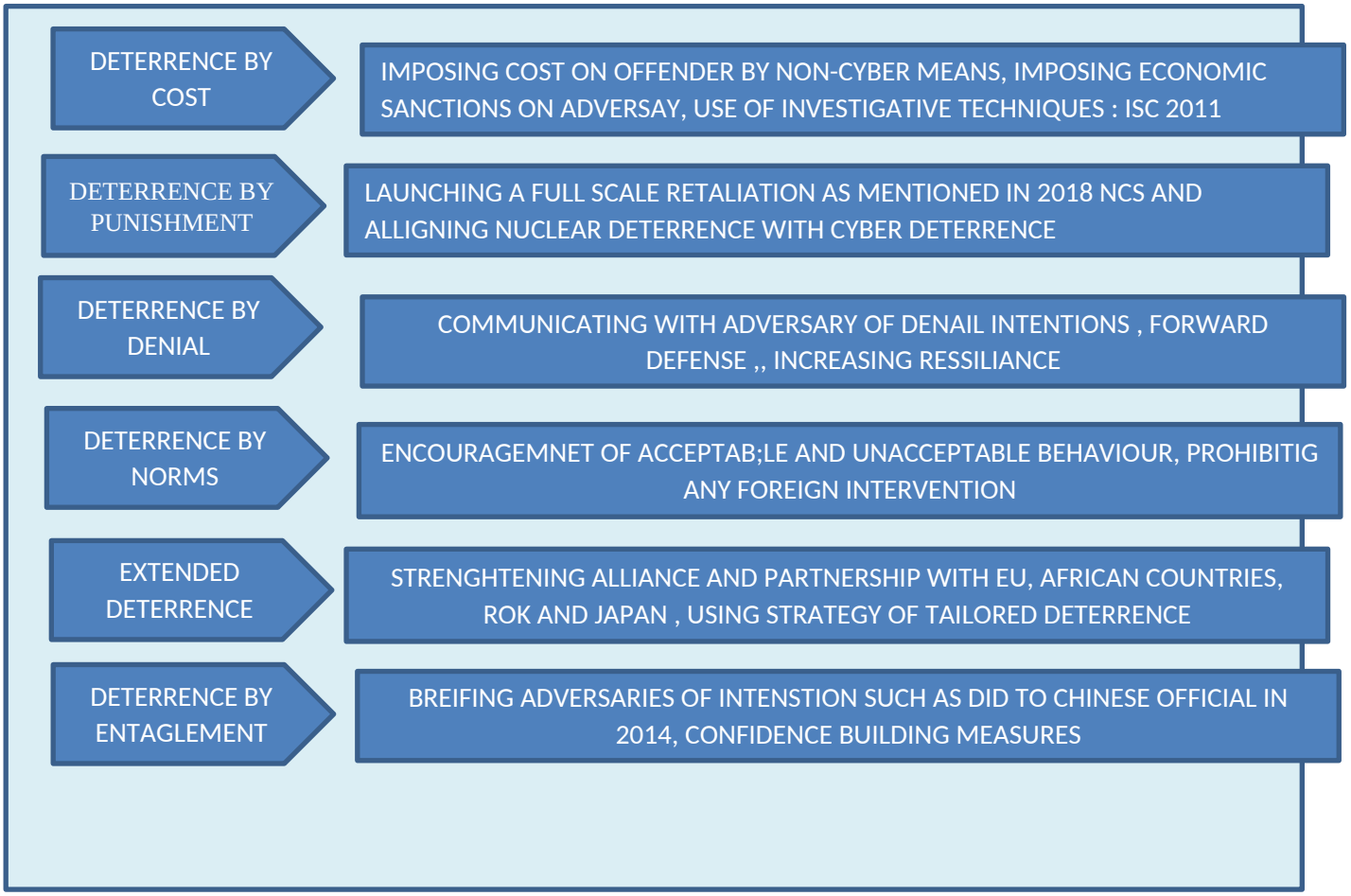
2021 CISA information release for APT-29 virus. This strategy also involves communicating with adversary of the denial intentions (Lonergan, 2021).

- **DETERRENCE BY PUNISHMENT:** The imposition of credible costs on adversary in response to attack is what comes under deterrence by Punishment strategy. Retaliation in response to cyber-attacks comes under the frame of cyber deterrence and this right of US was reserved in the Obama International cyber strategy 2011, 2018 National cyber strategy of launching a full-scale retaliation was part of its process. In case of larger cyber-attack of existential nature, it was resorted in 2018 that nuclear posture review and that of 2018 Nuclear Posture Review that conventional capabilities will be put in practice in case of massive attack. The most frequent mode of punishment in case of cyber-attacks by US involves imposition of economic sanctions as per the executive order in 2015 during Obama administration. The shift towards cyber offensive posture and conducting cyber offensive operations as Washington Post reported that along with 300 sanctions imposed this offensive posture is an indication of staunch policy. Half a billion dollars reserved for building lethal cyber weapons is an indication of this strategy. Moreover, the statements from US defense Secretary and Chairman armed house committee Mc Thornberry of considering retaliation as an option.
- **NORMATIVE CYBER DETERRENCE:** In order to fill up grey areas in US cyber deterrence strategy US has focused its attentive on developing norms for deterring attack where it was established by Lewis that a better defense could be ensured by standard setting of acceptable behavior thereby imposing costs on violation of them by multilateral means. The encouragement of acceptable and reasonable behavior by states was put into the agenda of 201 US international strategy for Cyberspace and that of DoD strategy for operating in cyber space. The acceptance of Russia and China of GGE 2003 report by UN was indeed a success of US strategy of norm setting at international level. The norms US wanted to establish involves prohibiting any foreign interventions in state cyber space, Internet openness for political, economic and strategic reasons. US also aims to ensure cyber stability and baseline security. The 2010 till 2017 GGE expert process were part of efforts for creating norm,

establishment of ICT threats focused bilateral working group in 2012 and December 2015 a joint dialogue was conducted. US is also aiming of shaping a credible cyber diplomatic behavior. The US officials has publicly showed commitment GGE report and Paris call cyber principles. The Summit of democracy under Biden administration was to strengthen partnership with democracies was an indication against the authoritative governments of IRAN, North Korea and China. Biden administration has also issued recent public warnings on cases of violations of cyber norms (Ellinger, 2022).

- **DETERRENCE BY ENTANGLEMENT:** This deterrence strategy involves imposition of restraint on state behavior because of the cooperation between parties based on mutual interest of vulnerabilities that exists in cyber space. The brief of US to Chinese officials of US strategy in 2014 with an intention of giving indication to Chinese forces about the fact that US could use against that resulted in Xi Jinping resorting and committing to avoid using cyber espionage on its visit. In but Chinese government didn't give up on the deep Panda group responsible for APT-2 attacks. the efforts to combat cyber differences were resorted in confidence building measures between US and Russia since 2013 (Scott, 2018).
- **BILATERAL ALLIANCES AND EXTENDED DETERRENCE:** The primary concern of United States strategy is to counter non state actors' malicious activities and also to avoid destructive retaliation with a fear of escalation non digital tools. In order to gain a strategic advantage, you S has aimed to connect with like-minded countries and allies from European Union and Asia Pacific including Brazil India Indonesia and South Africa along with Australia Japan and South Korea. US provide an extended cyber umbrella to ROK aimed of framing joint surveillance and reconnaissance strategies in 2013 Tailored Cyber deterrence strategy. US has maintained alliance with ROK Japan and Australia

4.3 TYPOLOGY OF US CYBER DETERRENCE POSTURES



Source: Drawn by Researchers, Data Source: (Dykstra, & Met, 2022).

4.5 US CYBER DETERRENCE STRATEGY

4.5.1 THRESHOLD TO CYBER WAR: DRAWING RED LINES

United States threshold to cyber work would be assessed from the statements given by senior officials the presidential policy directors and reports or strategies. The nature of threshold depends on factor-based approach rather than on the type of cyber-attack from the very start in U strategy such as in May 1999 it was written in the assessment of the international legal basis and information operations that the use of force would be triggered based on the effects of attack. The US to threshold is based on international law principles where it was under Obama administration recognized that in case of major attacked of armed nature the article 24

would be triggered if the malicious activities would meet the criteria of article 51. During Obama administration a cyber-attack resulting in kinetic consequences was considered worthy of cyber war. A coherent perspective in this regard was given by Legal advisor of Obama Koh that involves the continuity of Obama 2011 ISC strategy that translate laws of war in cyber domain. It was in 2016 that ambiguity in threshold establishment was the character of US strategy as indicated from the statements given by secretary for homeland defense and global security. However, during trump administration, the attack on critical infrastructure was considered to be an act of war and trigger the threshold as indicated from the head of the NSA named as Paul Nackasone. But the statement given by assistant secretary of defense for cyber policy that threshold for cyberwar would be triggered based on case-by-case analysis by the US government. It was in the National Defence authorization act 2019 that for a proportional cyber retaliation the congressional authorization was considered to be essential and a presidential approval was considered to be important under the PD20. It was established in the trump era that any attack on the industrial electoral and critical infrastructure would invite a DoD response (Jr, 2018). During the Biden administration a 16-area list of critical US infrastructure was handed over to Vladimir Putin in 2021 which indicated that those are the red areas that the Russian forces must avoid otherwise it would invite an armed attack from the US.

4.5.2 US COMMAND AND CONTROL SYSTEM AND CYBER DETERRENCE

The consolidation of US command and control a system comes under US CYBERCOM, Cyber command of Navy and Marine forces. It was established by Defense Secretary Gates and Michael Warner thereby assigned with the planning, consolidation and direction of activities. A full spectrum control over defensive offensive in formation grid operations is being carried out by US CYBERCOM thereby providing a leadership and training for all sectors. Assigned with the task of bolstering resilience of the information and communication networks and creating a synergy in between DoD cyber expertise and capabilities cyber expertise and capabilities. For conducting the global network operations to centers have been established that include joint operations center and joint task force in order to centralize the system. Because single Commander supervise the activities of NSA and CYBERCOM under

Title 50 and 10 respectively that put the latter in friction with military services (Porche & Paul 2023). The vision statements given by commander of EU S central command and control system lieutenant general Alexander in 2010, 2014 Micheal Roger being Vice Admiral, 2018 Lieutenant Paul Nackasone Intended to confront the persistent engagement of US critical infrastructure with the adversaries and to maintain Cyber space superiority. There were two visions issued by USCYBERCOM in 2014 titled as "Beyond the Build: Delivering Outcomes through Cyberspace" and 2018 statement titled as "Achieve and Maintain Cyber Superiority". With the former mission statement indicating a resolve to not only defend the US critical infrastructures but also to shape a full spectrum response by integrating the cyber capabilities and the letter involves north only over matching the adversaries' capabilities but also to create a cyberspace an information advantage by deepening the operational partnerships (Zegart & Lin 2018). With that the national intelligence agency had 15 intelligence communities with some under FED and DoD. With the threat of cyber-Pearl harbor given by director NSA 2015, proliferation of malicious activities. These agencies are assigned with the task of building, resilient capabilities and information systems, Defensive operations identification of attacks intelligence policy options providers and damage assessment.

The following table elaborates the US cyber command and control system along with the role and function of each body

4.5 US CYBER C2 SYSTEM AND FUNCTIONS OF VITAL BODIES

BODIES	ROLE AND FUNCTIONS
Department of Homeland Security	1. In charge of CGI& IA 2. To protect US critical infrastructure and territory 3. Respond to attacks 4. Synergy of Information

Department of Defense	1. Operational Source of IC 2. Main Source of Cyber Intelligence info 3. Devise Policy Recommendations 4. Control Nine agencies
State Department	- To supervise the operations and coordinate them
Private Sector	1. Overseen by ISAC 2. Assistance to Federal and Local Governments 3. Collaborate with DHS, DoS, FBI

SOURCE: drawn by Author, Data Source: (Zegart & Lin 2018)

4.6 U.S. CYBER DETERRENCE POSTURE

The essence of United States cyber deterrence strategy rests on the collaboration with allies and responding to the cyber-attacks by collectively are attributing and responding to the malicious activities. Do operations like glowing Symphony emphasized the importance of persistently engaging with adversaries and successful offensive operations this was considered to be the core objective of third pillar in the national cyber strategy that aimed to establish peace by means of strength.

4.6.1 DEFENSIVE POSTURE

The aim of this posture is to minimize and prevent the cyber-attacks by bolstering the resilience of critical infrastructures. In order to protect the key critical infrastructure as it was inscribed in the edge as 2013 strategy that vulnerable infrastructures would be recognized and sector specific agencies/ councils will be protecting the system. The close Collaboration in between DoD, NSA, USCYBERCOM have yearly objectives of increasing the resilience of their systems as per Joint Info Environment & Cross Agency Cyber security as in 2013 PD 21, EO 13636. Moreover, the information sharing by private companies as per DoJ guidance.

It was also written in DoD Cyber strategy 2018 that in order to deter the malicious cyber activities the US forces must constantly engage with the cyber adversaries. It also involves the maneuvering of outer spaces as per the doctrine of US cyberspace solarium Commission and 2021 National Defense authorization act to proactively engage with other states. To serve this purpose information operations were considered to be essential and in December 2021 about $75 million were reserved by USCYBERCOM for this purpose. As per DoD 2021 Active cyber defense strategy was adopted in order to initiate the time sensitive proactive attacks. In this strategy the information assurance directorate and the critical infrastructure and degree resources along with the decision makers play an important role as but the White House 2011 executive order stated that a whole of government approach is needed to be installed in order to ensure active defense (Willett, 2014). The forensic technologies must be used to our tribute which are essential for defending the critical infrastructures and multiple projects like Intelligence and Defense and Cyber Genome Project to detect the malicious activities (Thayer, 2015).

4.6.2 OFFENSIVE POSTURE

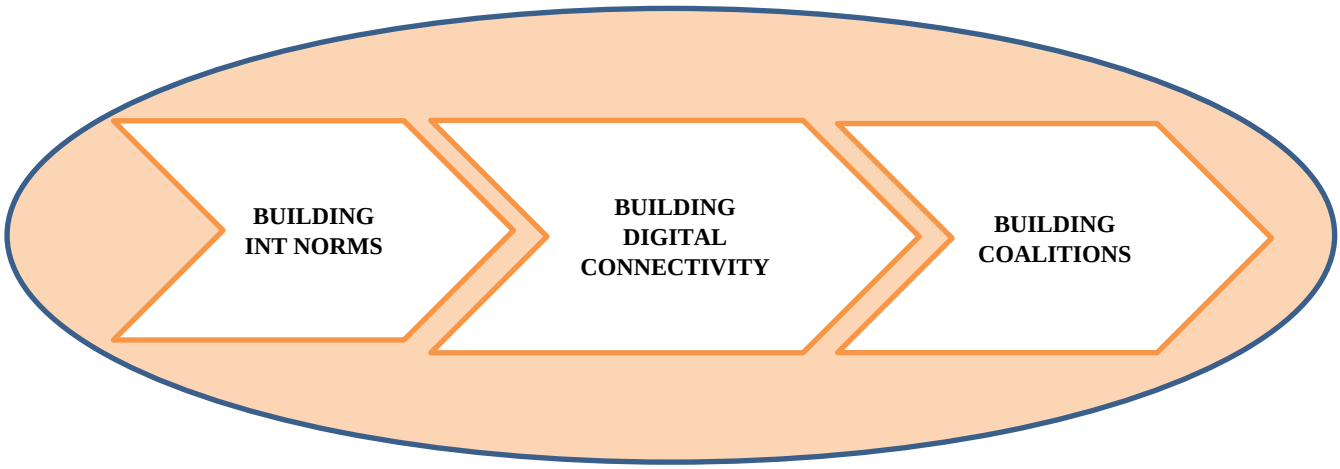
For a coherent deterrence strategy, the United States in need to issue a clear-cut declaratory policy with offensive poster and to serve this purpose in 2015 about 100 cyber offensive operations were conducted to deterred the adversaries and in order to launch retaliation the example of which is Stuxnet policy. The United States also reported in 2013 that it would use non kinetic means of retaliation. President Obama resorted to the option of capabilities and tailored cyber deterrence in order to deter the adversaries like China and Russia by warning them in their statement. The United States as Edward Snowden noted that who is the considerable offensive cyber capabilities That could turn Russia China and Iran into aggrieved parties. The United States has resorted to a conscious policy of careful attitude towards an adversary capable of strong retaliation and the proportionality principle must be kept in mind before initiating a cyber offensive operation against a capable adversary in that case low level cyber war must be the option. Sometimes our middle cyber power when pose a threat must be sometimes US preferably adopt a cyber offensive rather than kinetic option of

attack. Launching preemptive attack is a considerable and viable option as mentioned by U S National Security Agency (Labicki, 2015).

4.6.3 COMPONENTS OF US CYBER-DETERRENCE STRATEGY

The basic components of United States deterrence strategy involve building consensus based on the acceptable international cyber norms and harvesting the knowledge of quantum technologies artificial intelligence and computing networks in the private sector it also involves the cooperation and collaboration of the private sector with the public one. by means of cyber diplomacy. The United States national security strategy aims at strengthening the 2014 global coalition to defeat also the state department aims to build coalition and to mobilize them in order to fight against the adversaries and to encircle them. Because the international cyber spaces are highly interdependent. In this regard the state department has strengthened In this regard this state department has strengthened partnerships like digital connectivity and cyber security partnership 2018 in the indo Pacific region and also the malign Kremlin influence was countered by a development framework initiated by USAID 2018. The blue dot network in between United States Australia and Japan in 2019 The blue dot the blue dot network in between you S Australia and Japan aims to build the capacity of these countries against Chinese threat other initiatives include clean network programmed and 5G clean path initiative. The competitive mindset was needed for the deterrence strategy being adopted in different statements of the leaders such as 2020 statements of Mike Pompeo and also the intent in 2019 policies to compete with China with the help of Five Eyes airlines and also Global Engagement Center (Goldman, 2020). The following ilustration encompass the componenets of USA deterrence staretgy

4.6 COMPONENETS OF USA DETERRENCE STRATEGY



Source: Drawn by Researchers, Data Source: (Goldman, 2020).

4.6.4 FACTORS OF CYBER DETERRENCE STRATEGY

Signaling has been made the part of United States strategy where it has in listed a number of retaliation options in caves of aggressive attacks and has clarified thresholds at multiple levels such as in EO 13694. It is the following the NATO policy inscribed an earth charter that with the declaration of policy the risks could be reduced. **Attribution** also the aggressors responsible for attack on the infrastructure by using forensic capabilities**.** There are multiple retaliation options that US consider involving tailored deterrence as Clapper pointed out. **Retaliation** by means of threatening the adversaries of kinetic response and loud cyber-retaliation coupled with the policy of imposing international sanctions search a sanctioning of Russian individuals involved in 2016 elections theft under the Obama administration EO 13757 resorting to mode of sanctions imposition against DPRK and other hostile governments. Imposing criminal charges using the Budapest convention and that of the Department of Justice inductions of the criminal individuals involved in malicious activities is another part of US cyber deterrence strategy (Goyachayev, 2017).

4.7 CYBER THREATS AND DETERRENCE STRATEGY

4.7.1 DETERRING RUSSIAN CYBER THREAT

There has been a significant damage caused by the attacks from the Russian Federation on the United States critical infrastructure that demands a proactive and active defense strategy for which the United States is working with NATO counterparts in order to attribute these attacks and to devise a strategy to deter them. Dwarf the most recent cyber-attacks on the United States critical infrastructure involved the ransom attack in 2021 on the colonial pipeline that is meant for about 45% of the supplies resulting in the shortage of the gas also the complete shutdown of meat packing firms in the United States by the attack from the Russian hackers in June 2nd 2021 resulting in serious ID disruptions and meat shortages. The attacks do not store pair as in 2017 the major Not Petya cyberattacks from Russia impacted France Germany UK Norway Denmark and even United States resulting in the cost imposition of about $10 billion. Also, the Ukrainian infrastructure and system was turned down by the dark one barred over show and 2022. **Strategies** put in place by the United States in order to counter the Russian

cyber aggression involves close collaboration with the private sector because most of the ransom attacks from the Russian authorities are being projected towards the United States firms. For example, in 2021 a statement came from the director FBI that the office of private sector is working in close collaboration with the firms in order to identify and share the information with the US national and governmental entities and close collaboration with the private cyber security such as apple and Microsoft which are primarily focused on the individuals and consumer behavior. The United States with the help of NATO is the training the private firms to secure their cyberspace is and this is considered to be a common strategy and part of Department of Defense resulting in the National Defense Education Act asks for the governmental agencies to invest heavily in the private sectors. NATO has also revised its action plan of 2017 in 2022 by re-emphasizing the role of collective defense in building a robust cyber defense and the norm developer which is essential for the United States strategy off cyber deterrence. The Russian threat is being encountered in NATO by grows to main retaliation options being under consideration And the Russian strategy also blurring the lines in between cyber and conventional warfare capabilities is resulting in a dangerous competition for which the United States need to build a coherent strategy in order to counter in-attributable sources of attack. Another tactic being adopted by United States to counter Russian attacks is to impose economic sanctions and to include the aggressors in the list of specially designated national blocked person list (Chace, J. 2022).

4.7.2 DETERRING CHINA THREAT

The Chinese threat to the United States infrastructure has been most prominent as the Biden national cyber security strategy 2023 highlighted. The attack on OMP of US was eye opening for the US strategists when it exposed the considerable US data. There are multiple strands of United States cyber deterrence strategy towards China that involves passive deterrence. These strategies involve communicating the declaratory policy with the Chinese authorities such as Biden did but also improving the cyber security measures that act as a passive deterrent for the adversary which in this case is China. The deterrence strategy of delegitimization which involves criminal trial of the Chinese hackers involved in attacks is another strategy of United States along with the diplomatic protests that it adopts in order to

expel the Chinese individuals involved in ransom activities from the United States. Another important strand of United States strategy towards China is adaptation of legal measures and induction of the Chinese individuals what is sometimes the United States has to reveal sensitive information in order to accuse and trial the Chinese individuals in the court and could avoid similar inductions from China of innocent individuals. Another could also deter attack as the trump in his new clear poster review 2018 revealed that any attack on the side word facilities of existential nature would invite a nuclear retaliation which is sufficient for deterring Chinese authorities (Putten, 2015).

It has been speculated that USA pre-dominance in cyber spaces is in decline with the increasing power of other parties and powers. The new trends in cyber spaces along with the intense strategic competition followed by hyper globalization has opened the doors of new challenges to USA system that asks for immediate fixture. USA deterrence strategy has changed its posture from time to time, from offensive to defensive and again offensive.

CHAPTER 5

CHINA AND RUSSIA CYBER DETERRENCE STRATEGIES

'People's Liberation Army Rocket Force' of China and 'Strategic Rocket Force' of Russia alongside the 'Strategic Command' of U.S. have had a history of lengthy traditions of operationalizing deterrence in nuclear framework, but in the contemporary scenario it is the nature and the very existence of deterrence in the fifth domain of cyber world, which remains under the debate. This chapter explores the debate of cyber deterrence in Russian circles on how there exist a skeptical attitude in Russia in regards to cyber deterrence. The definition of cyber deterrence concept and phenomena as per Russian strategic though have been looked into the offense and defense balance along with the principles on which Russian cyber deterrence is based have been chalked out in the second half of this chapter the cyber deterrence strategy of China have been the main focus

5.0 DETERRENCE IN CYBER SPACE: IMPERATIVES OF RUSSIA AND CHINA

Within cyber domain, deterrence has been upheld as both i.e., as source of stability which helps improve the overall security of cyberspace, as well as a tool of exploitation amidst cyber persistence engagement. How this phenomenon unfolds in cyber space has already been discussed in the above chapters but analysis of how other countries perceive this trade-off requires a more nuanced evaluation of each state's cyber space calculations and definitions. Understanding such behaviors of countries in cyber space can be very challenging given the technical nature of cyber space which may include issues of attribution and its ephemeral effects in addition to the obscure motivations and covert strategies of actors involved. Such conceptual challenges are often analyzed from a tactical and a defensive perspective, including the building of a threat perception by a deterrence posture. Previous chapter explored in great detail, the deterrence posture and strategy of U.S. in cyber space, while this chapter is going to focus on the framework of evolving cyber deterrence imperatives of Russia and China, latter two being in a loose alliance against U.S.

5.1 RUSSIAN PERSPECTIVE ON CYBER DETERRENCE

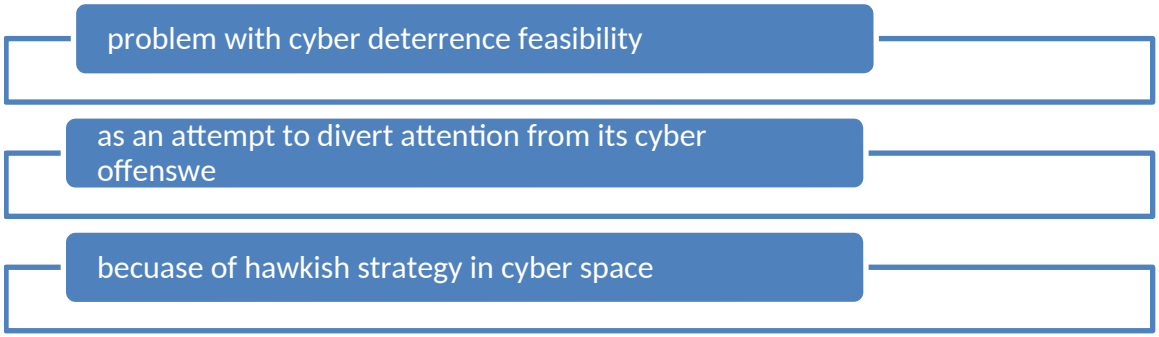
The idea of deterrence as a way to dissuade enemy attacks, has constantly been under debate and consideration in order to address the increasing instability in cyber space. National Cyber Security Strategy of UK (2016-2021), places significant emphasis on deterrence. U.S. policy.

Cyber deterrence in the context of Russia however, is much of a complicated debate with distinct narratives when it comes to Russian perspectives and Russian practice. There has been much research on Russian overall cyber conduct but little focus has been placed on its approach towards cyber deterrence. But as the cyber threat landscape continues to evolve, deterrence in cyber space looms largely in discussions of contemporary Russian cyber space posture, given the country's history of engaging in state-sponsored cyber-attacks and other forms of cyber offenses and cyber aggressions. This discussion is of highly critical nature with 'deterrence' viewed to be as an unworkable construct by many Russian policy makers, academics and strategists. Such views are rooted in the distinctive Russian conception of '**cyber as one indivisible element within a broader deterrence strategy.**' Russian skepticism about applying nuclear deterrence theory to cyber space is one another limitation to its cyber deterrence posture. However, in spite of such limitations and doubts, Russia has been witnessed to be publicly endorsing and espousing a cyber deterrence policy in all but name, mainly as a reaction to the arms proliferation by the West within cyber space. According to the Russian narrative, it is the arms build-up by the West and the pursuit of offensive cyber capability by Western states, which acts as the cause of destabilization of cyber space and thus is forcing Russia to respond and reciprocate by the means of cyber-attacks. Media usually reports on the origins and the vectors of cyber-attacks, tools and techniques utilized, the generated impacts and on how to mitigate such attacks. But a broader strategic perspective to understand the very nature of this act itself, acquires answers to questions dealing with the adversary's conducts of cyber-attacks, adversary's intentions and its perceptions of threat and escalation, in addition to whether such attacks can be deterred by the adversary (Connell & Vogler, 2017). Therefore, in order to understand the cyber deterrence posture of Russia, it is important to not only answer these questions but to examine

the very key Russian conceptual dimensions and the practical implementation of this concept i.e., to examine the overall narrative and the practice which appears to be quite in contradiction in terms of Russian cyber deterrence posture. This contradiction is based upon three major causes:

- Firstly, the self-criticism of Russian thinkers, as many Russian strategists think to have genuine reservations about the feasibility of deterrence in cyber space given the difficulties related to accurate attribution and the possibility of miscalculated escalation (Fischekeller & Harknett, 2017). The risk of arms race in information space can lead to a provocation of cyber-war and as well as can endanger the nuclear stability.
- Secondly, upon a theoretical basis, Russian criticism is a self-serving attempt to divert attention from its own cyber operations by hindering the global pressure of regulation.
- Thirdly, there exists disagreements and dissonances within Russia's defense and strategic community regarding the use of deterrence in cyber space. Although the Russian diplomats lobby for cyber agreements but Russian long-term interest is side-lined by the hawkish element of having all options available. A deterrence strategy will keep a check on Russian power projection.

5.1 REASONS FOR RUSSIAN SCEPTICISM ON CYBER DETERRENCE



Source: Drawn by Researchers (Connell & Vogler, 2017)

5.2 CYBER DETERRENCE IN RUSSIAN STRATEGIC THOUGHT

Generally, the way Russia defines cyber and views its employment for strategic use is much different than its western counterparts' approach towards cyber space, given that as per the statement of James Wirtz, Russia unlike other actors seems to have devised a way to integrate cyber warfare into a grand strategy in order to achieve political objectives (Wirtz, 2015). The Russian military doctrine of 2014, the National Security Strategy of 2015 and Information Security Doctrine of 2016, consider the information space as a domain of warfare. According to Russian narrative, it is the space where war against Russian digital sovereignty is waged and thus Russia responds in defense. Russian defensive posture includes protection of critical infrastructure, protection of critical information and increasing digital sovereignty via improving the readiness of defensive action as well as by improving the capabilities of isolating the Russian internet. Yet, it is to be understood that a credible defense also requires a credible deterrence (Turunen & Kari, 2020).

Contextualization of deterrence approach in cyber space by Russia, depends upon a number of factors. By large, it depends upon the **Russian strategic thought** which views the term 'deterrence' to be most commonly associated with the idea of '**strategic deterrence**.' According to the Defense Doctrine of 2014, this concept encompasses both nuclear and conventional domains. National Security Strategy of 2015, includes within these domains the cyber space as well, making strategic deterrence a design to 'prevent armed conflict via interrelation and integration of political, military, military-technical, economic, diplomatic and informational as well as other measures' (2015). As compared to NATO thus, the Russian deterrence construct is much holistic, seeking to produce a combined deterrent effect through a range of military and non-military means (Bruusgaard, 2016).

Furthermore, Russian way of building deterrence can best be explained by the factors and elements of Russian strategic culture, with main factors being the sense of vulnerability, fear of surprise attack, the concept of a permanent war and the narrative of Russia being a besieged fortress (Kari, 2022). To cater these factors, Russian deterrence encompasses a combined and coordinated toolkit with elements such as coercion, compellence and

containment in order to ‘deter and dominate’ instead of preventing any military action at all. According to mainstream western perspective, such a posture seems more aggressive i.e., more of an offense rather than a defense and thus might create an overall deterrence instability, but particularly within the context of NATO-Russia relationship.

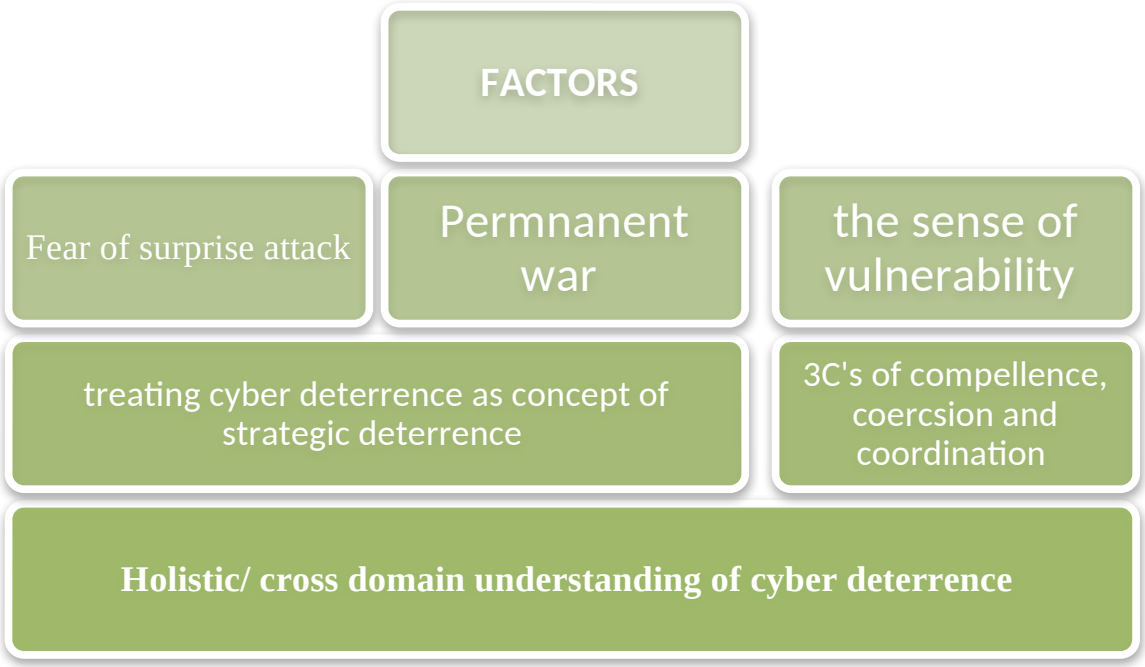
Furthermore, unlike Western perspective, Russian perspective of deterrence is not conceptualized through separate domains of conventional, nuclear, and cyber. Russia upholds only one posture of deterrence i.e., strategic deterrence which is applicable in all spheres of warfare. In terms of cyber space, in Russian strategic thinking, it is viewed as a subset of ‘informatsionnoe prostranstov’ and ‘information sfera’ i.e., information space and information sphere, while cyber operations are considered to be a part of Information Warfare (IW), thus making deterrence in information space a key component of the overall posture of strategic deterrence.

Russian officials define information warfare (IW) as ‘carrying out psychological campaigns against the masses to destabilize society and the state in order to force the state into making decisions in the interests of the adversary’ (Frear &Kulesa, 2018). This concept is rooted broadly in the Soviet traditions of reflexive control and maskirovka and provokatsiya, which draws on actions of electronic warfare, information and disinformation operations as well as cyber operations. As stated in 2007 by the Russian defense minister, Sergey Ivanov, ‘information warfare is a weapon that allows would-be military actions to be carried out in any theatre of war without having to use actual military power.’ In 2013, in his article, Valeriy Gerasimov recognized information warfare as largely a framework for victory (Galeotti, 2014).

Therefore, quite in contradiction to the West which recognizes cyber space as the fifth domain strategy; Russian strategic thought does not contextualize cyber space as a separate domain in its own right, but as a subset within the umbrella of Information Space, and thus an important constituent of its strategic deterrence. Unlike the western perspective, which showcases separate deterrence thinking for each domain i.e., conventional, nuclear and cyber,

Russian perspective encompasses deterrence as a holistic approach under the category of strategic deterrence. Russian strategic deterrence stands out in quite peculiarity as a result of its three unique features i.e., its universality, continuousness and its combining of deterrent and coercive logic. Its universality is in its approach to seek to dissuade all types of security threats via the use of all kinds of measures available, by formulating and implementing strategy for thwarting threats at different levels. Measures used include not only deterrence but **coordinated tools of offense and defense** as a way for Russia to achieve its policy goals in, out and through information space (Meakins, 2018).

5.2 FACTORS IN RUSIAN CYBER DETERRENCE UNDERSTANDING



Source: Drawn by researchers, Data source (Meakins, 2018).

5.3 RUSSIAN CYBER DETERRENCE STRATEGY: IN PRACTICE

At the height of nuclear proliferation during the cold war era, USSR and U.S., both were reluctant to use the nuclear weapons because of the fear of a full retaliatory response. The fear

of Mutually Assured Destruction (MAD) was enough to keep both the parties at bay and it was precisely this fear which kept the posture of deterrence throughout. To keep such a posture of deterrence in the cyber space is however, different given that it involves no direct military involvement, rather such cyber-attacks are caused by governments and hackers via the use of espionage, information misconstruction and sabotage of physical infrastructure. While there exists a broad agreement that at some point, such cyber-attacks would be considered an act of war, but no one knows quite well where the Red Line is. Within cyber operations, no one knows where the threshold truly lies. The on-going confrontation between U.S. and Russia, in the face of military spending, maneuvering and aggressive rhetoric alongside the continuous and ever-narrowing space for diplomatic communication, has reignited the focus on deterrence i.e., deterrence as a practice for avoidance of war in cyber space.

Within the context of Russia, this approach towards deterrence in cyber space is somewhat unique, or as some say non-existent in theory, but albeit practical, provided that its contextualization is much distinct as compared to the Western concept of deterrence. As discussed above, Russian approach is that of an '**integrated strategic deterrence**' which envisages the idea of deterrence and significant pre-emptive actions in all domains, not as a way defend but to dominate the conflict. Russia is said to be relying on creating a sense of unpredictability to keep the adversary off-balance by being assertive and aggressive (Frear & Kulesa, 2018).

In terms of cyber deterrence specifically, the Russian approach is marked by two paradoxes i.e., a consensus of unworkability of deterrence in cyber space in addition to Russia espousing a cyber deterrence policy in all but name. According to a report of 2011 on the 'activities of Armed Forces of Russia in Information space', it was stated that 'in any event of conflict in information space, Russia can exercise its right of individual and collective self-defense.' This statement is viewed to be an assertion and an attempt of deterrence signaling by promising a retaliation in response to an attack. In 2016, in response to the rumors of incoming British cyber-attacks, it was stated on behalf of Krutskikh that Russia will not forgive any cyber-attack. In 2018, further statement was added regarding 'Russia not turning

the other cheek'. This statement is particularly true in terms of how Russia unfolds its practice of deterrence in the information and cyber space by leading cyber-attacks, as a vehement way to dissuade and deter adversaries from conducting cyber-attacks against Russia.

5.4 RUSSIAN DETERRENCE POSTURE IN CYBER SPACE

Over the past years, Russian administration has been accused of a range of cyber-attacks. From the damage done by 'Not Petya' and attacks against Ukraine and Georgia, to the hacking operations of Democratic National Committee in 2016 and leaking operations in U.S. and European elections, Russia's offensive operations are a consistent threat in the cyber channel. Russia has also been accused of engaging in cyber espionage, intellectual property theft and other forms of cyber aggression against Western countries. Such an **offensive posture** is stated to be a part of ongoing strategy of 'information confrontation' on behalf of Russia (Hakala & Melnychuk, 2020).

Furthermore, such aggressive cyber posture of Russia has been explored in much in detail in a report by NATO, the findings of which dictate Russian cyber conception of confrontation in cyber space as an approach to attain the end strategic objective of 'information superiority.' Therefore, based upon Russian thinktanks and official policy documents, the Russian doctrine and posture for information space is clarified to be as constant, extending from information protection to information confrontation, for which Russia actively uses cyber strategy alongside military and non-military means to attain the strategic objectives. The tactics utilized by Russia in this information environment involve electronic warfare, kinetic action and psychological and influence operations, all three used for physical and cognitive attacks in order to gain 'information superiority' (CCDCOE, 2021).

This behavior however, has now come in some ways to mirror the position that of the West (Meakins, 2018). In 2017, another public statement was made regarding deterrence posture of Russia, which quite resembles the posture that of the West, as Russia announced its approach of not attacking anyone but also to not let anyone attack it – this statement being epitome of deterrence i.e., not attacking but preventing attacks. This posture is displayed in the face of Russian **defensive posture** of 'information security' (Hakala & Melnychuk, 2020).

5.4.1 OFFENSIVE POSTURE: INFORMATION CONFRONTATION

Activities and actions in cyber space are usually the tools of warfare in information sphere which can include electronic warfare, psychological operations, kinetic actions and other physical and cognitive attacks on infrastructure of society, respectively. Russian led actions in cyber space are derived from its strategy of 'information confrontation' which is derived from its understanding of relations between states i.e., a struggle for influence in the world. According to Russian thinkers, the information confrontation is a constant, an ongoing and an overreaching concept with the aim of achieving means to gain superiority in this increasingly digitalized world (Hakala &Melnychuk, 2020).

It is a concept generally referring to the hostile informational activities carried by Russia. According to Russian Ministry of Defense, the information confrontation can be defined as 'a clash of national interests and ideas with the aim of seeking superiority by targeting the enemy's information structure and protecting one's own objects from the similar influence.' Such confrontation includes significant psychological merit, as they tend to gravitate via the perception of events. **Cyber operations** which are carried out to gain superiority are the examples of such information confrontation strategy. In the last multiple years of President's Putin reign, Russia has been involved in information confrontations, as a constant geo-political and a zero-sum competition for great power influence via the military and non-military means. Such operations prove to play an essential role in compensating for conventional force, in disabling critical civil infrastructure and also help in command and control (C2) capabilities to hinder the war fighting capability of the adversary (Giles, 2016).

5.4.2 PRINCIPLES OF RUSSIAN INFORMATION CONFRONTATION

Russian practice of information confrontation as a way to enact hostile activities, galvanize the domestic population and misdirect public opinion, has its roots in the Soviet practices of reflexive control and active measures.

- **REFLEXIVE CONTROL**

Leading a target to act unknowingly in a predefined manner, often against its own interest is what is called as reflexive control. This can be done by influencing the channels of information of the target and by manipulating the flow of information in the favor of oneself.

According to Lefebvre, the essence of reflexive control lies in the mutual attempt of the adversaries to reflexively control each other (Kramer, 2003). The susceptibility of a country to be reflexively controlled emanates from unchecked access to its information via hacking or attribution by another state which can lead to manipulation of data within cyber or information space. Moscow uses reflexive control as one of the tactics of its information confrontation, by making the enemy to act and decide on manipulated information (Rasmussen, 2015).

- **ACTIVE MEASURES**

Cyber operations seeking to affect the target nation's policies often involve active measures which unlike public diplomacy are undertaken secretly in a covert manner via manipulation of information space. It involves violation of laws, blackmail, disinformation, propaganda and bribes as well as exploitation of enemy's societal and political infrastructure. Russian information confrontation strategy largely makes use of such active measures, which are often undertaken secretly via sophisticated malware software and other hacking tool kits.

- **MASKIROVKA**

Inherited from Soviet era, maskirovka is an information confrontation method which Russia makes use of for concealment and deception, in order to convince the adversary of the presence of objectives which actually are not. The concept is rooted in the idea to make the enemy fall into error by disrupting its Command and Control in order to make the enemy take decisions which otherwise would not be taken (Keating, 1981).

- **ADVANCED CYBER CAPABILITIES**

For ensuring information security, deterrence as a tactic is largely utilized in the global landscape of cyber domain. Although Russia not really focuses on any specific posture or strategy for deterrence in cyber space and rather upholds a strategic posture of deterrence which contradicts itself from its thought and practice, but nonetheless Russia does involve the use of cyber weapons and other advanced cyber capabilities to launch **offense as its way of defense** in the information sphere i.e., as a way to prevent or deter cyber-attacks against itself by launching cyber-attacks in the first place. According to Krutskikh, 'cyber weapons are used every day and are used offensively' (2017).

It is important to note that Russian posture in information space emphasizes on the development of confrontation and security, but it has also focused on the development of **Robust Cyber Arsenals** which include hacking tools and advanced malwares to carry out espionage, sabotage and other malicious activities in information space i.e., activities which target the critical infrastructure, political targets as well as military assets.

One example of Russian cyber arsenal is that of '**Sofacy**' or 'fancy bear' which is a malware operated by Russian military intelligence to target enemies' agencies, governmental sectors, organizations and other actors across the globe. This is a malware designed to exfiltrate information and manipulate data, as a part of 'information confrontation' strategy.

'**Sand Worm**' is another one among the Russian cyber arsenal tools. It was utilized in 2015 in a cyber-attack against Ukraine's power grid. It is a malware designed to target industrial control systems (ICS).

One another example and quite famous is that of '**Not Petya**', which was utilized as a destructive malware to cause damage to world companies in 2017. While Russia denies its involvement in the attack, but the advanced and sophisticated malware says otherwise i.e., it being a part of Russian broader campaign for cyber aggression as a way to secure its feat in information or cyber space.

5.4.3 DEFENSIVE POSTURE: INFORMATION SECURITY

In addition to 'information confrontation' as an offensive strategy, 'information security' is utilized by Kremlin as a defensive measure to secure Russia's own information space from foreign influence. Even though Russia lags behind other countries in the context of development of a competitive information technology, but Russian perception of its strategic vulnerability in cyber space is much strengthened and for it ensures maximum security. Its cyber deterrence consists of improved protection of its critical information structure via means such as isolation of Russian internet, intensified surveillance and use of Russian made and produced Information and Communication technology (Kari, 2019).

It is also to be noted that Russian notion of 'information security' is distinctive from Western notion of 'information security' for it encompasses not only the protection of critical digital

networks but also the cognitive integrity of society. Moreover, the term information security is used by Russia for the overall cybersecurity, for the protection of which Russia has been invested and engaged in not only offenses but defenses. The Russian strategic thinking operationalizes the protection of its information or cyber space via the use of extensive web of code, legal controls and other surveillance measures.

Russia also utilizes the concept of '**information sovereignty**' as its way of information security by protecting its own information space. The law for 'Russia's sovereign internet' came into force in 2019 and has allowed the government to isolate and disconnect from the internet, as a means to secure the digital sovereignty of Russia and as a way to avoid any incoming cyber threats. The fraudulent Duma election of 2012 led the Russian officials to acknowledge the power of internet sphere and the influences it causes in people's minds, and thus an essential component of Russian digital sovereignty is also the Russian Internet (RuNet).

5.3 ELEMENETS OF RUSSIAN CYBER DETERRENCE STRATEGY



SOU

RCE: Drawn by researchers Data Source: (Kari, 2019)

5.5 DETERRENCE IN CYBER SPACE: IMPERATIVES FROM CHINA

From being labelled as a hacker state by the mainstream media to being called out as the most advanced in terms of military capability in cyber space, People's Republic of China has fielded cyber capabilities at various levels of command. In 2015, a substantial reorganization of the armed forces was introduced. Reforms were cut across the entire People's Liberation Army (PLA) with one major reform regarding the establishment of a new service branch called as Strategic Support Force (SSF) as necessary for advancement in the twenty first century warfare, by elevating control of cyber operations to the highest echelons and to ensure a cyber sovereignty for safe guarding the Chinese dream across all domains.

Such military growth and advancement in cyber capabilities have garnered much global attention, on how China would leverage these capabilities in situations short of conflict and for deterrence in peacetime and for deterrence in crisis (Mustafaga, 2023). Much emphasis is also on the wartime operational impacts which could be generated by such an advancement on behalf of China i.e., impacts particularly for the U.S, given the constantly looming threat of an impending cyber war between the two states, provided that both the states have been involved in a persistence engagement with each other within cyber space. In the face of increasing cyber capabilities of China, there has been an escalating rise in the number of cyber disputes between both states in recent years i.e., disputes which have created an environment of deterrence in cyber space. From U.S. perspective as discussed above, deterrence is synonymous to a defensive posture. Contextualization of deterrence from a Chinese perspective however, entails the narrative of 'offense as the best defense' and that of 'coercion', which when applied to cyber space leads to an offensive and an aggressive cyber posture and strategy.

5.5.1 DETERRENCE IN CHINESE STRATEGIC THINKING: DEFINITIONS AND COMPONENTS

The term often equated with deterrence in Chinese perception is 'weishe' while the term 'weishe zhanlue' is used to denote the 'strategy of deterrence.' In a traditional sense, deterrence perspective in Chinese strategic thought can broadly be categorized as being

equivalent to **Thomas Schelling's concept of coercion**, which includes both deterrence and compellence. Quite similar to the Western notion of deterrence, Chinese perspective of deterrence involves the action of dissuading an adversary from doing something, but unlike the Western perspective, Chinese deterrent thinking also involves compelling an adversary to do something i.e., in traditional Chinese strategic thinking, deterrence is not only about **maintaining the status quo** but also involves efforts to **change the status quo**. This entails the conception that for China, deterrence is not only a means for avoiding military conflict but it is also a means of **coercion** (RAND, 2021). In the words of Dean Cheng, 'Chinese see deterrence in both coercive and dissuasive terms' (Cheng, 2018). The coercive side of deterrence can be used as a tool to gain both either political and military advantages.

Deterrence in Sino strategic thinking is linked to actions leading to political objectives with the fundamental purpose being that to influence the enemy's decision-making calculus (Twomey, 2011). For Chinese officials and decision makers, successful deterrence entails three important elements i.e., being an act of political persuasion, an act of psychological warfare and a military strategy, leading way for China to achieve its goals' (Cheng, 2018). This stance is based on Chinese official military doctrines, which provide a series of definitions of deterrence, all entailing one important element, in the face of offensive capability of China.

In terms of PLA military language, deterrence is an act of compellence in order to make the enemy accept one's will. It is also defined as an action utilized to contain enemy's hostile actions (Jixun & Tilin, 2004). Commander Zhao Xijun defines deterrence as 'a continuation of politics' and as 'a military strategy to influence the other side's thinking' as well as a 'a psychological process with the intention to influence the strategic judgement of the other side' (Zhao Xijun, 2004). As per the 2011 PLA definition of deterrence strategy, 'it is the act of displaying or threatening to use armed power in order to compel the enemy to submit.'

Chinese strategic thinking regarding deterrence is fundamentally based on the three **core components** of capabilities, resolve and communication. 2013 edition of PLA's Science of Military Strategy categorize these components as deterrence strength, resolve and information transmission, respectively. **Deterrence strength** refers to the overall capability

and undergirding ability of a state to deter others i.e., the more powerful the deterrence strength is, the greater is the possibility for deterrence activities to succeed.' This capability for deterrence is found in the military realm and is used as an offensive posture, particularly by China in its approach towards deterrence and broader foreign policy (Fangzhou, 2020). In addition to having the strength and capability of deterring, one must also demonstrate a **credible resolve** to use that strength i.e., to make the enemy fearful of potential deterrence. Communication or **information transmission** is an extremely important determinant of successful deterrence.

Overall contextualization of deterrence in Chinese strategic thought entails in it a few essential aspects which greatly unfold the practical approach up taken by China in terms of its strategic deterrence posture, in all of the three recognized domains. Initially it is important to note that, China views deterrence as not an illusionary course of action to avoid a war situation but stresses upon **deterrence signaling** i.e., the realistic it is, the more credible it becomes, thus stimulating the fact the closer to war an event unfolds, the greater is the success rate of deterrence. Upon the basis of such an assumption, it is rather correct to state that Chinese deterrence thinking involves the use of actual attacks intended as '**warning strikes**' to convey to the enemy the maximum resolve in any given conflict (Kaufman & Hartnett, 2016).

This Chinese perspective on deterrence holds true for both kinetic and cyber-attacks, and thereby is characterized as China's posture for '**strategic deterrence**' which steers China's course of action in every domain of strategy other than that of the nuclear (Cunningham, 2022).

5.5.2 CHINESE CONCEPTION OF CYBER SPACE

Before exploring the deterrence posture which China holds in the cyber space, it is necessary to understand the very dynamics of Chinese cyber conception i.e., how China views cyber space as a domain of strategy for the pursual of a deterrence strategy to gain its national objectives. Much like Russia, Chinese activities in cyber space revolve around its conception of 'cyber' as an **information operational zone** with an on-going strategic competition.

From a Chinese perspective, cyber is a small component within a larger operational concept of '**information operations**' (IO) which include electronic warfare, space activities and psychological operations as well, all utilized in coordination as strategic weapons in the overall military capability of China, for attack, defense, deterrence as well as and compellence. Information operations thus, is a broad operational concept in Chinese perspective, centered on defending China's ability to collect, use and share information while influencing the enemy's ability to do the same. Such a perception makes 'cyber space' and 'information space' as the critical resource in modern battlefield to ensure victory (Kitchen, 2022). Cyber in its essence is thereby, viewed by China as the 'tip of the spear' in any future conflict to obtain information superiority via paralyzing command systems of the adversary (Grzegorzewski & Marsh, 2021).

Furthermore, Chinese perception of cyber is focused on cyber space as an 'information space' with '**informatized wars**' i.e., a space used as a means to extend military strategy as well as a battle ground for war itself (Kitchen, 2022). This makes 'cyber space' not only a means of instrument to gain strategic benefits in a competition or a conflict, but the very space for a conflict itself with the use of defensive, offensive and reconnaissance capabilities. This has been displayed in Chinese discipline-centric structure of individual warfare units of cyber, electronic, space and psychological operations, which organized by missions utilized offense and defense.

China has further expanded its comprehension of cyber space with the creation of **Strategic Support Force (SSF)** in 2015. Analysts view the creation of SSF as an enhanced Chinese counterpart to USCYBERCOM. Strategic Support Force (SSF) is a part of China's extensive military reforms, established with the primary responsibility of holding cyber operations, by housing different cyber enabled capabilities for an integrated campaign during wartime. The basic operational organization and structure of SSF is a constituent of two mission divisions i.e., two system departments – Space System Department (SSD) and a **Network System Department (NSD).** While the former focus on functions of command, launch, telemetry and tracking related to outer space, latter has three important missions in direct association with

‘information’ i.e., electronic warfare, psychological operations and specifically cyber operations.

China is said to have in acquirement the most extensive and most practiced cyber capabilities in Asia given that it has a long history of being involved in missions related to cyber and information space. From beginning to implement information warfare (IW) tactics since 1995, China has since then thoroughly improved its military development in aspects related to cyber space. In 2000, it established ‘Net Force’ – a strategic international warfare unit designed to wage combat via computer networks in order to manipulate the enemy information systems. It has also by 2010 developed an ‘information protection base’ for defense and security operations via computers. By 2015, it has established an integrated force for cyber operations only.

5.6 CHINESE CYBER DTERRENCE POSTURE

Cyber space as a domain among the ‘**three warfare**’ is important for China to control the information within China. The control of this information space is considered by China to be as vital as ‘controlling the maritime and air domains in the 18th and 20th century, respectively.’ When it comes to cyber operations within the dynamics of cyberspace realm, **it is much easier to attack than to defend** (Blair, 2010). Such is the Chinese cyber space overall posture in terms of its cyber capabilities which emphasize more on the attack aspect than the defensive aspect. This is mainly true given that the speed of cyber-attacks and the anonymous nature of cyberspace greatly falls in the favor of using offense as this gives an initial advantage in case a conflict unfolds. It also provides a cyber superiority to enable a full spectrum informatized warfare, to deter and to manage escalation (Kitchen, 2022).

Chinese cyber space strategy can be explained through three different time periods i.e., era of offensive dominance (1990s-2008), Cyber offense and deterrence (2009-2014), defense and deterrence (post-2015).

- **OFFENSIVE DOMINANCE**

In early stages of PLA's 'informatization leap forward', Chinese cyber posture emphasized much on cyber offense and preemptive strikes as being effective as a coercive tool in a cyber space strategy given the PLA approach of 'computer network war as an important means for paralyzing the enemy' (Xianoyan, 2002). While USA was focusing on deterrence as a retaliatory tool in cyber space, Chinese leading cyber space strategy was of **offensive dominance** i.e., 'whoever possess superiority in integrated network electronic operations, will possess control and win future wars' (Shengwei, 2008). This **'ideology of the offense'** was Chinese cyber posture from early 1990s to 2008 based on the ideology of 'whoever strikes first prevails' (Yuliangm 2006). One another factor of such offensive posture was that cyber-attacks were perceived as low cost and covert while being extremely destructive at the same time, which would lead China to acquire the upper hand.

- **OFFENSE AND DETERRENCE**

The debate between using defense or offense as the approach in Chinese cyber space began in 2008, after the 'hinge point' in the face of continuous global cyber-attacks, for instance cyber-attacks against Estonia, Georgia, Stuxnet in Iran and PRISM revealed by Snowden. These incidents led to a profound impact on Chinese thinking regarding cyber security, and led a defensive conception to begin given that China too needed to defend itself against such cyber-attacks, and therefore began the idea of **deterrence in cyber space** in Chinese cyber space thinking.

- **DEFENSE AND DETERRENCE**

Since 2015, deterrence in cyber space has become an important and a necessary national security concern in Chinese cyber strategy (Qingling, 2016). From military as well as non-military aspect, for China to develop its cyber deterrence strategy has been emphasized upon since 2015 and it has been debated that China also needs to understand the role of punishment in different kinds of cyber-attacks from other big powers, by emphasis placed on linking China's nuclear deterrence with cyber deterrence. Moreover, since 2015, there have been debates about China creating a balance in hiding and brandishing its capabilities i.e., to perplex and dissuade the enemy, respectively (Yi, 2015).

While China has not openly published an official strategy for cyber space, but there is a wide spread agreement on how China adheres to an offensive and an aggressive cyber behavior, as a way to control the flow of information to and within China in order to ensure domestic stability. It uses military and non-military signals as well as threats of deterrence, compellence, control escalation, signaling and demonstration of resolve as well as attribution as its overall cyber space strategy, which is based on Chinese classical thinking regarding warfare i.e., 'subjugating the enemy's army without fighting' (Mazanex & Thayer, 2015).

Three main reasons why China maintains and utilize an aggressive cyber capability include:

1. Deterrence i.e., to deter other states by infiltrating their critical infrastructure
2. Information i.e., to gain information via espionage
3. Advancement i.e., increased military development
4. Economic growth i.e., to preserve economic gains via commercial espionage.

According to Dan Verton, Chinese cyber war capabilities in the contemporary age of information are the most advanced of all, inculcating methods of industrial espionage and deterrence, which largely presents a threat to the technology leadership to the U.S., and by extension also presents a threat to its national security (Verton, 2008). Chinese capabilities in cyber space thus, are analyzed through a strategic lens and it is argued that the purpose of development of such capabilities and strategies is to deter U.S. and ensure China's ascent to a future super power. According to experts, however whatever the type of strategy, the more powerful the capability is, the better positioned China will be to use it effectively.

5.7 CHINESE DETERRENCE POSTURE IN CYBER SPACE

While deterrence as a concept appears in white papers in China in terms related to nuclear and military forces, cyber space and cyber operations' conceptualization is not in terms of deterrence but rather in terms of security. But nonetheless, Chinese approach of cyber deterrence is not an oversight, given that it is consistent with country's overall foreign policy statements (Vuori, 2022). This is especially true in the era of Xi Jinping, who has overseen the production of cyber strategy for China by enhancing the 'cyber security defense and deterrence capabilities.' This has made cyber defense to become an extremely branch with

PLA, which has been accompanied by legislative policies in China for its cyber security and for its domestic stability as well as for international status and power in its competition with U.S.

As discussed above, Chinese military perspective on deterrence is a broad concept, one with multidimensional set of military and non-military capabilities all of which combine to constitute an approach of '**integrated strategic deterrence'** which is China's conceptualization of the highest level of deterrence with respect to comprehensive national power.

Such an approach has been a crucial component of Chinese military strategy throughout, provided that according to 2013 edition of 'Science of Military Strategy' published by the Academy of Military Science (AMS), China recognizes **three domains of strategy** i.e., nuclear, outer space and cyber-space (Xiaosong, 2013). These three domains are regarded as the new strategic '**triad**' by Chinese military thought and thereby, military strategy including 'deterrence' as a means to gain strategic objectives is utilized in all three domains which includes cyber domain as well, leading to cyber deterrence on behalf of China.

It is a posture acquired by China to pursue its strategic interests across the various domains of strategy, via the use of several types of capabilities i.e., nuclear, conventional, space and cyber capabilities (Chase & Chan, 2016). According to Chinese military perspective as suggested in 2013, Chinese posture of deterrence i.e., of initiative prior to combat, includes 'an integrated and a whole favorable posture by actively seeking initiative in war' as well as expanding deterrence measures i.e., '**by applying military deterrence means in new domains such as outer space and cyber space.'** This will lead to sabotage the war command system of the adversary. In such a scenario, if deterrence fails and a war breaks out, then the attack-defense confrontation will lead to command dominance in cyber space and thus comprehensive dominance in battle field to gain victory over the adversary (Xiaosong, 2013). The offensive nature of China in its advancement in cyber capabilities hence is of no much surprise, given that such a posture directly draws from its very strategic thought i.e., of coercion which includes both the practice of deterring and compelling in cyber space.

According to a definition by AMS in 2013, **cyber deterrence** is 'an action displaying network attack and defense operational capability, alongside a firm resolve for retaliation to forcibly prevent an adversary from carrying a large-scale network attack' (Lindsay, Cheung & Revero, 2015). Deterrence in cyber space is usually the one of punishment given that denial is difficult and not really an option when it comes to security risks.

There are several unique characteristics of deterrence in cyber space which China recognizes. Firstly, China seeks a strategic approach towards deterrence in cyber space in order to deter and dissuade network attack actions. Secondly, Chinese posture recognizes Kinetic attacks as a part of cyber deterrence posture in addition to creating a 'fuzziness of peacetime-wartime boundaries in cyber space.' China recognizes two types of cyber deterrence i.e., **strategic level cyber deterrence** and **tactical level cyber deterrence**. While both the types maintain on containing opponent's 'network attack intention' through the display of 'network attack capability' and 'strategic destruction effect', but the former strategy specifically focuses on deterring largescale cyber-attacks and the latter one focuses on small scale peace-time cyber-attack and defense (Tianliang, 2020).

Cyber deterrence concept in Chinese perspective is changing and evolving given that China's deterrence requirements are increasing i.e., from it being focused solely on the U.S. to the current policy being tilted towards other states as well given the increase in the number of China's potential adversaries in cyber space. Hence, so is evolving Chinese cyber capabilities given that deterrence now requires not only the **demonstration of ability to penetrate** networks but also requires an **ability to generate real effects** i.e., not only instill the fear of retaliation but also credibility, resolve and capabilities to retaliate, for which China has been engaged in the advancing its information operations units with enhanced skills in cyber-espionage and cyber-enabled information operations.

The evolving thinking of Chinese cyber deterrence is further enhanced by the creation of SSF in 2015, which immediately deviates from the 2013 AMS approach of Chinese deterrence, by explicitly making 'deterrence an important content of military strategy on cyber space' which holds great diversity in the very thinking and understanding of cyber deterrence in theory and practice (Shou, 2017). Furthermore, for China, the conception of cyber security also

constitutes the concern for sovereignty in the cyber space. This principle of **cyber sovereignty** is a principle which China has consistently highlighted on Chinese cyber security policy i.e., in **2016 National Cyber space Security Strategy (CCM 2016)** and as well as in the **2017 International Strategy for Cooperation in Cyber space (MFAPRC 2017)**, both of which rank sovereignty as the first priority principle and strategic objective for China in cyber space.

5.8 RUSSIA-CHINA ALLAINCE IN CYBER SPACE

The development of cyber space as a global domain of strategy with contested and competitive state behavior over the past two decades has led the very space to become a new battleground between states and as well as a major foreign policy and a security concern. Information or cyber space is now a domain with primary contestation of values, ideologies and strategic interests which has resulted in a growing cyber space '**Great Game**' in the face of tri-lateral cyber competition between U.S., China and Russia. From conventional domain to cyber space, when it comes to focus on great power competition, the three states i.e., U.S., China and Russia loom large. While U.S. policy is transparent, clear and open regarding its strategy and posture in the cyber space, Russian 'Gerasimov policy' and Chinese conception of 'three triad' presents no official posture of how the militaries of these two states act in cyber space. Furthermore, latter two work in a loose alliance, in covert ways within the very information space to carry information operations as central Russian and Chinese ways of war with cyber applications as central mode and a tool of warfare. This has led the cyber arena to reach the very '**commanding heights of strategic competition**' with both Russia and China viewing themselves as to be currently engaged in a nexus of information warfare against the U.S. Being played out in the cyber realm, this war is the reflection of a **tri-lateral cyber competition** between the three states; with all three utilizing military application as the instrument of war to basically 'defend and advance national interests beyond' via cyber operations. According to the analysis done upon researching the Chinese-Russian cyber space strategies, it can be said that while U.S. is acquiring a defensive posture with advancement in deterrence tactics, but China and Russia are leading offensive and aggressive cyber policies which constitute deterrence as well as compellence as a way to engage the U.S.

asymmetrically in a competition in cyber space, with latter state being in a **Five Eyes Alliance** i.e., UK, Australia, Canada and New Zeeland in the face against the **Sino-Russian bloc.**

As discussed above, within information space, the strategy of 'information warfare' along with 'information security' is a context shared and underpinned by both Russia and China – both defining information space as a space of confrontation between two or more states with the purpose to inflict damage to information systems and processes, as well as on critical infrastructure and resources by undermining political, social and economic systems. Both the states also constitute of massive psychological manipulation campaigns and compellenece behavior in order to destabilize the state and society. Both states use tools of malware software and hacking tools in addition to conducting massive operations within cyber space with determinants of both deterrence and compellence as a way to control the command systems of the enemy.

In case of Russia and China, the one main enemy is the U.S. against which both the states have joined hands in the face of closer ties since 2015. This has attracted quite some speculation about Sino-Russian closer relationship and cooperation in cyber space realm which have further deepened into an alliance, given that since 2015, China-Russian cyber relation has further been marked into a cooperation as a result of a **bi-lateral cyber security deal** which in media is called as the '**non-aggression pact.**' The frame of the pact is largely borrowed from the previous agreement of Shanghai Cooperation Organization (SCO). The effectiveness of the pact lies in the '**pledge not to hack each other.**' The pact between Russia and China in cyber space has two key main features i.e., **mutual assurance on non-aggression** and **language advocating cyber-security.** Another important element illuminated as a key feature in the very said agreement is that of China's and Russian pronounced support for each other for the concept of **cyber sovereignty,** which provides a challenge to U.S. dominance in the international system. Such a **tri-lateral cyber nexus** and arrangement has led to grave implications on the norms of global cyber space and security, which have been explained in the following chapters.

USA has adopted a proactive approach when it comes to countering the Russian cyber threat where the prime factor is the policy of extended deterrence in order to combat the attack on its infrastructure. However considerable attention is being paid to the Chinese threat. In response to this strategy of USA which is not implied in any context is being countered by both Russia and China adopting almost similar approach of framing strategy in implied terms. This trilateral strategic competition or “Cyber Great Game” is leaving multiple consequences on other states which is explained in chapters below.

CHAPTER 6

IMPLICATIONS OF CYBER DETERRENCE STRATEGIES OF USA RUSSIA ANS CHINA

This chapter briefly analyses the impacts that cyber deterrence strategies is leaving on the international order. So far it has been evaluated that somehow a new Cold War has been initiated in cyberspace. However, the international norms have been increased as all of these three states consider it their responsibility to frame strategies in order to established certain norms of acceptable and non-acceptable behavior in international system. This chapter in the second-half analyze the impacts and implications of all three of the stairs including United States of America Russia and China separately not only on their domestic systems but also on the international system.

6.1 INTERNATIONAL SYSTEM AND DETERRENCE STRATEGIES

6.1.1 A NEW COLD WAR?

To protect the critical infrastructures for which states are framing deterrence strategies at the international level indicates an intense competition because of the persistent engagement and the development of offensive capabilities by all of the major powers including China, United States and Russia. This is reflective of a cold conflict in between these powers. In order to protect the critical infrastructure all kinds of tactics are being put in place for example in an article published in the Economist titled as ‘Cyberspace and the state’, heavily criticized the Chinese deterrence strategy of securing their cyberspace by restricting Internet regulation and projecting state sponsored cyber-attacks in order to impose a cost on the adversaries’ infrastructure. In the response of it was decided on part of US government that these Chinese firms would be taken down which is reflective of the frozen conflict that exists in cyberspace is between the major powers. A reputation and credibility crisis is being recreated with the stairs no longer are ready to interest their confidence in the intentions of the other states where every cyber-attack and espionage is being directed by the Western powers towards either Russia and China along with North Korea and Iran and it has also resulted in the increase of likelihood when it comes to cyber conflict prospects. Also, it is being highlighted that

because of the differential approach that each state is injecting in the international digital order and engineering the dynamics in its own favors it is expected that an ideological conflict and psychological war in the information spaces could be triggered. In this case of intense persistent engagement and continuous distress or the lack of confidence the intentions could be misprinted and the flashpoints like that of Taiwan and Pacific arena could trigger a cyber conflict also resulting in a cross-domain implications. It was not a general assessment but a statement given by US Air Force chief of information operations named as Barrington Barrett. It is because of this conflict that some secret traps are being installed by both China and Russia with the strategy of concealing both their identity and attack and thereby polluting the United States infrastructures and also the United States is persistently engaging without any respect and allegiance being shown to the cyber norms of open Internet policy. This spiral of action reaction could likely result in the deterrence instability. Everyone tends to frame its logic in a defensive color and consider their offensive strategies as part of retaliation policy. Some of the stairs like that of China and Russia are taking advantage of attribution problems and the structural contradictions that exist in the cyberspace is whether to comes to the deterrence strategies and it has invited a new strategic competition of building cyber warfare capabilities and to increase the resilience of the critical infrastructures and the Cold War which was long being framed as ideological war could be equated in the cyber spaces to be a word of hostility perceptions and misperceptions (Julian, 2014).

6.1.2 GROWING CYBER LEGALISM

There have been considerable efforts put forth by all of the powers in order to legalize cyberspace is and limit the likelihood of cyber conflict. however still the international cyber legal frameworks rests on the binary of war and peace as per the western strategic doctrine. this has led to pave the way for the clash of interpretations when it comes to legal frameworks and doctrines and sometimes revisionist states draw their own realities this is mainly because of the uncertainty that prevails at the international level in cyberspace is. However, one of the strategic benefits of this cyber legalism is that states are aligning their policies with the adherence to law for example the persistent engagement and forward defense policy of United States of America seems to align with the international law. Also, the parties like

European Union and NATO often frame their strategies and tool boxes in compliance with international law such as that happened in 2019 EU foreign policy. In the legitimacy of international law sometimes these large nations and organizations try to control the trends as per the power politics. however, the other parties see this cyber legalism as the policy of normative imperialism. However, one of the benefits of these cyber legal frameworks growth is that even major powers like that of United States reflect restraint in their policies while using cyber weapons even though the other version is states failed to do so when tactical or strategic considerations supported that (Kellos, 2022).

6.1.3 CHINA RUSSIA ALIGNMENT AND ITS IMPACTS ON TRILATERAL CYBER DETERRENCE DYNAMICS

Both Russia and China consider offensive cyber capabilities, intelligence theft, control over public and private cyberspaces, imposing controls over cyberspaces, inflicting damage on the adversary's critical infrastructures to be vital for their cyber security and also tutor any party from inflicting attack on their systems. Both of the stairs copy each other's style of cyber authoritarianism and install sensors coupled with overthrowing American hegemony in the international digital order. they consider these operations to be an important part of the grey areas strategies and to inflict damage on the United States system. They share a common goal of taming United States control both normatively practically over cyberspace. A whole of government approach is being used by both parties to ensure the success of their cyber enabled foreign influence campaigns and to conduct the operations of hacking and leaking information. They not only carry cyber-attacks but also use their media outlets to conceal the impact and origin of these attacks because of their shared tactical similarities of operational dynamics coupled with their agreement over the norms of Internet operations they were more likely to establish a cooperation in order to tame the United States influence that happened officially in 2015 when they signed an intergovernmental agreement on cooperation and international information security. This agreement gave them a leverage of protection from each other attacks and collaboration in order to this table eyes the digital order that you trying to project also the joint statement given by Putin and Xi Jinping while 2016 visit and on the forum of communication technologies development our security they shared the incentive of

Internet governance mechanisms instalment and the respect towards cyber sovereignty. It was in the year 2019 that they even signed a strategic cooperation agreement and thereby strengthening their cyber systems specially during the testing times of COVID-19. There are certain flaws that lies with the Chinese, Russian alignment that gives a whole for a deterrence stability as both of the parties lack the expertise for effective mechanism building with the China lagging far behind in technical expertise in comparison to Moscow does not have a market leverage. It is because of this alignment that the United States is investing a lot of capital and expertise in strengthening cyber deterrence strategy and using the artificial intelligence technologies for building effective and complex cyber weapons. But it is because of this alignment that both of these parties enjoy two strategic leverage is with the first one is that they keep their attacks below the threshold level so as not to avoid any retaliation and also their propaganda campaigns launched by state medias instantly negate the allegations on part of United States to be hypocritical. this has triggered a situation of perplexity in the international digital order coupled with the fact that the United States convincing power to international firms and corporate sectors that China and Russia being the revisionist stairs in their digital realm has been limited. by far both of the parties have been successful in imposing a cost on United States to build its cyber capabilities unilateral resulting in the failure of the Western powers a strategy to isolate both of the parties in the digital realm. Another implication of this realignment is that there are lots of agreements that United States has conducted with the European powers including the cyber security agreement signed in between Great Britain and United States at the G8 summit. This realignment has resulted in United States considering the options of deterrence by entanglement for which it has conducted cooperation with the Chinese government in the steel sector and also conducted an agreement on cyber security with Putin in 2017 (Arquilla, 2007).

6.1.4 PARTIAL PEACE RESTORATION

One of the considerable advantages of cyber deterrence strategy is the fact that peace has been partially restored constraining many revisionist attitudes and attacks on stairs infrastructures. It is not the matter of perfection that peace is persistent and should always be retained in cyberspace because of deterrence but is the realization that cyber deterrence has been

successful and maintaining peace between three major powers United States of America China and Russia resulting in no big cyber war that could go beyond the cyber domain and boundaries of conflict resulting in many unconventional and conventional implications of cyber attitudes. These deterrence declarations has resulted in a better outcome of temporary yet partial restoration of peace in cyberspace is and also resulted in the protection of national interests and democratic values. The reason for that is even though in case of cyberattack and dissatisfaction with the failure of cyber deterrence strategy sometimes the states does not relinquish all the opportunities that are available for them to take actions and there is likelihood is that consensus of not exploiting the vulnerabilities of other systems based on the reciprocity element have maintained stability in the cyberspace (Segal, 2016).

6.1.5 GROWING TREND OF ACTIVE CYBER DEFENSE STRATEGY IN CYBER SPACES

One of the consequences of these cyber deterrence strategies is that the relevance of active and forward defense also known as persistent engagement has increased and it has increased its relevance as it uses the punishment card in order to constrain any adult on the national infrastructures and one point worth noting is that persistent engagement is not a policy to declare the death of veterans budget it is another part of the strategy to fix the dilemmas that cyber deterrence in the space is have to confront with. Even though the proponents of persistent engagement stability theory consider cyber deterrence to be a problem and unrealistic approach in cyberspace is the truth is that persistent engagement is nothing but a more proactive and muscular form of veterans by denial and punishment approach. This has paved the way for the trend of imposing costs on the adversaries and multiple punishment cards like economic sanctions and criminal indictments are being used in case of non-compliance (Kello,2022).

6.2 CONSEQUENCES OF CHINA, RUSSIA AND US CYBER DETERRENCE STRATEGY ON INTERNATIONAL DIGITAL ORDER

There are multiple consequences being inflicted on the international order because of this trilateral cyber deterrence strategies being framed by different states as at one hand it is unbundling the openness that exists are the international level. China warns to maintain the

ideological leverage in the international digital order while the US concentrates on technical threats being faced by its critical infrastructure. By Also there has been considerable evidence that these deterrence strategies have resulted in the proliferation of actors that exist in the international arena each of which is involved in persistent engagement with the adversary resulting in parallel lines of competition and contestation and has also evaded the element of collaboration and cooperation in the international digital order. Also, the lines in between conventional and cyber capabilities and conflict has been blurred because sometimes kinetic attacks are being used as a means of retaliation and likewise. Where there has been increased revelry mistress and a lack of confidence resulting in misperceptions and perceptions about each other's intentions these strategies rather than creating stability are likely cause of constant conflict that exists in the international digital order. Both policy and pragmatic confusions are being created in not only the national digital circles but also in that of civil society military affairs and the individual ones resulting in constant intelligence leaks stacking off the individual computers and the breach of privacy because of these conflicts. There have also been structural implications of these contestations that exist in between major powers which tend to be detrimental for the security of small states cyberspaces which are often becoming collateral damage in this struggle between giants of the international digital order (Lindsay, 2015).

6.2.1 IMPLICATIONS OF US DETERRENCE STRATEGY

Cyber deterrence strategy of US aims at preventing cyber-attacks whilst promoting stability in the fifth domain via a combination of measures involving diplomatic, legal and military tactics characterized by the use of defensive and offensive capabilities as a deterrent posture. Although the strategy is effective in its goal i.e., deterring cyber threats but it has various implications which are both positive and negative.

1. **INTERNATIONAL NORMS:** One major impact of US cyber deterrence strategy is its leading role in the development of international norms and rules regarding activities in cyber space and cyber security in order to create a more stable and predictable environment for cyber activities. According to a report by Atlantic

Council, U.S. has worked to promote voluntary and non-binary norms for state behaviour in cyber space.

Its potential impact is on international norms and laws regarding cyber space as formulated in 2015 via a report of UN Group of Governmental Experts. When it comes to establishing the norms, U.S. stands at the fore front as being a responsible state as being a hegemon and therefore, U.S. leads the cyber realm in terms of its own cyber policy and strategy which ultimately impacts the state behaviour of other nations in cyber space and as well as shapes the security landscape of cyber space. The deterrence strategy of U.S. in cyber space aims to promote these norms in order to protect the critical infrastructure of the cyber domain by holding accountable the malicious cyber actors and impose consequences for violating the norms for activities such as cyber espionage and cyber-attacks (Council on Foreign Relations, 2019).

2. **INCREASED TENSIONS WITH ADVERSARIES:** For U.S., the focus on cyber security is a way to achieve its strategic objectives in cyber space for which it utilizes a number of tactics and techniques. According to a study by RAND Corporation, the efforts put by U.S. to deter cyber-attacks may have unintended consequences in the face of a cycle of retaliation and escalation which might undermine international and global instability. This ultimately leads to escalated and increased tensions with other nations and adversaries such as China and Russia (2018).
3. **RELATIONS WITH ALLIES:** The use of offensive cyber capabilities as a way to deter against the malicious cyber activities is a part U.S. cyber deterrence posture which has led many of its allies to be hesitant about cooperating with the U.S. U.S. deterrence strategy in cyber space also potentially impacts its allies and partners in terms of international cooperation for security within the cyber space. U.S. has been active in promoting international cyber cooperation via multiple initiatives such as CISA – Cybersecurity and Infrastructure Security Agency to improve cyber intelligence capabilities like shared threat intelligence and also coordinating with international partners (Department of Defence, 2018). This has led to constricted relations with allies as some partners may be hesitant to work with the US due to country's own offensive cyber potentialities, the deployment of which raises concerns

about the escalation in cyber space with unintended consequences. The impact of U.S. cyber deterrence strategy thus is not only for the adversaries in the face of growing escalation but also for allies given the offensive nature of U.S. cyber deterrent posture which promotes the opposite of stability in cyber space (Wilson Centre, 2019).

6.2.2 IMPLICATIONS OF RUSSIAN DETERRENCE STRATEGY

Following are the implications of Russian deterrence strategy mentioned.

1. **GROWING ROLE OF RUSSIA IN INTERNATIONAL CYBER POLITICS:** Domestically Speaking of one of the advantages and implications that cyber deterrence strategy of Russia is it having on the national security is the fact that it has strengthened its bureaucracy so that it could coordinate with the other states. Also, another important advantage an implication that cyber deterrence strategy is having on the Russian role in international cyber politics is the fact that Russia is actively part taking in framing international norms for example it has initiated resolutions on in the field of cyber security in the United nations General Assembly in 2018 that calls for acceptable and responsible state behaviour. It is because of this deterrence strategy that Russia has even modified its behaviour to an extent where it is now considering itself to be a defender of the rule based international order it also is saying that illegal activities should become battered in cyberspace.
2. **GROWING REVISIONISM**: Russia concentrate its deterrence posture on offensive lines and sometimes it also considered war as an instrument to introduce reforms add international level. It is because of these offensive and contentious policies also Russian military that cyberspace has become a central area of contention. The main reason for that is the Russia assigned a vital important to confrontational politics and offensive deterrence posters where it believes in taking pre-emptive strikes because of the belief that it is in constant war with the western powers. These constant confrontational and contentious status posture often pertains and persist the element of terror in cyberspace and keep the flashpoints open such as Ukraine. It is because of these revisionist policies that the Eastern European region which is Russia considered to be its backyard has become the central focus of cyber hotspot where a

war could be initiated an escalated by mere malicious cyberattacks. Also, Russia considers this offensive was sure to be a substitute of conventional means of confrontation. These have awakened the new possibilities of espionage and logic of cyber competition where cyber spaces are being constantly manipulated (Hjelm, 2021).

3. **AGGRAVATING GRIEVANCES WITH ADVERSARIES:** One of the biggest consequences of Russian cyber deterrence strategy is that it has aggravated the geopolitical grievances that Russia Pryor had with the Western powers. the western circles are also frustrated when it comes to the malicious activities that Russia often project towards them constantly in tangling them in this confrontational behaviour in open Internet societies. Western powers often blame the instability in cyberspace is to Russian aggression and considered the continuous violation of international norms and law where it has resulted in castigation of Russia to be a transgressor and the enemy of the Western powers against which they should protect their critical infrastructures. It is because of this fact that whenever a cyber-attack of larger scale magnitude took place and of sophisticated nature it is often attributed to Russian authorities. it is also resulted in the fact that often Russia is kept out of the debates conducted on the norms and institutions of cyberspace that often happens in between democratic partners. This has led to the Russian desire in order to refashion its role in the cyber spaces. The confrontational politics of Russia and the bold deterrence poster used by it often result in the paradox of risk that is defined as a phenomenon where a state in order to avoid direct and larger scale confrontation with the other party often resort to take risk and frame their strategies on confrontational and offensive lines against the order being established many techniques are then employed in order not only to protect the national security interests but also to bypass the systematic and normative trends that exist in the international order either of cyberspaces and other domains. data
4. **CONTESTATION WITH DEMOCRATIC SPIRIT OF INTERNATIONAL ORDER:** Another major impact of Russian cyber strategy is that it stars and share controls to the democratic spirit of Internet opponents and privacy matters in

cyberspace. it is often being estimated that the gains of cyberattacks often are being limited by the cost that far exceeds the benefits of these offensive politics. Russia constantly has to invest in sophisticated technologies that are needed to carry on the deterrence by punishment and deterrence by cost imposition policies that often are likely to drain the economy of the state that that often struggles. this also keeps the door of confrontation open. an example of the economic cost inflicted on the Russian public was the disc location of economic resources resulting in 15% decline in GDP of Russia.

6.2.3 IMPLICATIONS OF CHINESE DETERRENCE STRATEGY

The interconnectedness and ubiquity of computers in the digital age alongside increasing digitalization in global commerce, civil society and military affairs have created crosscutting challenges in the policy directives and security area for international community. Such challenges and confusion are largely acute in the case of China, which has the most active cyber operations programs going on. As outlined in its military doctrine and policies, Chinese cyber deterrence strategy has other various implications of great significance at both international and national level. Cyber space in Chinese strategic discourse is viewed as a domain critical for national defense and thus is a space with active development of capabilities in order to deter potential enemies. Such developments influence the balance of power in cyber space as Chinese robust cyber space capabilities and its very cyber deterrence strategy is viewed as a threat with various implications in several key areas:

1. **NATIONAL AND CYBER SECURITY:** Chinese deterrence strategy in cyber space is aimed at the protection of its own infrastructure and government systems from cyber intrusions (Xi, 2017). This involves the development of defensive capabilities and cyber defence mechanisms such as detection systems and firewalls, as well as the development of offensive capabilities including information espionage, cyber reconnaissance and cyber warfare tactics (Chinese Defense White Paper, 2019). Such developments influence the national security of China itself and as well as endangers the national security of other states, mainly the U.S.

According to U.S. National Security advisor Tom Donilon, the prevalent Chinese cyber operations and intrusions are a major national security concern for U.S. state department. Also, these are a major challenge for firms given the Chinese industrial and commercial cyber espionage campaigns which result in sophisticated and targeted theft of confidential business information and technologies (Donilon, 2013).

2. **MILITARY MODERNIZATION:** The military modernization part of Chinese cyber deterrence strategy involves the active incorporation of offensive cyber capabilities which upon operational planning leverages the capabilities to gain information dominance, degrade enemy's military capabilities during times of conflict and disrupt enemy communications (Department of Defense, 2020). Such developments i.e., militarization of cyber space have grave implications globally but specifically for the balance of power in the Indo-Pacific region as well as affects the military strategies of other nations.
3. **INTERNATIONAL RELATIONS AND GEO-POLITICAL DYNAMICS:** Chinese cyber deterrence strategy has massive implications on the geo-political dynamics of International Relations, given that Chinese state has been accused of engaging in a number of offensive cyber capabilities and activities such as espionage and attacks against other countries. These activities have impacted the geo-political dynamics and diplomatic relations of China with other countries leading to geo-political tensions and conflicts.
4. **CHINA GROWING ROLE IN INTERNATIONAL NORM ESTABLISHMENT:** Chinese cyber deterrence strategy also impacts the development of global cyber norms and governance, with China being an advocate for the development of a new cyber global governance system, the norms of which deviate from the norms put forward by US and other countries. According to Chinese state, state sovereignty, information control and non-interference should be the key approaches in cyber space (Xi, 201). While U.S. and its allies emphasize upon a free and a secure cyber space. Such differing views have led to divergent understandings of cyber behaviour deemed as acceptable and thus has a tendency to lead towards potential conflicts in international cyber relations.

5. **TECHNOLOGY GOVERNANCE:** One major aspect of Chinese cyber deterrence strategy is that of active cyber defense which advocates for cyber sovereignty, and has implications for technology governance at the international level. Cyber sovereignty emphasizes upon the rights of states to regulate and govern cyber space within their territory (East West Institute, 2019). Chinese cyber strategy of cyber sovereignty thus focuses largely on influencing technological movements within its territory and also influence data privacy, data localization, cyber norms and therefore shape the global technological landscape by influencing the technology governance i.e., global cyber policies and regulations. Furthermore, not only on technological governance but the Chinese cyber deterrence strategy also impacts the technological realm in advancement and innovation capabilities, given that China has been actively investing in the development of advanced cyber capabilities such as Artificial intelligence (AI), 5G networks and quantum computing (National Intelligence Council, 2019). These capabilities have increased the threshold of global technology competition.
6. **ECONOMIC AND TRADE RELATIONS:** Chinese cyber strategies also impact its economic and trade relations with the global world, provided that Chinese cyber deterrence strategy also involves economic and commercial espionage alongside operations targeted at intellectual property, trade secrets, trade negotiations and business relationships. All these strategies carried out through the cyber realm aim at the proprietary of information to impact the economic competitiveness while shaping the regional and global economic dynamics (U.S. Trade Representative, 2020).

While most of the impacts resulting in the face of Chinese activities in cyber space and its deterrence strategy in cyber space include direct implications on an unprecedented scale but mainly for the U.S i.e., according to U.S. perception, China has established cyber war military units while simultaneously lacing the U.S. infrastructure with digital bombs. While the chances of a full-fledge cyber war between U.S. and China like U.S.-China conventional war are highly unlikely, but nonetheless, military skirmishes between the two states in cyber realm alongside economically driven proliferation of information technology enables the

emergence of numerous incidents of friction in the face of persistent competition, all of which fall below the threshold of direct violence.

This chapter has descriptively analyzed the implications and consequences that each state cyber deterrence poster is leaving on the international order. however, in the next chapter the need to comparatively analyze the strategies of all three of these states and in order to comprehend better the effectiveness of their strategies a critical appraisal is being carved out.

CHAPTER 7

COMPARITIVE ANALYSIS OF CYBER DETERENCE STRATEGIES: A CRITICAL APPRAISAL

In this chapter in the first section the comparative analysis of the deterrence strategies of all three states in fifth domain has been traced. In the second section the critical appraisal highlighting flaws and problems with Chinese, Russian and US cyber deterrence strategy has been looked into. This chapter the strategies of all three of the states are critically analyzed and issues challenges are also being high lightened.

7.0 COMPARITIVE ANALYSIS OF CYBER DETERRENCE STRATEGIES OF USA/ RUSSIA AND CHINA

The strategic environment in international digital order is characterized by intricate interdependency private and corporate sector dominance or monopoly and individualistic behaviors shaping the dynamics of cyber realm the states has framed their policies in order to counter and that or any attack or malicious activities being projected towards their systems. Each state wants to securitize at cyberspaces and to protect its vulnerabilities being exploited by the adversaries. this information age has changed the dynamics of military conflicts and also that of deterrence concept with you just stared playing its role to frame the norms that exist and could shape the trends in cyber spaces (Thomas, 2001). There has been one established fact in cyber realm that achieving cyber superiority in digital spaces is not a likeable option. transparency and attribution of the attacks is the most important aim of strategists. A comparative analysis of the deterrence strategies and the objectives that stairs want to achieve our being explained in the table below.

7.1 COMPARITIVE ANALYSIS OF DETERRENCE POSTURES

Category	**UNITED STATES**	**RUSSIA**	**CHINA**
Objectives	The goals of cyber deterrence strategy involve 1. Influencing and disrupting the cyber kill chains. 2. Framing acceptable and non-acceptable cyber attitudes 3. Persistently engage and compelling adversary for molding its behavior accordingly 4. Cross domain cyber deterrence strategies to carry out retaliation. 5. Denying access of rivals to critical infrastructure.	The objectives of cyber deterrence strategy of Russia involve 1. Protecting the national interests in cyber spaces 2. To secure information sector at national and private level 3. Inducing disruption in adversary cyber arms development 4. Playing a role in international norms development 5. Deterring any access of unsanctioned nature to critical	There are multiple goals of Chinese cyber deterrence strategy that involves 1. Attaining cyber sovereignty 2. Exercising full control over Chinese cyber spaces. 3. Safeguarding and protecting Cyber and information security 4. Effective executions of offensive operations for deterring adversaries.

		infrastructure	
Institutions	The institutions to execute and frame cyber strategy includes FBI, DHS, NSA, USCYBERCOMMAND, CIA, DoD. Also, the armed force cyber command, marine force cyber fleet and twenty fourth air force	The major bodies responsible for carrying out cyberattacks involves Intelligence agency of the general staff of Russian armed forces also known a GRU, FSB also known as federal security service of Russian federation, Cyber defense Centre established in 2013. Also, the Internet research agency plays an important role	The major role played by MIIT, Commission for science technology and science technology and industry for national defense, Computer network emergency response center technical team.
Lexicons and Terminologies used	The terminology cyber deterrence was coined by US policy makers. All of the terminologies like that of corpulence, persistent engagement, coercion.	In the Russian discourse the information security is the term used quiet often to discuss the deterrence mechanisms and also terms like Third offset strategy and cross domain synergy	The terminologies used in cyber realm for deterrence involves interchangeable use of deterrence coercion, containment
Deterrence Posture	The extended deterrence, deterrence by denial,	The deterrence posture of Russia is	The deterrence posture of Chinese

	punishment, de-legitimization is used considerably	predominantly of offensive nature	strategy entails character of cost imposition, punishment and coercive operations.
Strategy of deterring adversary	The sanctions methodology is used with cross domain character to carry on cyber-attacks. another important element is the persistent engagement etc.	The strategy of interference and information warfare of conducting malicious activities is the most important element of Russian cyber-Deterrence strategy	The policy of exfiltration is used to deter the rival factions in cyber realm.

Source: Data Source: (Thomas, 2001).

7.1 CRITICAL APPRAISAL OF CHINESE CYBER DETERRENCE STRATEGY

7.1.0 VULNERABLE SYSTEMS

The vulnerability of Chinese cyber systems which appears to be unprotected and are prone to exploitation gave the opportunity to western and rivals to launch attacks and project malicious activities towards it. The INFOOPS of Chinese origin which are backed by substantial SIGNIT resources are the strongest in cyber spaces. The excessive reliance on private hackers of Red Hackers alliance makes the system vulnerable and exposed to attacks. Even the target of Chinese CNO tend to be the foreign governments as part of deterrence by cost imposition but before leaving they contaminate the Chinese system. In a bid to build world class cyber force, Chinese systems heavily rely on INFOOPs capabilities (Nagy,2012). There are multiple vulnerabilities in Chinese cyber spaces and these deficiencies become visible when in in 2000 when PLA cyber combat exercises were halted. Most of the denial-of-service attacks are being orchestrated by individual hackers where fairly simple but not

sophisticated ways are being adopted making them more prone to attribution. While comparatively the defensive cyber infrastructure of adversaries are of more sophisticated nature. The cyber offensive capabilities of China are effective only if used pre-emptively (Ball, 2011).

7.1.1 DEFENSE OF FRAGMENTED NATURE

The Chinese command and control system is primarily of Anarchic nature and a large number of attacks are being carried out by private individuals. The Chinese infrastructure have been made prone to hacking by the individuals as per report that came in 203 that about 88 percent increase in the use of internet was witnessed which seems to be unregulated by the Chinese authorities. The computer systems in China are being made prone to exploitation (Hjortdal, 2011). The Chinese cyber policies are illegal and as the use of internet by Chinese individuals has increased it has risked the replacement of liberal norms governing the system with Chinese cyber ethics. So far there seems to be absence of the technical and centralized information network security to back the political ambitions of China. The cyber bureaucracy in China is fragmented that makes the system exposed to private criminal activities. Moreover, the operations conducted by Chinese underground online community could leave impact on the overall system efficiency. The system is fragmented to an extent in China that the hacked and stolen data is being used on online platforms namely Tencent. It was estimated in year 2011 that cost of these private malicious activities extended to be 830 million dollars. The authority of agencies like that of State council are of de-facto nature.

However, according to the recent reports How the Chinese authorities are in the process of building a robust cyberspace and information governance regime that spend over cyber security digital economy and other information aspects. The Chinese ban on the use of HTTP which ensures secure communication for the individuals has been placed in order to retain the governmental authority over the use of Internet by individuals thereby leaving even the governmental websites unencrypted and more prone to exploitation by the international agencies this grey area has been used by western governments such as United States to adopt the strategy of deterrence by delegitimization and to investigate into the Chinese systems

Even the organizations such as PLA the Chinese central governments networks and the ministry of foreign affairs are not being safe.

7.1.2 CHINESE CYBER SPACE EXPLOITATION BY WEST

Chinese cyberspaces are being exploited by the western measurements who differentiate in between the surveillance of systems for profit and for security and have criminalized the Chinese activities are the international level. Recently as per the report from the International Institute for Strategic Studies the Chinese cyber capabilities has been ranked to be of tier two nature. The Chinese cyber spaces are being constantly spied on by United States. There are multiple factors that provide a leverage to the western stairs including the monopoly of western technological firms in the cyber market the one rebel cyber defense system of China and an even development in the industrial sector give a space to the Western powers to exploit the Chinese system. The Chinese espionage is a lack the ability of industrial absorption for which they are being projected and as making the United States cyber intelligence to be more technically adapt and sophisticated.

7.1.3 NEGATIVE TRENDS

It was marked in 2016 cyber security strategy that an intricate link exists in between threat assessment and countries cyber security capabilities where are the Chinese cyber defensive capabilities fragmented and rudimentary nature as part of 2001 survey. Even though by 2017 the joining the government has made considerable efforts in order to structure the cyber security situation and to make the cyber laws clearer and easier to understand but still the attack on the Chinese infrastructure from foreign sources are being frequent which are largely off this denial-of-service nature and also the domestic sources of one row abilities are also being extensive. it was also noted that a majority has been witnessed in the dark web business models and advanced persistent approach of the Western powers is continually threatening the national security of China and its cyberspace its stability (Austin, 2018).

7.2 CRITICAL APPRAISAL OF RUSSSIAN CYBER DETERRENCE STRATEGY

7.2.1 OVER RELIANCE ON OFFENSIVE STYLE OF CYBER DETERRENCE

The Russian style of cyber deterrence is overtly offensive in nature which is demanding a lot of the Russian style of cyber deterrence is overtly offensive in nature. Considerably the focus of Russian strategists is on the offensive cyber operations rather than on building sophisticated weaponry and infrastructure for projecting these operations for example a lot of Russian hackers backed by the Russian intelligence services were being detected and these offensive operations are not sufficient to inflict a proportional damage as expected by the experts. For example, in Estonia even though the 'Denial of Service' attacks inflicted huge damage resulting in shutdown off the countries networks but it led to Estonia restoring its network back on line. These heavy reliance capabilities on the offensive side of Russian weaponry led to the systematic vulnerability and disruptions in the Russian network system and there is a huge risk that these nationalistic hackers would eventually turn up against the state and the national cyber war capabilities should not be entrusted to them. Also, the Russian financial discrepancy is pushing the state backward in deploying finances for defensive cyber weaponry build up (Reveron, 2012).

7.2.2 LACK OF CYBER PORTFOLIO: DOCTRINAL DILEMMAS

There are multiple challenges being faced by the Russian policy which is even long term and coordinated. Russia warns to maintain its sovereignty over digital spaces but the technology is advancing so rapidly that it is becoming difficult for Russia to cope up its legislations with the technological revolution. One of the major one of the major flaws in Russian cyber strategy is it does not address the issue of deterring cyber-attacks separately in a doctrine but still it under the criteria of information warfare and security separate command and control system to ensure cyber security and resilience of the critical infrastructures (Hjelm 2019). Also there has been the lack of consequential understanding of Russian cyber deterrence strategies in the doctrine for example the over reliance on aggressive cyber tactics is resulting in the Russian alienation from the western cyber systems with Russian technological firms facing a reputational and financial damages because of the mistress and between Russia and

the West. there has been no strategy to address this concern in the Russian cyber or information doctrines. every time an attack happens in the western circles it is being attributed and projected towards Russia and its broadcast systems. The only strategy in place is to deny the attacks suspicious being attached to Russia which is no longer effective. Another dilemma of Russian cyber deterrence doctrine is that it lacks clear horizon of another flaw in the Russian cyber deterrence doctrine is that they lack clear and a comprehensive approach on deterring cyberattacks and also lack the ability to frame a proportionate response and retaliation to cyber-attack. Moreover, the Russians are not ready whatever the Russians are not ready to frame a separate doctrine for cyber deterrence as there does not consider it a viable strategy and to retain the possibility to maneuver (Meakins, 2018).

7.2.3 TECHNICAL COMPLEXITY AND FLAWS IN RUSSIAN CYBER-DETERRENCE STRATEGY: DOMESTIC CHALLENGES

There are multiple vulnerabilities that are the Russian system is encountering with. These involves some irrational steps like unplugging the Russian computer is from the global Internet and the decision to move away from the international servers that would expose weaknesses in Russian cyber deterrence strategy to counter the major cyberattacks on its infrastructures. These also exhibited that Russia does not have enough cyber defensive capabilities to counter these threats and deny their access. The 2017 incident of Wannacry attacks heavily impacted the Russian vulnerable system in the corporate sector specially. And sometimes the attacks launched by the Russians often will you would the domestic network systems for example it is expected that NotPetya attacks were orchestrated by Russians living even the Russian natural gas joined Rosenft system being exposed to the damage. The Russian hackers have access to sophisticated cyber weaponry that sometimes the Russian corporate sector find themselves being exposed to these criminal activities resulting in the loss of billions for example as estimated by as Sberbank That about 600 billion rubles were being lost to the cybercrimes also a number of pirated software exist in the Russian cyber infrastructure of Soviet times Also add to another vulnerability. Russia right now is facing a cyber isolation as a lot of countries in Europe allied with the US making it difficult for the

Russian firms like Kaspersky Labs, Group I.B Are often accused of criminal activities and being viewed suspiciously.

7.3 CRITICAL APPRAISAL OF US CYBER DETERRENCE STRATEGY

7.3.1 ATTRIBUTION CHALLENGE

The time of identification and cyber-attack attribution always stand in paradox. The attribution of cyberattacks on which the US cyber deterrence strategy relies heavily is not a visible option at it may take months for the identification of attacker good eating a vacuum difficult for retaliation response to fill and sometimes only attributing the attacker is not sufficient as the policymakers would have to assess the purpose behind the attack and the situation in which the attack took place. The attribution dynamics are being heavily influenced by the purpose behind the attack which sometimes entails the compelling elements for which the communication is a vital ingredient. Another aspect which defines the effectiveness of attribution is the fact that the size of retaliation after attribution should be extensive enough to deter the attacker. Or multiple types of attackers involving the terrorist groups and the private hackers which becomes difficult to our tribute and the ambiguity that comes with the attribution of cyberattacks involves multiple risks. These involves dragging the third party into the conflict which could be risky enough because of the interdependency that exists in the cyberspace. Also the public private divide that exist while are attributing the cyber-attacks is another problem that comes with the framing of United States cyber deterrence strategy because sometimes the investigations being carried out by the private sector contradict with the national level attribution of the cyberattacks resulting in the obstruction of law enforcement and the conduct of military operations an example of which would be fine at the time of attribution investigation being gathered out by the United states counter terrorism operation in 2018 towards Russian firm known as Kaspersky Lab. Also there exist are tendency among the private firms 2 be the first one in investigating the attack which would result in the Russia investigations and inaccuracy that accompany them.

7.3.2 PROBLEM IN DETERRING COUNTER VALUE AND COUNTER MILITARY ATTACKS

There are multiple problems in deterring counter military and counter value attacks sometimes conventional capabilities are being used. for a retaliation response and in order to maintain the principle of reciprocity it becomes difficult for the United States to says the weaponry used in inflicting cyber damage because sometimes kinetic attacks are being used in order to inflict cyber damage because of the blurring lines in between conventional and cyber capabilities especially in case of Russia. It is more over a common perception that uncertainty of war is detrimental for deterrence stability and same is the case with the cyber deterrence stability where counter military cyber capabilities would likely increase the uncertainty of stairs about each other's conventional capabilities and thereby resulting in the failure of deterrence resulting in a cyber war because with increased uncertainty in cyberspace comes more likeability of cyber conflict. another problem being associated with during cyber-attacks involved United States should be able to determine not only the cyber offence of the states but also the conventional capabilities that are sometimes used for framing counter military attacks (Glaser, 2011).

7.3.3 TECHNICAL PROBLEMS

There exists a lot technical problems with the US cyber deterrence strategy that exposes the vulnerabilities that exist in the United States critical infrastructures. In cyberspace is because of different analogy that exist and characterize different cyber threats. At the bubble treasure specific declaratory policy must be put in place in order effectively deterred the cyberattacks. The reason for that is huge cyber threat possess different motivation and different purpose and was a different type of threat to the infrastructure. there exist no clear and coherent mechanism for net assessment of adversaries' capabilities which are essential to shape the principle of proportionality being essential in the deterrence policy another important technical flaw that exist in United States strategy is there exist no coherent and comprehensive mechanism of adversaries' capability analysis which is essential to shape the proportionality aspect of retaliation and cost-imposition. Also, it becomes a difficult list of specific thresholds for cyber-attacks as there are multiple levels of cyber-attack of different

intensity that demands a different kind of response from the system. There exist a lot of ambiguity when it comes to the cyber-attack intensity and as it becomes difficult to establish a holistic threshold for every cyber-attack being directed towards the system these technical difficulties are being faced by The United States cyber deterrence strategy. Also, there is no clear indication in EU S cyber deterrence strategy as to control the escalation of low intensity attacks being turning into high intensity one and running on the escalatory ladder. The United States and policymakers need to coherently decide the proportionality of retaliation in order to deter the cyberattacks at low intensity level and to stock a balance. a lot of sensitive dealing should be set in place in order to control escalation. lastly the important technical difficulty being faced by US cyber deterrence strategy is to device echo horrendous narrative for the third parties being involved in the cyberspace is and the likely possibility of damage being inflicted on their systems which could turn them into adversaries and create friction in the international order. The United States policymakers need to devise a system of protecting the critical infrastructures from these activities (Kuglar, 2017).

7.3.4 PROBLEMS WITH DETERRENCE STRATEGIES OF NORM/ ENTANGLEMENT

One of the major problems with the normal development on verge US cyber deterrence strategy heavily relies on which is the essence of United States extended deterrence policy is faulty in nature as sometimes the private sector is intentionally deny the com that are central to the United States normal development strategy in the cyberspace compliance with the norms in the cyberspace is that sometimes they have a different view over policies like that of encryption. There are multiple incidents and examples in the history involving the Twitter decision to block the intelligence agencies of United States when they demanded information of the users. United States intelligence agency FBI once contested with the private firms over the issue of bypassing encryption. Moreover, sometimes it happens that private companies get in the way of the cyber deterrence strategy by entanglement because they have interests and concerns in every market and government and they don't want to become a tool in the hand of one segment of government.

7.3.5 ISSUES WITH ACTIVE AND PERSISTENT CYBER ENGAGEMENT

One of the central concern and strategy of United States cyber the transporter is that of active cyber defense that involves constant engagement with the adversaries which becomes a sometimes legally questionable and illegitimate because of the constant exploitation of the cyberspaces. Sometimes United States have to adopt some contentious policies like that of hacking back which stands in contestation to the laws like that of Computer Fraud and Abuse 1986 Act. The risks of collateral damage and exploitation of the third-party cyber spaces becomes so vibrant and high that it becomes difficult to avoid them. Another problem accompanied with active cyber defense strategy is the proliferation of actors and their malicious activities that accompany them resulting in not only disruption in the international cyber order but also culminating in two cyber deterrence instability. Sometimes it happens that the intelligence sharing which is vital for the cyber deterrence strategy to work well stand in contradiction with the domestic laws for example the international cyber strategy of United States stands in sheer contradiction with the domestic laws of privacy and antitrust. The United States often awards the public disclosure of attacks on its firms as it might disrupt the reputation of firms resulting in the losses. For example, as per the United States the board in 2019 it was highlighted that the private sector assistant intelligence agencies in information shooting at a minimal level (Lilli, 2017).

7.3.6 INFRASTRUCTURAL PROBLEMS

There are multiple infrastructure problems that involves the lack of commitment and investment on a large scale and to update the technologies. there are multiple developments that are in need as far as to update of infrastructure in cyberspace is concerned that involves test beds development overcoming the current weaknesses in the system and two free network data of more representative nature and adequate strategies of data traffic. Also, the cyber strategy of interest rates is indeed more reliant on defensive capabilities and not the defensive ones and this segment needs improvement and immediate scrutiny. Also there has been no effort on part of the United States to remove the asymmetrical nature of the cyberspace. There exists a strategic advantage in cyberspace for defensive cyber capabilities that is the main reason for the water ability of the cyberspace. It was in 2008 that a large

intrusion took place into the defense department laptops resulting in digital beach head. search incidents are the examples that there exist structural flaws in the cyberspace is at the international level because of the intractability of technological spaces resulting in the upper hand offense in the cyberspaces.

7.3.7 POLITICAL COMPLEXITIES

There exists a narrative that the cyber deterrence strategy of United States does not fill the criteria being drafted by juice at Belgium and the international law as it is neither of the nature to prove its right football personal it is considered to be a last resort by the United States. First of all, the cyber deterrence strategy of United States is not purely on self-defense criteria and its reliance on the element of surprise makes the transparency of this strategy under scrutiny. These strategies would eventually turn United States into a tyrant if executed properly and holistically verge in cyberspace and domain is not possible even for a great power like that of United States because of the intense interdependence that exists in the cyberspace and the domination of the private sector with the lack of any authority at the international level. These vulnerabilities are because of incoherent and rogue behavior in cyber spaces. The persistent engagement considered to be vital for these strategies effectiveness is itself faulty in nature that demands revision. One of the most difficult complexities that demands aversion is the mindset of US policymakers that they are sometimes unwilling to impose the cost on adversaries are the expense of financial expenditures and the willingness to threaten the adversaries by attacking their infrastructure is sometimes missing in US policy circles that results in in effective and delayed retaliation there by imposing a serious reputation yes damage to US cyber deterrence credibility. One of the fundamental problems in the American reluctance is that the belief in US policy circles that retaliation could be costly. They also they believe that diplomatic bargaining tactics are more effective than the military ones and they could tame the adversity with the war of words. This result in the self-deterrence of United States and thereby hindering any effort towards effective cyber deterrence declaratory policy.

7.3.8 COUNTER MEASURES FROM ADVERSARIES AND CYBER DETERRENCE

One of the biggest challenges being faced by the United States of deterrence policy is that sometimes the attackers discussed their identity which eventually leads to attribution problem

by concealing their origin making it difficult for the United States policymakers to frame their retaliation. and sometimes with forensics even if it becomes possible to detect the attacker geographical location it is practically impossible to delve into the intentions of that tag and together if the hardware used was from governmental offices or some private individuals and criminal organizations. This results serious attribution challenges to US cyber deterrence strategy. And sometimes the evidence collection becomes so difficult that the strategy of deterrence but delegitimization and criminal investigation against the attackers becomes ineffective. Another important strategy offered adversaries that pose a threat to US cyber deterrence strategy is the method of attacks cost concealment. Sometimes the attacker is even concealed the attack and it becomes difficult that computer system has been polluted by the virus or a weapon being used by the adversary. Also, there is a technical aspect to this concealment that sometimes it becomes difficult to assess the value of espionage sabotage and psychological operations that happened most of the times in IP theft. A lot of you know it's an institution being established by China in order to reinvent the stolen IP addresses. Thirdly an important strategy being used by adversaries is that they avoid symbolic triggers that could provoke the public of the democracy against the cyber strategies of those stairs, for example an incentive is needed for the public to compromise sometimes its privacy which is essential for the retaliation attack to be framed. The asymmetrical attacks from the adversaries are one of the most dangerous bonds to respond and it could essentially make the deterrence strategy or policy of the defending state specially United States being incredible. this is symmetrical attacks involved ransom activities being projected towards the infrastructure where the other state could not respond well and could not carry on with the principle of reciprocity for example as China does not have its own IP it attacks on the United States IP addresses and any asymmetric and conventional retaliation from United States could result in escalation of the conflict which US policymakers avoid in at all costs. firstly, the salami slicing tactics used by the adversaries in order to inflicted the damage on the United States at a times when the critical infrastructures become vulnerable specially during election could not invite a timely response from the United States policymakers and thereby resulting in the loss of deterrence credibility. The manipulation of the open Society of United States by the adversaries is another tactic being used which becomes difficult for the

policymakers to start again as the United States promotes open Internet and restricts the domestic laws being passed to control the activities in the digital spaces (Andres, 2017).

7.3.9 CYBER VULNERABILITIES AND DETERRENCE STRATEGY

There has been multiple information vulnerabilities created in the national infrastructure as indicated by 1991 landmark National Research council that highlighted the issue of overdependence on the digital infrastructure there are multiple vulnerabilities being associated with a computer systems that makes it difficult to frame deterrence posture The control of supervisory data acquisition systems over proliferation and computer system integration is an another vulnerability that exist in The United states critical infrastructures. There has been wide range of exploitation targeted towards the critical infrastructure for multiple purposes that involves the commercial ransom attacks two individual computer hacking incidents and even at the national level resulting in the shutdown of major firms. The United States system is a soul vulnerable data from private entities to commercial ones and even at the national level there are multiple demonstrations of vulnerabilities experienced over the course of history. Moreover, the United States cyber deterrence strategy has messed with the element that the international digital order is being governed by a symmetrical nature of cyber relations multilateralism intractability and extremely inter-dependent cyberspaces which put the stakes in trusts powers and even the defense systems of multiple countries at risk of conflictual engagements (Sterner, 2011). At the federal level there exist a lack of adequate coordination that could bolster cyber resilience and there are overlapping responsibilities being given to different agencies sometimes resulting in the conflict over the control and supervision of cyber defense missions for example that emerged in between national cyber security and communication intelligence center and other agencies over intelligence gathering at the area of Utah. Sometimes a gap that existed between the national strategic environment and the operational value it widens with the lack of transparency in multiple intelligence agencies like national Security Agency and the dissonance does reflect in DHS not being able to fully supervise the competitive environment for private sector in the Silicon Valley and there is no proper strategy put in place to de-conflict these confrontations. The off the shelf technologies are being constantly used by United States government which

exposes the hardware failures. these facilities could be altered and modified Where almost all of the hardware on which the cyberspaces of United States are being operational were manufactured internationally.

CHAPTER 8

CONCLUSION

With the technological advancements stairs has projected their strategies in the 5th domain there by militarizing the digital spaces but the strategic environment that exists in the 5th domain have some unique elements do it. it is often regarded as a domain being malleable volatile and inter dependent created by human beings in which multiple kinds of actors involving private sector governmental forces and some non-state actors involved. But it is extremely difficult to regard it as a separate domain because of the cross domain features it carries with it. The actors' pluralism along with militarization of this domain has sparked intense strategy competition and increasing the likelihood of clash or conflict in between states. it's because of this threat that states are now making policies to protect their critical infrastructures from any kind of adventurism. to serve this purpose cyber deterrence strategy come comes into play. The purpose of this strategy is to protect the infrastructures from punitive attacks either sophisticated or unsophisticated. and there are multiple types of cyber deterrence strategies that states use to protect their systems from malicious activities and cyber adventurism. However, this concept entered into the discourse of Strategic Studies with an article written by David Ronfeldt and John Arquilla. It was later highlighted that cyber deterrence is a strategy that often does not comply with the structural set up of cyberspaces.

The genesis and evolution elucidated that not only cyber deterrence as a phenomena or strategy has been explained comprehensively thereby highlighting the essential requisites needed to frame a successful cyber deterrence strategy but also the types of cyber deterrence posters that exist. It has also been highlighted that what challenges cyber deterrence as a strategy faced that often makes it a neglected concept in International Relations. As there exist multiple ambiguities in the cyber deterrence phenomena which could not be better explained under the theory of cyber persistent engagement stability. This theory not only explores the issues with cyber deterrence but also suggest some alternatives that could be picked in order to constrain the behavior of the opponent in acceptable manner. In this research work in the second chapter cyber persistent engagement stability theory has been

delved into and also its critical appraisal has been provided US cyber deterrence strategy has been explained comprehensively under different administrations and different types of strategic posture in US cyber strategy has been explained. Fifth-domain has been defined as a digital space contingent as multifaceted T-junction of cyber geography and IT system in the verge not only economic social and political interactions took place but also the military ones. Under these military interactions cyber competition and the possibility of cyber war persists. in the wake of this strategy competition states protect they are critical infrastructures by deterring cyber-attacks. It is often defined as the strategy of defending the system and to maintain the status quo by establishing the phenomena of mutually assured destruction of assets by inflicting a cost on the offender in case of any malicious activity. the components of successful cyber deterrence strategy involve considerable capability to carry out retaliation in case of punitive attack, credibility of the state and the communication of deterrence declaration with the opponent. Other elements that state need to take care of involves attribution signaling and principle of proportionality. There are multiple types of cyber deterrence posters such as deterrence by punishment, by norms development by entanglement by and by cost imposition. However, there are multiple pragmatic technical and conceptual challenges that this phenomenon has to face. It is also an established fact that cyber deterrence as a strategy or phenomena in the discourse of Strategic Studies and pragmatically does not evolve in holistic and coherent manner. Its journey started when it was mentioned for the first time in United States national security strategy and then it developed in different regions as per the strategic requirement of the cyber spaces that exist there.

It has been pointed out that over the course of history cyber deterrence strategy faced multiple challenges and has been exposed to failure for multiple times. the reasons for these challenges and flaws that exist in cyber deterrence strategy has been talked about in cyber persistent engagement stability theory. This theoretical framework not only points out the problems with cyber deterrence strategy that involves multiple structural technical and pragmatic reasons but also provides with some alternatives. cyber persistence has been defined as proactive yet continuous engagement with the adversary by means of tactical bargaining and in order to maintain a tactical advantage. It is also regarded as active defense and forward

defense policy where its roots could be traced back to 1996 in the deception or denial strategy and officially inscribed in the vision of US Cybercom. it is aimed to ultimately shape the strategic environment in fifth domain in the favor of defending state. Its intellectual roots could be traced to madman theory and offence defense balance theory. Also, the Clausewitzian theory carry the central roots of this strategy. It recommends the state to frame their strategies to be of continuous and proactive nature by constantly projecting their power in cyberspace so that they could exploit its environment in one's own favors. It also provides an alternative of espionage and offensive cyber operations and that lies in the persistent engagement with the opponent and threatening the other state with the cross-domain escalation risk factors associated with the conflict. However, this theory treats cyber deterrence as a dilemma that carries a paradoxical relationship with the cyber strategic environment. but it also recommends some ways in which the cyber deterrence theory could be made successful that involves effective communication credibility and capability. This theory also highlights the fact that cyber deterrence could not be possible in the digital space is because the interaction of states even though of contentious nature falls short of the armed conflict usually that makes it difficult for the deterrence poster to maintain. also the issue with cyber deterrence strategy is that it could often escalate into a full blown conflict because of the reciprocal principle that exist or persists in cyberspaces. The problems with the cyber deterrence strategy have been highlighted the primarily includes the problem with the deterrence stability because of the structural reasons. Also, this theory recommends some of the alternatives that states could opt for against deterrence that involves persistent engagement and fait accompli. However, the strategy that this cyber persistent engagement stability theory recommends have some technical problems with it as it also misses out on the private public security dilemma and also does not address the operational aspect of the strategy. However, it has been delved into that digital Pax Americana of United States is in decline because of the offensive capabilities that the rivals has achieved and are getting preemptive strikes in order to limit the US strategic advantage that being a founder of digital space is it carries. There are multiple scholars in the United States that has talked about and addressed the problem of cyber deterrence in the digital spaces. also, it started in the Clinton era when it was highlighted in the national security strategies of 1995 and 1996 that critical

infrastructures must be protected by the during the adversaries. The pattern was then followed by Bush administration where multiple institutions such as DHS FBI and Department of Defense and justice were relegated with this responsibility off countering and constraining the options available for the adversaries in digital spaces it was then followed by Obama administration where most of the cyber deterrence posture was framed on offensive lines followed by trump administration and Biden administration. Also, the types of deterrence posters in the US cyber deterrence strategy has been highlighted with specific emphasis on how United States is countering the Chinese and Russian threats by establishing a threshold and using a cyber command and control system. also, it has been deducted that there exist a balance of offence and defense in US cyber deterrence strategy. The ones pre dominated space by United States is considered to be getting out of the hands of this major power. the reasons for this decline involves' the invention of new technologies new friends the growing cyber powers of other revisionist States and there's like China and Russia along with India and multiple other factors. However, the point is worth noting that United States has long comprehend the concept of cyber deterrence and has maintained a strategic environment in which cyber deterrence strategy flourished. The first wave of cyber deterrence in the United States circles lasted till 1996 where not only cyber deterrence was defined based on the concept of nuclear deterrence but also adversaries has been identified. In the second wave the issues and challenges being faced by United States highlighted while in the third stage a more muscular approach to cyber deterrence also known as cyber persistent engagement was developed. there has been a shift from offensive to defensive end then an offence defense balance in United States deterrence posture. During Clinton administration at first the cyber deterrence phenomena was explained and deterrence strategy started to develop on defensive lines while the Bush administration started framing the strategy on offensive lines by aiming to launch retaliatory attacks and also maintain the balance in between deterrence by punishment and denial while the Obama administration focused a lot on the policy of cyber deterrence. During this administration not only, new bodies were established but also a holistic cyber deterrence strategy was developed which was later given an offensive change in trump administration and for the refined during Biden administration. However, there are many faces of United States cyber deterrence strategy that involves its policy to impose costs

on the parties that inflict damage to its critical infrastructures, bolstering the resilience offers defensive systems so that the access of these parties to the critical infrastructure could be denied and also the strategy of punishing the offender is another vital part of United States policy. United States has also played an important role in the establishment of cyber legal frameworks and also it has maintained multiple bilateral alliances on the principle of extended deterrence. The red lines have been drawn by United States for each of the threat to its critical infrastructure. The United States cyber command and control system is also very strong that involves the bodies like Department of Homeland security Department of Defense and state department. Disable deterrence strategy of United States reflect both defensive and offensive posters and also have important components like attribution retaliation signaling communication with the adversity et cetera however it has framed differential strategies to confront the threat of China and Russian cyber aggression.

The fifth chapter discusses in detail the cyber deterrence postures of Russia and China, and their very conceptualization of cyber as the information space, within which both the states pursue their strategic interests and national objectives via the use of offensive and aggressive cyber strategies constituting of deterrence and compellence. Within the context of Russia, it is argued that Russia does not have a deterrence policy for cyber space due to the very ambiguity of the concept itself, but it does have a strategic posture in cyber space which resembles that of deterrence policy. Thus, Russia has a cyber deterrence behavior in all but name, which is centered around the principle of 'active defense' i.e., Russian being capable enough to defend its interests while responding to any incoming cyber threats. This is the policy based on Russian proportionate and decisive action, for which it utilizes a deterrence strategy mainly centered around the use of offensive cyber capabilities in order to deter the potential adversaries from launching cyber-attacks against Russia itself. The cyber deterrence strategy pursued by Russia relies on a combination of offensive and defensive measures both of which are deployed as tactics to shield the Russian national security interests and critical infrastructure. Offensive measures involve the use of 'information confrontation' and defensive strategy is that of 'information security' – both used by Russia to attack and protect within the cyber realm, respectively. Another key element discussed in the chapter is that of

the development of advanced cyber capabilities by the Russian state, which it uses as offensive means. These capabilities include the use of sophisticated malware and hacktivism. These capabilities enable Russia to launch cyber-attacks and information operations against potential enemies. Russia has invested heavily in defensive measures as well, such as dedicated cyber defense units and vast military and intelligentsia as well as advanced cyber security protocols, to protect its own critical infrastructure from any incoming cyber threats from other states. To achieve this goal, Russia has developed a number of offensive cyber capabilities, including advanced malware and hacking tools, as well as dedicated cyber units within its military and intelligence services. These capabilities are designed to allow Russia to launch cyberattacks against potential adversaries, and to disrupt their operations and infrastructure. The chapter also discusses Russian conception of cyber deterrence as a part of its overall 'strategic deterrence.' Attacks against Ukraine, Georgia and Estonia and the NotPetya campaign, are a few examples mentioned in the chapter to explore the deterrent behavior of Russia in the information space.

Chapter Five also discusses the conception and behavior of Chinese government and PLA in the cyber space or as Chinese call it 'weishe' i.e., the informization space. Cyber space is regarded as a part of its 'three warfare's' or as a part of 'the triad' as a result of which it is considered as a domain of military strategy. In this context of Chinese cyber posture, it is argued that how China does not really have an official cyber strategy but it does possess advanced capabilities which are a combination of offensive and defensive measures, regarded as a 'coercive' posture including both deterrence and Compellence for the pursuit of active defense within the cyber realm. This active defense include the use of sophisticate technology to detect and bloc any threat perception. The use of offense as a part of active defense is also an attitude highlighted in the Chinese character of deterrence, provided that Chinese cyber strategy is an extension of its military strategy which revolves around the classical thought of 'subjugation of the enemy' which within cyber space can happen by the use of information operations and control of command systems of the enemy. Chinese capability of cyber espionage for commercial and industrial purposes has also been discussed in the chapter. The chapter also discusses in detail the evolution of Chinese strategic posture in cyber space

which has evolved from the ‘ideology of the offensive’ to ‘offensive deterrence.’ Furthermore, Sino-Russian alliance in cyber space against their mutual adversary i.e., U.S., has also been explored in the given chapter of the document, provided that both the states have since 2015 agreed on a cyber security deal which includes their mutual understanding on not using offense against one another and to not hack each other’s infrastructure while conspiring against the Five Eyes Alliance states, particularly the United States. In addition to the in-depth exploration of cyber postures and deterrent strategies of the three states i.e., U.S., Russia and China, the implications these strategies inflict have also been discussed in this document. The implications reflect the face of a tri-lateral cyber nexus and a tri-lateral cyber competition with all mentioned states being embedded in a persistent engagement in the cyber space. The result includes grave security concerns for not only the concerned states but for the entire world.

The implications of United States of America Russia and China deterrence strategies has been evaluated. At first it has been identified that because of all three states projecting their powers in cyber domain towards each other a frozen conflict has been paved. some scholars have pointed out that states in order to protect their critical infrastructures are persistently engaging in the cyber domain of not only their alliances and partners but also defending their critical infrastructure by forward engagement in the cyber realm of adversary. It has also been highlighted that can you Cold War has been started in between these three stairs with the many flashpoints such as Ukraine emerged on the scene. however, one of the positive impacts of these states strategies is that new norms has been crafted by all three of the states in order to regard what is acceptable and unacceptable behaviors in the cyber space. all three states are not only playing their role in framing cyber norms but are also passing resolutions in United nations General Assembly. However, the Chinese Russian alignment is leaving implications of giving a strategic advantage to offensive cyber capabilities intelligence theft attribution problems and also majorly speaking overthrowing the American hegemony in cyberspace. The grievances has been aggravated because of the revival of geopolitics in cyberspace which all of the stairs have to suffer with.

It is in the 7th chapter that United States Russian and Chinese deterrence posters has been critically analyzed and a comparison has been drawn in their objectives of the deterrence strategies the institutions that are responsible for framing and executing these policies and the terminologies they use in the discourse for cyber deterrence. The Chinese cyber deterrence strategy has its flaws that includes the vulnerable systems that becomes difficult to defend and the fragmented nature of cyber defense infrastructure as most of the attention is being paid to offensive cyber operations and the negative trends that exist in Chinese cyber command and control system. The Russian cyber deterrence poster involves the problems of over reliance on offensive style of cyber deterrence also there exist a lack of cyber portfolio and doctrinal dilemma as cyber deterrence phenomena has been addressed under the information security paradigm and sometimes the technical complexities that exist often constraint the possibility of cyber deterrence. the problems with the US cyber deterrence strategy includes technical problems attribution challenges problems into turning counter value and counter military threats and multiple infrastructure and political issues. All three major powers deterrence posters when carefully analyzed reveals the fact that the issues and challenges being faced by all three of the states are because of the structural intricacies that exist in cyber domain. this is a domain that is being manipulated by not only state actors but also the individuals and private sector which makes it difficult for one state to achieve preeminence and dominance and ultimate control in the cyber space. The comparison of United States Russia and China deterrence strategies reveals that they have different goals where United States is aiming to constrain and securitize its cyberspace from any malicious activities. it is using its strategic and leverage to persistently engage with the other two powers and using its hegemonic powers to frame norms and behaviors. The objectives of Russian deterrence poster is to protect national interests and to avoid disruptions and the international digital order while also playing its part in the norm development. Similar is the case almost with China where it is trying to attain cyber sovereignty in the wake of digital openness. And intense interconnectedness. The effective execution of offensive operations is then another goal that China is trying to achieve. All three of the stairs has special bodies department and institutions assigned not only to frame the strategies but also to effectively execute where United States of America has institutions like FBI, CIA, DHS. The Russian

cyber deterrence strategy is being framed by bodies like GRU and FSB etc. The Chinese cyber deterrence strategy is being framed by Commission for science technology and industry for National Defense. both of the parties also use different terminologies to address the issue of cyber deterrence. however, all three of the parties have to face multiple challenges in order to sustain their strategies. For China these challenges involve the vulnerable systems and excessive reliance on private hackers of red hackers' alliance which especially become visible in the denial-of-service attacks. The other challenge being faced by Chinese authority is that the defense is off fragmented nature where there exist no explicit cyber deterrence doctrine and posture or thresholds established those Chinese cyber spaces are also being exploited by the Western powers. It comes to the challenges being faced by Russian cyber deterrence strategy these involves its over reliance on the offensive style of deterrence and cost imposition also there exist no cyber portfolio and some doctrinal dilemmas. these issues need to be fixed along with the some of the technical complexities. The challenges faced by United States cyber deterrence strategy involves attribution problems the problems in deterring counter value and counter military tasks some technical issues and difficulty in unilateral establishment of norms and acceptable behaviors.

Disabled veterans is a complex phenomena that demands a lot of care and consciousness with the in depth analysis of the cyber strategic environment but still this strategy is relevant as far as United States is persistently engaging with China and Russia after their cyber realignment and using this strategy as a tool to counter and deterred attacks on its critical infrastructures projected by the revisionist states of the international digital order.

However it has been suggested that the problems in at first the cyber persistence theory that is the theoretical paradigm used to analyze the cyber dilemmas needs revision as it focuses only on one perspective. following are the suggestions and recommendations given in the wake of improvements in cyber persistent engagement stability theory

- This theoretical perspective primarily focuses on the US centric perspective focuses primarily on US centric perspective. It only deals with the feasibility of persistent engagement strategy for the United States of America but not for the other States and

does not generically elaborate the relevance of the strategies recommended in this theoretical framework four other states.

- Also, in this theoretical framework the prime focus has been on the attackers' cognitive mindset and perspective but not on how the other state with the witch the former one is engaging will respond. This is a major problem that needs to be reevaluated an attacker's perspective should not only be given prime attention while the defender perspective should also be taken into account.
- This theoretical framework should also shed light on the problems of private sector and how the strategy is that it often recommends would likely be of disastrous impact for the private sector especially of the individual.

Nevertheless, this theory comprehensively analyzes the problems with the cyber deterrence which exist in reality but it fails to bury the phenomena and strategy as states like United States of America Russia and China are still practicing these policies and are still interested when it comes to deterring cyber-attacks on their critical infrastructures. However, while doing so they faced many challenges that needs to be fixed. for example, for the challenges faced by United States of America in executing cyber deterrence strategy could be fixed in the following ways

- rather than focusing on the attribution of attack after it happens the United States should act preemptively and detect the cyber-attack before it happens.
- where it should focus on offensive side of the deterrence poster a considerable attention should be paid to fix the vulnerabilities in the system and the technical problems that exist.
- it should also ensure that the allies are in confidence when it persistently engage with the adversaries.

The deterrence strategy of Russian Federation also needs revision for which the following suggestions are given

- Russian Federation should focus on building a cyber deterrence posture and focus should paid on it separately in doctrines apart from information warfare perspective

- The Russian Federation should also focus on bolstering defense as its prime focus has been cyber aggression and contentious cyber policies.
- New sophisticated technologies should be evolved and Russia should avoid cyber isolation at all cost by participating more in cyber norms debates.

As for the Chinese cyber deterrence strategy the following methodology is could work well

- China should retain a soft washer at international level while denying the access to its critical infrastructures as it has always focused on the offensive line of its deterrence policy.
- China should also play a considerable attention to its vulnerable systems and increase their resilience.
- Cyber deference problem should be died separately in a doctrine where cyber thresholds should be established.

This research work has not only explained the cyber that runs phenomena elaborately by highlighting its characteristics purposes types but also it has analyzed the problems of cyber deterrence with one of the emerging theoretical paradigms of cyber persistent engagement stability theory. This research work has also analyzed that cyber persistence theory does not perfectly and comprehensively explains the dilemmas of cyber deterrence strategy and it is a policy that still persist in spite of its non-compliance with the systematic intricacies of the cyber domain. it has also descriptively mentioned the cyber deterrence posters of all three of the stairs including United States of America China and Russia but it has also the value added the implications comparative analysis and critical scrutiny of their deterrence policies.

References

Akdag, Y. (2017). Cyber Deterrence against Cyberwar between the United States and China: A Power Transition Theory Perspective. *Digital Commons, University of South Florida.* Retrieved from: https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=8190&context=etd

Austin, G. (2017). Cyber Security in China: The Next Wave. *Springer*. Retrieved from: https://link.springer.com/book/10.1007/978-3-319-68436-9

Andres, R. (2017). Cyber Gray Space Deterrence. *Institute for National Security.* Retrieved from: https://cco.ndu.edu/PRISM-7-2/Article/1401927/cyber-gray-space-deterrence/

Arquilla, J. (2007). In Athens Camp: preparing for conflict in the Information Age. *RAND Corporation.* Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.rand.org/pubs/monograph_reports/MR880.html&ved=2ahUKEwjX1oDsqNL-AhXtgP0HHbfUCQYQFnoECBIQAQ&usg=AOvVaw0YRLgi-NnAaPapaARqiqwg

Burton, J. (2018). Cyber Deterrence: A Comprehensive Approach? *CCDCOE*. Retrieved from: https://www.ccdcoe.org/library/publications/cyber-deterrence-a-comprehensive-approach/

Brantly,A.(2018). The Cyber deterrence Problem. *Department of Political science, Virginia Polytechnic and state university.* Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.amazon.com/Cyber-Deterrence-Problem-Aaron-Brantly/dp/1786615657&ved=2ahUKEwiettfIkYf9AhVFDOwKHRFoDikQFnoECBAQAQ&usg=AOvVaw1tIvbT3C3Gh4I_ldCqID2E

Burton, J. (2018). Cyber Deterrence: A Comprehensive Approach? *CCDCOE*. Retrieved from: https://ccdcoe.org/uploads/2018/10/BURTON_Cyber_Deterrence_paper_April2018.pdf

Brantly, A. (2018). Conceptualizing Cyber Deterrence by Entanglement. *The University of Oklahoma.* Retrieved from: https://www.ou.edu/cis/research/cyber-governance-and-policy-center/the-cyber-governance-blog/conceptualizing-cyber-deterrence-by-entanglement

Bates, C. (2022). Deterrence Thru Transparent Offensive Cyber persistence. *The Cyber Defense Review*. Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.jstor.org/stable/48703302&ved=2ahUKEwjY5sPGr43-AhX27bsIHUlSDpUQFnoECAwQAQ&usg=AOvVaw2-qEA8a6zzQ4I70sZShJg_

Boys, J. (2018). The Clinton administration development and implementation of cyber security strategy. *Intelligence and national security*. Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.tandfonline.com/doi/full/10.1080/02684527.2018.1449369&ved=2ahUKEwigv9XGov_9AhWV-LsIHfswD2IQFnoECA4QAQ&usg=AOvVaw15eSDlmg1WiSCzWU6-TLXD

Bruusgaard, V, K. (2016). Russian Strategic Deterrence. *Survival*. Retrieved from: https://www.tandfonline.com/doi/pdf/10.1080/00396338.2016.1207945?needAccess=true

Ball, D. (2011). China's Cyber Warfare Capabilities. *Institute of Regional Security*. Retrieved from: https://www.jstor.org/stable/pdf/26461991.pdf?refreqid=excelsior%3A28fefd86717df944520ead21779cfeec&ab_segments=&origin=&initiator=&acceptTC=1

Borogan, I. (2018). Russian Approach to Cyber: the best defense is good offense. *European Union Institute for Security Studies*. Retrieved from: https://apps.dtic.mil/sti/pdfs/AD1019062.pdf

Ball, D. (2011). Chinese Cyber warfare capabilities. *Institute of regional security*. Retrieved from: https://indianstrategicknowledgeonline.com/web/IB-323_China%E2%80%99s-Developing-Cyber-Warfare-Capabilities.pdf

Casapoglu, C. (2017). Cyber Security: Understanding the Fifth Domain. *EDAM*. Retrieved from: https://www.jstor.org/stable/resrep14048?seq=1#metadata_info_tab_contents

CCDCOE. (2021). Russia's Strategy in Cyberspace. *NATO Strategic Communications Centre of Excellence*. Retrieved from: https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_15-06-2021.pdf

Caudill, S, & Healey, J. (2020). Success of persistent engagement in Cyberspace. *Strategic Studies Quarterly- Policy forum.* Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-14_Issue-1/Healey.pdf&ved=2ahUKEwj5nejm2dD7AhV7gv0HHY9kDY8QFnoECA4QAQ&usg=AOvVaw05zlOvMycqvANFvxA5gCO3

Chace, J. (2022). US Warfare Within the Fifth Domain: Deterring Russian Cyber aggression. *Helms School of Government: Liberty University.* Retrieved from: https://digitalcommons.liberty.edu/cgi/viewcontent.cgi?article=1267&context=hsgconference

Connell, M. & Vogler, S. (2017). Russia's Approach to Cyber Warfare. *CNA Analysis and Solutions.* Retrieved from: https://www.cna.org/archive/CNA_Files/pdf/dop-2016-u-014231-1rev.pdf

Chase, M. & Chan A. (2016). China's Evolving Approach to "Integrated Strategic Deterrence." *RAND Corporation.* Retrieved from: https://www.rand.org/pubs/research_reports/RR1366.html

Carter, L, C. (2021). Reading the Tea Leaves: Understanding Chinese Deterrence Signaling. *National Defense University Press.* Retrieved from: https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2808049/reading-the-tea-leaves-understanding-chinese-deterrence-signaling/

China Defense White Paper. (2019). China's National Defense in the New Era. *State Council Information Office.* Retrieved from: https://www.airuniversity.af.edu/Portals/10/CASI/documents/Translations/2019-07%20PRC%20White%20Paper%20on%20National%20Defense%20in%20the%20New%20Era.pdf?ver=akpbGkO5ogbDPPbflQkb5A%3D%3D

Council on Foreign Relations. (2020). Cyber Operations Tracker: China. Retrieved from https://www.cfr.org/interactive/cyber-operations/china

Council on Foreign Relations. (2019). US Cyber Diplomacy and Strategy. Retrieved from: https://www.cfr.org/backgrounder/us-cyber-diplomacy-and-strategy

Devanny, J. (2021). Madman Theory or Persistent Engagement? The coherence of US Cyber Strategy under Trump. *Journal of applied Security Research.* Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.tandfonline.com/doi/abs/10.1080/19361610.2021.1872359&ved=2ahUKEwjFlaqr2tD7AhUahf0HHQ3ID8kQFnoECA4QAQ&usg=AOvVaw35SlxGP-WgI86s_b-xEAVy

Dykstra, J & Met, J. (2022). Sludge for Good: Slowing and imposing costs on cyber attackers. *John Hopkins Bloomberg school of public health.* Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://nsarchive.gwu.edu/sites/default/files/documents/rmsj3h-751x3/2022-11-29-arXiv-Sludge-for-Good-Slowing-and-Imposing-Costs-on-Cyber-Attackers-Cornell%2520Tech.pdf&ved=2ahUKEwjApdiNof_9AhWVhP0HHbSdAgsQFnoECBIQBg&usg=AOvVaw3HH9_3M2bwUgeKPHbm54PK

Dr. Saalman, L. (2017). Rethinking China-Russia -U.S. Deterrence in Cyber Space. *Think China– University of Copenhagen.* Retrieved from: https://www.thinkchina.ku.dk/documents/ThinkChina.dk_Policy_Brief__Rethinking_China-Russia-U.S._Deterrence_in_Cyberspace.pdf

Davis, E. (2021). Shadow Warfare: Cyberwar Policy in the United States Russia and China. Rowman & Littlefield London. Retrieved from: https://rowman.com/ISBN/9781538149676/Shadow-Warfare-Cyberwar-Policy-in-the-United-States-Russia-and-China

Domingo, C, F. (2016). Conquering a new domain: Explaining Great power Competition in cyberspace. *Academia.* Retrieved from: https://www.academia.edu/12966842/Explaining_Great_Power_Competition_in_Cyberspace

Department of Defense. (2020). Military and Security Developments Involving the People's Republic of China. *Office of the Secretary of Defense.* Retrieved from: https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF

Ecke, M. (2018). Clausewitzian Cyber Strategy. *Tufts University*. Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.cs.tufts.edu/comp/116/archive/fall2018/mecke.pdf&ved=2ahUKEwizrOrD2tD7AhUwhv0HHX5qDaEQFnoECBQQAQ&usg=AOvVaw1S_f1umWydmr30rXViDfQt

Ellis, M & Carmack, D. (2021). For Cybersecurity, the best defense is good offense. *Centre for technology policy.* Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.heritage.org/technology/report/cybersecurity-the-best-defense-good-offense%23:~:text%3DAlthough%2520the%2520Administration%2520should%2520continue,these%2520efforts%2520are%2520not%2520sufficient.&ved=2ahUKEwi_6qWZov_9AhWDhv0HHeFWAu4QFnoECA0QBQ&usg=AOvVaw0N_T1biT0iInWAvPrTtKdW

Ellinger, E. (2022). Competition and restraint in Cyber space: The role of international norms in promoting international security. *RAND Corporation.* Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.rand.org/pubs/research_reports/RRA1180-1.html&ved=2ahUKEwjeqdzNoP_9AhV1_7sIHUGoDBUQFnoECBUQAQ&usg=AOvVaw0sLODOJir_x713CMQ07SXA

Fischerkeller, M. (2022). Cyber operations could lead to accidental escalation in militarized crisis. *Government matters broadcast group.* Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://govmatters.tv/tag/michael-fischerkeller/&ved=2ahUKEwiyyaj32tD7AhVk_7sIHZ0cCUUQFnoECC0QAQ&usg=AOvVaw2tfvRvYZaj0PH0r6ckcJ8G

Fischerkeller, M, Harknett, R, & Goldman, E. (2022). Cyber persistence theory: Redefining National Security in Cyber space. *University of Oxford.* Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://academic.oup.com/book/41918&ved=2ahUKEwjfwr6F29D7AhVU7rsIHVE7BQgQFnoECC8QAQ&usg=AOvVaw158vosqdmBbS1LR2sHFgjR

Fischerkeller, M, & Harknett, R. (2017). Deterrence is not a credible strategy for Cyber space. *Foreign policy research institute by Elsevier Ltd.* Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.jstor.org/stable/pdf/resrep22904.3.pdf&ved=2ahUKEwiCsvS72dD7AhXI_7sIHfeLBc8QFnoECC0QAQ&usg=AOvVaw2oPzWzBgX9ii2jHxKFpUGE

Fidler, D. (2020). President Trump legacy on Cyber space policy. *Council on Foreign Relations.* Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.cfr.org/blog/president-trumps-legacy-cyberspace-policy%3Famp&ved=2ahUKEwjnxojNof_9AhUZg_0HHZTHBCUQFnoECB4QAQ&usg=AOvVaw17b691TWgeX948D7I-j_Gt

Fischerkeller, P, M. & Harknett, J, R. (2020). Cyber Persistence Theory, Intelligence Contests and Strategic Competition. *Institute for Defense Analyses (IDA).* Retrieved from: https://apps.dtic.mil/sti/pdfs/AD1118679.pdf

Frear, T., Kulesa, L. & Raynova, D. (2018). Russia and NATO: How to overcome deterrence instability? *European Leadership Network.* Retrieved from: https://www.europeanleadershipnetwork.org/report/russia-and-nato-how-to-overcome-deterrence-instability/

Fidler, D. P. (2017). Cybersecurity and International Relations: US Efforts to Secure the Information Age. *Polity.*

Gorwa, R. & Smeets, M. (2019). Cyber Conflict in Political Science. *SOC ARXIVE.* Retrieved from: https://osf.io/preprints/socarxiv/fc6sg

Gold, J. (2020). The Five Eyes and Offensive Cyber Capabilities: Building a 'Cyber Deterrence Initiative'. *CCDCOE.* Retrieved from: file:///C:/Users/User/Downloads/Five-Eyes-and-Offensive-Cyber-Capabilities%20(1).pdf

Gori,B. (2022). From Kinetic to cyber attacks and back: The Israeli approach to deterrence in cyberspace and the multi-dimensional threats to Hamas. *Centre for cyber security and IR studies.* retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.cssii.unifi.it/upload/sub/Pubblicazioni/2022_Gori_Beatrice.pdf&ved=2ahUKEwikq-ybkof9AhUUPuwKHfAwBYEQFnoECBIQAQ&usg=AOvVaw0FZeI3XNwLTI-tQ6F-GpuT

Goyachayev, R. (2017). Cyber Deterrence and Stability: Assessing Cyber Weapons Analogues through Existing WMD deterrence and Arms Control Regimes. *Pacific Northwest National Laboratory.* Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-26932.pdf&ved=2ahUKEwj66tXcnP_9AhXHgf0HHbl0Bj0QFnoECAwQAQ&usg=AOvVaw3fF2LdVKbzfrk_etEoJyU_

Goldman, E. (2020). From Reaction to Action: Adopting a Competitive Posture In Cyber Diplomacy. *Texas National Security Review.* Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://tnsr.org/wp-content/uploads/2020/09/TNSR-Vol3-Iss4-Goldman.pdf&ved=2ahUKEwjL8azEnP_9AhVPhv0HHXPpDNwQFnoECBIQAQ&usg=AOvVaw1OoAYWEEC16F0LzmJwQEP1

Giles, K. (2016). Handbook of Russian Information Warfare. *NATO Defense College.* Retrieved from: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/NDC%20fm_9.pdf

Glaser, C. (2011). Deterrence of Cyber Attacks and US national Security. *Elliot School of International affairs.* Retrieved from: https://cspri.seas.gwu.edu/sites/g/files/zaxdzs4106/f/downloads/2011-5_cyber_deterrence_and_security_glaser_0.pdf

Goldsmith, J. L. (2018). Governing the Internet: Power, Law, and Technology. *Cambridge University Press.*

Healey, j. & Caudill, S. (2020). Success of persistent engagement in Cyberspace. *Strategic Studies Quarterly Policy Forum.*

Hjelm, M. (2021). Projecting Power in the Fifth Domain. *Swedish Defense University*. Retrieved from: https://www.diva-portal.org/smash/get/diva2:1564267/FULLTEXT01.pdf

Hoffman, C. (2019). Is Cyber Strategy Possible? *The Washington Quarterly.* Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.tandfonline.com/doi/full/10.1080/0163660X.2019.1593665%23:~:text%3DCyber%2520deterrence%2520in%2520the%2520narrowest,broadly%2520presents%2520a%2520trickier%2520problem.&ved=2ahUKEwjSjJ2J2tD7AhUFgP0HHexpD-sQFnoECA0QBQ&usg=AOvVaw3h1k5hGbNGlrpgTOlMBWjy

Healey, J. (2019). The implications of persistent (and permanent) engagement in cyber space. *Journal of Cyber Security: School of International and Public affairs Colombia University.* Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://academic.oup.com/cybersecurity/article/5/1/tyz008/5554878&ved=2ahUKEwii94v82dD7AhXGiv0HHd1HAAgQFnoECAwQAQ&usg=AOvVaw2PuDPIBHWpanMPfqvu8c9s

Hardin, B. (2016). Cyber Deterrence. *Air University*. Retrieved from; https://apps.dtic.mil/sti/pdfs/AD1037682.pdf

Harknett, R, & Fischerkeller, M. (2019). Persistent Engagement Agreed competition and Cyber Space Interaction Dynamics and Escalation. *Institute for Defense Analysis.* Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://cyberdefensereview.army.mil/Portals/6/CDR-SE_S5-P3-Fischerkeller.pdf&ved=2ahUKEwivrKPDqo3-AhU-gf0HHSTmCdsQFnoECA4QAQ&usg=AOvVaw2ioD5YUgOM13RSJ9t7tbyo

Hjortdal, M. (2011). China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence. *Journal of Strategic Security*. Retrieved from: https://www.jstor.org/stable/pdf/26463924.pdf?refreqid=excelsior%3Aa14dddf9feff4363dfcaa619bd1a7769&ab_segments=&origin=&initiator=

Hakala, J. & Melnychuk, J. (2021). Russia's Strategy in Cyberspace. *NATO Strategic Communications Centre of Excellence*. Retrieved from: https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_11-06-2021-4f4ce.pdf

Hjortdal, M. (2011). China use of cyber warfare. *University of South Florida*. Retrieved from: https://www.jstor.org/stable/26463924

Hjelm, M. (2019). Moscow Digital Offensive Building Sovereignty in Cyber space. *Technology and Cyber security policy*. Retrieved from: https://www.foi.se/rest-api/report/FOI%20Memo%207521

Hjelm, M. (2021). Moscow Digital Offensive Building Sovereignty in Cyberspace. *Swedish Defence Research Agency:* Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.foi.se/rest-api/report/FOI%2520Memo%25207521&ved=2ahUKEwiwx5bPqNL-AhXLhP0HHSl9DhwQFnoECAsQAQ&usg=AOvVaw1Jo8OwEmERVNFee47j_v_m

Ibrahim, A. (2022). Israel Cyber Prowess: A benchmark in Cyber warfare. *Centre for strategic and contemporary research.* Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://cscr.pk/explore/themes/defense-security/israels-cyber-prowess-a-benchmark-in-cyber-warfare/%23:~:text%3DToday%252C%2520with%2520470%2520cyber%252Dsecurity,private%2520investment%2520in%2520cyber%2520security.&ved=2ahUKEwi31NeLkof9AhUWrqQKHVMyBBgQFnoECBIQBQ&usg=AOvVaw2kL3xxeg3_L1yw8XIU7R7i

Iasiello, E. (2018). Is Cyber Deterrence an Illusory Course of Action? Air University. Retrieved from: https://www.airuniversity.af.edu/Portals/10/ASPJ_French/journals_E/Volume-09_Issue-1/iasiello_e.pdf

Julian, R. (2014). A new Cold War? Russia China The US and Cyber War. *Palgrave.* Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://link.springer.com/chapter/10.1057/9781137399625_4&ved=2ahUKEwjvwajnxY7-AhUI_qQKHQ-VA2gQFnoECAkQAQ&usg=AOvVaw0sVGYh4BrGIf7tumlHvKgV

Jiang, T. (2019). From Offense Dominance to Deterrence: China's Evolving Strategic Thinking on Cyberwar. *Chinese Journal of International Review.* Retrieved from: https://www.worldscientific.com/doi/pdf/10.1142/S2630531319500021

Jaitner, M. (2016). Applying Principles of Reflexive Control in Information and Cyber Operations. *Research Gate*. Retrieved from: https://www.researchgate.net/publication/311983748_Applying_Principles_of_Reflexive_Control_in_Information_and_Cyber_Operations

Jr, P. (2018). Crossing the Line. *The International Lawyer*. Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.thriftbooks.com/w/crossing-the-line_jr-roberts/726146/&ved=2ahUKEwj-1orin__9AhUegP0HHTlSCPkQFnoECAoQAQ&usg=AOvVaw3gg8eh_U1bSZwP5jM7VWgm

Joe, D. (2022). Madman theory or persistent engagement? The coherence of US cyber strategy under Trump. *Journal of applied security research.* Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.tandfonline.com/doi/abs/10.1080/19361610.2021.1872359&ved=2ahUKEwiXtuHoof_9AhVZhP0HHcHzADgQFnoECAwQAQ&usg=AOvVaw35SlxGP-WgI86s_b-xEAVy

James A. Lewis. (2015). Deterrence in the Cyber Age. *CSIS*. Retrieved from: https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/141117_Lewis.pdf

Jiang,T.(2019). From Offense Dominance to Deterrence: China's evolving strategic thinking on cyber war. *School of international and public affairs Shanghai International Studies University.* Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.worldscientific.com/doi/pdf/10.1142/

S2630531319500021&ved=2ahUKEwjhreG4kof9AhXN3KQKHfUfCW0QFnoECBMQAQ&usg=AOvVaw3Yz8-39aputoaqdSgwOA_

Jensen, E. (2012). Cyber Deterrence. *Emory International law Review.* Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://scholarlycommons.law.emory.edu/cgi/viewcontent.cgi%3Farticle%3D1071%26context%3Deilr&ved=2ahUKEwjSgsr7j4f9AhVlxgIHHSL1BcoQFnoECA8QAQ&usg=AOvVaw3vgyMGZKxjC2H2vPrKM0cV

Jian, T. (2019). From Offense Dominance to Deterrence: China's Evolving Strategic Thinking on Cyberwar. *Chinese Journal of International Review.* Retrieved from: https://www.worldscientific.com/doi/pdf/10.1142/S2630531319500021

Julian, R. (2014). A new Cold War? Russia China The US and Cyber War. *Palgrave.* Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://link.springer.com/chapter/10.1057/9781137399625_4&ved=2ahUKEwjvwajnxY7-AhUI_qQKHQ-VA2gQFnoECAkQAQ&usg=AOvVaw0sVGYh4BrGIf7tumlHvKgV

Knake, R. & Clarke, R. (2019). The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats.

Kostyuk, N. (2021). Deterrence in the Cyber Realm: Public versus Private Cyber Capacity. *International Studies Quarterly.* Retrieved from: https://academic-oup-com.eres.qnl.qa/isq/article/65/4/1151/6287900

Kugler, R. (2009). Deterrence of Cyber Attacks. *Potomac books, University of Nebraska Press.* Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-13.pdf%3Fver%3D2017-06-16-115053-773&ved=2ahUKEwiCiq7MkIf9AhVOPewKHUnaA5AQFnoECAwQAQ&usg=AOvVaw10_mXXPJZj8S30husl_98s

Kari,M.(2022).The Cumulative Cyber Deterrence. *Finish National Defense University*. Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.tandfonline.com/doi/full/10.1080/01402390.2015.1115975&ved=2ahUKEwiyzNupkof9AhXBO-wKHTugCrEQFnoECBIQAQ&usg=AOvVaw2S2Ia1UQ3OtuxdNe4YjfGC

Kugler, L, R. (2009). Deterrence of Cyber Attacks. *University of Nebraska Press.* Retrieved from: file:///C:/Users/User/Downloads/deterrence-of-cyber-attacks%20(1).pdf

Kasapoglu, C. (2017). Cyber Security: Understanding the Fifth Domain. EDAM. Retrieved from: https://www.jstor.org/stable/resrep14048#metadata_info_tab_contents

Kumar. (2019). Credible Cyber deterrence in Armed forces of India. *Vivikananda International Foundation.* Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.vifindia.org/sites/default/files/Credible-Cyber-Deterrence-in-Armed-Forces-of-India_0.pdf&ved=2ahUKEwjHm-fdkof9AhUSHewKHUjCCcUQFnoECBsQAQ&usg=AOvVaw23m8Mpzt9IKgy2jSZuDjd6

Kello, L. (2017). The Security Dilemma of Cyber space: Ancient Logic, New problems. *Lawfare Review.* Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.lawfareblog.com/security-dilemma-cyberspace-ancient-logic-new-problems&ved=2ahUKEwigkZy42tD7AhXzhf0HHfi1BfAQFnoECAoQAQ&usg=AOvVaw12vRMsXYzu_vAy9SRDxrze

Kolton, M. (2017). Interpreting China's Pursuit of Cyber Sovereignty and its Views on Cyber Deterrence. *The Cyber Defense Review*. Retrieved from: https://www.jstor.org/stable/pdf/26267405.pdf?refreqid=excelsior%3Af7839a94af36d37751387c3c256ef02e&ab_segments=&origin=&initiator=&acceptTC=1

Kuglar, R. (2017). Deterrence of Cyber Attacks. *National Defense University.* Retrieved from: https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-13.pdf?ver=2017-06-16-115053-773

Kello, L. (2022). The end of Peace in Cyber space and how to restore it. *Yale University Press.* Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.amazon.com/Striking-Back-Failing-National-Security/dp/0300246684&ved=2ahUKEwirjci4qNL-AhUzi_0HHSf1AjAQFnoECBYQAQ&usg=AOvVaw3fN_97Mj7VR7jFvWL4fQQy

Kamphausen, D. (2023). Modernizing Deterrence: How China Coerces, Compels, and Deters. *The National Bureau of Asian Research (NBAR).* Retrieved from: https://www.nbr.org/wp-content/uploads/pdfs/publications/modernizing-deterrence_feb2023.pdf

Lilli, E. (2021). Redefining Deterrence in Cyber space: Private Sector Contribution to National Strategies of Cyber deterrence. *Contemporary Security Policy.* Retrieved from: https://www.tandfonline.com/doi/full/10.1080/13523260.2021.1882812

Lindsay, J, R. (2015). The Impact of China on Cybersecurity: Fiction and Friction. *International Security.* Retrieved from: https://direct.mit.edu/isec/article/39/3/7/30310/The-Impact-of-China-on-Cybersecurity-Fiction-and

Lindsay, J, & Gartzke, E. (2016). Coercion through Cyber space: The stability Instability Paradox Revisited. *University of Oxford press.* Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://deterrence.ucsd.edu/_files/LindsayGartzke_CoercionThroughCyberspace_DraftPublic1.pdf&ved=2ahUKEwie3OGc29D7AhV4i_0HHWTHDiEQFnoECBMQAQ&usg=AOvVaw1q2_VVHIjamiWVkNXJI9At

Labicki, M. (2015). Waging Cyber war the American way. *Tandfoline.* Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.tandfonline.com/doi/pdf/10.1080/00396338.2015.1068551&ved=2ahUKEwjcmK73nP_9AhXZg_0HHTAKA3AQFnoECB4QAQ&usg=AOvVaw22ks55SrWuauB3ndZ9l4Xn

Lonergan, S. (2021). Deterrence by denial in Cyber space. *Journal of strategic studies*. Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.tandfonline.com/doi/full/10.1080/01402390.2021.1944856&ved=2ahUKEwj-

xq6zof_9AhXj7rsIHZOSDpsQFnoECBAQAQ&usg=AOvVaw103-0BoFhe3-Rg41PY2Dx9

Lilli, E. (2018). President Obama and US cyber security policy. Clinton institute of American studies: university of Dublin. Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.tandfonline.com/doi/full/10.1080/23738871.2020.1778759&ved=2ahUKEwjU172sov_9AhWPhv0HHfh2C8oQFnoECAkQAQ&usg=AOvVaw36kKKz0YJuDEATWFrvTF6D

Lotrionate, C. (2014). A Better Defense: Examining the United States Norm based Approach to Cyber Deterrence. Georgetown Journal of International Affairs. Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.jstor.org/stable/43134324&ved=2ahUKEwjm5qWJo__9AhW7_rsIHZJABrcQFnoECAsQAQ&usg=AOvVaw37LYDdFzOYlyEWq0CxTpBc

Lupovici, A. (2011). Cyber warfare and Deterrence: Trends and challenges in research. *Journal of military and strategic, Tel Aviv University*. Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.inss.org.il/wp-content/uploads/2017/02/FILE1333533336-1.pdf&ved=2ahUKEwi8noKokYf9AhWhNOwKHXX3C-MQFnoECA8QAQ&usg=AOvVaw1W9TNPMLLQ6EYJzdbnr6zq

Lewis, J. A. (2016). Deterrence in Cyberspace. *Center for Strategic and International Studies.*

Martellini, N. (2013). Cyber Security Deterrence and IT protection for critical Infrastructures. *Springer*. Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.tandfonline.com/doi/full/10.1080/01495933.2017.1361202&ved=2ahUKEwiEh5OIkYf9AhUPrqQKHRVpAycQFnoECCMQAQ&usg=AOvVaw0mtzZwgtA8hDmryI8xSdjy

Moiz, A. (2023). Cyber Deterrence and Confidence Building between Pakistan and India. *Centre for international security studies Islamabad.* Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.researchgate.net/publication/368189125_Cyber_Deterrence_and_Confidence_Building_Between_Pakistan_and_India&

ved=2ahUKEwjngdHMkof9AhWR7KQKHewCB3kQFnoECA0QAQ&usg=AOvVaw1nQ_Ssjye-lxKrC3okz0U6

Manjikan,M. & Romaniuk, N.(2021). Routledge Companion to global cyber security strategy. *Routledge: Taylor & Francis Group.* Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.taylorfrancis.com/books/9780367024239&ved=2ahUKEwjz5IXrkof9AhXRwKQKHZlRDJEQFnoECBMQAQ&usg=AOvVaw3PClduJTqIYhC8Q6mc6hYv

Monaghan, S. (2022). Deterring hybrid threats: Towards a fifth wave of deterrence theory and practice. *Hybrid CoE.* Retrieved from: file:///C:/Users/User/Downloads/20220331-Hybrid-CoE-Paper-12-Fifth-wave-of-deterrence-WEB%20(1).pdf

McKenzie, M, T. (2017). Is Cyber Deterrence Possible? *Air Force Research Institute.* Retrieved from: https://media.defense.gov/2017/Nov/20/2001846608/-1/-1/0/CPP_0004_MCKENZIE_CYBER_DETERRENCE.PDF

Martin C. Libicki. (2009). Cyber Deterrence and Cyber Warf. *RAND.* Retrieved from: https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf

Monarez, G. (2021). Persistent engagement and Private sector. *Journal of Information warfare.* Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.jstor.org/stable/27036533&ved=2ahUKEwj7jvzqoI3-AhUUPOwKHWUTBzYQFnoECAoQAQ&usg=AOvVaw0xlj1nUwxKyAiWUfJx77Gn

Maschmeyer, L. (2022). A new and better quiet option? Strategies of Subversion and Cyber Conflict. *Journal of Strategic Studies.* Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.tandfonline.com/doi/abs/10.1080/01402390.2022.2104253&ved=2ahUKEwjEx7nTqo3-AhWQ_7sIHXwNBn0QFnoECBwQAQ&usg=AOvVaw1Ewp_vV1_-yx7Py9skhZq-

Meakins, J. (2018). Living in (Digital) Denial: Russia's Approach to Cyber Deterrence. *European Leadership Network.* Retrieved from: https://www.jstor.org/stable/pdf/resrep22130.pdf?refreqid=excelsior%3A0b17427ed43dcf9ed70d47cb564f3530&ab_segments=&origin=&initiator=&acceptTC=1

Manson, K. (2022). Nobody Knows Where the Red Line Is for Cyberwarfare. Bloomberg. Retrieved from: https://www.bloomberg.com/news/articles/2022-05-02/russia-cyberattacks-raise-questions-about-hacking-red-lines?leadSource=uverify%20wall

Meakins, J. (2018). Living In (Digital) Denial: Russia's approach to Cyber deterrence. *Euro-Atlantic Security Report.* Retrieved from: https://www.russiamatters.org/analysis/living-digital-denial-russias-approach-cyber-deterrence

Morgan, N. (2019). Russian Cyber Blind spots: Vulnerabilities and Measures. *Global Risk Insights.* Retrieved from: https://globalriskinsights.com/2019/03/russia-cyber-attacks-blindspot/

Nevill, L. & Hawkins, Z. (2016). Cyber Deterrence. *JSTORE*. Retrieved from: file:///C:/Users/User/Downloads/resrep04232.6.pdf

Nye, J. (2017). Deterrence and Dissuasion in Cyberspace. *Journal of international security at Harvard College.* Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://direct.mit.edu/isec/article/41/3/44/12147/Deterrence-and-Dissuasion-in-Cyberspace%23:~:text%3D36-,Four%2520Means%2520of%2520Deterrence%2520and%2520Dissuasion,%252C%2520entanglement%252C%2520and%2520normative%2520taboos.&ved=2ahUKEwiC2fjkkYf9AhUH2aQKHWRVCEQQFnoECAgQBQ&usg=AOvVaw2m12KKQ2M26S40b3-eJFzc

National Intelligence Council. (2017). Global Trends: Paradox of Progress. *National Intelligence Council.* Retrieved from: https://www.dni.gov/files/documents/nic/GT-Full-Report.pdf

Nye, J. (2016). Can China Be Deterred in Cyber Space? *The Diplomat.* Retrieved from: https://thediplomat.com/2016/02/can-china-be-deterred-in-cyber-space/

Nagy, V. (2012). The geostrategic struggle in cyberspace between US, China and Russia. *National University of Public service, Budapest Hungry*. Retrieved from: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/14025/Since%20the%20early%202000s,%20geopolitics%20has%20been%20affected%20by%20a%20new%20domain%20of%20human%20activity.pdf;jsessionid=DDECFA4117328C2856C6596D1E959872?sequence=1

Philbin, J, M. (2013). Cyber Deterrence: An Old Concept in a New Domain. *US Army War College.* Retrieved from: file:///C:/Users/User/Downloads/cyber%20deterrence%20an%20old%20concept%20in%20a%20new%20domain%20(1).pdf

Polyakova, A. & Boyer, P, S. (2019). The Future of Political Warfare: Russia, the West, and the Coming Age of Global Digital Competition. *The New Geo Politics – Brookings Institute.* Retrieved from: https://www.brookings.edu/wp-content/uploads/2018/03/the-future-of-political-warfare.pdf

Putten, F. (2015). US Deterrence against Chinese Cyber Espionage: The Danger of Proliferating Covert Cyber Operations. *Cling deal Institute*. Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.jstor.org/stable/resrep05348&ved=2ahUKEwiflIePjYz-AhUd8LsIHfaFBFQQFnoECAsQAQ&usg=AOvVaw35v4XqSHRuOrE3Ojn_h5i0

Porche, I & Paul, C. (March 2023). Cyber forces and US cyber-Command. *RAND Corporation.* Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.jstor.org/stable/10.7249/j.ctt1287m89.11%3FSearch%3Dyes%26resultItemClick%3Dtrue%26searchText%3Dau:%26searchText%3D%2522Elliot%2520Axelband%2522%26searchUri%3D%252Fopen%252Fsearch%252F%253Fpage%253D1%2526amp%253BQuery%253Dau%25253A%252522Elliot%252BAxelband%252522%2526amp%253Bsi%253D1%2526amp%253Bso%253Dnew%2526amp%253Btheme%253Dopen&ved=2ahUKEwjY48azn__9AhWu7LsIHXYZDggQFnoECBAQAQ&usg=AOvVaw1cMu61A3fHy0WUcEsvSxuS

Rosenzweig, P. (2010). The organization of the United States Government and private Sector for achieving Cyber Deterrence. *Proceeding of a workshop on deterring cyber-attacks.* Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://cs.brown.edu/courses/csci1950-p/sources/lec26/Rosenzweig.pdf&ved=2ahUKEwiFoZfpov_9AhV-g_0HHWh9DjsQFnoECBcQAQ&usg=AOvVaw2LsVy8vyAbJyu_BLvJUQMp

Remington, T., Spirito, C., Chernenko, E., Demidov, O. & Kabernik V. (2016). Toward U.S.-Russia Bilateral Cooperation in the Sphere of Cybersecurity. *US-Russia Futur*e Org. Retrieved from: https://futureofusrussiarelations.files.wordpress.com/2016/06/wg_working_paper7_cybersecurity_final.pdf

Reveron, D. (2012). Cyber space and National Security: Threats, Opportunities and Power in a Virtual World. *Georgetown University Press.* Retrieved from: https://www.researchgate.net/publication/297297678_Cyberspace_and_national_security_Threats_opportunities_and_power_in_a_virtual_world

Soesanto, S. & Smeets, M. (2020). Cyber Deterrence: The Past, Present, and Future. *Springer*. Retrieved from: https://link.springer.com/chapter/10.1007/978-94-6265-419-8_20#Fn1

Smeets, M. (2016). What Do We Talk About When We Talk About 'Cyber'? *SSRN*. Retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2860839

Soesanto, S. (2022). Cyber Deterrence Revisited. *Air University Press.* Retrieved from: file:///C:/Users/User/Downloads/CPP_0008_Soesanto_Cyber_Deterrence_Revisited%20(1).pdf

Scott, J. (2018). US strategic Cyber deterrence options. University of reading. Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://centaur.reading.ac.uk/79976/1/22839264_Jasper_thesis.pdf&ved=2ahUKEwi-npSuoP_9AhUzh_0HHY16DsUQFnoECBUQAQ&usg=AOvVaw2RdThmYKlf_395u3iB6GzT

Segal, A. (2016). The Hacked World Order: How Nations Fight Trade Maneuver and manipulate in the digital age. *A council on Foreign Relations.* Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.amazon.com/Hacked-World-Order-Maneuver-Manipulate/dp/1469065894&ved=2ahUKEwjG5dn_n__9AhXZif0HHQV7DacQFnoECBMQAQ&usg=AOvVaw2uHqK8jyrKJYRc3F9fxNsM

Schneider, J. (2019). Persistent Engagement: Foundation Evolution and Evaluation of a strategy. *Lawfare blog: Academia.* Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.lawfareblog.com/persistent-engagement-foundation-evolution-and-evaluation-strategy&ved=2ahUKEwjgg-uV2tD7AhWn_7sIHdxzA_gQFnoECAoQAQ&usg=AOvVaw0V5E8JzaeCOkTkDqTnyC9f

Saalman, L. (2017). Rethinking China-Russia -U.S. Deterrence in Cyber Space. *Think China, DK.* Retrieved from: https://www.thinkchina.ku.dk/documents/ThinkChina.dk_Policy_Brief__Rethinking_China-Russia-U.S._Deterrence_in_Cyberspace.pdf

Segel, A. (2016). An Expansive, and Dangerous, Chinese View on Cyber Deterrence. *Council on Foreign Relations.* Retrieved from: https://www.cfr.org/blog/expansive-and-dangerous-chinese-view-cyber-deterrence

Sterner, E. (2011). Retaliatory Deterrence in Cyber-space. *Strategic Studies Quarterly.* Retrieved from: https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-05_Issue-1/Sterner.pdf

Thomas, T. (2002). Information security thinking: A comparison of US, Russian and Chinese Concept. *International seminar on nuclear war and planetary emergencies.* Retrieved from: https://community.apan.org/wg/tradoc-g2/fmso/m/fmso-monographs/240293

Tolstukhina, A. (2017). We should not play madness in the explosive information field. *International Affairs Magazine.* Retrieved from: https://interaffairs.ru/news/show/17460

Thornton, R. & Miron, M. (2019). Deterring Russian cyber warfare: the practical, legal and ethical constraints faced by the United Kingdom. *Taylor & Francis Online*. Retrieved from: https://www.tandfonline.com/doi/abs/10.1080/23738871.2019.1640757

Turunen, M. & Kari, M. (2022). Cyber Deterrence and Russia's Active Cyber Defense. *Finnish National Defense University.* Retrieved from: https://www.proquest.com/openview/9d0ed8c941aef559d1375fca7d8dbbb8/1?pq-origsite=gscholar&cbl=396497

Thayer, B. (2015). Deterring Cyber warfare: Bolstering Strategic stability in Cyber space. *Palgrave Mcmillan.* Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://link.springer.com/book/10.1057/9781137476180&ved=2ahUKEwjcu-2bkYf9AhUEuaQKHfDdAv0QFnoECA4QAQ&usg=AOvVaw2FNle9KE_Yv0pKa_ujkUBh

Trujillo, C. (2014). The limits of cyber-space deterrence. *Quarter 2014.* Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-75/jfq-75_43-52_Trujillo.pdf&ved=2ahUKEwixvO3ZkYf9AhVmxgIHHfcjB9oQFnoECBsQAQ&usg=AOvVaw2BqFMgEthIbUX0Yf02w5kR

Tolga, I. (2018). Principles of Cyber Deterrence and the challenges in Developing a credible Cyber Deterrence posture. *NATO CCDCOE Strategy Branch Researcher.* Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://ccdcoe.org/uploads/2018/10/Challenges_in_Developing_Credible_Cyber_Deterrence_Posture_in_Cyberspace-1.pdf&ved=2ahUKEwjE-776kYf9AhVMDuwKHT9MC_8QFnoECBcQAQ&usg=AOvVaw2SOkLXvkq-I10TJKI9fLco

Taddeo, M. (2018). The challenges of Cyber deterrence. *Digital Ethics Lab, oxford Internet Institute.* Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://link.springer.com/

chapter/10.1007/978-3-030-17152-0_7&ved=2ahUKEwjW-b3qkIf9AhUPrqQKHRVpAycQFnoECAoQAQ&usg=AOvVaw0JXpaU80Yt4eAk3n-9bX8b

Thayer, B. (2015). Deterring Cyber Warfare: Bolstering Strategic Stability in Cyberspace. *George Mason University.* Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://link.springer.com/book/10.1057/9781137476180&ved=2ahUKEwi2han7nf_9AhX5g_0HHXJfAJUQFnoECCcQAQ&usg=AOvVaw2FNle9KE_Yv0pKa_ujkUBh

Vuori, J. (2022). The Curious Absence of Chinese Cyber Deterrence. *Directions Blog*. Retrieved from: https://directionsblog.eu/the-curious-absence-of-chinese-cyber-deterrence/

Weitz, R. (2022). The New China- Russia Alignment: Critical Challenges to US Security. *Praeger security International.* Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.amazon.com/New-China-Russia-Alignment-Challenges-International/dp/1440847363&ved=2ahUKEwjjs4mBxo7-AhXSt6QKHZS0BaQQFnoECCoQAQ&usg=AOvVaw0dzRpcDa6JPmZD0xz_Scxy

Welch, D, L. (2011). Cyberspace – The Fifth Operational Domain. *Institute for Defense Analyses (IDA).* Retrieved from: https://www.ida.org/-/media/feature/publications/2/20/2011-cyberspace---the-fifth-operational-domain/2011-cyberspace---the-fifth-operational-domain.ashx

Willner, A. (2017). Cyber deterrence and critical-Infrastructure Protection: expectation, application and limitation. *Tandfoline.* Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.tandfonline.com/doi/abs/10.1080/01495933.2017.1361202&ved=2ahUKEwitt_f4kIf9AhWHDuwKHdblAGMQFnoECBYQAQ&usg=AOvVaw1hPCdDpfhVaFDZPFp_c9Dw

Wilner, A. (2015). Contemporary Deterrence Theory and Counterterrorism: A Bridge Too Far? Retrieved from: https://nyujilp.org/wp-content/uploads/2015/11/NYI207.pdf

Wilner, A. (2019). US cyber deterrence: Practice guiding theory. *Journal of strategic studies,* Retrieved from https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.tandfonline.com/doi/full/10.1080/01402390.2018.1563779%23:~:text%3DAt%2520its%2520core%252C%2520the%2520strategy,and%2520mitigating%2520damage%2520from%2520cyberattacks.&ved=2ahUKEwjIvbSXo__9AhX_h_0HHSs8AykQFnoECAwQBQ&usg=AOvVaw0F8mV26Htk1Qk72GBc3kke

Wren, C. (2012). Strategic Cyber deterrence. *The Fletcher School of law and Diplomacy*. Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://sites.tufts.edu/fletcherrussia/files/2018/09/2012-Christopher-Fitzgerald-Wrenn-Strategic-Cyber-Deterrence.pdf&ved=2ahUKEwic2pj7ov_9AhVv_rsIHc3gB-IQFnoECBYQAQ&usg=AOvVaw0LxNxFFF1sorZrLA8V5N8q

Willett, K. (2014). Active Cyber Defense: A vision for real time Cyber Defense. *Journal of Information Warfare.* Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.jstor.org/stable/26487121&ved=2ahUKEwj2_vPXnf_9AhUi7rsIHUuCAx8QFnoECAoQAQ&usg=AOvVaw0UJdVi8IHswqyVFemQjK3R

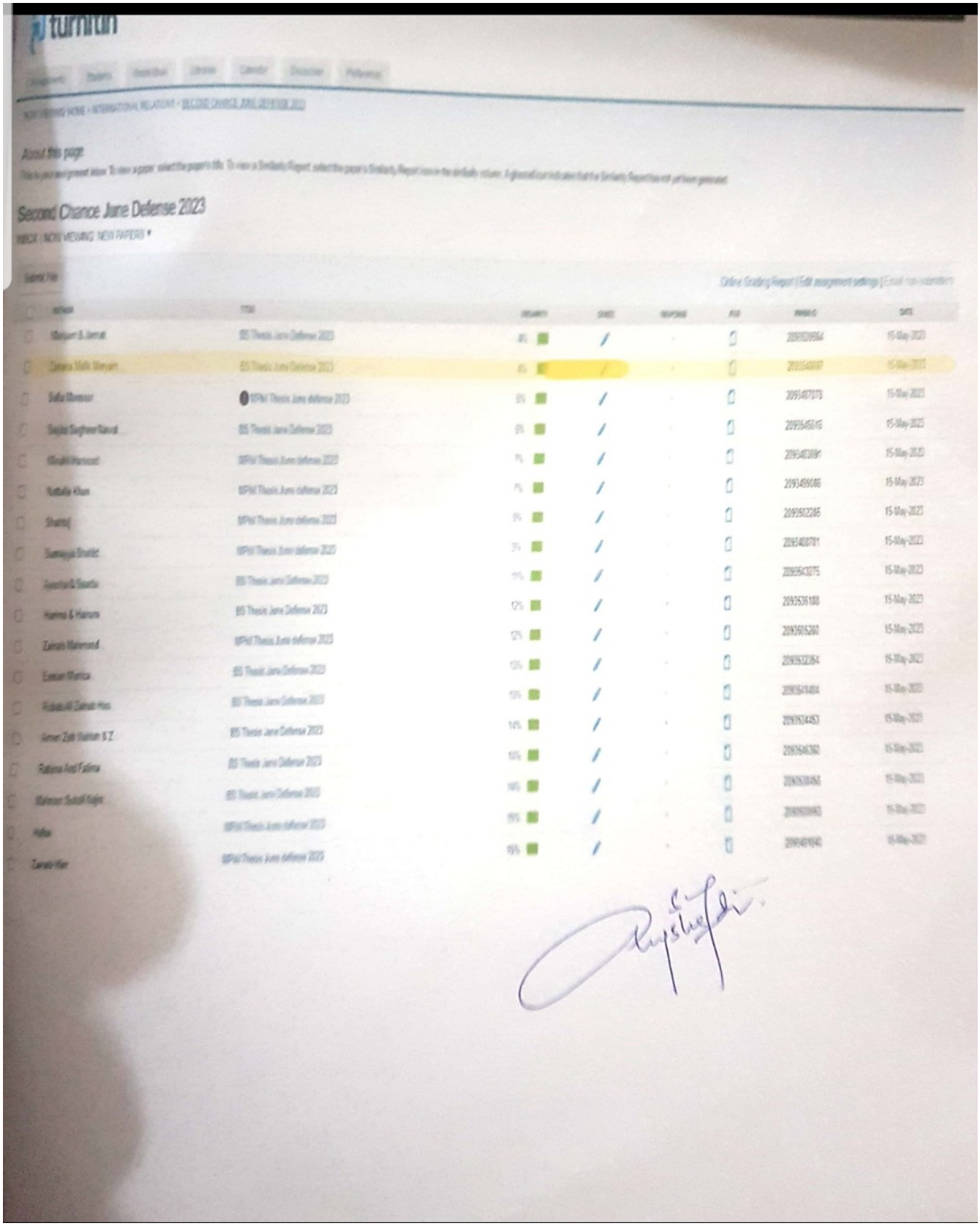
Weitz, R. (2022). The New China- Russia Alignment: Critical Challenges to US Security. *Praeger security International.* Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.amazon.com/New-China-Russia-Alignment-Challenges-International/dp/1440847363&ved=2ahUKEwjjs4mBxo7-AhXSt6QKHZS0BaQQFnoECCoQAQ&usg=AOvVaw0dzRpcDa6JPmZD0xz_Scxy

Whyte, C. (2020). Poison Prison and Cascade effects: AI and cyber conflict. *Strategic Studies Quarterly*. Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-14_Issue-4/WhyteRev.pdf&ved=2ahUKEwj33tax29D7AhVThf0HHextDO4QFnoECBEQAQ&usg=AOvVaw2UvWCu4RNPOVFxadit05kz

Xi Jinping. (2017). Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects and Strive for the Great Success of Socialism with Chinese Characteristics for a New Era. *19th National Congress of the Communist Party of China.* Retrieved from: http://www.xinhuanet.com/english/download/Xi_Jinping's_report_at_19th_CPC_National_Congress.pdf

Zhang, E. & Creemers, R. (2023). The Evolution of Chinese Perspectives on Cyber Deterrence and Attribution. *Leiden Asia Centre.* Retrieved from: https://leidenasiacentre.nl/wp-content/uploads/2023/03/Chinese-Perspectives-of-Deterrence-and-Attribution-in-Cyberspace-1.pdf

Zegart, A & Lin, H. (2018). Bytes Bombs and Spies. *The brooking Institute.* Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.brookings.edu/book/bytes-bombs-and-spies/&ved=2ahUKEwjypaWanv_9AhV58rsIHX-hBSMQFnoECBAQAQ&usg=AOvVaw2C9PIA7ynedol0cxBwQNFi


turnitin
About this page
Second Chance June Defense 2023