

**CHINA'S CYBERWARFARE: THREATS, INTENTIONS AND
CAPABILITIES, 2003 – 2012**

Dissertation submitted to Jawaharlal Nehru University

for award of the degree of

MASTER OF PHILOSOPHY

KAUSHAL KISHORE CHANDEL



Chinese Studies Division

Centre for East Asian Studies

School Of International Studies

JAWAHARLAL NEHRU UNIVERSITY

NEW DELHI 110067

2013

जवाहरलाल नेहरू विश्वविद्यालय
CENTRE FOR EAST ASIAN STUDIES
SCHOOL OF INTERNATIONAL STUDIES
JAWAHARLAL NEHRU UNIVERSITY
NEW DELHI- 110 067 (INDIA)



Phones : 91-11- 2670 4346
Fax : 91-11-2670 4346

Date: 26th July 2013

DECLARATION

I declare the dissertation entitled “China’s Cyberwarfare: Threats, Intentions and Capabilities, 2003 – 2012,” submitted by me in partial fulfillment of the requirements for the award of the degree of **Master of Philosophy** of Jawaharlal Nehru University, is my own work. The dissertation has not been submitted for any other degree of this University or any other university.

A handwritten signature in black ink, appearing to read 'Kaushal Kishore Chandel', written in a cursive style.

Kaushal Kishore Chandel

CERTIFICATE


We recommend that this dissertation be placed before the examiners for evaluation.


A handwritten signature in black ink, appearing to read 'Srikanth Kondapalli', written in a cursive style.

SRIKANTH KONDAPALLI
Chairperson, CEAS

A handwritten signature in black ink, appearing to read 'Srikanth Kondapalli', written in a cursive style.

SRIKANTH KONDAPALLI
Supervisor

 Chairperson
Centre For East Asian Studies
School of International Studies
Jawaharlal Nehru University
New Delhi - 110067

 Supervisor
Centre For East Asian Studies
School of International Studies
Jawaharlal Nehru University
New Delhi - 110067

Dedicated to
My Family

ACKNOWLEDGEMENTS

This research attempt would not have been possible without the encouragement of the people I have come across in my life so far. They all contributed in shaping my personality in one form or the other. Their impact and influences have some reflections on this work.

One person who is to be always remembered through this research work is my supervisor, Prof. Srikanth Kondapalli. I am very fortunate to be under his blessings for all the formative years of my life. His meaningful suggestions have been helpful not only in betterment of my research but also in my personality and life. I humbly express my heartfelt gratitude to the distinguished faculties of Chinese Studies Division of CEAS Dr. Varaprasad S. Dolla, Prof. Alka Acharya, Dr. Ritu Agarwal for their intellectual support. I would also like to thank the other faculty of the centre for their guidance and support.

I am thankful to the support staff of my Center, Central Library of Jawaharlal Nehru University and the library of Institute of Defense Studies and Analysis for their cooperation.

Most importantly my family has been my support system in the achievements and failures so far. My parents are the source of my identity and the source of my strength. I express my gratitude, love and admiration to my family through this work.

For all the errors and omissions in this research work I am solely to be held responsible.


Kaushal Kishore Chandel

CONTENTS

	Page No.
Acknowledgements	i
Contents	ii
Figures and Table	vi
List of Acronyms and Abbreviations	vii
Chapter – 1 Introduction	1-14
1. Background.....	1
2. Literature Review.....	3
3. Official Discourse (Government Position).....	9
4. Gaps in Literature.....	10
5. Definition, Rationale and Scope of the Study.....	11
6. Research Questions.....	11
7. Hypotheses.....	12
8. Research Methodology.....	13
9. Chapterisation.....	13
10. Limitations of the study	14
Chapter – 2 Understanding the Concept of Cyberwarfare	
(Global Discourse on Cyberwarfare)	15 - 41
1. Tracing the Roots.....	15
1.1. In Official Documents.....	16
1.1.1. Of UN.....	16
1.1.2. Of U.S.....	17
1.1.2.1. Evolution of the Concept.....	17
i. Information Warfare (IW)/ Information Operation (IO).....	17
ii. Cyberspace.....	18
iii. Cyberspace Operation.....	19

iv. Cyberwarfare.....	20
1.1.3. Of NATO (North Atlantic Treaty Organization).....	21
1.1.4. Russian Federation (Russia).....	21
1.1.5. United Kingdom (UK).....	23
1.1.6. Japan.....	23
1.1.7. Taiwan (Republic of China).....	24
1.2. In Un-official Documents (Available Literature – Global Discourse).....	24
2. Locating Cyberspace and Cyberwarfare (Establishing Relations with Other Terms).....	28
2.1. In Information Environment.....	28
2.2. In Information Operation (IO/IW)	31
2.3. Among Others Terms.....	34
2.4. Among Other Domains.....	36
3. Controversy with the Concept.....	38
4. Conclusion.....	39
Chapter 3 The Chinese Concept of Cyberwarfare.....	41 - 60
1. Tracing Chinese Views on Cyberspace and Cyberwarfare.....	41
1.1. Official Documents.....	41
1.2. Un-official Documents (Available Literature).....	42
1.2.1. Chinese Views on Origin of Cyberspace.....	42
1.2.2. Origin and Definition of Chinese Cyberwarfare.....	44
2. Characteristics of Chinese Cyberwarfare	50
3. Chinese Views on Its Relationship with other forms of Warfare & Domains.....	53
4. Similarities and Differences- Cyberwarfare with Chinese Characteristics.....	56
5. Conclusion.....	60
Chapter 4 Organisations Involved in China’s Cyberwarfare.....	61 - 99
1. General Staff Headquarters/Department (GSD) (总参谋部).....	63

1.1. GSD Second Department (Intelligence Department [情报部]/ 2PLA).....	67
1.2. GSD Second Department (Intelligence Department [情报部]/ 2PLA).....	69
1.2.1 Research Institutes.....	73
1.2.2. Bureaus (局).....	74
1.2.3. Beijing North Computing Center (BNCC).....	77
1.2.4. Other Organisations under the Third Department.....	78
1.2.4.1. Training Institutes.....	78
1.3. GSD Fourth Department.....	79
1.4. Communication Department (通信部)	81
2. General Armaments Department (zong zhuangbei bu [(总装备部)]).....	81
3. China's Cyber Command.....	82
4. Ministry of State Security (MSS).....	82
5. Ministry of Public Security (MPS).....	84
6. Commission for Science, Technology and Industry for National Defence (COSTIND).....	84
7. Academy of Military Sciences (AMS [军事科学研究院]).....	85
8. State Informatization Leading Group (SILG).....	85
9. National Defence University (NDU).....	87
10. Joint Campaign Command HQ.....	87
11. Wuhan Communications Command Academy (CCA).....	87
12. PLA Information Warfare Militia Units.....	88
13. Technical Reconnaissance Bureaus (TRB).....	89
14. Hackers and Hacker Groups.....	95
15. National University of Defence and Technology (国防科学技术大学).....	97
16. PRC Military-Industrial Companies.....	97
17. Conclusion	97

Chapter 5 Intentions and Capabilities of

Chinese Cyberwarfare.....99 – 122

1. Intentions	99
---------------------	----

1.1.For Technology Leapfrogging and Economic Espionage.....	101
1.2.Anti Access/ Area Denial (A2/ AD)	
(Counter- intervention Operation).....	103
1.3.For Buying Time	104
1.4.Supplement to Conventional Forces.....	104
2. Capabilities.....	105
2.1.Cyber Power – The New Component of CNP.....	106
2.2.Intelligence (SIGINT/ ELINT/HUMINT).....	108
2.3.Supercomputers.....	109
2.4.Cyber Security Experts.....	110
2.5.Military Digital (Cyber) Drills	110
2.6.Chinese President Xi Jinping’s US Visit and	
Snowden’s Disclosure.....	111
3. Incidents attributed to China.....	112
3.1.Trend Analysis.....	114
4. China’s Response.....	116
5. Conclusion.....	120
Chapter 6 Conclusion.....	123 – 131
1. Concept of Cyberwarfare – Global and Chinese Discourse.....	123
2. Threats, Intentions and Capabilities of Chinese Cyberwarfare.....	127
References.....	132 – 141

Figures, Graph and Graphic

Figures

Figure 1: The Content of Information Environment.....	29
Figure 2: The Three Dimensions of Information Environment.....	30
Figure 3: Location of Cyberspace in Information Environment.....	30
Figure 4: Relationship between IO & Cyberspace.....	32
Figure 5: Relationship of Cyberwarfare with CNA, CND &CNE – A different Perspective.....	33
Figure 6: Components of Cyberspace.....	35
Figure 7: Relationship between Cyberspace and Other Related Terms.....	36
Figure 8: Relationship between Cyberspace and Other War Fighting Domains.....	37
Figure 9: Relationship between Cyberspace and Other Domains.....	55
Figure 10: Relationship of Cyberspace with Warfare Waged in Other Domain.....	55
Figure 11 Hierarchical Organisations of Chinese Military.....	63
Figure 12: Organisational Structure of GSD.....	65
Figure 13 Position of GSD and its Sub-ordinate Departments in PLA.....	66
Figure 14: Sub-ordinate Organisational structure of GSD.....	66
Figure 15: Composition of GSD.....	67
Figure 16: Sub-ordinate Organisations Functioning under the Third Department.....	73
Figure: 17 China’s Ministry of State Security.....	83
Figure 18: Cyber Incidents Allegedly Attributed to China from 1999 to 2009.....	113
Figure 19: Companies Involved in Classified Surveillance Programme ‘PRISM’.....	117
Figure 20: Locations of Root Servers.....	118
Graph 1: Reported Cyber Attacks on China.....	119
Graphic 1: The Development Process of Cyberspace.....	43

ABBREVIATIONS

A2	Anti Area
ACSI	Advisory Committee for State Informatisation
AD	Area Denial
AMS	Academy of Military Science
APCERT	Asia Pacific Computer Emergency Response Team
C2	Command and Control
CCA	Communication Command Academy
CERT	Computer Emergency Response Team
CMC	Central Military Commission
CNA	Computer Network Attack
CND	Computer Network Defence
CNO	Computer Network Operations
CO	Cyberspace Operations
COSTIND	Commission for Science, Technology and Industry for National Defence
CPC	Communist Party of China
CYBERCOM	Cyber Command
DoD	Department of Defense (US)
ECM	Electronic Countermeasures
ELINT	Electronic Intelligence
ESM	Electronic Support Measure

EW	Electronic Warfare
FAS	Federation of American Scientists
GAD	General Armament Department
GPD	General Political Department
GSD	General Staff Department
GZ	Guangzhou
HUMINT	Human Intelligence
IA	Information Assurance
ICT	Information and Communication Technology
IDS	Institute of Defence Studies and Analyses
INEW	Integrated Network and Electronic Warfare
IO	Information Operations
IT	Information Technology
IW	Information Warfare
JP	Joint Publications
MIIT	Ministry of Industry and Information Technology
MILDEC	Military Deception
MPS	Ministry of Public Security
MR	Military Regions
MSS	Ministry of State Security
NATO	North Atlantic Treaty Organisation
NDU	National Defence University
NIPRNET	Non-classified Internet Protocol Router Network

OPSEC	Operation Security
PHYOPS	Psychological Operations
PLA	People's Liberation Army
SASTIND	State Administration for Science, Technology and Industry for National Defence
SILG	State Informatisation Leading Group
SINGINT	Signal Intelligence
TRB	Technical Reconnaissance Bureau
UK	United Kingdom
UN	United Nations
US	United States of America
WMD	Weapons of Mass Destruction

Chapter 1

Introduction

1. Background

The recent 'Stuxnet (震网)' virus attack on Iran nuclear enrichment centres, which were reportedly approved by President of United States of America (US) Barack Obama, marked a beginning of new era: The era of so called 'Cyberwar'. Though US Department of Defense (DoD), in 2011, had already declared cyberspace as the fifth domain of warfare (after land, water, air and space), but the recent virus attacks, which delayed Iran's nuclear program at least by 2 years, had taken the world by surprise. Stuxnet was one of the many 'cyber-weapons' allegedly developed by US in collaboration with Israel. Others malicious computer program, that were used to attack the computer network of Iran and other countries of Middle-East, were Flame, Duqu, Mahdi, Gauss etc. After these incidents, cyber attacks have largely increased across the globe which could be clearly observed in the newspaper headlines (e.g. Armenia vs. Azerbaijan, North Korea vs. South Korea, Israel vs. Iran, Israel vs. Palestine, Pakistan vs. India etc.). With the increasing threats in cyberspace, more and more nation states have started realizing the importance to cyberspace security. Optimum utilization of cyberspace is being attempted by countries all over the world. China is no exception to it. 'Cyberwarfare' was being treated by Chinese scholars and experts as asymmetric form of warfare, which could serve as a tool for militarily weaker nation states to bring down militarily advanced adversary. At the same time, cyberspace also provided favourable domain to carry out espionage activities which could help China in leapfrogging in certain technologies.

Cyberspace is the latest entrant in the category of war fighting domain. More a country is dependent on computer and computer networks, more vulnerable the country is, for e.g. Estonia (where 97 percent of the facilities were wired - had to face prolonged cyber attacks for almost two to three weeks in 2007), Georgia (which faced the same fate in 2008- followed by military attacks by Russia). Cyberspace domain has become Achilles heel of the most of the developed countries especially US, which is heavily dependent on internet and computer networks and can be targeted even by militarily less advanced adversaries. Thus, 'Cyberwar' has given an asymmetric option to militarily less advanced countries to gain equality or sometimes superiority in the battlefield during the time of conflict. The United Kingdom's (UK) 2012 National Security Strategy identified Cyber-attacks as one of the four highest-

priority risks faced by the UK. US President Obama has declared cyber security as one of the most serious economic and national security challenges the US faces as a nation and probably that's why President himself in his article published in Washington Post appealed US citizens to support and pass the Cyber Security Bill in Senate, which was finally defeated. General Keith Alexander (Director of NSA and USCYBERCOM) stressed that cyber attack on US computer network has increased seventeen times from 2009 to 2011. The Cyber Policy Review stated that industry estimates of losses from intellectual property to data theft in 2008 range as high as one trillion dollar. Around ten to twenty terabyte of data has been downloaded from US websites. US Secretary of Defense Leon Panetta has warned Americans of the danger of a "Cyber Pearl Harbour" attack on the US.

Cyberspace is said to be the only artificial domain in which all instruments of national power (diplomatic, informational, military, economic) can be concurrently exercised through manipulation of data and gateways. Cyberspace is a domain in which the classic constraint of distance, space, time and investment are reduced. One more reason that makes 'Cyberwar' more lethal is the range of the 'Cyber Weapons' which is greater than any form of conventional weapon and can hit any corner of the world from wherever we want. The issue of attribution adds to the lethality of the cyber attacks. And since it is difficult to trace the origin of cyber attack, the issue of deterrence also becomes difficult. Absence of international legal framework and international governing organizations attract more and more nation states to take advantage of cyberspace.

In case of China it is much more relevant not only because China is blamed for most of the hacking incidents around the globe, but also because of the number of internet user China has. China has the highest number of 'netizens (网民)' in the world. It surpassed the United States in Internet users in mid-2008, when it reached an estimated 253 million. It reached 457 million by the end of 2010, an increase of 19 percent (or 73 million users) over 2009. Its Internet penetration rate of 34.3 percent is still relatively low compared to that of developed countries, although it is higher than the world average. Speculations are being made about China using Mao's era 'Peoples War' in cyber warfare, in which each Chinese can participate as 'Cyber Warriors'. China's white paper on defence lays great emphasis on 'informatisation' (信息化) and seeks to cover up their shortcomings in mechanization of military through 'informatisation' of military.

2. Literature Review

As far as 'Cyberwarfare' is concerned literature is available in plenty (both books and articles), but books available on 'Chinese Perspective of Cyberwarfare' are quite few. Most of the articles have Western perspective and not much is available on Chinese perspective as most of the Chinese authors have worked on US perspective and capabilities. Available literature present three different schools of thought: first (radicals) – 'Cyberwar' has brought revolution in war fighting methods and can replace conventional warfare (John Arquilla, Richard A Clarke, Robert Knake, Qiao Liang, Wang Xiangsui etc); second (moderates) – 'Cyberwar' has brought unprecedented change in war fighting methods and can make conventional warfare more lethal (Jeffery Carr, Joseph S Nye, Martin C Libki etc); third (skeptics) – 'Cyberwar' is too much hyped and it does not even deserve to be referred as 'War' (Thomas Rid, Brandon Valeriaono etc.)

The term 'Cyberwar' was first used by John Arquilla in his work '*Cyberwar is Coming*' long back in 1997. Since then, scholars and experts all over the world have attempted to analyze this concept and have come up with their opinion and understanding of, which resulted in emergence of rich literature and schools of thought. John Arquilla came up with similar sounding concepts namely 'Netwar' and 'Cyberwar'. He distinguishes between them by saying, "Netwar' is societal-level ideational conflicts waged in part through internetted modes of communication and 'Cyberwar' is at the military level." Regarding 'Cyberwar' John Arquilla, says:

Cyberwar refers to conducting, and preparing to conduct, military operations according to information-related principles. It means disrupting if not destroying the information and communications systems, broadly defined to include even military culture, on which an adversary relies in order to 'know' itself: who it is, where it is, what it can do when, why it is fighting, which threats to counter first, etc. It means trying to know all about an adversary while keeping it from knowing much about oneself. It means turning the 'balance of information and knowledge' in one's favour, especially if the balance of forces is not. It means using knowledge so that less capital and labour have to be expended (Arquilla 1997: 30).

Richard A. Clarke defines 'Cyberwar' as actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption (Clarke 2012). Another author Jeffrey Carr, inspired by Sun Tzu, defines Cyber Warfare as an art and science of fighting without fighting; of defeating an opponent without spilling their blood (Carr 2009). IDSA task force defines 'Cyber warfare' as "actions by a nation-state or its

proxies to penetrate another nation's computers or networks for the purpose of espionage causing damage or disruption" (IDSA Task Force Report: 2012: 31). Shashi Tharoor defines 'Cyber War' as unauthorised invasion by a government into the systems or networks of another, aiming to disrupt those systems, to damage them partially, or to destroy them entirely (Tharoor: 2012). James Mulvenon in his work identifies PLA definition of computer network warfare:

The general term for all sorts of information offense and defence actions in which computers and computer networks are the main targets, in which advanced information technology is a basic means, and which take place throughout the space occupied by networks. The core of computer network warfare is to disrupt the layers in which information is processed, with the objective of seizing and maintaining control of the network space (Mulvenon: 2009).

Joseph S Nye defines 'Cyber war' as "hostile action in cyberspace, whose effects amplify or are equivalent to major physical violence". He further says, "Cyber war, though only incipient at this stage, is the most dramatic of the potential threats. Major states with elaborate technical and human resources could, in principle, create massive disruption and physical destruction through cyber attacks on military and civilian targets. Technology today favours an offensive actor rather than defensive one. States have the greatest capabilities, but non-state actors are more likely to initiate a catastrophic attack. A 'cyber 9/11' may be more likely than the often-mentioned 'Cyber Pearl Harbour'" (Nye: 2012). Martin C Libicki points out to two types of 'Cyberwars': Operational 'Cyberwar' and Strategic 'Cyberwar'. He says, "Operational cyberwar— cyberattacks to support warfighting— may have far greater purchase than strategic cyberwar, cyberattacks to affect state policy. An operational cyberwar capability may well be an effective niche weapon if correctly timed. Strategic cyberwar campaigns are more problematic and hence merit less emphasis" (Libicki: 2009: 06).

Thomas Rid, based on Clausewitz's three main elements of war (violent character, instrumental character & political nature) argues in three steps that cyber war has never happened in the past, that cyber war does not take place in the present, and that it is unlikely that cyber war will occur in the future. He examines past incidents of cyber attacks through the lens of these three elements label them unqualified to be called as examples of 'Cyberwar' (Thomas Rid: 2012).

Chinese author Qiao Liang (乔良) and Wang Xiangsui (王湘穗) assert that although the present components of unrestricted warfare like terrorist attacks, financial attacks, hackers' attacks etc might not fall in category of war, but would probably become modes of future

warfare and would enter our understanding of warfare soon. He asserts, "If these unrestricted modes can create damages equivalent to conventional war, that also in very short period of time, why these should not be considered as the potential warfare options?" They argue that US attack on Iraq was not purely military; rather it was accompanied by media war, control of news, trade embargos, financial restrictions etc. Thus, they point out that unrestricted modes of warfare are already being extensively used. They also argue that along with the change in the principle of warfare, there will be changes in the rules and norm of warfare. There is no unalterable rule of war and no unalterable principle of war. (Qiao & Wang: 1999)

Chou Xinliang and Dong Shouji who have analyzed the 'Stuxnet' virus, say, "Stuxnet is highly sophisticated virus with clear objective and strategic intention which has typical characteristic of Cyberwar that could not be possible without the support of nation state."

As far as evaluating PRC's capability is concerned, we can identify three schools of thought. First school of thought (comprising authors like Mattia Nelles, Desmond Ball, Steve Armstrong etc.) advocates that China's 'Cyberwarfare' capabilities are fairly limited and rudimentary; China itself is a victim of cyber attacks and other hacking activities; and hence China is not a big threat in cyberspace domain. Second school of thought (comprising of Jeffery Carr, James Cartwright, McConnell etc.) argue that China is a big threat to major powers (especially US) and even US can face defeat in this war if a war is waged in cyberspace. (Available Western literatures suggest that the reason why US will lose is more because of its unpreparedness and less because of PRC's capabilities.) Between these two there exists a third school of thought (comprising James Mulvenon, Bill Woodcock, Lary M Wortzel, Qiao Liang, Wang Xiangsui, Dai Qingmin etc.) which says PRC's Cyberwarfare capabilities might not be up to the level of US or Israel but it can help in deterring major powers' and even the superpower's military forces in wartime.

Mattia Nelles argues that the military side of China's cyber foreign policy is still relatively underdeveloped. In scenarios facing superior maritime powers, such as the US, China's cyber assets could not give the country any advantage that could possibly bridge the gap in military strength. Regarding cyber activity, however, espionage plays a big role. Theft of intellectual property from private businesses and the intrusions of Chinese government and government related hacker groups pose a significant problem for US interests. Mattia Nelles summarizes that China's military cyber capability might be growing but it is expected that it cannot, at

this stage, be effectively used in direct military clashes between the US and China to potentially overcome the great difference in size and efficiency of the US military.

Desmond Ball on the one hand says that China has the most extensive and most practiced cyberwarfare capabilities in Asia, which is very destructive in nature. On the other hand he argues that China's cyberwar capabilities are fairly limited and rudimentary that cannot compete with advanced adversaries in case of prolonged war, but could prove helpful if used pre-emptively. (Ball: 2011)

IT expert Steve Armstrong argues that China's own network appears to be unprotected, and other countries can launch attacks through China, which makes it appear the primary suspect. He further states that "it's too easy to blame China. In fact, legitimate countries are bouncing their attacks through China." (Mulvenon: 2009)

Jeffrey Carr in his article, '*Why US Will Lose a Cyber War*,' argued that we currently witness a 'Rise of a Cybered Westphalian Age'. The basic argument is that due to the increasing reliance on technology in both the civil and military sectors vulnerability increases drastically. Given the described advantage of the offensive and the fact that countries with vastly growing economies like China that currently massively invest into offensive technology the outcome of a potential cyber war might already be determined. Author further says, "There's not another nation in the world that can wage kinetic warfare as effectively as the United States, and that's probably at the heart of the reason why the United States will lose a war fought in cyberspace" (Carr: 2011). James Cartwright, former vice chairman of the Joint Chiefs and notable cyber expert, also has somewhat similar opinion. In addition he also believes that Chinese cyber activities are largely supported by the Chinese government. He emphasizes, "Chinese cyber spies largely backed or directed by the government" are stealing key data. James Cartwright has also said that a full-scale Chinese cyber attack potentially has the same effect as weapons of mass destruction (Nelles: 2012).

Bill Woodcock (research director at Packet Clearing House - a non-profit Internet security and stability research institute) says, "The PLA's 'People's War' doctrine argues that all able-minded People's Republic computer users have a responsibility to fight for China with their laptops." He argues that Beijing might call on ethnic Chinese hackers in any part of the world, hoping they might help. Even non-hackers might be asked to participate in 'denial of service' (DoS) attacks – a weapon to shut down enemy websites that requires massive numbers of computers to accomplish. "The power of numbers is on their side,"

Woodcock adds, “China has the largest DoS capability in the world, which is a huge concern to private-sector companies as well” (Marquand & Anroldy: 2007).

Larry M Wortzel also agrees that “China currently is thought by many analysts to have the World’s largest denial-of-service capability.” Mr. Wortzel opined that such persistent, systematic and sophisticated attacks, some of which have taken place in the United States, in China, in Germany, and in the United Kingdom, most likely are state-directed. In addition to the Google attacks, there have been attacks on such religious groups as Falun Gong and on adherents of the Dalai Lama, both of which have been singled out by the Chinese Communist Party leadership for suppression (Wortzel: 2011).

James C Mulvenon says, “It is important to note that Chinese CNA doctrine focuses on disruption and paralysis, not destruction.” Philosophically and historically, the evolving doctrine draws inspiration from Mao Zedong’s theory of “protracted war,” in which he argued that “We must as far as possible seal up the enemies’ eyes and ears, and make them become blind and deaf, and we must as far as possible confuse the minds of their commanders and turn them into madmen, using this to achieve our own victory. The goal of this paralyzing attack is to inflict a “mortal blow” [*zhiming daji*], though this does not necessarily refer to defeat.

Many Western authors have asserted that the patriotic hackers are “controlled” by Beijing, and should therefore be included in PLA CNO capabilities estimates. The argument presented to support this is that consistently harsh punishments are given to individuals in China committing relatively minor computer crimes, while patriotic hackers appear to suffer no sanction for their brazen contravention of Chinese law. Others argue that since the Chinese government ‘owns’ the Internet in China, therefore patriotic hackers must work for the state (Mulvenon: 2009).

Josh Rogin writings for the Foreign Policy in 2010 stated that it is widely believed in US security circles that the Chinese government is supporting hackers that attack anything and everything in the U.S. national security infrastructure on a constant basis. Moreover, Rogin lists the top ten Chinese intrusions of which perhaps the most famous example is the major theft of tactical information from Lockheed Martin’s F-35 fighter program, one of Americas most advanced airplanes. The multi-layered infiltration apparently went on for years without detection. The first reports in 2009 suspected Chinese hackers were behind the attacks. Reports in 2010 backed the claim (Rogin: 2010).

Magnus Hjortdal asserts that China's offensive cyber capabilities are identified in numerous additional UK reports from analysts and defence ministries. They describe a Chinese military exercise as early as 2005 directly aimed at practicing hacking into enemy networks. The public part of cyber warfare in China is directed by the PLA General Staff, 4th Department (Electronic Countermeasures and Radar). CND and CNE are delegated to the PLA General Staff, 3rd Department (Signals Intelligence and Technical), that roughly is equivalent to the U.S. National Security Agency. He observes presence of Chinese government everywhere:

“Training in CNO occurs across all People's Liberation Army service branches, from command to company level, and is considered a core competence of all combat units. Field exercises include joint operations in complex electromagnetic environments, and sources indicate the existence of a permanent 'informationized Blue Force' regiment, drilled in foreign Information Warfare tactics. Indications of the formal and informal cooperation between the military and civilian parts are also seen in PLA's sponsorship of numerous universities and institutes supporting research and development in information warfare. These include the Science and Engineering University in Hefei, the Information Engineering University in Zhengzhou, the National University of Defense Technology in Changsha, and the Communications Command Academy in Wuhan.” (Hjortdal: 2011)

James A. Lewis produced this concise analysis of the attacks: “This is a big espionage program aimed at getting high-tech information and politically sensitive information—the high-tech information to jump-start China's economy and the political information to ensure the survival of the regime. This is what China's leadership is after. This reflects China's national priorities” (Mulvenon: 2009). Lynn, Chertoff, and McConnell published an op-ed called “China's Cyber Thievery Is National Policy- And Must Be Challenged.” They argue that it is fair to counter that a lot of countries and criminal non-state actors nowadays embraced cyber espionage to gain a competitive edge, but it seems as if China stands out as especially aggressive.

No Chinese author has evaluated China's capability as it might be considered as going against the authoritarian regime. It is also difficult to analyze China's real capabilities as it falls under highly sensitive and classified area. However Chinese authors have studied closely the way US wages war and have evaluated capabilities and weaknesses of US (many of the Western authors have also been doing the same with PRC). That's why Chinese authors' evaluation of their own nation's capabilities is not available. They rather suggest Chinese leadership to adopt and develop such a mode of warfare that could have an advantage over the capabilities of adversaries (mainly US- as others would be automatically covered). Hence views of Chinese authors are crucial so as to know on what basis they

consider a particular mode of warfare better suited to their nation or to know how they want to wage war.

Qiao Liang and Wang Xiangsui assert, “If the motive and consequence of war is achieved through means other than war which ensures minimum casualties to people, why should we not go for such options that can also serve as an alternative to war?” They also wrote in ‘*Unrestricted Warfare*’, that in the information age, the influence exerted by a nuclear bomb is perhaps less than the influence exerted by a hacker. Nu Li, Li Jiangzhou, and Xu Dehui write “We must send a message to the enemy through computer network attack, forcing the enemy to give up without fighting” (Nu Li et. al.: 2000). Wang Houqing and Zhang Xingye argue that computer network attack is one of the most effective means for a weak military to fight a strong one. They also thank computers, which has made long distance surveillance and accurate, powerful, and long distance attacks possible for their military (Wang & Zhang: 2000). Wei Jincheng in his article (Wei: 1996: 6) writes, “An information war is inexpensive, as the enemy country can receive a paralyzing blow through the Internet, and the party on the receiving end will not be able to tell whether it is a child’s prank or an attack from an enemy.” Lu Daohai states, “Computer warfare targets computers—the core of weapons systems and command, control, communications, computers and intelligence (C4I) systems—in order to paralyze the enemy” (Daohai: 1999). Qiao Liang, Li Ming, Zheng Hui worked together on EM algorithm and powerful error correction code to design a new anti-jamming communication technique. Simulation results show that the proposed technique can still provide a reliable communication link, even when the SINR equals 0 dB.

3. Official Discourse (Government Position)

The Department of Defense (DoD) has said that the Chinese government, in addition to employing thousands of its own hackers, manages massive teams of experts from academia and industry in “cyber militias” that act in Chinese national interests with unclear amounts of support and direction from China’s People’s Liberation Army (PLA). A Northrop Grumman report, “Capability of the People’s Republic of China to Conduct Cyber Warfare and Computer Network Exploitation,” said that Beijing appeared to be conducting “a long-term, sophisticated, computer network exploitation campaign against the U.S. government and its military contractors” (Northrop Grumman 2009: 51). The follow-up report reiterated that trend and explicitly mentioned China and Russia as being the most active countries, engaged

in cyber espionage (Northrop Grumman 2012). Over the recent past, official U.S. concern over alleged Chinese espionage has consistently grown.

The spokesperson from the Chinese Ministry of National Defense said, "Linking the cyber hacking with the Chinese Government and military is baseless, highly irresponsible, and hype with ulterior motives." China denies having any military hackers in the country. Other countries would most likely deny the same.

Both U.S. and China have different views on the issue of 'what actions in cyberspace would be considered as act of war?' PLA states, "Conventional counterattack would be sought if cyber attack targets military capabilities of another country and does significant damage." (Wortzel: 2011). On the other hand US assert, "Not only military, even if critical infrastructure is attacked, it would be considered as act of war."

4. Gaps in Literature

There exists no universally agreed definition of 'Cyberwarfare' and it is still being studied across the globe. There is no clear distinction between Information war and 'Cyberwar'. Some literatures consider both the same. Most of the literature suggests that 'Cyberwarfare' is an asymmetric mode of warfare that could be more helpful to militarily less advanced nation states as compared to militarily advanced nation states (as they have less to lose while already developed nation states have much to lose, for e.g. military technology etc.). This has been proved wrong by the recent Stuxnet and other virus attacks (if the newspaper report of involvement of US and Israel is true).

While evaluating China's 'Cyberwar' capability majority of the available literature talk more about China's Information warfare capabilities and cyber domain is still not analyzed thoroughly. Most of the evaluations are done by foreign authors, but none by Chinese authors. Mattia Nelles throws light on two recent studies of national cyber power which have placed China near the bottom of the table. On the EUI-Booz Allen Hamilton Cyber Power Index China is ranked 13th after Argentina, Mexico, and Brazil but better off than Russia, Turkey, South Africa, and India. Interestingly, the United Kingdom, United States, and Australia are the top three (The Cyber Hub, 2012). The second ranking on cyber security or cyber defense was made by the Brussels-based Security and Defense Agenda, which places China with Italy, Russia, and Poland in the fifth tier (the U.S. and the U.K. are in the third tier, below Finland, Sweden, and Israel and the top group is empty) (Miks 2012). Adam Segal, Senior Fellow at

the Council on Foreign Relations, reviewing these two studies concludes that both mentioned studies are very subjective as they are based on interviews, surveys, and vague metrics (Segal 2012).

Tom Gjelten quoted Mandiant Beytlich, an intelligence officer, saying that Chinese hackers can't be identified by their IP address but solely by the way they work: "They have quirks, maybe even the way that they type, the way that they select commands and the way that they build their software. There are probably twenty or more characteristics you can use, none of which involve an IP address"

5. Definition, Rationale and Scope of Study

My research puzzle starts with: "Can the ongoing conflict in cyberspace be referred as 'Cyberwar'? (If not why); If 'Cyberwar' does not go with the definition of traditional warfare, why 'Cold War' can be referred as 'War' and 'Cyberwar' cannot? Why and how China is using cyberspace as an asymmetric mode of operation? Is it still asymmetric (after Stuxnet incident)? My work uses both primary and secondary sources. Both Chinese and English language sources have been used. My work initially looks into the basic concepts involved in the study like 'Cyberwarfare,' Information Warfare, Cyber Attacks, Cyber Espionage, Cyber Sabotage, Cyber Defense, Computer Network Operations (CNO), Computer Network Attack (CNA) and Computer Network Defense (CND), Computer Network Exploitation (CNE) etc. It looks into similarities & differences between these concepts and their existing Chinese equivalents. Then, it probes into Chinese perception of 'Cyberwarfare' so as to understand the trends of China's 'Cyberwarfare' and to analyze the capability of China's 'Cyberwarfare'.

6. Research Questions

1. What constitutes Cyberwar? What are the differences and similarities between: Cyberwar and Information War; Cyberwar and Cyber Attack; Cyberwar and Cyber Espionage, Cyberwar and Cyber Sabotage?
2. What are the advantages that Cyberwar has on conventional warfare? Can Cyberwar replace the conventional warfare?
3. Is there a war already going on in cyberspace?
4. What is the Chinese perspective on 'Cyberwarfare'?

5. What is the nature of Chinese 'Cyberwarfare'? Which countries are the major adversaries?
6. What is the level of sophistication of China's 'Cyberwarfare'? What capabilities does China possess? Can it match with US level of sophistication?
7. What are China's goals behind conducting 'Cyberwarfare' (if any)?
8. What are the organizations involved in China's 'Cyberwarfare'?
9. What is the level of priority given to Cyberwarfare in the official military doctrine of PRC?
10. Which branch/department of PLA controls the military domain of cyberspace (of China)? Which branch/department is responsible for defence and attack in cyberspace?
11. Are all the incidents of cyber attacks are carried out by military sector of China or the civilian sector is also involved? If yes, up to what extent? Are they both coordinated and organized? Are hacker groups affiliated to PLA (or the government of PRC)?
12. If the problem of attribution (i.e. uncertainty in tracing the hackers or the origin of cyber attacks) is so serious, how can China be blamed for most of the hacking activities across the globe with such amount of certainty? Is China really responsible for most of the hacking activities across the globe?
13. Is China's cyberspace not vulnerable to cyber attacks? If yes, up to what extent?
14. Is deterrence possible in Cyberwar? What deterrence measures China has or will adopt if its cyberspace is attacked? Will military retaliation be used? If yes, when? What would be the threshold?
15. Is there any international legal frame work or organization in practice to check these activities of cyber attacks?
16. Is there any global convention on Cyberwar? Has any international treaty or agreement been signed between two or more nation states?
17. Is Cyberwarfare the latest WMD (Weapon of Mass Disruption) option?

7. Hypotheses

- The ongoing conflicts in the cyberspace carry full potential to convert itself into a total warfare.
- China's cyberwarfare capabilities are fairly limited and rudimentary.

8. Research Methodology

An inductive approach has been followed in this study. A host of primary sources are used like white paper on defence, government reports, documents published by US Department of Defense (DoD), USCYBERCOM etc. Both Chinese and English language secondary sources like books, articles and journals have been extensively used. Other sources of information based on electronic domain like interview recordings of experts etc. are also used. In this study cyberwarfare has been considered as independent variable, which can alter the lethality of dependent variable namely conventional warfare. Chinese government/ CPC/ hacker communities have been considered as intervening variable which can influence the latter one by making use of former one.

9. Chapterization

1. Introduction - Cyberwarfare and Related Concepts

This chapter introduces my research puzzle and the gaps in the existing literature. It lays the foundation for the research.

2. Understanding the Concept of Cyberwarfare – Global Discourse on Cyberwarfare

This chapter looks into the global discourse of cyberwarfare. It further traces the origin and definition of the term ‘cyberwarfare’ in both the official and unofficial documents so as to understand various perspectives of international organisations and nation states. It discusses the similarities and differences between cyberwarfare and other similar terms.

3. Chinese Concept of Cyberwarfare

This chapter probes into the existing equivalents of cyberwarfare in Chinese. It also discusses the views and opinions of various Chinese authors and military strategists so as to compare the similarities and differences between Chinese discourse on cyberwarfare and global discourse of cyberwarfare conceive this mode of warfare.

4. Organisations of Chinese Cyberwarfare

This chapter looks into the details of which institutes and organizations are associated with China’s cyberwarfare and how are they involved in it.

5. Intentions and Capabilities of Chinese Cyberwarfare

This chapter looks into the details of various cyber incidents in which China has been allegedly involved. A trend analysis of previous cyber incidents has been done so as to understand China's intentions and capabilities.

6. Conclusion

This chapter concludes with my research findings. It analyses cyber threats originating from China. It also analyses China's intentions and capabilities in the domain of cyberwarfare.

10. Limitations of the Study

The study on cyberwarfare cannot be limited to any timeframe. Hence, while tracing the origin and definitions of the term cyberwarfare, this study, sometimes might have gone beyond the given timeframe. In this study translation of Chinese language texts has been done in order to understand the perception of Chinese scholars. While doing the translation, few technical terms also encountered, which have been dealt with my limited Chinese language skills gained after five years of study in India and one year of study in China.

Chapter 2

Understanding the Concept of Cyberwarfare (Global Discourse on Cyberwarfare)

1. Tracing the Roots

The term 'cyberwarfare' has been quite popular recently especially after 'Stuxnet incident', a virus attack on Iranian nuclear enrichment centre, which damaged the centrifuges of nuclear enrichment centre. It is being discussed almost everywhere (in newspapers, blogs, tweets, talk shows etc.) (*USA Today* April 5, 2013) (*WSJ* July 06, 2012). Even nation states have also started attaching importance to it as it has become a serious national security threat. Therefore, the term 'cyberwarfare' is increasingly being used both in media and government reports (of countries like the US, UK etc. - which are discussed below). But what actually 'cyberwarfare' means and how is it defined is not known to all. It is somewhat similar to the argument put forward by Sarooshi, a professor of 'Public International Law' in the University of Oxford and a fellow of the Queen's College Oxford, in context of 'sovereignty'. Professor (2005) asserted that the concept of sovereignty is similar to the concept of god, everyone routinely refers to it, but just a few (or none) have deep knowledge about what this concept really means. It seems true for the case of cyberwarfare as well. So, is cyberwarfare the successor of 'Information Warfare (IW)' or is it a part or a subset of IW? Or is it used as synonym of IW, 'Network warfare', cyber attack, hackers' attack etc.? News reports keep on referring hacking incidents as cyberwar. Can these conflicts (like hacking, cyber intrusions etc.), which are going on in cyberspace be referred as cyberwarfare? So, what actually 'cyberwarfare' is and how is it related to other existing concepts such as Information Warfare (IW), Information Operations (IO), Computer Network Operation (CNO), Computer Network Attack (CNA), Computer Network Defence (CND), Computer Network Exploitation (CNE) etc., need to be analysed. In order to make the study of 'cyberwarfare' convenient, differences, similarities and relations between these concepts also need to be established. But first of all, origin of the term has to be traced. This chapter traces the origin of the term cyberwarfare: first in official documents of various nations and international organisations; and then in available global literature so as to understand the concept of cyberwarfare at international level. While doing so, this chapter also looks for official definitions (if available) provided by various nation and international organisations. This chapter also try to understand it in relation to various other similar terms. Towards the end this chapter discusses whether the term cyberwarfare deserves to be associated with the term warfare or not.

1.1 In Official Documents

Tracing the term is crucial but where to trace it from is much more crucial issue. For any researcher first priority is primary sources (like government documents, white papers, policy documents etc.), then comes secondary sources (such as books, journals, articles, newspaper articles etc.). Hence for tracing the roots same methods are followed. First, roots are traced in primary documents (i.e. in official documents) and then in secondary documents (i.e. in unofficial document or available literature on cyberwarfare). Since, this chapter covers the global discourse on cyberwarfare, for tracing the origin of the term official documents of United Nations (hereafter UN) and a few major powers like the United States of America (hereafter US), United Kingdom (hereafter UK), Russian Federation (Russia), Japan etc are considered.

1.1.1 Of United Nations (UN)

A document published by ‘United Nations Institute of Disarmament Research (UNIDIR, 2011)’ titled ‘Cyberwarfare and International Law’ written by Nils Melzer (which says that the views expressed in this publication are the sole responsibility of the author. They do not necessarily reflect the views or opinions of the United Nations, UNIDIR, its staff members of sponsors) defines the term ‘cyberwarfare’ as warfare conducted in cyberspace through cyber means and methods. Even when ‘cyberwarfare’ is broken into other two concepts: ‘warfare’ waged in ‘cyberspace’, definitions of none of the two is provided by UN. War by UN is defined in terms of ‘use of force’ and ‘aggression’. UN defines aggression in Article 1 of the UN General Assembly Resolution 3314 as “the use of armed force by a state against the sovereignty, territorial integrity, or political independence of another state.” A state of war may exist when a nation violates Article 2(4) of the UN Charter. Article 2(4) prohibits states from threatening or using force “...against the territorial integrity or political independence of any state.” However, not all force is prohibited. The UN Charter outlaws the use of aggressive force while recognizing the right of states to use force in self-defence as specified in Article 51. So, which action in cyberspace would be equal to ‘aggression’ and would ‘use of force’ be considered legitimate for it, remain unanswered. The only definition by UN says:

Cyber warfare is the use of computers or digital means by a government or with explicit knowledge of or approval of that government against another state, or private property within another state including: intentional access, interception of data or damage to digital and digitally controlled infrastructure. And production and distribution of devices which can be used to subvert domestic activity (UN Security Council Resolution 2011).

1.1.2 Of the United States (US)

The US was the first nation which recognized cyberspace as the fifth war fighting domain (after land, sea, air and space). The concept of 'cyberwarfare' was also developed and used for the first time by the US. The US was again the first country to establish a cyber command (CYBERCOM). The US has done plenty of research on how to exploit cyberspace for its strategic advantage and has published a lot of documents related to cyberspace (both military and academic). When these documents are looked at, it is observed that the concept of 'cyberwarfare' did not emerge suddenly rather it evolved over a period of time from pre-existing concepts.

1.1.2.1 Evolution of the Concept

i. Information Warfare (IW)/ Information Operation (IO)

An Air Force (US) document titled 'The Foundation of Information Warfare' makes a distinction between information age warfare and information warfare: the former uses computerised weapons and the latter uses information as a weapon, an independent field. The doctrine of the Joint Chiefs of Staff committee (JP 3-13, 1998) identifies 'computer attacks' as one of the offensive activities of 'Information Operations'. It also includes a few computer related terms like computer network attacks (CNA), computer security (COMPUSEC) etc. It defines CNA as "operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks or the computers and networks themselves (though this term and its definition were approved for inclusion in the next edition of Joint Pub 1-02)." Thus it can be observed that computer was already a part of information warfare ever since the inception information warfare.

Another US Air Force document AFDD 2-5 (later on changed to AFDD 3-13) titled 'Information Operations', published on 11 January 2005, no longer used the expression 'information warfare', rather emphasis was given on information operation which could be implemented any time: peace, war or when returning to peace. According to the document information operations were integrated use of three capabilities out of which one component was – network warfare operations: attack (Net A), defend (Net D) and support (NS). These all belonged to the category of computer network attack (CNA). On 13 February 2006, Joint Chiefs of Staff committee published another doctrinal document JP 3-13 called 'Information Operations', in which the expression of 'information warfare' was missing again. The document again used the term 'information operations', having five components out of which

one was – computer network operation (including the traditional attack, exploitation and defence operations: Computer Network Exploitation (CNE); Computer Network Defence (CND) and Computer Network Attack (CNA)). In the 22 March 2007 version of the Dictionary of Department of Defence, the expression ‘information warfare’ practically disappeared. Here, it can be observed again whether it was information warfare (IW) or information operation (IO) computer and other cyber components (like computer network etc) were always a part of it.

ii. Cyberspace

For the first time, the term cyberspace was used in the Joint Publication JP 2-0 (March 2000) [was missing in JP 3-13 (1998)] however its definition was missing. It was defined later on in JP 2-01.3 (May, 2000) and JP 1-02 (April 2001) as ‘the notional environment in which digitized information is communicated as over computer networks’, implying cyberspace was simply a communications medium of a theoretical or imaginary nature. ‘National Strategy to Secure Cyberspace (NSSC, 2003)’ defines cyberspace “ as nervous system of national critical infrastructure¹ which is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that make our critical infrastructures work. In 2006, the Chairman of Joint Chiefs of Staff referred to cyberspace as a “domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures,” which recognized cyberspace as a domain that stretched beyond computers.

The same expression is perceived otherwise by other organisations of same country. For instance, Air Force’s Cyber Task Force in 2006, deemed cyberspace as an operational war fighting domain where the electromagnetic spectrum was the manoeuvre space. Even Department of Defence (Hereafter DoD) by 2006, achieved the important milestone of a common cyberspace definition that designated it a warfighting domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures (National Military Strategy for Cyberspace Operations, 2006).”

Later on, in 2008 definition of cyberspace matured as “global domain within the information environment consisting of the interdependent network of information technology

¹ National Critical Infrastructure according to NSSC s are composed of public and private institutions in the sectors of agriculture, food, water, public health, emergency services, government, defence industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping.

infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers” (JP 1-02, Oct 2008). Cyberspace policy review (2009) defines cyberspace as the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. Common usage of the term also refers to the virtual environment of information and interactions between people. AFDD 3-12 (July 2010) again defines cyberspace as “global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers”

Going ahead in the series of information and information superiority, ‘DoD Dictionary of Military and Associated Terms (2013)’ after defining cyberspace (in a similar way as AFDD 3-12 and JP 1-02 have defined) also defines cyberspace superiority – “The degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations by that force, and its related land, air, maritime, and space forces at a given time and place without prohibitive interference by an adversary.” Latest in the ‘Superiority Series’ is ‘Full Spectrum Superiority’, which ‘DoD Dictionary of Military and Associated Terms (2013)’ defines as – “The cumulative effect of dominance in the air, land, maritime, and space domains and information environment (which includes cyberspace) that permits the conduct of joint operations without effective opposition or prohibitive interference.”

iii. Cyberspace Operation

Next in the series was ‘Cyberspace Operation’. It was initially considered a part of ‘Information Operation’, which is visible from the following document.

IO is not about ownership of individual capabilities but rather the use of those capabilities as force multipliers to create a desired effect. There are many military capabilities that contribute to IO and should be taken into consideration during the planning process. These include: strategic communication, joint interagency coordination group, public affairs, civil-military operations, cyberspace operations (CO), information assurance, space operations, military information support operations (MISO), intelligence, military deception, operations security, special technical operations, joint electromagnetic spectrum operations, and key leader engagement. (JP 3-13)

But it was defined later on in ‘Joint Publication (JP 3-0)’ as, “Cyberspace operations employ cyberspace capabilities primarily to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend DoD information networks.” For the latest definition ‘DoD Dictionary of Military and Associated

Terms (2013)' can be referred which also has the same definition (as that of JP 3-0) – “The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.”

This dictionary also includes another similar expression called ‘Defensive Cyberspace Operations (DCO)’ and defines it as – “Passive and active cyberspace operations intended to preserve the ability to utilise friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems.” Going further ahead dictionary adds on another expression called ‘Defensive Cyberspace Operation Response Action DCO-RA’ and defines it as – “Deliberate, authorized defensive measures or activities taken outside of the defended network to protect and defend Department of Defence cyberspace capabilities or other designated systems.” Without missing the offensive aspect of cyberspace operation, Dictionary includes and defines ‘Offensive Cyberspace Operations (OCO)’ as – “Cyberspace operations intended to project power by the application of force in or through cyberspace.”

iv. Cyberwarfare

Cyberwarfare, according to Congressional Research Service Report for Congress (CRS report, June 2001, titled Cyberwarfare), refers to ‘warfare waged in cyberspace’. This report says, “It can include defending information and computer networks, deterring information attacks, as well as denying an adversary’s ability to do the same. It can include offensive information operations mounted against an adversary, or even dominating information on the battlefield.”

Since 2001 CRS report, cyberwarfare has been upgraded from one component of information operations (i.e. information warfare) to the title of the reports (2004, 2006, 2007). Though subsequent CRS reports did not come up with any modifications in 2001 definition of cyberwarfare however they emphasised on its rapidly growing importance and suggested US government for adequate policy measures. Such was its importance that DOD in 2006 and CRS report in 2007 declared cyberspace a warfighting domain similar to that of land, sea, air and space. A separate cyber command (CYBERCOM) was also created under US air force.

Though the term cyberwarfare has been extensively used in government documents (US) and official discourse published after 2001, but it is still not included in JP 1-02 DOD Dictionary of Military and Associated Terms Nov 2010 (as amended through November 2012).

1.1.3 Of NATO (North Atlantic Treaty Organisation)

NATO in its 'Study Guide LIMUN 2012' defines cyberwarfare as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption." Though this definition is quoted from Richard A. Clarke's book 'Cyberwar (2010)' but the document further asserts that this definition is however only a rough and in no way conclusive definition. NATO document also says, "Serious security threats may also come from non-state-actors, such as companies, organisational units or terrorist networks." It has divided cyber-attacks in two categories: Distributed Denial-of-service (DDoS) also known as sabotage and espionage. NATO also provided assistance to Estonia in restoring its online services after it witnessed two weeks prolonged cyber attacks in 2007. NATO established 'Cooperative Cyber Defence Centre of Excellence' in Tallinn to conduct research on cyber related issues, a result of which has been recently published (Cambridge University Press, 2013) in the name of "Tallinn Manual on the International Law Applicable to Cyber Warfare". However the documents clearly mentions, "The Tallinn Manual is not an official document, but instead an expression of opinions of a group of independent experts acting solely in their personal capacity. It does not represent the views of the Centre, our Sponsoring Nations, or NATO. It is not meant to reflect NATO doctrine." Nevertheless the document is an important contribution towards the understanding of cyberwarfare.

1.1.4 Russian Federation (Russia)

Russia publishes its official documents by the name of 'Military Doctrine of the Russian Federation'. Two most recent documents were published in 2000 and 2010. The most recently published document of 2010 does not mention the term 'Cyberwarfare' directly, but the document divided into four sections, containing fifty three bullet points, uses the term 'Information' thirteen times and the term 'Information Warfare' thrice. This repetition of these terms itself portrays the importance being attached by Russian Government. Russia looks forward to develop the forces and means of information warfare (which also cover cyberwarfare) further (bullet point 41 c). Document also emphasises, "Early implementation of measures of information warfare for political purposes without the use of force, and subsequently, in the interest of shaping a favourable response from the international community to use military force (Bullet point 13 d)." This approach has already been implemented by Russians (only if the reports of cyber-attacks by Russians are true- which has

not yet been proven) when they attacked Georgia in 2008 followed by military attacks. The importance attached to information warfare by Russian military strategist can also be observed from the following document:

“From a military point of view, the use of Information Warfare against Russia or its armed forces will categorically not be considered a non-military phase of a conflict whether there were casualties or not . . . considering the possible catastrophic use of strategic information warfare means by an enemy, whether on economic or state command and control systems, or on the combat potential of the armed forces . . . Russia retains the right to use nuclear weapons first against the means and forces of information warfare, and then against the aggressor state itself (V. I. Tsymbal, 1995).”

Though this is an old document (speech), however it should still be taken into account. If deterrence by nuclear means would be considered by Russia in case of information warfare (including cyberwarfare) is waged against Russia, it itself expresses the high priority given to information warfare. More recently, in 2007 (against Estonia) and in 2008 (against Georgia), Russia showed its sophisticated cyber capabilities (if reports are to be believed – as these charges against Russia have not yet been proved). These incidents again emphasise the kind of priority given to cyberwarfare. Jeffrey Carr (2011) also emphasises, “Of China, Russia and the U.S., its Russia that has been the most active in the implementation of cyber attacks against its adversaries, which include Chechnya, Kyrgyzstan, Estonia, Lithuania, Georgia and Ingushetia.”

It is really difficult to trace Russia’s official definition of cyberwarfare as not many official documents are publicly available. However, five authors² of an article titled “RF Military Policy in International Information Security” from Moscow Military Thought (March 21, 2007) defined information warfare as:

The main objective will be to disorganize (disrupt) the functioning of the key enemy military, industrial and administrative facilities and systems, as well as to bring information- psychological pressure to bear on adversary’s military-political leadership, troops and population, something to be achieved primarily through the use of state-of-the-art information technologies and assets.

² Five authors were: I. N. Dylevsky; S. A. Komov- a Russian military theorist; S. V. Korotkov- attached to the Main Operations Department, General Staff of Armed Forces; S. N. Rodionov; A. V. Fedorov- served in the FSB’s Directorate of Counterintelligence Support to Transportation.

1.1.5 United Kingdom (UK)

Captain Ian A McGhie (2012) from 'Royal Navy, UK' writes, "The Ministry of Defence (MoD) shies away from using the term 'cyberwarfare', thinking in terms of 'warfare' more generically, which cyber actions in turn support. Consequently, no recent UK Government publication uses the term 'cyberwarfare'; 'cyber-power' is often used instead." This points out that it is difficult to find UK's official definition of cyberwarfare, still official documents have to be looked at so as to understand the kind of priority given to such threats. UK's National Security Strategy (NSS, 2010), while evaluating priority risks declares, "Hostile attacks upon UK cyber-space by other states and large scale cyber-crime" as Tier One priority risks to national security (Tier One has three more risks³)." In another official document titled 'The Strategic and Security Review (SDSR, 2010)', Prime Minister Cameron and Deputy Prime Minister Clegg said, "We will establish a transformative national programme to protect ourselves in cyberspace. Over the last decade the threat to national security and prosperity from cyber attacks has increased exponentially. Over the decades ahead this trend is likely to continue to increase in scale and sophistication, with enormous implications for the nature of modern conflict. We need to be prepared as a country to meet this growing challenge, building on the advanced capabilities we already have." SDSR allocated National Cyber Security Programme with 650 million pounds for four years (2009-2013) to protect the UK from cyber attacks from both nation states and individuals. Thus in terms of priority cyber threats rank almost on the highest level.

1.1.6 Japan

The Constitution of Japan (1947), called the constitution for Peace, forces Japan (in Article 9) to abandon the idea of war and bans it from having any war potential. Japan therefore has no army *per se*, but has self-defence forces. Japan is restricted by its alliance with US. Under these conditions, developing an independent doctrine, to include information warfare and distinct from US would be difficult (Daniel, 2009). The case of cyberwarfare cannot be different. Hence, Japanese cyberwarfare doctrine would be in alignment with US. Daniel (2009) mention about the serious crisis of the Yen in 1988 (Fall of Yen – 22 percent of its value in just 2 days), which was caused by a Trojan horse created by Chinese and Asian

³ Other three risks mentioned are: international terrorism; international military crises and major accidents or natural hazards.

criminal organisations. This incident must have compelled Japanese government to rethink about the importance of cyberwarfare. Probably that's why, since 2010 the issue of cyberwarfare and cyberspace has been incorporated in Japan's defence white papers under the theme of 'Issue in the International Community'. Unfortunately, the white papers neither define the term 'cyberwarfare' nor cyberspace; rather they are an attempt to do a trend analysis of cyberwarfare and cyberspace activities going on in international arena. These white papers instead of talking about Japan's own notion or efforts of securing cyberspace, talks more about other countries. Nevertheless, a separate section on cyberwarfare and cyberspace in defence white papers does emphasise the kind of importance attached by Japanese government.

1.1.7 Taiwan (Republic of China)

Republic of China (hereafter Taiwan) in its National Defence Report (Hundredth Anniversary) enlisted hacking of critical information system as emerging national threat. It also acknowledges the emphasis given on information warfare by the government of People's Republic of China (hereafter China), which indirectly emphasises strengthening Taiwan's own information warfare capabilities to counter China. Again in the case of Taiwan problem remain the same. Official documents do not explicitly mention cyberwarfare, nor do they define it.

1.2 In Un-official Documents (Available Literature – Global Discourse)

As per the definition of UNIDIR (2011) and CRS report 2001 Cyberwarfare is comprehended by breaking it into two other concepts: 'warfare' waged in 'cyberspace'. As far as act of war or warfare is considered no definition is provided by international law. Hence in order to understand war and warfare two widely referred authors are Clausewitz and Sun Zi (孙子 referred as Sun Tzu in West, though he does not belong to West but his translated version is widely referred in West).

Clausewitz's definition of war says, "War is merely continuation of politics— or of policy— by other means. War is nothing but a duel on an extensive scale...Each strives by physical force to compel the other to submit to his will...and thus to render an adversary incapable of further resistance. War therefore is an act of violence to compel our opponent to fulfil our

will.” Sun Zi’s definition of war is to defeat the enemy without actually fighting. He sees the use of force almost as a last resort in war. He focuses on victory with the least damage and the swiftest resolution. Sun Zi stresses the importance of out-thinking the enemy, while Clausewitz focuses on destroying the enemy’s army and occupying his lands. Sun Zi focuses on the end with many means, while Clausewitz stresses only one means to that end.

When the origin of second concept i.e. cyberspace is looked at, Martin Stallone (2009) suggest that ‘Cyberspace’ was first coined in 1984 by William Gibson in his novel ‘Neuromancer’. It calls cyberspace a ‘consensual hallucination.’ (Though Chinese scholars Ding Jianlin (丁建林) and Zhang Yong (张勇) (2012) trace the origin of the term ‘cyberspace’ three years earlier (1981) in another novel ‘Burning Chrome’ by the same Canadian author William Gibson.) Dan Kuehl, an information operations expert at the National Defence University identified over a dozen definitions of cyberspace in circulation, ranging from Google’s “the place between the phones” to several variations within the Department of Defence. His definition of cyberspace is

Cyberspace is a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information via interdependent and interconnected networks using information communications technologies (ICT).

Daniel (2009: 23) argues, “in a general way, cyberspace is made up of computers, communication, systems, networks, satellites, communication infrastructure and transport systems using information in its digital form (in cars, trains, air planes, elevators etc.), sound, voice, text and image data that circulates and is processed, system that can be controlled remotely via a network, all control systems operating energy supplies, digital watches, digital cameras, robots, as well as weapons, missiles, GPS systems, all technologies and communication tools (Wi-Fi, laser, modems, satellites, local networks, cell phones, fiber optic, computers, storage supports, fixed or mobile equipment, etc.)” Franklin D. Kramer and Stuart H. Starr, in their book ‘Cyberpower and National Security’ define cyberspace as a global domain within the information environment whose distinctive and unique character is framed by the use of electronic and electromagnetic spectrum to create, store, exchange, modify and exploit information via independent and interconnected networks using information communication technology.

As a combined term 'Cyberwar' was first used by John Arquilla in his work '*Cyberwar is Coming*' long back in 1993 (reprinted as chapter 2 in '*In Athena's Camp*' 1997). Since then, scholars and experts all over the world have attempted to analyze this concept and have come up with their opinions and understandings, which resulted in emergence of rich literature and schools of thought. John Arquilla came up with similar sounding concepts namely 'Netwar' and 'Cyberwar'. He distinguishes between them by saying, "'Netwar' is societal-level ideational conflicts waged in part through internetted modes of communication and 'Cyberwar' is at the military level." He further explains:

Netwar refers to information-related conflict at a grand level between nations or societies. It means trying to disrupt, damage, or modify what a target population "knows" or thinks it knows about itself and the world around it. A netwar may focus on public or elite opinion, or both. It may involve public diplomacy measures, propaganda and psychological campaigns, political and cultural subversion, deception of or interference with local media, infiltration of computer networks and databases, and efforts to promote a dissident or opposition movements across computer networks (Arquilla 1997: 28).

Regarding 'Cyberwar' John Arquilla, says:

Cyberwar refers to conducting, and preparing to conduct, military operations according to information-related principles. It means disrupting if not destroying the information and communications systems, broadly defined to include even military culture, on which an adversary relies in order to 'know' itself: who it is, where it is, what it can do when, why it is fighting, which threats to counter first, etc. It means trying to know all about an adversary while keeping it from knowing much about oneself. It means turning the 'balance of information and knowledge' in one's favour, especially if the balance of forces is not. It means using knowledge so that less capital and labour have to be expended (Arquilla 1997: 30).

Richard A. Clarke defines 'Cyberwar' as actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption (Clarke 2012). Another author Jeffrey Carr, inspired by Sun Zi, defines 'Cyber Warfare' as an art and science of fighting without fighting; of defeating an opponent without spilling their blood (Carr 2009). James Mulvenon in his work identifies PLA definition of computer network warfare:

The general term for all sorts of information offense and defence actions in which computers and computer networks are the main targets, in which advanced information technology is a basic means, and which take place throughout the space occupied by networks. The core of computer network warfare is to disrupt the layers in which information is processed, with the objective of seizing and maintaining control of the network space (Mulvenon 2009).

According to a definition of a website (uslegal.com- which claims it to be the legal definition), cyberwarfare refers to a massively coordinated digital assault on a government by another, or by large groups of citizens. It is the action by a nation-state to penetrate another nation's computers and networks for the purposes of causing damage or disruption. But it adds that "the term cyberwarfare may also be used to describe attacks between corporations, from terrorist organisations, or simply attacks by individuals called hackers, who are perceived as being warlike in their intent."

Joseph S Nye defines 'Cyber war' as "hostile action in cyberspaces, whose effects amplify or are equivalent to major physical violence". He further says, "Cyber war, though only incipient at this stage, is the most dramatic of the potential threats. Major states with elaborate technical and human resources could, in principle, create massive disruption and physical destruction through cyber attacks on military and civilian targets. Technology today favours an offensive actor rather than defensive one. States have the greatest capabilities, but non-state actors are more likely to initiate a catastrophic attack. A 'cyber 9/11' may be more likely than the often-mentioned 'Cyber Pearl Harbour'" (Nye 2012).

Martin C Libicki while defining 'Information Warfare' identified seven major components: command and control warfare (C2); intelligence warfare; electronic warfare; psychological operations; hacker warfare (software attacks against information system); economic information warfare through the control of commercial information); and cyber warfare (virtual battles) . He, later on, pointed out to two types of 'Cyberwars': Operational 'Cyberwar' and Strategic 'Cyberwar'. He says, "Operational cyberwar— cyberattacks to support warfighting— may have far greater purchase than strategic cyberwar, cyberattacks to affect state policy. An operational cyberwar capability may well be an effective niche weapon if correctly timed. Strategic cyberwar campaigns are more problematic and hence merit less emphasis" (Libicki 2009: 06).

Daniel Ventre in his detailed account of information warfare, based on the different doctrines which are formulated in US and all over the world, has identified computer network attacks (CNA) as one of the components of information warfare (others are Psychological Operations [PSYOPS], Electronic Warfare, military deception, Operation Security [OPSEC] and Information Assurance [IA]). William Hagestad says cyberwarfare is "Calculated use of offensive & defensive computer network attacks (CNA); & computer network exploits (CNE); taking advantage of computer network vulnerabilities (CNV) at the geo-political level, nation to nation, fighting in – cyber space." George Rattray points out that "the use of non-

violent digital attacks to achieve political objectives must be understood as part of a new form of warfare.” Colin Gray contributes to the debate by contending that cyberwarfare is all about information, it “refers to warfare in cyberspace; bloodless electronic warfare in the struggle or deny or gain information.

Institute of Defence Studies and Analyses (IDSA) an Indian think tank defines ‘Cyber warfare’ as “actions by a nation-state or its proxies to penetrate another nation’s computers or networks for the purpose of espionage causing damage or disruption” (IDSA Task Force Report 2012: 31). Shashi Tharoor defines ‘Cyber War’ as unauthorised invasion by a government into the systems or networks of another, aiming to disrupt those systems, to damage them partially, or to destroy them entirely (Tharoor 2012).

2. Locating Cyberspace and Cyberwarfare (Establishing Relations with Other Terms)

In order to understand the term cyberwarfare properly, understanding it in isolation is not enough. It has to be understood in relation to various other already existing terms and expressions; it has to be located among them so as to understand the similarities and differences between them.

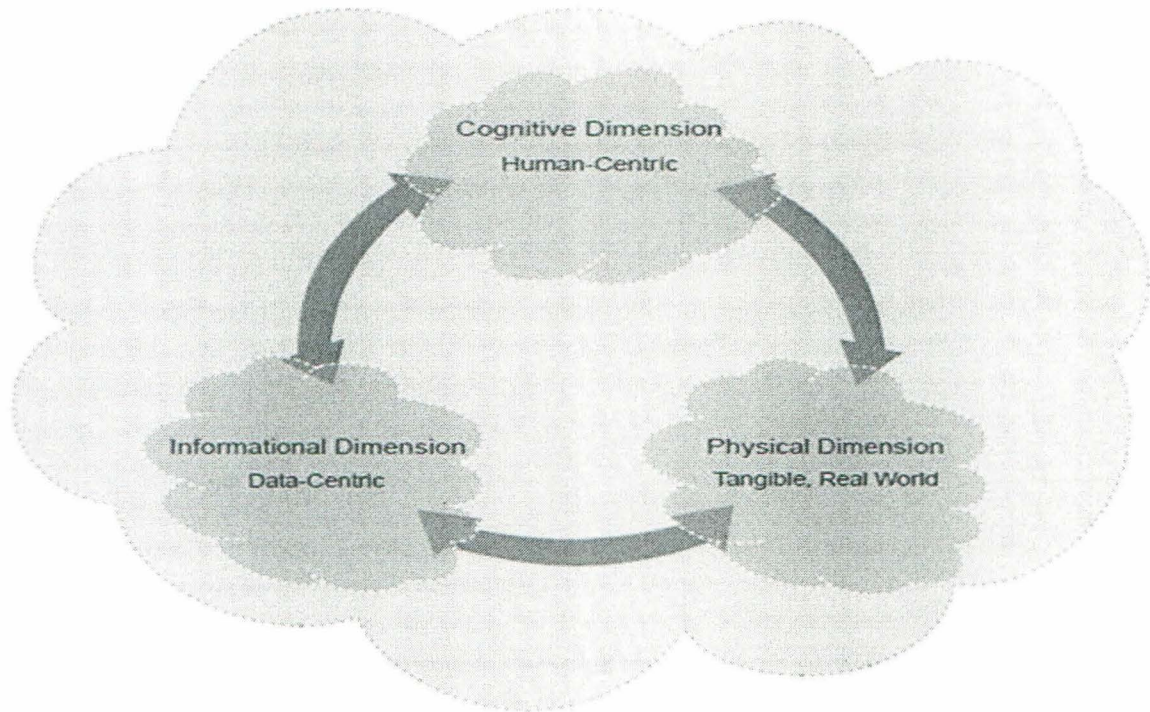
2.1 In Information Environment

While reconsidering the definition of cyberspace which is defined in Joint Publication as “global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers (JP 1-02, Oct 2008),” another concept of ‘information environment’ is encountered. So according to this definition, cyberspace is a subset of information environment. In order to understand cyberspace first information environment has to be studied well so as to locate cyberspace within it.

‘Information Environment’ is defined as the aggregate of individuals, organisations, and systems that collect, process, disseminate, or act on information (JP 3-13). This environment consists of three interrelated dimensions, which continuously interact with individuals, organisations, and systems. These dimensions as shown in the figure below are known as physical, informational, and cognitive.

Figure 1: The Content of Information Environment

The Information Environment



Source: JP 3-13, 2012 (Chapter 1, Page 2)

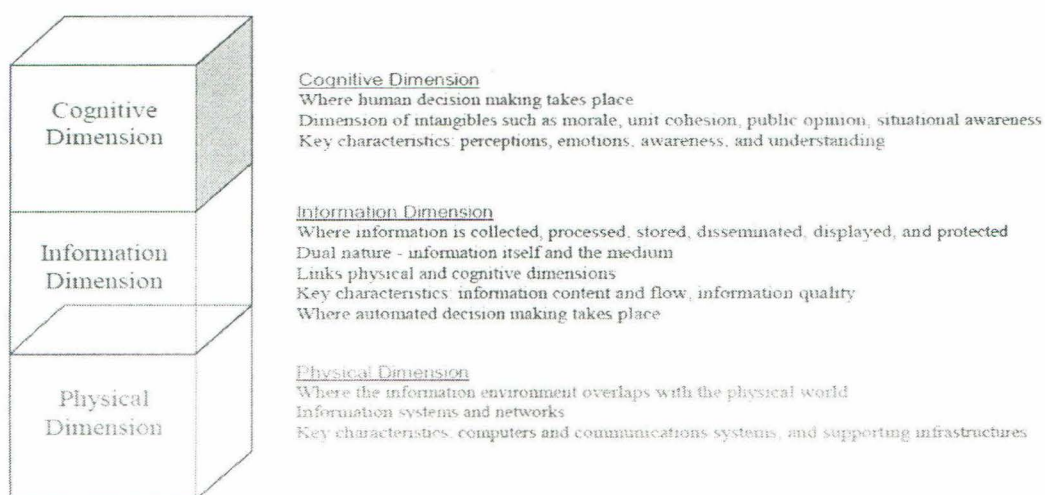
Joint Publication (JP 3-13) explains each one of these dimensions using the figure below. The Physical Dimension is composed of command and control (C2) systems, key decision makers, and supporting infrastructure that enable individuals and organisations to create effects. It is the dimension where physical platforms and the communications networks that connect them reside. The physical dimension includes, but is not limited to, human beings, C2 facilities, newspapers, books, microwave towers, computer processing units, laptops, smart phones, tablet computers, or any other objects that are subject to empirical measurement. The physical dimension is not confined solely to military or even nation-based systems and processes; it is a defused network connected across national, economic, and geographical boundaries (JP 3-13). The informational dimension specifies where and how information is collected, processed, stored, disseminated, and protected. It is the dimension where the C2 of military forces is exercised and where the commander's intent is conveyed. Actions in this dimension affect the content and flow of information (JP 3-13). The cognitive dimension encompasses the minds of those who transmit, receive, and respond to or act on information. It refers to individuals' or groups' information processing, perception, judgment, and decision

making. These elements are influenced by many factors, to include individual and cultural beliefs, norms, vulnerabilities, motivations, emotions, experiences, morals, education, mental health, identities, and ideologies (JP 3-13).

Martin Stallone (2009) also explains the composition of information environment and tries locating cyberspace in it. Using the following figures, he draws a link between information environment and cyberspace and asserted that cyberspace comprises a part of the ‘physical and information dimensions’ of the larger ‘information environment.’

Figure 2: The Three Dimensions of Information Environment

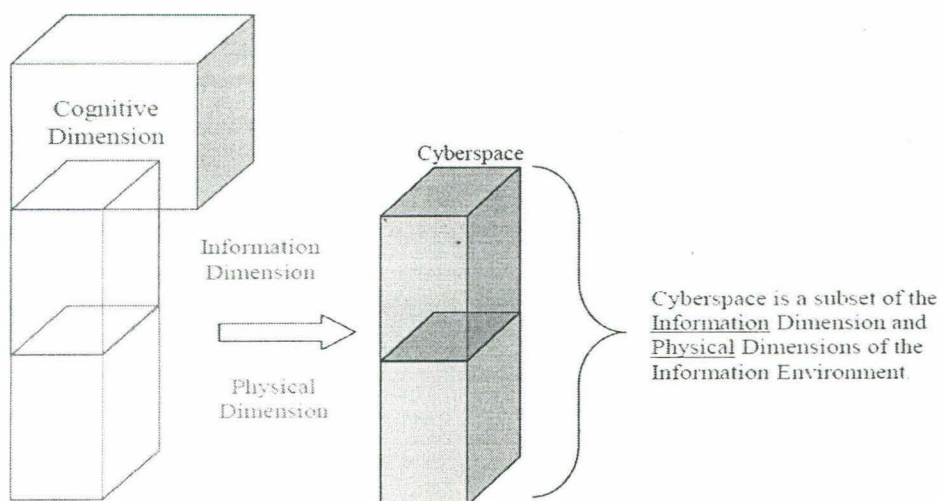
The Information Environment, consists of the physical, information, and cognitive dimensions.



Source: Martin Stallone (2009), (Figures, Page – 19)

Figure 3: Location of Cyberspace in Information Environment

Cyberspace consists of part of the information environment. It primarily encompasses the physical (interconnected) dimension: this is a function of our interconnected world. Information that is exchanged through networks is also *created, modified and stored* through electronics and associated networks



Source: Martin Stallone (2009), (Figures, Page – 19)

2.2 In Information Operation (IO/IW)

Department of Defence Directive (DoD Directives 3600.1) says, “Information Warfare (IW) involves actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one’s own information, information-based processes, information systems, and computer-based networks.” It is further defined as Information Operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries (IATAC TR- 97-002).

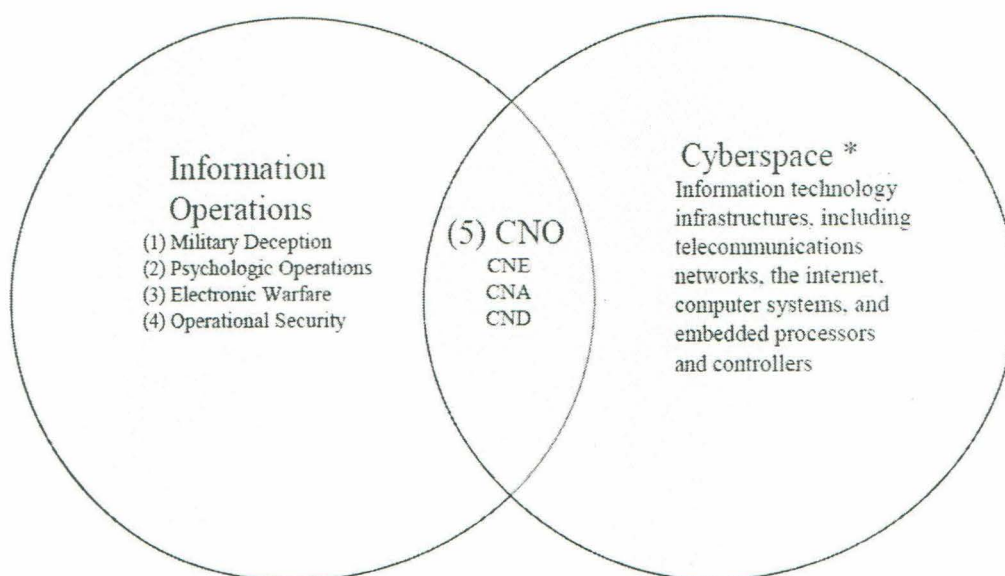
Above definition of ‘Information Warfare’ also include a term called ‘Information Superiority’; which according to ‘Joint Publication (JP 3-13)’ is – “The operational advantage derived from the ability to collect, process and disseminate an uninterrupted flow of information while exploiting or denying an adversary’s ability to do the same.” ‘Information Operations’ is almost same and an upgraded version of ‘Information Warfare’. It is defined as – “The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own.” There are five Components of Information Operations are – Psychological Operations (PSYOPS); Military Deception (MILDEC); Operations Security (OPSEC); Electronic Warfare (EW) and Computer Network Operations (CNO including CNA, CND & CNE). (JP 3-13) (CRS Report 2004)

According to ‘Joint Publication (JP 3-13)’, out of these five components, the last component ‘Computer Network Operation (CNO)’ also belongs to cyberspace which is quite evident from the figure below. Not only ‘Computer Network Operation (CNO)’, its sub components (i.e. ‘Computer Network Attack (CNA)’, ‘Computer Network Defence (CND)’ and ‘Computer Network Exploitation (CNE)’ also belongs to cyberspace. Thus, one relationship is established between cyberwarfare and information operations (IW/IO), however ‘Computer Network Operation (CNO)’ is just one part of cyberwarfare. What constitutes ‘Computer Network Operation (CNO)’ and its sub-components are discussed below.

Computer Network Operations (CNO) - Computer Network Operations are comprised of two specific yet complementary mission areas; Computer Network Defence and Computer Network Attack. CNO involves the ability to attack and disrupt enemy computer networks, protect military information systems, and exploit enemy computer networks through

intelligence collection. CNO is composed of methods for attack, defence and exploitation of information. (DOD Directive 3600.1 "Information Operations,")

Figure 4: Relationship between IO & Cyberspace



Source: JP 3-13, Information Operations

Computer Network Attack (CNA) - are operations designed to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers or networks themselves. (Department of Defence Directive 3600.1) (CRS Report 2004)

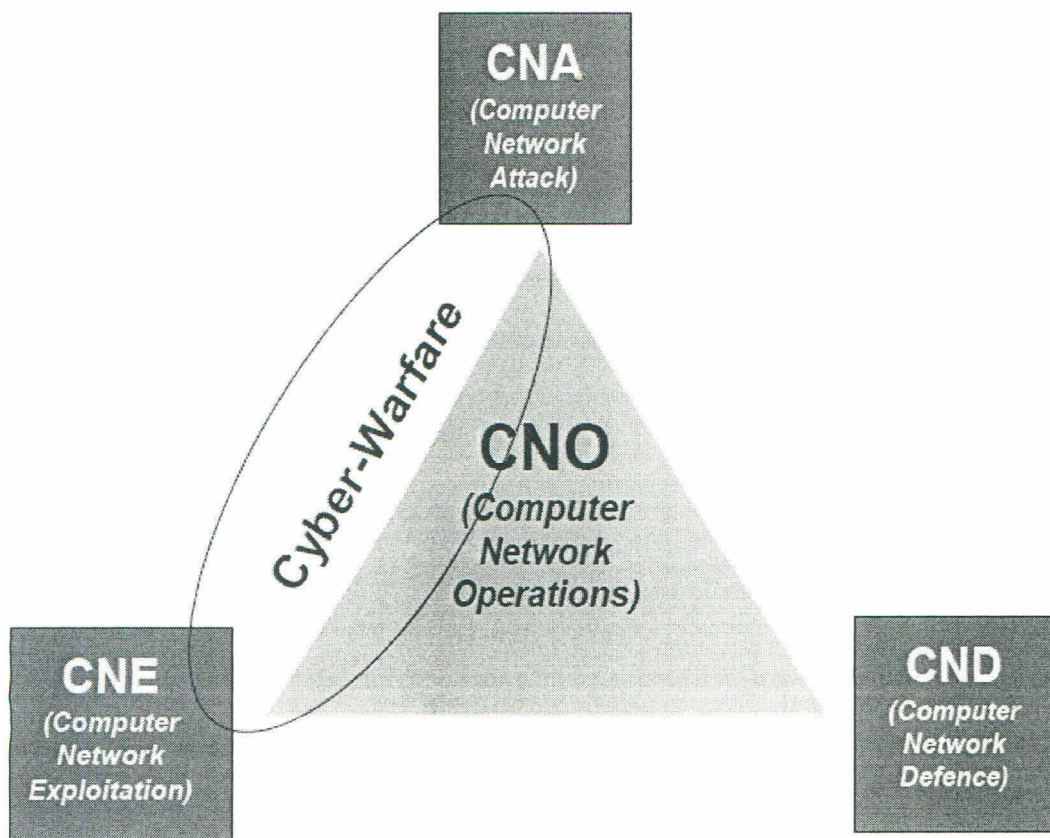
Computer Network Defence (CND) - is defined as defensive measures to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction. CND includes actions taken to protect, monitor, analyze, detect and respond to unauthorized activity within DOD information systems and networks. Defensive information warfare involves measures intended to prevent, detect, and subvert an enemy's direct, or indirect, actions against our information systems. (CRS Report 2004)

Computer Network Exploitation (CNE) - is an area of Information Operations that is not yet clearly defined within DOD. Information exploitation involves espionage that in the case of information operation is usually performed through network tools that penetrate adversary systems to return information or copies of files that singly, or collectively, enable the military

to gain an advantage over the adversary. Tools used for CNE are similar to those used for CNA, but configured for different objectives. (CRS Report 2004)

Captain Ian A McGhie (2012) from 'Royal Navy, UK', with the help of following figure tries to locate cyberwarfare among CNO, CNA, CND and CNE. This figure does not include CND as a part of cyberwarfare, which is slightly different from the explanation in the figure above. Thus it can be observed that there is no universally accepted definition of cyberwarfare. This point of view is again different from Fred Schreier, who says, "Computer Network Operations (CNO) covers only a narrower section of all cyber attacks."

Figure 5: Relationship of Cyberwarfare with CNA, CND & CNE – A Different Perspective



Source: Captain Ian A McGhie (2012, p.n. - 09)

Regarding the relationship between information operations and cyberwarfare, Eric D. Trias and Bryan M. Bell (2010), both from US Air Force, argue:

IO can be conducted in the cyberspace domain, as it has been for decades in other operational domains. However, not all IO can be considered cyberspace operations. For example, influence operations seek to achieve effects resulting in a change in the enemy's observe, orient, decide, act loop. Traditional means include dropping leaflets or using human messengers to conduct psychological operations (PSYOP). IO often consists of non-kinetic actions to defend our decision cycle and influence the adversary's, but it can also take the form of physical attack against tangible information infrastructures. The offensive counter-information activities of PSYOP, military deception, and information attack all have a place in the cyber realm. Well-trained cyber forces can influence enemy decision cycles by presenting misleading Web content or even changing information presented by reputable sources. Defensive counter-information activities such as information assurance and operational-security protocols are already in place at all Air Force installations, some in non-cyber form.

Thus, CNO seems to be only one part of cyberwarfare. IO and cyberwarfare seem to overlap, which means IO can be conducted in cyberspace and cyberwarfare can be conducted in information domain, but not all IO can be considered as cyberspace operations and not all cyberspace operations can be considered as IO.

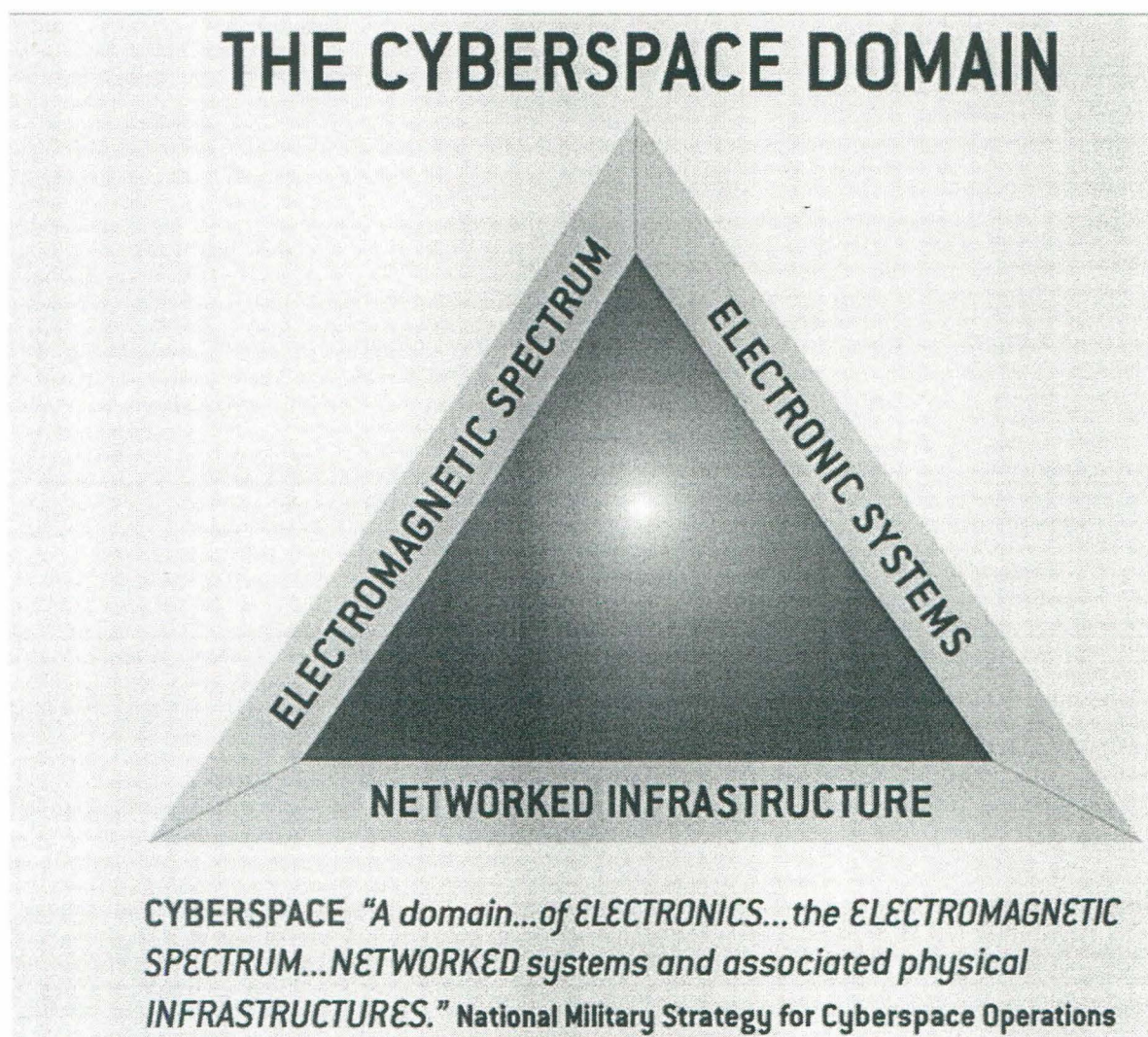
2.3 Among Others Terms

There are numerous terms and expressions linked to cyberwarfare and cyberspace (like IO/IW, Network Warfare/ Netwar, Net Centric Warfare, C2 Warfare, Electronic Warfare/ EW), on the contrary not much of literatures are available which could establish the link between them or demarcate the difference between them. According to the U.S. 'Air Force CYBERCOM Strategic Vision 2008', cyberspace is not just about computers and (computer) networks, it also includes electronic and electromagnetic spectrum. Franklin D. Kramer and Stuart H. Starr also argued the same in their book, which is illustrated in the figure below.

According to this figure, if electronic and electromagnetic are component of cyberspace, electronic warfare (EW) and warfare waged in electromagnetic spectrum (using electromagnetic pulse i.e. EMP etc.) would also be a part of cyberwarfare. However, Eric D. Trias and Bryan M. Bell (2010) argue, "Currently, Information Operations consists of influence operations, network warfare operations, and electronic warfare (EW) operations. With the advent of cyberspace operations, it is apparent that network warfare operations fall under this new concept. However, a debate continues over the future of EW."

Regarding electronic warfare, they again say, “EW operations seek to achieve effects across the electromagnetic domain, including radio frequencies as well as optical and infrared regions of the spectrum. Traditional EW operations conducted by aircrews over the past 50 years are considered non-cyber.”

Figure 6: Components of Cyberspace



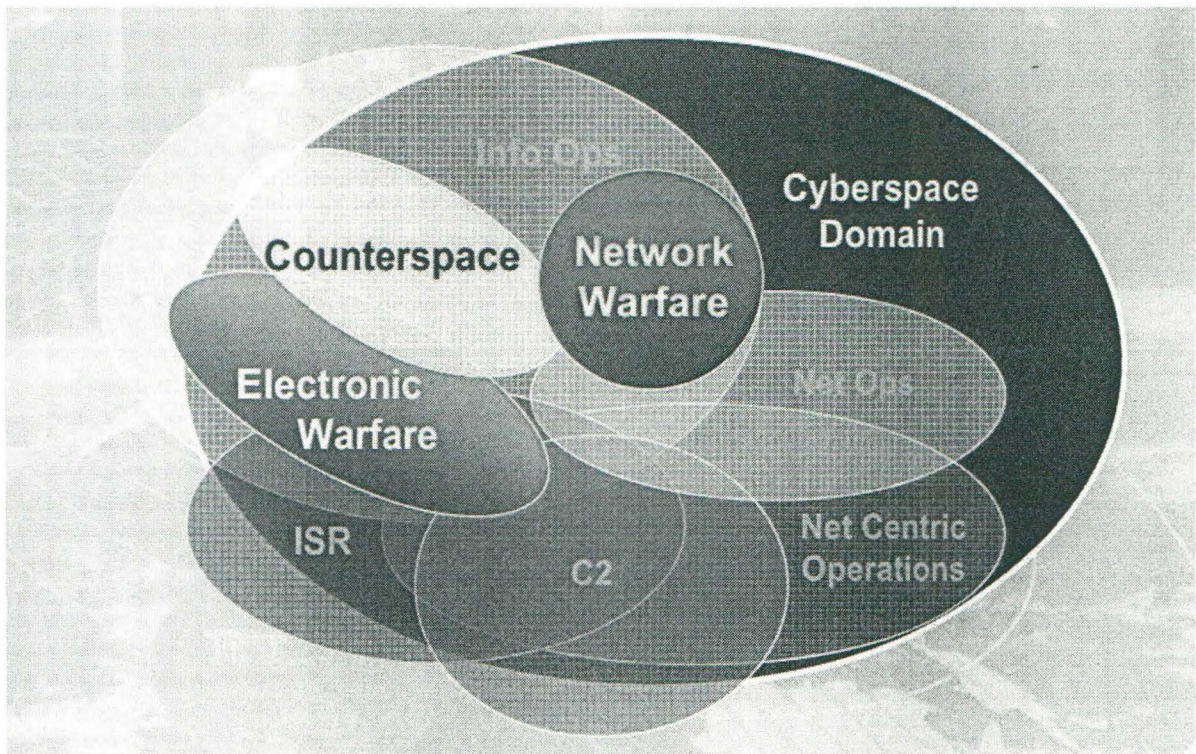
Source: U.S. 'Air Force CYBERCOM Strategic Vision 2008

Network Warfare, in short, is also referred as netwar, which according to Arquilla is societal-level ideational conflicts waged in part through internetted modes of communication (And 'Cyberwar' is at the military level). After comparing it with the US official definition of cyberwarfare (warfare waged in cyberspace), the contradiction can be observed as networked infrastructure (hence netwar also) is a part of cyberspace and thus netwar should also be

considered as cyberwarfare (according to official US definition). Or one more statement can be deduced that netwar is also a kind of cyberwarfare but not at the military level, if cyberwarfare has both military and non military (societal) component.

A comparative analysis was presented by Lani Kass (US Air Force Cyberspace Task Force) in form of following picture, which shows how cyberspace is related to other various terms and expressions.

Figure 7: Relationship between Cyberspace and Other Related Terms



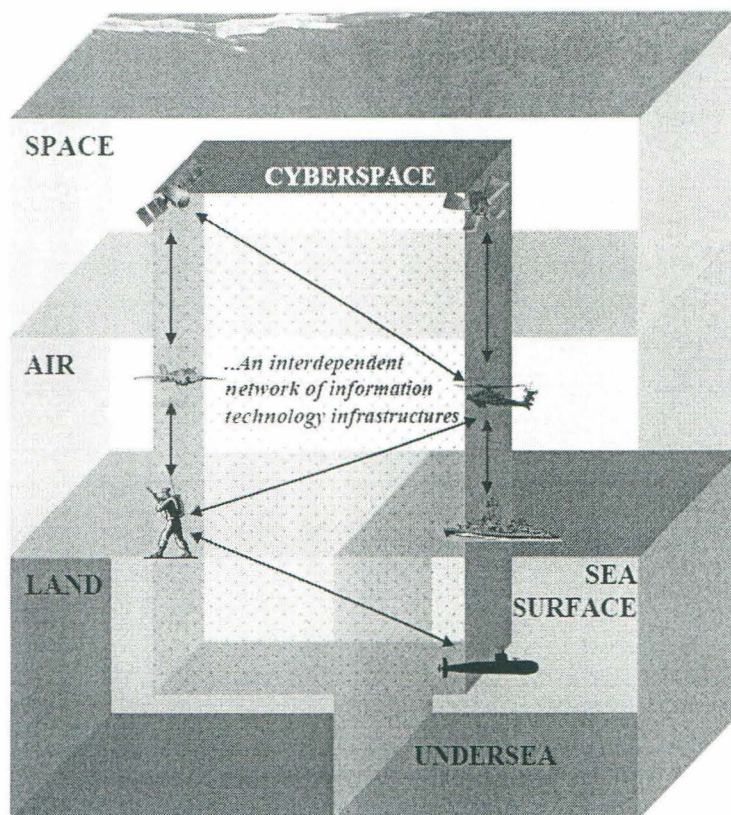
Source: Lani Kass (US Air Force Cyberspace Task Force, 2006)

2.4 Among other Domains

Cyberspace might have been declared a separate domain, but is it really separate from other domains? It is not that cyberspace does not exist in other domains. Computer, computer networks and other cyber components have their presence everywhere. So how can it be separate from other domains? Trias and Bell (2010) endorse the idea that cyber operations may be conducted in all war-fighting domains: air, space, cyberspace, land, and sea. Hence cyber elements are present in all other domains. The figure below also asserts, “For war fighter, this interdependent network of information technology infrastructures is a new kind

of physical space through which an adversary may be connected. It can overlie the other domains wherever ‘connections’ exist as per the definition of cyberspace.”

Figure 8: Relationship between Cyberspace and Other War Fighting Domains



Source: Martin Stallone (2009), (Figures, Page – 19)

Eric D. Trias and Bryan M. Bell (2010) again assert:

Despite the immaturity of cyberspace operational doctrines, the doctrines from air and space remain relevant and applicable to the cyberspace domain. Cyber operations are just another set of tools in the commander’s toolbox. Although cyber operations have distinct ways of achieving effects, from an Air Force perspective they are similar to other air and space operations that support air and space (and cyberspace) functions. Known and established cyber operations provide war fighters with viable options to kinetic means.

Thus, it can be observed that cyberspace might be separate war fighting domain but elements of cyberspace lie in all other traditional domains. Hence, other domains are also at risk as they are accessible through cyberspace. If cyberwarfare is waged, not only cyberspace but other traditional domains would also be involved.

3. Controversy with the Concept

Libicki suggests that the concept that cyberspace as a war fighting domain is misleading because the concept is “not helpful when it comes to understanding what can and should be done to defend and attack networked systems.” Bruce Schneiner (2010) argues that the threat of a cyber war has been ‘exaggerated’ due to a power struggle between US government agencies that are trying to control the state’s cyber security strategy. Due to the persistence of the U.S. Department of Defence and the National Security Agency, cyberspace has largely been ‘militarized’ through discussions of a cyber war allowing military to control the current US cyber security strategy. David Betz (2011) argues that the concept of cyberwar as a ‘single focus’ option for states is unrealistic because of the expanse and range of their interests and capabilities. As an alternative, Betz proposes ‘cyber-skirmish’ as the correct frame to describe current low-level cyber attacks against different states.

Thomas Rid, based on Clausewitz’s three main elements of war (violent character, instrumental character & political nature) argues in three steps that cyber war has never happened in the past, that cyber war does not take place in the present, and that it is unlikely that cyber war will occur in the future. He examines past incidents of cyber attacks through the lens of these three elements and announces them unqualified to be called as examples of ‘Cyberwar’ (Thomas Rid: 2012). Countering his argument, Jeffery Carr (2011) says, “The environment within which war is conducted has been permanently altered since Clausewitz’ time. Sun Tzu would have been a better choice because he at least considers the superior option of winning a war without fighting.” But even within the parameters that Professor Rid has established, Carr gave three examples that fit the Clausewitz test of being lethal, instrumental and political:

1. Kyrgyz Intelligence assassinates Gennady Pavlyuk. Kyrgyz intelligence cracked Pavlyuk’s email account and used the information they obtained to lure him out of the country under false pretenses resulting in his murder.
2. Mossad assassinates mahmoud Al-Mabhouh. Israel’s Mossad mounts an operation to assassinate Hamas leader Mahmoud Al-Mabhouh which includes infecting Al-Mabhouh’s computer with a trojan horse virus.
3. Iran’s IRGC arrests 30 dissidents after cracking U.S. hosted web servers.

Apart from these there are a few more incidents that support the argument of Jeffery Carr. In August 2012, huge exodus of north east people started from south Indian cities. Reports claimed that more than 15,000 people fled from Bangalore and more than 1,000 from Chennai. The Hindu reported, "The combined power of the mobile phone, the Internet and the social media was on display in the crisis that led to thousands of people from the northeast fleeing Bangalore." These acts in cyberspace did not just result in such a huge mass exodus, but it also created a few incidents of violence (9 held for targeting N-E students, 14 Aug 2012, The Hindu). One more incident that resulted into kinetic effect was 'Delhi metro train breakdown incident'. News report (*The Hindu*, June 12, 2013) says,

Peak hour commuters on Delhi Metro's Jahangirpuri-HUDA City Centre Line had a harrowing experience after the train they were travelling by developed a fault and broke down in a tunnel on Tuesday. The Delhi Metro Rail Corporation (DMRC) attributed the fault to a probable 'software malfunction' that led to emergency brakes being applied automatically to the train.

If software malfunction can stop the train imagine what software manipulation can result in. Capabilities of cyberspace were also underestimated again when it was considered that cyberspace cannot bring in 'kinetic effect' or it cannot result in physical damage. The 'Stuxnet (震网)' incident has changed the way cyberspace capabilities were conceived as it proved that cyberspace has the potentials to bring in physical damages (Stuxnet virus damaged the centrifuges of nuclear enrichment centre of Iran). Thus, neither violence nor physical damage (kinetic effect) is impossible for cyberspace to achieve.

Even the way 'cyberwarfare' should be written is an issue of debate. Some of the US official documents use the term 'cyberwarfare' and some of the US official documents also use 'cyber warfare'. Similarly some authors prefer to write it as 'cyberwarfare' and some as 'cyber warfare'.

4. Conclusion

As the available literature suggest there seems to be no universally accepted definition of cyberwarfare. There are no international organisations except UN which can help built consensus on the issue of cyberwarfare or which can define or can set the rules of cyberwarfare in international arena. The UN definition emphasises that involvement of nation state is necessary if an act has to be referred as cyberwarfare but nation states define it the way they like and some don't even bother to define it. This act of not defining cyberwarfare

might be a deliberate act by nation state so that they do not have to follow any rules or norms as defining cyberwarfare would put forward their views on the issue and that would explain what is acceptable and what is not for a particular nation. However, there is no guarantee that those who define it would follow the norms themselves. The literature review suggests that there is no consensus among nation states on what constitutes an act of cyberwar. What is acceptable for a nation state might not be acceptable for another. Many of the nation states do not even mention clearly what acts in cyberspace would not be acceptable for them crossing which a military retaliation would be sought. Thus it can be observed that there is anarchy in cyberspace. As far as views of scholars are concerned, they also differ from one another. According to some of the definitions the ongoing hacking and other cyber attacks can be referred as cyberwarfare and according to some they do not deserve to be. For example according to the definition of uslegal.com, cyber attacks from terrorist organisations, from individual hackers and from corporations can also be called cyberwar, if their intents are warlike. Now determining the intent of hackers, terrorists etc can be troublesome. It again may differ from nation to nation. Thus as of now it's all up to nation states, which can set the rules of engagement, cooperation and retaliation as per their own convenience.

Both the concept of 'Cyberspace' and 'Cyberwarfare' are complex. One reason for it is that ever since the concept of cyberspace has evolved its range, scope and contents have always been changing. Initially it was supposed to be related to computers and networks, but now even electronic and electromagnetic components belong to cyberspace. The term cyberwarfare emerged from IW/IO and hence it can be considered as a sub-set of IW/IO, but as it developed with time it included many aspects (like EW, CNO etc.) of IW/IO. Hence, it becomes difficult to understand a concept, whose contents keep on changing. The concept of cyberspace and cyberwarfare, as Joseph S Nye point out, are in their initial stage and are still developing as concept. In this process of development contents of cyberspace and cyberwarfare have also been changing. Initially only computer, network, internet, computer related peripherals etc. were associated with cyberspace, but now it also includes electronics and electromagnetic spectrum. Hence, as of now electronic warfare (EW) and electromagnetic weapons are also components of cyberwarfare. However, as per trends in past, future cyberwarfare may include new components and features.

Chapter 3

The Chinese Concept of Cyberwarfare

1. Tracing Chinese Views on Cyberspace and Cyberwarfare

China is one of the most active players in cyber domain. China allegedly has not only targeted non-classified networks of major powers but also targeted some classified weapon information of the US. China has been blamed for most of the hacking incidents that took place in last few years including a few high profiles hacking of the US government websites like Pentagon and White House etc. Recently a report published by an American private cyber security firm named 'Mandiant' claimed that most of these attacks are originating from a thirteen storey building located in the outskirts of Shanghai, which is an unit of People's Liberation Army (PLA) operating under the name of Unit 61398. China's foreign ministry spokesman Hong Lei rendered the report as "Groundless criticism", which is "irresponsible and unprofessional" (*Peoples' Daily* Feb 20, 2013). China's Defence Ministry also responded by arguing that the report's accusations are scientifically flawed and not reliable. The ministry also said that gathering information is not "online spying" (*CNN* Feb 20, 2013). Then where according to Chinese government lies the demarcation line crossing which would be unacceptable for China? Up to what extent China want other nation states to accept China's cyber exploitations? Is there any common consensus among nations on the issue? Is cyberwarfare the one concept which can serve in building consensus? How does Chinese government conceive this concept and what are the views of Chinese scholars? This chapter first looks into the official documents so as to understand the views of Chinese government. Then this chapter looks into the views of various Chinese scholars through their work and finally similarities and differences between Chinese and international discourse on cyberwarfare are analysed.

1.1. Official Documents

China's official documents (mainly white papers) do not talk much about cyber operations or cyberwarfare openly, so searching for an official Chinese definition of the concept does not seem possible. Though, China's 2004 defence white paper does talk about "informatisation (信息化)" of defence forces. One more expression on which China lays great emphasis is "networkisation (网络化)". Cyberspace and cyberwarfare fall under these two broad concepts.

Since both “informatisation” and “networkisation” are emphasised, cyberwarfare is also supposed to be given great importance. It is due to the fact that China cannot compete with technologically superior adversary in conventional warfare and cyber domain has exposed the weakness and vulnerabilities of most advanced nation states providing China asymmetric advantage to exploit. The most recent white paper (published in April 2013) uses the term ‘Cyber space’ (for the first time) twice under the topic “New Situation, New Challenges and New Missions”, which acknowledges the changing landscape of conflict and reaffirms the importance being attached to cyberspace.

1.2. Un-official Documents (Available Literature)

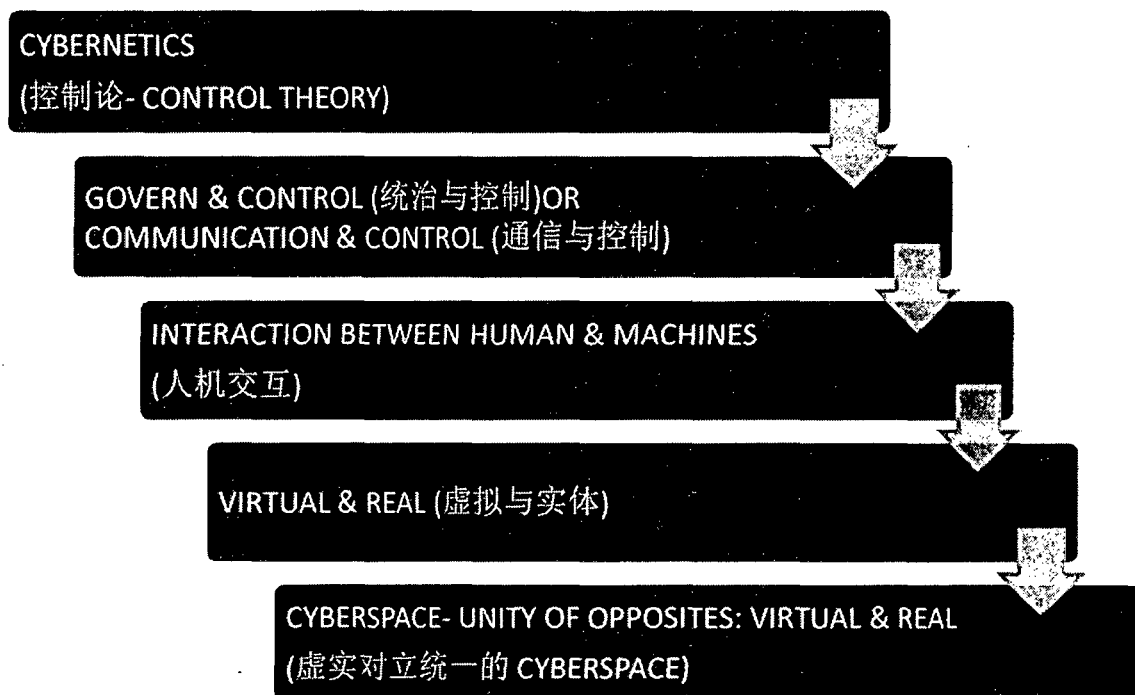
There is plenty of Chinese literature available on cyberspace and cyberwarfare. Though both of these concepts are of Western origin, however some of the Chinese scholars have completely different view from their Western counterparts and some of the Chinese scholars having different perspectives have added their own valuable inputs giving them some unique Chinese features and thereby making them richer in content.

1.2.1. Chinese Views on Origin of Cyberspace

Both the concepts of cyberspace and cyberwarfare have their origin in West. Most of the Western and Chinese authors (like Martin Stallone, Meng Fansong, Han Yining, Shi Rong, Li Jian, Huang Pengtao, Li Hao, He Minjue etc.) trace the origin of the term cyberspace in a novel named ‘Neuromancer (神经漫游者)’ written by William Gibson published in 1984. However, two Chinese scholars Ding Jianlin (丁建林 2012) and Zhang Yong (张勇 2012), trace the origin of the term ‘cyberspace’ three years earlier (i.e. in 1981) in another novel ‘Burning Chrome’ by the same Canadian author William Gibson. They argue that the term was first used in 1981 but became popular in 1984 with publication of Gibson’s second novel ‘Neuromancer’, which seems quite possible. Another discourse by a group of Chinese scholars consisting of Sun Zhixin (孙智信), Zhao Zhao (赵焯), Li Zili (李自力) and Shui Chao (水超), in their work titled ‘Conception Analysis and Thought on the Term Cyberspace (2012)’ trace the origin of cyberspace in William Gibson’s work of 1982. Now which year is the correct year of origin? Wikipedia says the novel ‘Burning Chrome was published in 1982 but Gibson first read the story at a science fiction convention in Denver, Colorado in the

autumn of 1981. Hence, 1981 can be considered as the year of origin, but if verbal narration is not considered as authentic proof, 1982 is the year of origin. Sun, Zhao and group went further ahead and looked into the origin of word ‘cyber’ and it started being associated to the world of computers. They argue that the word ‘Cybernetique’ had originated from the Greek word, which according to Britannica Encyclopaedia is ‘*kybernetikos*’ (meaning good at steering). They argue this word was first used by a French physicist Andre Marie Ampere in 1834, which meant ‘Science of Governance’ but its meaning changed (even the word changed to cybernetics) in 20th Century and its contemporary meaning comes from ‘Macy Conference’ of 1940’s. It is argued that the term cyber was associated with computer in 1970’s when Control Data Company (控制数据公司 CDC) while promoting its super computer products proposed ‘Cyber’ as a synonym of computer. In their detailed account, they trace the following path, on which the term ‘Cyber’ travelled after its origin to reach to its current position.

Graphic 1: The Development Process of Cyberspace



Source: Sun *et al*, Conception Analysis and Thought on the Term Cyberspace (2012, p. 05)

Another group of Chinese authors Shi Rong (石荣), Li Jian (李剑), Huang Pengtao (黄鹏滔), Li Hao (李昊), He Minjue (贺岷珏) in their work “Comprehension for cyberspace and cyber-war in information warfare (2010)” argue that American mathematician Norbert Wiener was the founder of cybernetics after he published his book named ‘Cybernetics’ in 1948. Britannica Encyclopaedia clarifies the confusion by saying, “In the first half of the 19th century, the French physicist André-Marie Ampère, in his classification of the sciences, suggested that the still nonexistent science of the control of governments be called cybernetics. The term was soon forgotten, however, and it was not used again until the American mathematician Norbert Wiener published his book *Cybernetics* in 1948”.

1.2.2. Origin and Definition of Chinese Cyberwarfare

As far as the term cyberwarfare is concerned, Chinese scholars have used various equivalents for cyberwarfare (such as 计算机网络战, 网络战, 赛博空间作战, 赛博战) such as Network War, Computer Net war, and Cyberspace Operation, Cybewar etc. Just like the American cyberwarfare Chinese cyberwarfare has also originated from information warfare. Hence in order to understand the Chinese concept of cyberwarfare investigation has to be started from Chinese information warfare. Let’s take a look at the different views of various Chinese authors.

General Wang Pufeng, considered to be father of China’s information warfare doctrine, who was impressed by the superiority of the Americans during Gulf War, emphasises, “What matters now is not fire power so much as the capacity to see and know before the enemy, to act more quickly and to strike more precisely.” He asserts that information warfare initiated the ‘networkisation’ (网络化) of the battlefield opening up the era of a new battlefield made up of computers. He observed that battlefield is no longer seen the same way; it has become multidimensional, the dimensions being integrated; we no longer speak of front lines and rear areas. He treats information warfare as the justification of ‘informatisation’ (信息化) of armies which would help the Chinese army to gain in speed, mobility, agility and capacities to deeply attack in a battle without front lines, modifying the traditional war methods. General Wang was not just impressed by the American ways of waging war; rather he wanted to integrate (not just replicate) these concepts in Chinese context and while attempting that he brought back Mao’s concept of “People’s War”. This concept makes each citizen a combatant. The simple civilian, from his home, with a simple computer connected to networks could

serve the interests of the nation by attacking (hacking) enemy targets, civilian or military. Information technology, networks, electronics and telecommunication experts could become the new heroes in the new form of battle (Daniel 2009).

Colonel Wang Baocun (王保存 1997) considered cyberspace and hacking as major components of information warfare. He asserts, "Major components of information warfare are C2, intelligence, electronic, psychological, cyberspace, hackers, economical, strategic and precision wars (as cited by Daniel 2009)." Regarding information warfare he says, "It can be carried out in times of peace, crisis and war (as cited by Daniel 2009)." Thus, what Colonel Wang Baocun is suggesting is that the benefit of cyberspace and hacking can be taken all round the year; irrespective of whether it is peace, crisis or war time. Wang Baocun (王保存 2001) believes, "cyberwarfare (计算机网络战) has its origin in network centric warfare (网络中心战)."

Chinese authors Qiao Liang (乔良) and Wang Xiangsui (王湘穗 1999) assert that although the present components of unrestricted warfare like terrorist attacks, financial attacks, hackers' attacks etc might not fall in the category of war, but would probably become modes of future warfare and would enter our understanding of warfare soon. They assert, "If these unrestricted modes can create damages equivalent to conventional war, that also in very short period of time, why these should not be considered as the potential warfare options?" They argue that US attack on Iraq was not purely military; rather it was accompanied by media war, control of news, trade embargos, financial restrictions etc. Thus, they point out that unrestricted modes of warfare are already being extensively used. They also argue that along with the change in the principle of warfare, there will be changes in the rules and norm of warfare. There is no unalterable rule of war and no unalterable principle of war (Qiao & Wang 1999). Regarding the role of computers and information war, Qiao Liang and Wang Xiangsui assert, "Information warfare is not the same as computer warfare. Information warfare is the war where information technology is used to obtain or destroy information. Computer warfare combines all forms of warfare enhanced and accompanied by information technology" (Daniel 2009). Liu Zengliang (刘增良 2001) identifies cyberwarfare (计算机网络战) as a form of information warfare. He says, "Cyberwarfare refers to the information attack and defence activities in cyberspace conducted by information system networks allocated for it."

Zheng Kun(郑坤) and Tian Xiaopeng (田晓朋 2009) defines it as:

Cyberwarfare (计算机网络战, They refer it as Computer Netwar) is computer and computer network centred scramble revolving around information supremacy (or control of information). It uses advanced information techniques as basic methods, wired and wireless networks as battlefield, central equipment of weapon control, C4ISR and other systems (i.e. computers) as the main attacking point. It includes taking the advantage of loopholes in adversary's computer network system and vulnerabilities in their electronic equipments, using network command and special software to enter into adversary's network system or using strong electromagnetic pulse and other similar weapons to destroy their hardware facilities, thereby reaching the objective of disrupting and destroying enemy's networked information system and at the same time securing one's own of networked information system. Thus, information superiority is achieved.

Wei Yuejiang (魏岳江) and Huang Tiecheng (黄铁成) define it as:

Cyberwarfare (计算机网络战) refers to the scramble between two sides in the field of computer network for information superiority by weakening and destroying the information residing in opponent's computer system and by reducing its efficiency. It also includes ensuring security of one's own computer network system and ensuring safe environment to conduct and carry on information operations. Thus it could be observed that cyberwarfare (计算机网络战) falls in the category of information operation (信息作战) whose target is opponent's computer network; objective is to seize network superiority; main part is to arm the cyber warriors (网络战士) with equipments and information technique; battlefield is vast cyberspace (计算机网络空间); methods of operation are various computer viruses, logic bombs, chip weapons etc. developed on the basis of computing techniques.

Liang Yan (梁炎 2008) defines Computer Network Operations (CNO) as "a new action component of information operations, CNO occurring in the cyberspace is a warfare based on the information and communication. CNO has three components: Computer Network Attacks (CNA); Computer Network Defence (CND) and Computer Network Exploitation (CNE)." He defines CNA as "operations to disrupt, deny, degrade, or destroy (also known as 4D activities) information resident in computers and computer networks, or the computers and networks themselves." He further elaborates that CNA is based on the concept of cyberwar, future technology, precision design and warfare without the smokes of gunpowder.

Chen Zhong (陈钟 2010), head of college of software and micro-electronics, Beijing University, attempts to define cyberwarfare from two different vantage points. One is from

military perspective which is comparatively strict set up. Military cyberwarfare (网络战), according to him, include warfare, battle, war tactics, weaponry, military organizations etc. He says, “The themes of military cyberwarfare- whether it is being talked secretly or publicly are not many at present. It is also difficult to say who will discuss this issue?” Another vantage point is from non-military (civilian) angle which he asserts, “has a certain symbolic meaning.” He elaborates, “Some describe it from the angle of literature and sociology involving real life network attack and defence, hackers’ actions, cyber security issues, cyber-crime and other matters. It is a general name given to acts like spying, stealing, detecting and destroying of information etc. Cyberwarfare discussed in civilian sector is not just an abstract concept, it involves tools, techniques, defending methods and hacking attack activities of a particular period under certain time, space and circumstances.”

Qiu Shan (邱山) and Huang Tiecheng (黄铁成) recognise cyberwarfare as a part of information warfare, whose motive is to strike the nervous system of the adversary so as to paralyse them and compel them to surrender without offering any resistance. Fan Zhenhua (潘振华 2008) defines cyberwarfare by saying, “Cyberwarfare (网络战) refers to infiltrating into the secret code of adversary’s computer system; gaining control on enemy’s intelligence; sending virus to destroy enemy’s system or to paralyse them; thereby using our dominant position of information technology and equipments to achieve ‘network superiority’ and ‘information superiority’; at the same time securing our own ‘information borders’ and ‘information sovereignty’.” Pointing towards the American concept of Cyberwarfare, he says, “US military’s cyberwarfare is not only about hackers and viruses”. He quotes Lani Kass, the head of US air force cyberspace task force, who once said, “The scope of cyberwarfare (网络战) will be extended to whole electromagnetic field.” He further elaborates that the kind of cyberwarfare (网络战) that US talks about is not only limited to the scramble inside network, but it also include scramble for network environment, for e.g. scramble for electromagnetic environment of Wi-Fi and satellite channels.

Zhang Mingzhi and Hu Xiaofeng (张明智, 胡晓峰 2012), while talking about cyberspace (赛博空间), point out three different discourses. First discourse suggests that cyberspace has virtual existence and it is a conceptual environment, just like it was mentioned in the novel “Neuromancer” in which the term cyberspace appeared for the first time. Second discourse, according to them, argue that cyberspace exists in reality as a physical space because

electromagnetism is also a part of cyberspace which has physical existence. US DoD memorandum defines cyberspace based on this discourse only. The third one says cyberspace has both virtual and real components; has both physical and virtual space. They take our attention towards US definition which define cyberspace as “global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers,” and say even this definition is not able to put forward the complete meaning of cyber space. Hence, understanding cyberspace (赛博空间) as ‘network space’ (网络空间), as ‘networked electromagnetic space’ (网络电磁空间), as ‘electromagnetic network space’ (电磁网络空间), as ‘domain controller’ (控域) etc. is not illogical. Looking from different vantage points will result in different results. Lastly, they go along with the third discourse on cyberspace. Regarding cyberspace operation (赛博空间作战), they argue, “Cyberspace operation (赛博空间作战) is considered as completely new form of conducting operations. It marks the new phase of development of information warfare.” They present two concise and comprehensive points of view about cyberspace operation. One pitches for, “Using the capacity of cyberspace” and second for, “Conflict within the cyberspace”. Both the scholars prefer the second point of view over first and define cyberspace operation as “Confrontation between two sides within cyberspace through use of various cyber technologies and means in order to achieve the objectives of war.” They consider cyberspace operation as a form of operation that still belongs to the developing process and hence many of its aspects are not completely clear. According to them, “There still exists controversy regarding its relationship with information operation, information warfare, electronic warfare, computer network warfare (计算机网络战).”

Shu Zhi’an (舒治安 2011) contends,

Cyberwarfare is operation conducted in cyberspace. It considers basic information infrastructure like networks, computers and other electronic information system as the target. Cyberwarfare is divided into two parts: cyber attack and cyber defence. Since, cyberwarfare is an asymmetric mode of operation, attacking is easy and defending difficult. Therefore, key cyberwar initiative would be to adopt ‘proactive attack’ mode of operation.

Chen *et al.* (陈洪超 2001) asserts:

Cyberwar (网络战, authors use English equivalent: ‘Network war’) is rivalry between two sides directed at exploitable information and network environment for warfare; is a scramble revolving around ‘Information Superiority’; assuring

safety of information and network system of one's own side, at the same time disrupting, destroying and threatening adversary's information and network system; unfolding of confrontation for achieving last victory of the war. Cyberwarfare falls in the category of information warfare; it is an important form of information warfare. Being a completely new form of warfare at the turn of the century, cyberwarfare has already displayed its charm of magical soft war in 'Kosovo War 1999', and has received the attention of military experts of various countries. Twenty first century is the century of cyberwarfare.

Cao Zhihong (曹志鸿 2003) and Wang Chunyong (王春永 2003) argue that cyberwarfare (网络战) refers to a completely new form of warfare which considers one's own battle field network as weapon and targets to paralyse adversary's battle field network; to attack and paralyze adversary's whole system of waging war. It has already started displaying its talent in 'Gulf War 1991' and 'Kosovo War 1999'. Zhao Lei (赵磊 2002) asserts that cyberwarfare refers to gaining access to adversary's secret computer programmes, collecting adversary's intelligence, spreading viruses to destroy adversary's system and paralyze it by taking advantage of internet; achieving information superiority and network superiority by taking advantage of one's own superior electronics and information technology; at the same time, securing one's own 'information boundary' and 'information sovereignty'. Yuan Xiuli (袁秀丽 2010), Zhou Hongyu (周洪宇 2010), Zhou Gu (周谷 2010) emphasise that the real cyberwarfare revolves around information network of battlefield (communication network and computer network) and attack-defence struggle unfolded by electronic warfare.

Chou Xinliang and Dong Shouji who have analyzed the 'Stuxnet' virus, explain, "Stuxnet is highly sophisticated virus with clear objective and strategic intention which has typical characteristic of Cyberwar that could not be possible without the support of nation state."

Chinese version of Wikipedia (维基百科) contends, "Cyberwarfare refers to politically motivated hacking to conduct sabotage and espionage. It is a form of information warfare sometimes seen as analogous to conventional warfare (although this analogy is controversial for both its accuracy and its political motivation)." Baidu says:

Cyberwarfare is a series of cyber attack and defence activities which are aimed at disrupting enemy's information system while assuring the operation of one's own information system. It is becoming an increasingly important fighting mode of high-tech warfare. It is a method of destroying adversary's command and control, intelligence information and air defence system. It can even silently destroy, paralyze and control adversary's business affairs, political affairs and other civil network system. It can subdue the enemy without fighting.

2. Characteristics of Chinese Cyberwarfare

After looking at the various definitions by Chinese authors let us summarise their views and look at the characteristics of Chinese cyberwarfare pointed out by them. This would not only help in understanding characteristic features of Chinese cyberwarfare but would also help us in comparing the Chinese and Western cyberwarfare.

Asymmetric nature - Cyberwar is helpful for militarily weaker nations in avoiding defeat. It has become a magical weapon for countries having comparatively weaker comprehensive national power and military, which can even help them in gaining victory over the stronger adversaries (Chen *et al.* 2001),. Since, cyberwarfare is an asymmetric mode of operation, attacking is easy and defending difficult (Shu Zhi'an 舒治安 2011).

The attribution issue - Tracing the origin of cyber attacks accurately is very difficult. Under normal circumstances, no one would directly use his/her own computer system to attack the target computer; hackers frequently change address and countries while attacking. Most of the computer attacks of botnet type attacks come routed from third or fourth country whereas hacker controlling these attacks is located in another country (Shu Zhian 舒治安 2011). Ding Jianlin and Zhang Yong (丁建林, 张勇 2012) argue that cyber attacks have strong invisibility which makes timely detection of attacks by victim extremely difficult. Similarly, tracing the location of attacks and evaluating the damage associated with attacks become difficult. For instance if 'Trojan horse (a computer virus)' is implanted in enemy's computer system from a distant place (using network or internet), one can stay there undetected for a long time and can even collect sensitive information. Chen *et al.* (陈洪超 2001) assert:

Any individual, located in any corner of the world, can carry out destructive activities by making use of the internet. Moreover attacking methods are not very complex. Cyber attacks can originate from the battle field, outside the battle field; inside one's own territory, inside adversary's territory or any place in the world which is connected to internet. Participants of the cyberwar can be military personnel, non-military (i.e. civilian) personnel, networking experts or internet lovers.

Borderless characteristic of cyberspace - Although cyberspace is not a global common (opposite to western discourse), its components belong to individuals, private enterprises or to nation states, however it has many elements that belong to international area and hence seems to be borderless; business on internet can be carried on uninterrupted without taking into consideration nation states' components; nation states and individuals can use

cyberspace equally enforcing free communication without any restrictions or with little restrictions (Shu Zhian 舒治安 2011). Ding Jianlin and Zhang Yong (丁建林, 张勇 2012) say that operational range of cyberspace has increased because electromagnetic frequencies are not restricted by physical boundaries. This gives rise to cyberwarfare with no frontline, no backline and no concept of traditional boundaries. All those areas which are accessible through information networks and electromagnetic signals may become battlefields. It can surpass land, sea, air and space to enforce full spectrum operation. It involves other forms of warfare like network warfare, information warfare, electronic warfare, space warfare, command and control (C2) warfare etc. Zhang Mingzhi and Hu Xiaofeng (张明智, 胡晓峰 2012) assert, "It has no clear distinction between frontline and backline. It has cross domain operational and borderless operational features." Shu Zhian (舒治安 2011) again emphasises, "Due to the borderless nature of cyberspace, attacks and their technical elements spread over the internet with a lighting speed, leaving the victim country clueless."

As Fast as Speed of Light – Cyber attacks are rapidly spreading over the internet; as soon as an attack is detected it's already too late. Hence, in order to avoid these attacks in cyberspace from becoming a potential disaster/ catastrophe, the response time has to be corrected to minutes and even to seconds. Cyber attacks take place within very short moment (Shu Zhian 舒治安, 2011). Ding Jianlin and Zhang Yong (丁建林, 张勇 2012) further assert that information is disseminated in cyberspace at the speed of light and this has enabled cyberwar to go beyond the reaction speed of any other warfare waged by conventional weapons. Zhang Mingzhi and Hu Xiaofeng (张明智, 胡晓峰 2012) emphasises:

In the field of time, cyberspace operations have already surpassed the conventional warfare. It has the capacity to conduct pervasive/ penetrative and manoeuvring activities within a few moments. Within few moments capacity to conduct cyberspace operations can be altered. Attacks can reach the targets with the speed of light. Tasks of cyberspace operations can be finished with twinkling of eyes.

Flexible Timing - Cyber attacks can be carried out at the time when situation is declared hostile; even before the outbreak of war; secretly during the war; at regular interval or randomly anytime, even every day, every time. Its timing is extremely flexible. Organising favourable network advantage for attack may help to bring about maximum efficiency of "subduing the enemy without fighting". It is also helpful for militarily weaker nations in avoiding defeat (Chen *et al.* 2001). There exists no difference between period of peace and

period of conflict, cyberwar can be initiated anytime and be terminated anytime (Ding Jinanlin and Zhang Yong 2012). Even Mingzhi and Hu Xiaofeng (张明智, 胡晓峰 2012) emphasise that war can be waged anytime.

Wide ranged objectives - Military networks are not the only target of cyber attack and defence, it also covers today's various information application areas like financial, trade and commercial related, transportation (traffic), telecommunication and scientific research networks etc. Any nation especially the developed ones have economic, political and military interest in these networks. Various examples of virus attacks and destruction of computer system by hackers in recent years have proved that these networks are easily subjected to information attack (Chen *et al.* 2001). Ding and Zhang contend:

Apart from attacking adversary's equipment and military information network, cyberwar can also carry out attacks on critical information infrastructure related to national economy and people's livelihood, for e.g. disrupting normal mobile communication terminal and power supply. Thus cyberwar include military, politics, economy, society and other areas. (丁建林, 张勇 2012)

Multiple method/means - There could be various ways and methods of participating in cyberwar like use of public telephone network, use of various kinds of specialized data network, use of trade methods, dispatch of agents/ spy to enemy's territory and other methods in order to access the network whether it's wired network, wireless or optical communication system (Chen *et al.* 2001). Zhang Mingzhi and Hu Xiaofeng (张明智, 胡晓峰 2012) assert:

Cyberwarfare includes new type of operation units, moreover also includes comprehensive use of various cyber units and fighting means emerging from connected networks among four warfighting domain i.e. land, sea, air and space. It also involves information perception and controlling related areas including C4ISR system and C2 activities. At the same time it also includes cyber activities adopted for controlling network of National critical infrastructure.

Change in trends with time - Cyber threats and their nature are undergoing remarkable change. The main threat in 1980's came from abnormal natured academicians; in 1990 from a few passionate youths, they looked for getting acceptance of their colleagues (from same industry) by invading the computer system; during last decade cyber crime has occupied the central stage; in coming decade cyber espionage would become main trend, cyber attack would become an effective means of propelling war very soon (Shu Zhi'an 舒治安, 2011).

Destruction Capability - Cyberwarfare is an asymmetric mode of warfare which requires less investment but can produce extreme adverse effects for a whole nation. These kinds of attacks are difficult to detect and identify because of their dynamic and destructive nature. The potential damage caused by cyber attacks is huge. In recent period of ten years cyber crime has become largest internet threat, causing an economic loss of more than \$ 1 trillion (一万亿) in 2008. Any organised cyber attack can easily paralyse the critical information infrastructure of any nation state. The US Federation Survey Bureau while estimating the potential consequences that could be produced by cyber attacks regarded their level of destruction only next to weapons of mass destruction (WMD 大规模杀伤性武器) (Shu Zhi'an 舒治安, 2011).

3. Chinese Views on Its Relationship with other forms of Warfare & Domains

For electronic warfare Ding and Zhang (2012) assert:

Cyberwarfare (赛博战) is not equivalent to traditional electronic warfare. Cyberwarfare includes all functions of electronic warfare completely and thus is an expansion and extension of the traditional electronic warfare. Electronic warfare is military activity of controlling electromagnetic spectrum which includes electronic attack, electronic defence and electronic support. Electronic support is interception, identification, analysis and location of adversary's source of radiations and thereby providing threat information timely. Electronic defence is avoiding adversary's disruption effectively in various areas like time, frequency, airspace, code or polarity by making use of information provided by electronic support; and providing useful frequency resources to electronic equipments. Electronic attack is carrying out disruption and destruction of adversary's electromagnetic signals.

While comparing cyberwarfare with computer network warfare, they say:

Cyberwarfare (赛博战) is not equivalent to traditional computer network warfare (计算机网络战) Computer network warfare is information attack and defence operation over the internet including network attack, network defence and use of network resources. The methods used in offensive computer network warfare are password analysis, scanning of network, detection of network, analysis of rate of flow of data, distortion of information, copying of information, denial of service, malicious code implantation etc. Defensive network warfare is mainly about adopting measures for network security like multiple encryptions, intrusion detection, firewall, digital signature, elimination of malicious code.

Ding and Zhang point out the limitation of computer network warfare, when they point out:

Due to the openness of internet and its evident weakness of affecting national security, many of the networked system are not directly connected to internet, many of the military command and control (C2) networks and air defence

system are isolated or closed, people from outside cannot visit these networks directly.

And here according to them comes the cyberwar (赛博战), which may carry out attack or access these networks which are not directly connected to internet by using electromagnetic capability so as to achieve the objective of information stealing and hardware destruction. Apart from this, they say, “Network warfare (网络作战) uses computer to conduct operation (it regards computer as platform for launching attack or operation.); target of war is adversary’s network system; generally, no personnel are injured directly. On the other hand cyberwar (赛博战) in the electromagnetic environment engages in real physical war or operations which may affect the location of enemy’s troops, command and control, weapon system’s ability to attack and can even achieve the objective of ‘hard kill (硬杀伤)’.” In the end they relate cyberwarfare with information warfare by saying, “cyberwarfare (赛博战) is information warfare in broader sense, which is not limited to traditional sense of electronic warfare and computer network warfare. It may be understood as: control and perception of comprehensive battlefield information in which network is considered as the base.” In summary, they assert that cyberwarfare is further development of network warfare and electronic warfare.

Regarding cyberspace and its components Zhang Mingzhi and Hu Xiaofeng (张明智, 胡晓峰 2012) elaborate:

Cyberspace is composed of physical space and virtual space. Physical space refers to traditional operational domains like land, sea, air, space etc. Virtual space refers to the information space created by controlled electronic information equipment and flow of information from it.

Thus according to them cyberspace becomes the largest domain which contains all other traditional domains within it. They again explain:

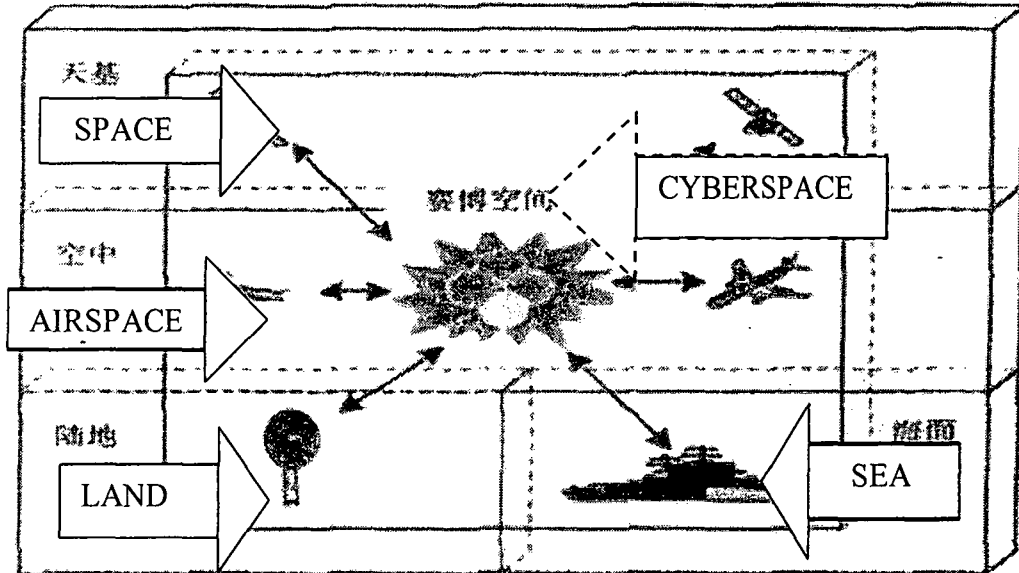
Cyberspace has multidimensional nature, cross domain characteristics and has large scale dimensions. It is composed of ‘System of Systems (SoS)’ or ‘Network of Networks (NoN)’. From the spatial angle, cyberspace operation has large range and has its reach to other domains as well. It has global range and can reach to both traditional warfighting domains and cyberspace.

Ding and Zhang also contribute in establishing the relationship between cyberspace and other domains. They, with the help of following figure, argue

Cyberspace is the fifth domain which co-exists with other traditional domains i.e. land, sea, air and space. It is a domain of numerous interconnected participants. It covers all the participants irrespective of their locations. In cyberspace,

physical location lies inside various electronic systems and equipments of traditional domains, interacting with cyberspace by using electromagnetic frequency; completing the integration process from information production to its usage.

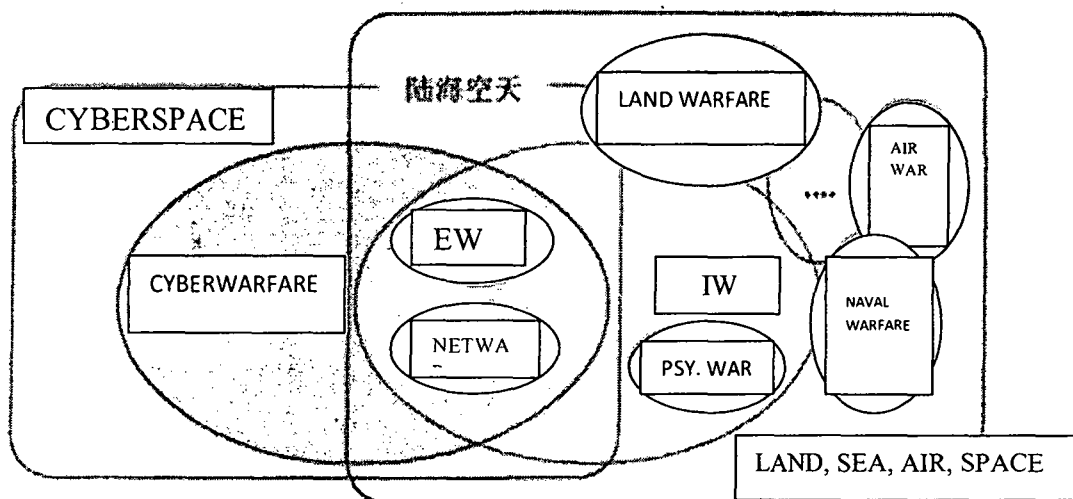
Figure 9: Relationship between Cyberspace and Other Domains



Source: Ding Jianlin and Zhang Yong (丁建林, 张勇) (2012) (p. 02)

Ding and Zhang through another figure elaborates how cyberspace and cyberwarfare is related to information warfare, electronic warfare, network warfare and warfare waged in other domains.

Figure 10: Relationship of Cyberspace with Warfare Waged in Other Domain



Source: Ding Jianlin and Zhang Yong (丁建林, 张勇 2012) (p.n. 04)

4. Similarities and Differences- Cyberwarfare with Chinese Characteristics

James Mulvenon (1998) identified similarities and differences between Chinese and Western information warfare. While doing so, he said that Chinese approach to the concept of information warfare is a simple copy of the American model with a few minor changes, because China is unable to move away from it in an original way. The fact that China has been closely examining American experiments since the First Gulf War, but has no operational or pragmatic experience itself would partially explain this “reproduction”. One more reason could be China’s technological backwardness as compared to that of the US. Any country being technologically inferior is left with no other option than to look towards and learn from technologically advanced nations, until the inferior does not become superior, (especially when both of them are close competitors).

Though Mulvenon tried identifying similarities and differences for information warfare, but most of them hold true for cyberwarfare as well. Similarities are numerous but differences are unique in their nature. These differences are worth paying attention at, as they have unique Chinese flavour which comes from China’s long military history and culture.

As far as similarities are concerned China also uses the terms as used by used by the US and other nations: CNO, CNA, CND, CNE, IW, Cyberspace, Cyberwarfare, Newar, Network Centric Warfare etc. Even the primary objective of cyberwar remains the same: affecting (to deny, degrade, disrupt and destroy etc) the adversary without being affected and attaining information dominance without letting adversary to do so. However, what are worth paying attention are differences, which can help us to to understand Chinese essence of cyberwarfare.

4.1. Differences

Apart from similarities there are many differences as well. These differences are due to China’s indigenous military history and culture. Well known military strategists like Sun Zi (孙子 also known as 孙武), Sun Bin (孙臆) and writings like ‘Thirty Six Stratagems’ etc. have far reaching influence on today’s military strategies. Later on Mao Zedong (毛泽东) also added his military thoughts to the existing classical military strategies. Reflection of all these Chinese thoughts and strategies can be seen in China’s Cyberwarfare. Thus, these differences have profound Chinese characteristics and hence could be referred as ‘Cyberwarfare with Chinese Characteristics’. These Chinese characteristics can be observed in following thoughts:

- i. **Fusion of Military and Civilian Cyberspace** – It is an inevitable trend. Ranging from one corner to another corner of the world, the global internet is continuously combining more and more civilian and military computers. Military information resources have already started integrating with social network system, at the same time civilian information resources have been continuously integrating with military network. It is giving rise to a cyberspace where there is no separation by national boundaries; no difference of identity between netizens; and all ‘netizens are becoming soldiers’ (网民皆兵) (Chen *et al.* 2001).

- ii. **Mao’s People’s War/ Cyber warriors** – Any organization or person can become ‘cyber warrior’ (网络战士) and can display one’s skill if he/she/it masters network transmission technology, excels in computer knowledge and advanced decoder technology. The two parties waging war can deploy their ‘cyber warriors’ by mobilizing their netizens all round the globe, irrespective of their geographical location and time period, to unfold offensive activities against adversary; to enter inside adversary’s multilayered encrypted network system, to penetrate and modify database, equipments vital for internet/network and computer systems across all domain; to steal crucial data from adversary’s network system; to intercept or disrupt important ‘National economy and People’s livelihood’ system and C2 power of military command system; to destroy it’s centre of command and weapon sytem; to carry out hidden, open or transnational cyberwarfare which is brand new kind of warfare surpassing traditional theories of warfare; to accommodate maximum numbers of personnel which can operate against enemies anytime, under any circumstances and from anywhere; to achieve anticipated objectives/ targets of operations which cannot be reached through normal modes of operations or which cannot be reached as swiftly (Chen *et al.* 2001).

- iii. **Cybercrime is cyberwarfare** - Difference between cyberwar and cyber crime is not very distinct. It is largely because of some nation states which consider these organizations conducting cyber crime as useful associations. These nation states have expressed their willingness in tolerating, supporting and even guiding these organizations to attack hostile targets. E.g. 2008 attack Georgia. According to a German cyber crime researcher, anyone can go to these organizations and rent botnet,

the only thing required is money even if one does not know how to do it (technically) (满凯艳 Man Kaiyan, 狄鑫 Di Xin 2011).

- iv. **‘Suter’ technology is cyberwarfare** - Yuan and Zhou (袁秀丽, 周洪宇, 周谷) say that American ‘Suter’ technology is also a part of cyberwarfare. ‘Suter’ technology is used in drones and UAVs (Unmanned Ariel Vehicles) for e.g. RC-135U (which can detect enemy’s radar system), EC-130H (which can infiltrate into and control enemy’s computer system and can even operate adversary’s sensor. Cyber attacks capabilities through ‘Suter’ technology include: electronic reconnoitre & disruption; destructive weapon; and cyber fraud. This technology is comprehensive application and close combination of these three things. This ‘Suter’ technology was successfully used in Iraq War and Afghan War

- v. **War Without the Smoke of Gunpowder** - Cyberwarfare is warfare ‘Without the Smoke of Gunpowder’ (无硝烟的战争), which is considered as revival of classical Chinese warfare where strategy mattered more than that of technology and it still seems to be relevant for China (“无硝烟”的战争将重新演绎古典战争的内涵) (Chen *et al.* 2001).

In the context of revival of classical Chinese warfare, it is surprising to know that Sun Zi (孙子) is still relevant today. Rather he is more relevant in the realm of cyberwarfare, that also up to this extent that Jeffery Carr’s definition of cyberwarfare is inspired by him. Another author Billy K Rios in his chapter “Sun Tzu was a Hacker: An Examination of the Tactics and Operations from a Real World Cyber Attack” argued that Sun Zi promotes fluidity, flexibility, surprise, deception and intelligence over sheer military might. Jeffery Carr (2011) has associated few of the 36 stratagems with modern day cyberwarfare. It is not known who wrote ‘Thirty Six Stratagems’, but historians date them as far back as Southern Qi dynasty (479-502), which was about 1000 years after Sun Zi wrote *The Art of War*. Carr emphasises that the 36 Stratagems like *The Art of War* still play a large role in shaping *Beijing’s* military strategy. He co-relates them in very unique way as follows:

Stratagem #3: “Kill with a borrowed knife”

This stratagem advises “Attack using the strength of another (in a situation where one’s own strength is not favourable).”

This could just as easily apply to the use of botnets as a means to launch DDOS (Distributed Denial of Service) attacks (routed through third country).

Stratagem #8: "Openly repair the gallery roads, but sneak through the passage of Chencang"

This stratagem advises "Deceive the enemy with an obvious approach that will take a very long time, while surprising him by taking a shortcut and sneak up to him. As the enemy concentrates in the decoy, he will miss you sneaking up to him."

Use backdoors or Trojan worms when attacking a network.

Stratagem #10: "Hide a knife behind smile"

This stratagem advises "Charm and integrate yourself with your enemy until you have gained his trust. Then move against him."

This could describe phishing schemes or other social engineering attacks.

Stratagem #15: "Lure tiger out of the mountain"

This stratagem advises "Hold out baits to entice the enemy."

This refers to luring an opponent from a position of strength, such as being protected by firewall and updated anti-virus program, to a position of weakness or vulnerability. One way to accomplish this is with adoption of social engineering techniques to get the target to accept a fake email as genuine and open a compromised attachment or click to an infected link.

Stratagem #17: "Tossing out a brick to get a jade gem"

This stratagem advises "Bait someone by making him believe that he gains something and obtain something valuable from him in return."

This could equate to a social engineering technique used to get the target to click on a link or visit a website where information will be covertly collected without his knowledge.

Stratagem #30: "The honey trap"

This stratagem advises "Send your enemy beautiful women to cause discord within his camp."

In contemporary computer parlance, this could refer to a honey pot, which lures visitors to rigged site that collects information about them.

In this way it seems that China's military classics are still relevant especially in the domain of cyberspace. Cyberspace provides China with ample opportunity to use its classic tactic of warfare without any bloodshed. The nature of cyberwarfare seems to be in alignment of China's classical methods of waging warfare and hence Chinese military would prefer using its classic tactics of warfare as an element of surprise for its adversaries.

Conclusion

The evolution process of cyberwarfare in China is similar to that of the US, as it has its roots lying deep into the term information warfare in both the cases. Unlike UN and other international views, almost none of the Chinese authors talk about involvement of nation states in cyberwarfare. There exists little or no difference between civilian and military cyberspace as the term used for warfare in both the realms is same (i.e. 赛博战 or 网络战) whereas in case in of the US, two different concepts exist: Cyberwar in military realm and Netwar (Network War) in civilian realm. However an official Chinese definition of the term demarcating the red lines which when crossed (by any nation state, organization or individual) won't be tolerated by China, is still missing. Due to China's long military history, the influence of Chinese thoughts is clearly evident in Chinese views on cyberwarfare. It has not only inspired Chinese scholars but has also influenced Western scholars that also up to such an extent that one of the author (Jeffery Carr) gave his definition of cyberwarfare based on Sun Zi's thoughts. Apart from Sun Zi there are many other Chinese military strategists and their works (both known and unknown like Sun Bin, 36 Stratagems etc.) that give China's cyberwarfare (Chinese views on cyberwar) its unique flavour.

Chapter 4

Organisations Involved in China's Cyberwarfare

Ever since cyber threats have become eminent national security threat, every nation state has started attaching great importance to these cyber issues, especially those nations which are more dependent (and hence considered more vulnerable) on Information and Communication Technology (ICT) and those nations as well which consider loopholes of ICT as an opportunity (that should not be missed) to strengthen their capabilities and thereby consolidate their power. Cyber attacks are also considered as an asymmetric means through which militarily weaker nations hope to take down militarily stronger nations. And militarily stronger nations which are ahead of other nations because of technology and are largely dependent on technology know that they are vulnerable to cyber attacks. Hence they want to secure their computers, networks and other cyber components so that no other nation can take undue advantage. On the other hand militarily weaker nations are leaving no efforts in developing cyber exploitation and attack techniques. For many nations it does not matter whether the reason is exploitation or defence/attack, more and more investment is being made across the globe. China is no exception to it. Just like any other nation state (including the US) the Chinese government has also been developing, sharpening and updating its defensive and offensive skills so that any cyber attack against China can be avoided, mitigated or retaliated against if required. For this purpose Chinese government has its specialised Organisations and departments which deal in cyber issues. But since some of these Organisations are also involved in intelligence collection, little information is publicly available. Moreover, neither the Chinese government nor Chinese scholars discuss their Organisations involved in cyber issues. Thus this limited flow of information and availability of little information could be a part of their cyberwarfare of misleading or confusing their adversaries and thereby compelling adversaries to take wrong decisions. Most of the works on 'Chinese Organisations involved in cyberwarfare' have been done by Western scholars especially Americans. However, in some cases scholars themselves agree with the fact that this kind of study is sometimes speculative.

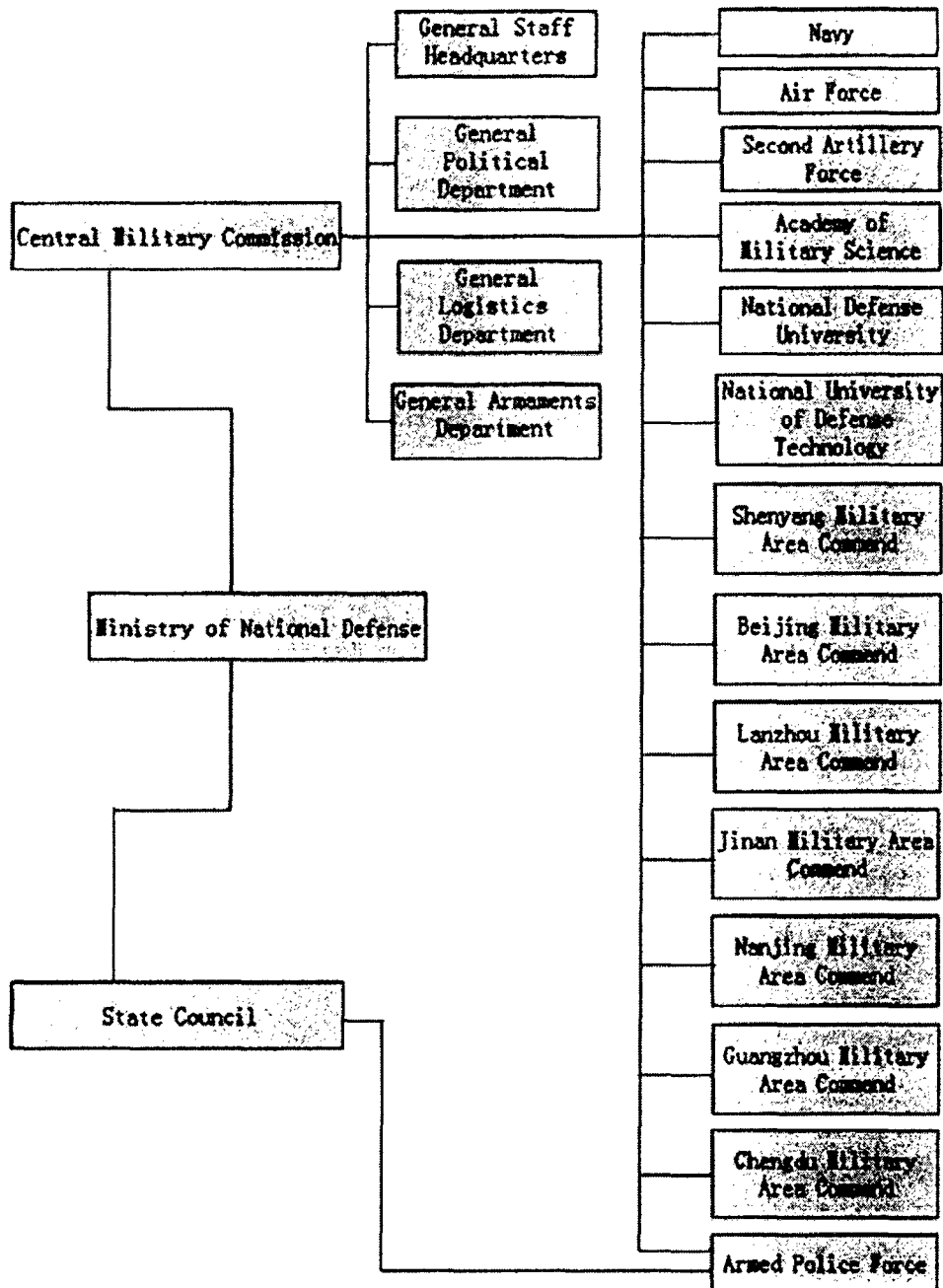
In case of China cyberspace is highly sensitive issue not just because of international threats but also because the threat of domestic unrest. Probably that is why People's Liberation Army (PLA) is one of the main Organisations involved in cyberwarfare. Strokes *et al.* (2011) consider the PLA General Staff Department (GSD) Third Department (总参三部) and Fourth

Department (总参四部) as the two largest players in China's burgeoning cyber-infrastructure. A report (titled – APT1 Exposing one of China's Cyber Espionage Unit) published by Mandiant, a US Virginia based cyber security firm, claims that Second Bureau of PLA GSD's Third Department (code named as Unit 61398) is one of the more than 20 'Advance Persistent Threat'⁴ (APT)' groups which is government sponsored and one of the main persistent of China's cyber threat actors. Jeffery Carr, a well known scholar who has written extensively on cyberwarfare, observes some flaws in Mandiant report and argues that the report has not included other State agencies of China who engage in this type of activity. James Mulvenon (2009), another well known scholar, categorises various involved organisations into three categories. He asserts, "The PLA's computer network operations (CNO) Organisations can be divided into three broad categories: command organisations; doctrinal and professional military education institutions; and research and development Organisations." His probable list of organisations include: GSD Third Department; GSD Communication Department; GSD Fourth Department; Joint Campaign Command HQ; Academy of Military Sciences (AMS); The National Defence University (NDU); and The Wuhan Communications Command Academy (CCA) etc. Carr comes up with a longer list of Chinese Organisations/entities that could possibly be involved in cyberwarfare, cyber-espionage and other cyber related attacks. His long probable list includes: The Ministry of State Security (MSS); Ministry of Public Security (MPS); GSD Second Department (2PLA); GSD Third Department of the PLA (3PLA); GSD Fourth Department (4PLA); Liaison Office of the PLA General Political Department (GPD); Intelligence departments of the PLA Navy; PLA Air Force; Second Artillery; State Secrecy Bureau; Commission of Science, Technology and Industry for National Defense (COSTIND); Research Institutes; PRC Military-Industrial Companies; Organised Chinese hacker groups etc.

Some components of these Organisations like their functions/missions, locations and Organisational structures, hierarchical positions can help us to predict their involvement in cyber activities (like cyberwarfare, cyber espionage, cyber attacks etc.) and State's sponsorship in the same. This chapter looks at some of the most prominent organisations one by one as mentioned by some Western authors and the US government. To begin with, the hierarchical positions of some of the above mentioned organisations can be seen in the following figure.

⁴ MANDIANT defines the APT as a group of sophisticated, determined and coordinated attackers that have been systematically compromising U.S. government and commercial computer networks for years.

Figure 11: Hierarchical Organisations of Chinese Military



Source: China.org.cn

1. General Staff Headquarters/Department (GSD) (总参谋部)

Regarding the functions of GSD, China's White Paper on defence (2006) asserts, "The General Staff Headquarters organises and directs the development of China's armed forces, and organises and commands their military operations. Under it are departments in charge of

operations, intelligence, communications, military training and arms, adjutant and force structure, mobilisation, electronic countermeasures, army aviation, foreign affairs, etc. Its main functions and powers are to put forward proposals on major issues of military building and operations, Organise and exercise strategic command, formulate programs, rules and regulations for military work, and Organise and direct war preparations, as well as military training and mobilisation". A website called 'globalsecurity.org' adds, "The GSD carries out staff and operational functions for the PLA and has major responsibility for implementing military modernisation plans. It serves as the headquarters for the ground forces under the seven subordinate military regions (MR – Beijing, Chengdu, Guangzhou, Lanzhou, Jinan, Nanjing and Shenyang) and contains directorates for the three other armed services: the PLA Air Force, PLA Navy and the Strategic Rocket Force (also called the 2nd Artillery)." The Mandiant report (2013) emphasizes, "The GSD is the most senior PLA department. Similar to the U.S. Joint Chiefs of Staff, the GSD establishes doctrine and provides operational guidance for the PLA." According to an article published on 4 February, 1997 in Liberation Army Daily (jiefangjun bao [解放军报]) GSD has the following functions:

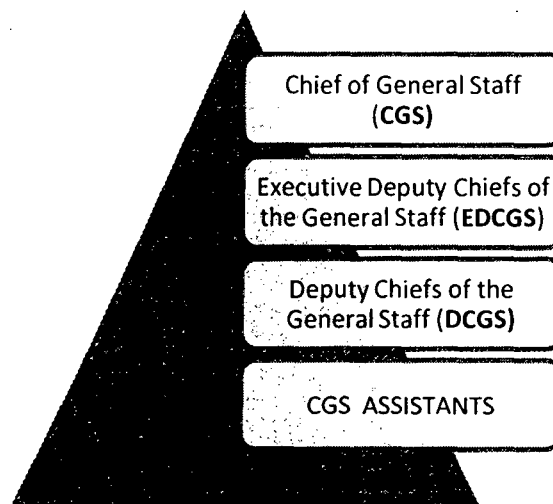
- Planning, Organising and directing military operations
- Conducting staff work for the top leadership of the PLA to assist them in decision making
- Serving as the lead organisation in the PLA for military modernisation program decision
- Co-ordinating the work of the (then) three General Departments
- Administering the military legislation and military legal system
- Providing guidance for logistical support
- Providing guidance for military science research
- Providing guidance for defence science and technology studies
- Providing information support

Out of so many functions (including the functions in the above mentioned other sources) it is only the last function which suggests that GSD has something to do with cyber issues (directly). Other functions like 'Providing guidance for military science research; and providing guidance for defence science and technology studies' also suggests that GSD could be involved in cyber related activities. However, allegations are not directly pointed against the GSD rather it's against GSD's sub-ordinate organisations.

In order to understand GSD's sub-ordinate organisations, organisational structure of GSD has to be understood first. While talking about the same, sinodefence.com says:

The GSD is the military department of the Central Military Commission (CMC) and the military command headquarters of the PLA. The GSD is headed by the Chief of the General Staff (CGS). He is assisted by the Executive Deputy Chiefs of the General Staff (EDCGS), three Deputy Chiefs of the General Staff (DCGS), and three CGS Assistants. The EDCGS, DCGS and CGS Assistants share the responsibility of overseeing operations, training, intelligence, equipment, discipline, mobilisation, and reserve forces, foreign relations, etc. Normally these positions include one person with background in the Air Force, one with background in the Navy, and one with background in the Second Artillery Corps to assist the liaisons with these service branches. The current CGS is General Chen Bingde (陈炳德), who was appointed the position in 2007. However, in the Party system, the former CGS and current Minister of National Defence, General Liang Guanglie (梁光烈), has retained the position of the Party secretary of the GSD, while Chen is only the first deputy secretary. The fourth most senior uniformed officer in the PLA, Chen is also a member of the CMC and the Chinese Communist Party (CCP)'s central committee.

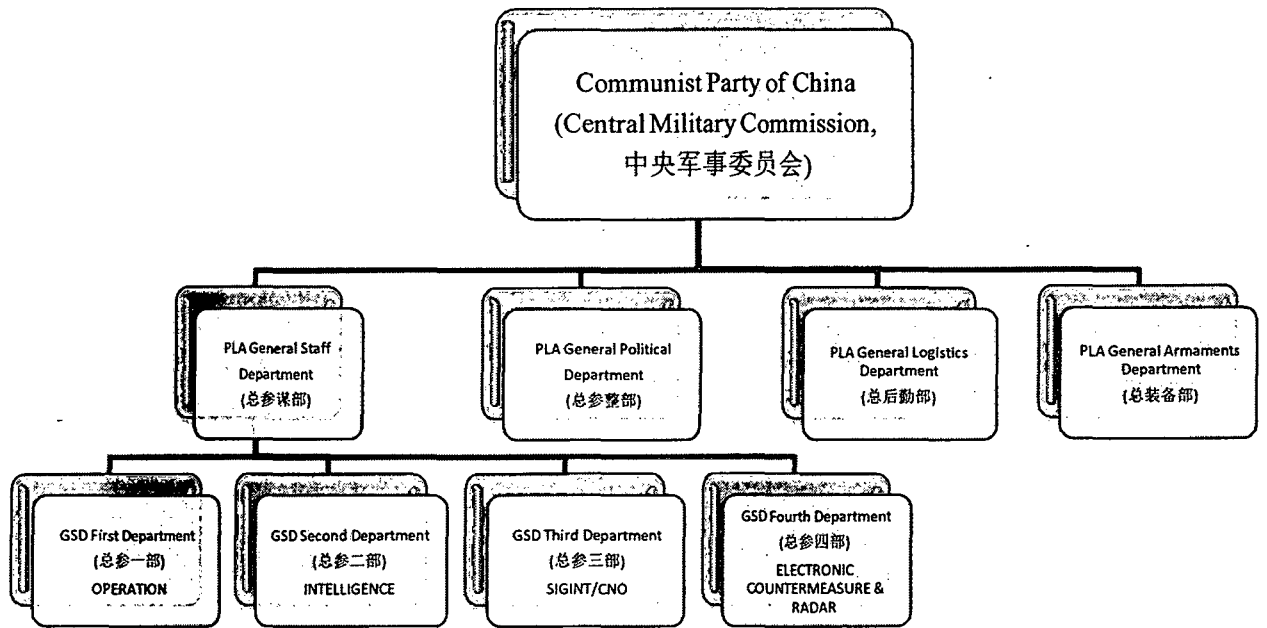
Figure 12: Organisational Structure of GSD



Source: Based on <http://www.sinodefence.com/overview/organisation/gsd.asp>

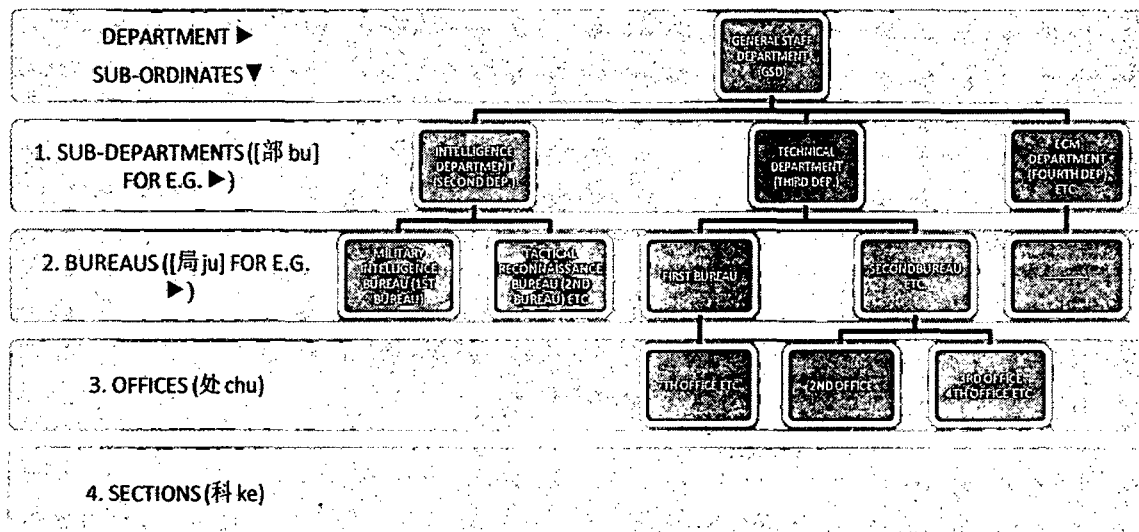
The hierarchical position of GSD and its subordinate Organisations/departments within the Chinese defence system and PLA can be located in the following figure.

Figure 13: Position of GSD and its Sub-ordinate Departments in PLA



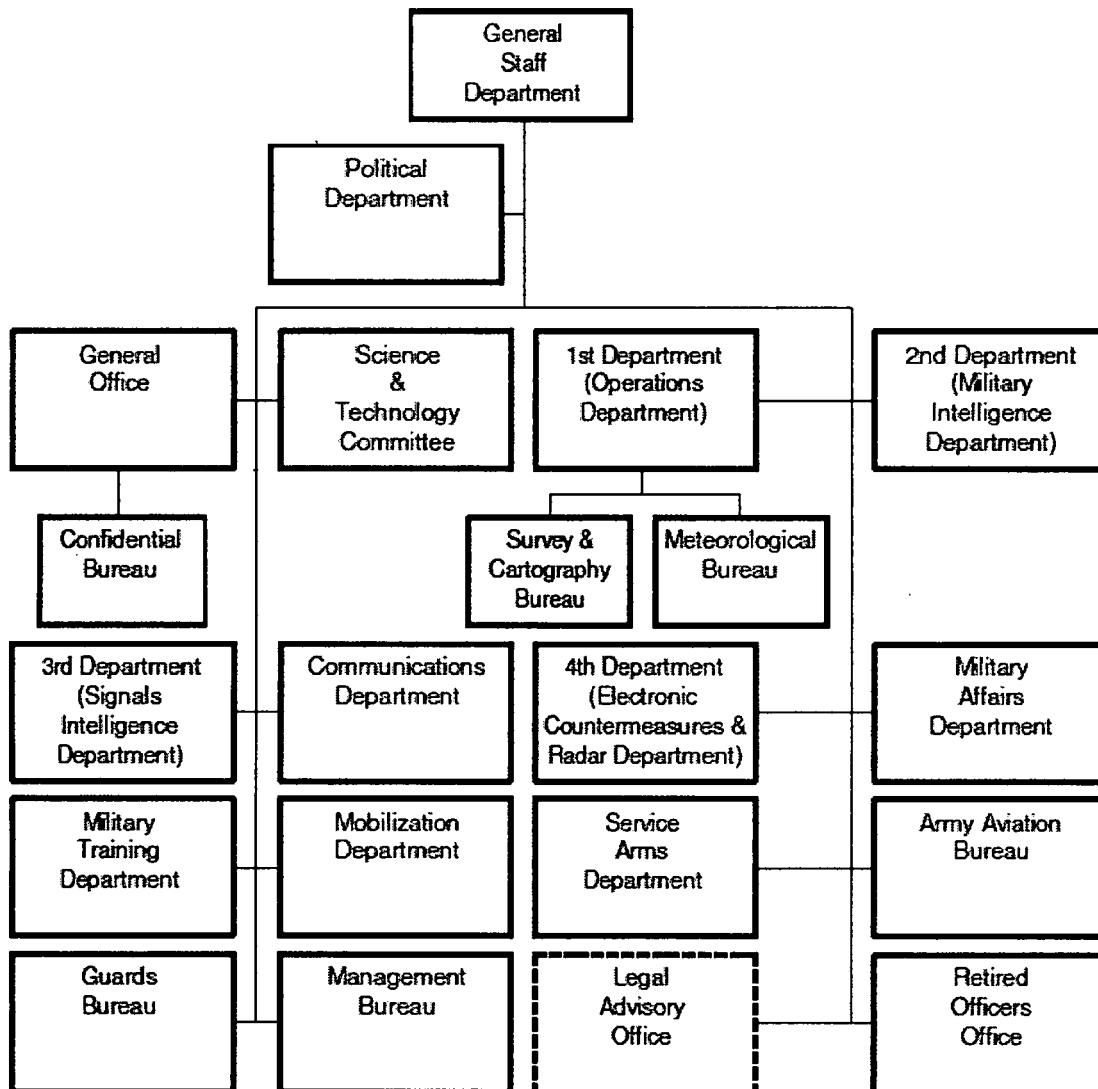
Source: Mulvenon and Yang, 'PLA as Organisation', 2002, p 35-37

Figure 14: Sub-ordinate Organisational structure of GSD



Source: James C Mulvenon and Andrew N D Yang, 'PLA as Organisation', 2002, p 129-130 and Stokes et al 'PLA Third Department'

Figure 15: Composition of GSD



Source: Mulvenon and Yang 'PLA as Organisation', 2002, p- 129

1.2. GSD Second Department (Intelligence Department [情报部]/ 2PLA)

Stokes (1999) asserts that GSD's Second Department is Chinese counterpart of the U.S. Defense Intelligence Agency. While talking about its functions, Mulvenon and Yang (2002) assert:

The Second Department seems to have two key missions. First it is responsible for the collection and analysis of strategic-level military and political intelligence. To a certain degree, its strategic intelligence missions may overlap somewhat with those of Ministry of State Security (MSS). Second, The Second Department *may* have the responsibility for providing operational-level intelligence to the Military Regions.

Adding to this, sinodefence.com emphasises, “The 2nd GSD Department (总参二部), also known as the Intelligence Department (情报部), is responsible for the collection and analysis of military and political intelligence at the strategic-level by means of human intelligence. The department monitors the activities of foreign military, especially those of the neighbouring countries and the U.S. troops stationed in Asia, and updates the Chinese leaders on latest developments on a daily basis. It is also responsible for counterintelligence within the PLA, dispatching military attaché to foreign countries, and overseeing the operations of the intelligence departments in military regions and service branches.” Stokes (1999) also elaborates, “GSD’s Second Department is the focal point for strategic and tactical military intelligence. The Second Department oversees military human intelligence (HUMINT) collection, widely exploits open source materials, fuses HUMINT, signals intelligence (SIGINT), and imagery intelligence data, and disseminates finished intelligence products to the CMC and other consumers. Preliminary fusion is carried out by the Second Department’s Analysis Bureau which mans the National Watch Center, the focal point for national-level indications and warning. In-depth analysis is carried out by regional bureaus.” Ian M Easton and L C Russell Hsiao (2013) further add, “The Second Department, also known as 2PLA, is responsible for military and political intelligence collection and analysis. It is increasingly reliant upon airborne and space intelligence, surveillance, and reconnaissance (ISR) systems.”

Regarding organisational structure sinodefence.com elaborates, “The department is headed by a Director, a Political Commissar, and two Deputy Directors. The main functional organs within the Second Department include a number of bureaus responsible for intelligence collection and analysis.” The website enlists following organs (but does not explicitly explain their functions):

- Political Department (政治部)
- Confidential Bureau (机要局)
- Comprehensive Bureau (综合局)
- Confidential File Bureau (保密档案局)
- 1st Bureau (一局) – Military Intelligence Bureau (军事情报局)
- 2nd Bureau (二局) – Tactical Reconnaissance Bureau (战术情报局)
- 3rd Bureau (三局) – Military Attaché Bureau (武官局)

- 4th Bureau (四局) – Intelligence analysis for Russia, former Soviet republics, and other Eastern European countries
- 5th Bureau (五局) – Intelligence analysis for U.S. and Western European countries
- 6th Bureau (六局) – Intelligence analysis for neighbouring Asian countries
- 7th Bureau (七局) – Technology and Equipment Bureau (科技装备局)
- Arms Control Bureau (军备控制局)
- Space Reconnaissance Bureau (航天侦察局)
- Computer Institute (计算机所)
- PLA College of International Relations (解放军国际关系学院)
- China International Institute for Strategic Studies (CIISS) (中国国际战略研究学会)

1.3. GSD Third Department (Technical Department [技术部]/ 3PLA)

Established in 1930s, the Third Department was previously known as the CMC Second Bureau and consisted of three entities responsible for collection, translation, and deciphering/encryption (Strokes *et al.* 2011). Another source says, “The Third Department was established in the early 1950s, with equipment supplied by the Soviet Union, primarily to provide strategic communications for the General Staff (*Manuel Cereijo*).” According to third the Federation of American Scientists (FAS), the Department was established in the early 1950s with Soviet assistance to provide the Chinese General Staff with a limited SIGINT capability and strategic communications support.

Regarding the function of Third Department, James C Mulvenon and Andrew N D Yang (2002) say, “The Third Department of the GSD is apparently responsible for ‘signals intelligence’ (SIGINT); meaning interception, processing and dissemination of communications transmissions from foreign entities.” Another source sinodefence.com says, “The Third Department also known as Technical Department is responsible for signal intelligence (SIGINT) operations, including the interception, processing, and dissemination of communications transmissions from foreign entities. As a collateral mission, it also monitors internal PLA communications as well as civilian international communications to and from China. This Department, also known as 61195 Unit in its military unit cover designator (MUCD) is considered equivalent to the American National Security Agency

(NSA).” Deepak Sharma (2010), a research fellow at Institute for Defence Studies and Analyses (IDSA), further elaborates the functions by saying:

The GSD Third Department deals in signals intelligence (SIGINT) role and its large staff of trained linguists and technicians make it well suited for oversight of the CND and CNE missions in the PLA. The Third Department maintains an extensive system of signals collection stations throughout China with collection and processing stations co-located with each of the PLA’s Military Region Headquarters. It is tasked with the foreign signals collection, exploitation, and analysis and also communications security for the PLA’s voice and data networks. This latter responsibility may encompass network defence as well, though little information is available to confirm this role.

The Third Department is allegedly responsible for large scale cyber espionage activities. Strokes and Hsiao (2012) argue that there are indicators that point to the Third Department serving as a national executive agent for computer network exploitation (CNE). Mulvenon (2009) also points out, “Given the known mission profile of the GSD Third Department, it is reasonable to speculate that it may have the lead role in the defensive/information assurance mission (CND) as well as intelligence preparation of the battlefield (CNE).” Even the recent Mandiant report (2013) asserts, “We believe that the PLA’s strategic cyber command is situated in the PLA’s General Staff Department, specifically its Third Department. The Third Department has a combined focus on signals intelligence, foreign language proficiency, and defence information system.” For the first time ever in the entire history of cyberspace and cyber attacks, this report traced the exact location (a 12 storey building of Shanghai) of the source of Chinese cyber attacks. However not everybody (including Jeffery Carr and Chinese government) seemed convinced by the amount of evidence presented in the report. Even before this report was published, Strokes and Hsiao (2012) predicted, “PLA GSD Third Department is likely a leading authority for cyber surveillance. In the absence of officially verified evidence, this informed hypothesis is based on an assessment of the department’s traditional core competency in signals intelligence, its high performance computing and encryption/decryption technical capabilities, and status as China’s largest employer of well-trained linguists.” One year before this, in 2011 Strokes *et. al* provided the probable reason why Third Department could be the source of cyber attacks. They say, “The GSD Third Department stands as a reasonable choice to act as the national PRC authority over cyber surveillance because of its traditional core competency in SIGINT, its high performance computing and encryption/decryption technical capabilities, and status as China’s largest

employer of well trained linguists. Third Department bureau, office, and section facilities and sites located throughout China report directly to Beijing, and are not under administrative jurisdiction of MR Commanders or Political Commissars (Strokes et. al. 2011).” One possible reason was put forward by Strokes and others. They say, “The Third Department bureau, office, and section facilities and sites located throughout China report directly to Beijing, and are not under administrative jurisdiction of MR Commanders or Political Commissars (Strokes et. al 2011).” One more reason could also be seen in the rise in the number of personnel. In 1999, Strokes estimated that there were around 20,000 personnel working in Third Department, which according to Ian Easton and Mark Strokes increased to 130,000 in 2011 (an increase by more than 6 times in 12 years). Even the most recent report (Mandiant 2013) estimates 130,000 personnel.

Apart from the number, location of the Third Department (and its sub-ordinate bureaus) should also be factored in since functions of these organisations vary depending upon their locations. Third Department headquarters is located in the vicinity of the GSD First Department (Operations Department), AMS, and NDU complex in the hills northwest of the Summer Palace (Stokes 1999; Stokes et al. 2011). Manuel goes one step further in locating the headquarters and control stations. He says, “The headquarters of the Third Department is located at Zianghongqi, in the Haidian District of Beijing, about 8 km from the Summer Palace, on the northwest outskirts of Beijing. The Department’s SIGINT net control station is located at Xibeiwang, about 5 km northeast of the headquarters.” Headquarters might be located in the capital city but Strokes (1999) emphasises that SIGINT sites for the collection of radio and satellite communication (SATCOM) are spread throughout China. Manuel also supports the argument when he asserts, “The Third Department’s principal SIGINT collection and processing stations are operated by the Third Bureau (discussed below) attached to the headquarters of each of the seven MRs –i.e. Beijing, Shenyang, Chengdu, Guangzhou, Lanzhou, Jinan and Nanjing. These Bureaus also control several subsidiary SIGINT stations in each of their respective Regions.”

Now why these SIGINT sites are located throughout China and how does it help Chinese government in conducting intelligence and surveillance activities? To answer this, Strokes (1999) explains:

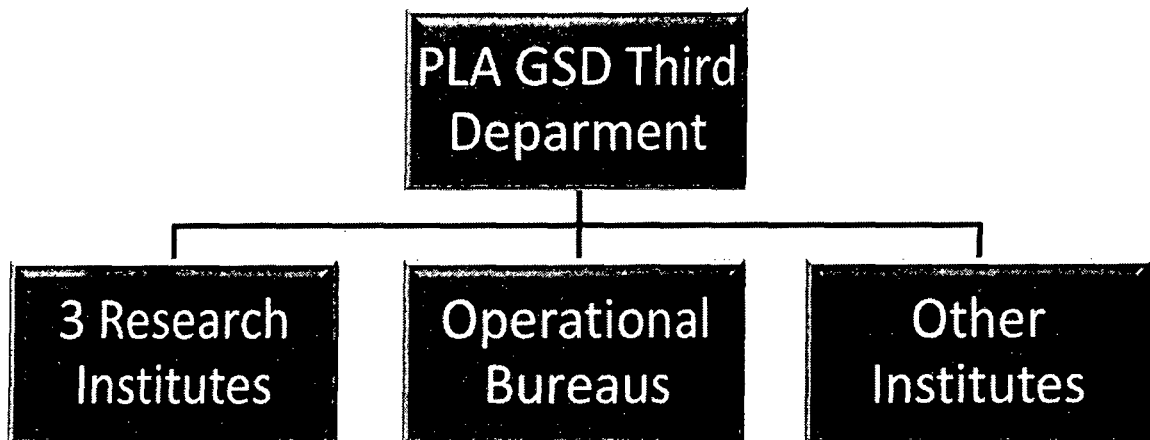
At one time, a site in Lanzhou was responsible for monitoring Russian signal traffic and for providing strategic early warning of a Russian missile attack. The Shenyang station covers signals from Russia, Japan, and Korea. The Chengdu SIGINT site controls the Third Department’s operations against India, Pakistan,

and Southeast Asia. The Nanjing site monitors Taiwan signal traffic, and the Guangzhou site covers Southeast Asia and the South China Sea. Other sites are located near the Sino-Russian and Sino-Mongolian border at Jilemutu, Erlian, and Hami. Several sites are in Northwest China.

Apart from these SIGINT sites located all over China, it is speculated that there are a few sites located outside China as well. Strokes (1999) elaborates, “Outside China, a SIGINT station has been established on Rocky Island (Shidao [石島]), near Woody Island in the Paracels (it is still debated – whether it’s inside or outside China, as it’s a part of South China Sea controversy). There have been persistent press reports of Chinese electronic surveillance sites in Burma, an ideal location for monitoring naval traffic in the Indian Ocean. China has also established multiple SIGINT sites in Burma and Laos.” These are basically meant for keeping an eye on the neighbouring nation states and the movement of the U.S. troops in these neighbouring nations. Strokes et. al (2011) point out the targets of Third Department which is expected to be the same whether it’s inside China or outside China. They say, “Third Department manages a vast communications intercept infrastructure and cyber surveillance system targeting foreign diplomatic communications, military activity, economic entities, public education institutions, and individuals of interest.”

There are many sub-ordinate organisations functioning under the Third Department. The Third Department has direct authority over 12 operational bureaus, a computing centre, and three research institutes (Strokes and Hsiao 2012). 130,000 personnel of the Third Department are divided between 12 bureaus (局), three research institutes (研究所), and 16 regional and functional bureaus (Mandiant 2013). 130,000 personnel are working in general headquarters staff positions, 12 operational bureaus, and three research institutes (Ian Easton and Mark Stokes 2011). Among these, the numbers of research institutes are the only common and consistent data whereas numbers of bureaus, computer centres etc. vary. Let’s see what further information about the subordinate organisations is available.

Figure 16: Sub-ordinate Organisations Functioning under the Third Department



1.3.1 Research Institutes

According to Strokes the three research institutes are: 56th Research Institute (also known as Jiangnan Computer Technology Research Institute [江南电脑科技研究所], located in Wuxi in Jiangsu Province, is the PLA's oldest and largest computing R&D Organisation, focus area – high performance computing, PLA owns some of the fastest supercomputers in the world which enable the making and breaking of sophisticated codes and passwords); 57th Research Institute (also known as the Southwest Institute of Electronics and Telecommunications Technology (西南电子电信技术研究所), focus area – satellite communication technology, works with the China Academy of Space Technology on satellite R&D); 58th Research Institute (also known as the Southwest Automation Research Institute [SWAI] [西南自动化研究所]), focus area – cryptology and information security technology, based in Mianyang (Sichuan), works in co-operation with Nanjing University of Science and Technology (南京理工大学).

1.3.2 Bureaus (局)

The exact number of bureaus operating under Third Department is not known. Even the sources (discussed above) do not point out to one concrete number. Some say they are 12 and some others say they are 12 to 16. Mandiant report (2013) refers bureaus with two different names: regional bureaus and functional bureaus, but do not explain the difference between them. Here, Mulvenon and Yang explain that bureaus that are targeted against specific countries are referred as regional bureaus and the bureaus that are targeted against specific types of communication systems such as satellite, fax, mobile phone etc. are referred as functional bureaus.

Regarding the functions of the bureaus, Strokes *et al* say, “Third Department bureaus likely have a specific mission, such as radio or satellite communications intercept, cryptology, translation, information assurance, and intelligence analysis. In addition to monitoring internal PLA communications traffic for security violations, Third Department offices and MR and MR/Service TRB intercept stations located around China’s periphery can monitor radio traffic and pinpoint the location of emitters through radio direction finding (e.g. homing).” While looking for the bureaus associated with cyber related issues, Strokes *et. al* (2011) say, “Specific Third Department bureaus with responsibilities for CNE remain opaque. The Third Department Seventh Bureau has been associated with technical aspects of cyber operations. Regional bureaus, such as the Shanghai’s Second Bureau or Qingdao’s Fourth Bureau, may be responsible for translation of information attained from communications intercepts and cyber surveillance, and production of intelligence reports based on translated materials.”

Not much of work has been done on the PLA Third Department bureaus. One of the sources, by Mulvenon and Yang (2002) talks only about two bureaus of Third Department (8th Bureau and 12th Bureau), but another source by Strokes *et. al* (Strokes, Lin and Hsiao 2011) argue, “The GSD Third Department has direct authority over 12 operational bureaus. Eight of the 12 bureau headquarters are clustered in Beijing. Two others are based in Shanghai, one in Qingdao, and one in Wuhan. The Third Department’s 12 operational bureaus mostly likely report to the Headquarters Department.”

Let’s briefly go through what these two sources have to say about bureaus of The Third Department and see if any one of these is related to cyber issues.

- First Bureau – Missions: include decryption, encryption, and other information security tasks. It has functional rather than regional mission; has mutually supportive relationship with related Organisations in Chengdu, such as Sichuan University's Information Security and Network Attack and Defence Laboratory [四川大学信息安全及网络攻防研究室].
- Second Bureau – Missions: appears to function as the Third Department's premier entity targeting the United States and Canada, most likely focusing on political, economic, and military-related intelligence. Locations: Bureau Second Office – in Dachangzhen ([大场镇], Shanghai), Third Office – Gucunzhen ([顾村镇], North Shanghai) and Chongming Island ([崇明岛], Shanghai), Seventh Office – Gaohangzhen ([高行镇] Putong Shanghai). According to a recent report by Mandiant (2013), the GSD 3rd Department, 2nd Bureau (总参三部二局), is the APT group that the report has tracked as APT1 whose location has been traced to a 12 storey building of Pudong New Area (浦东新区), Shanghai (上海) situated on Datong Road (大同路) in Gaoqiaozen (高桥镇), which is located in the Pudong New Area (浦东新区) of Shanghai (上海).
- Third Bureau – Mission: The Third Bureau appears to have a functional mission. The mission of the Third Bureau may be front end collection of line of sight radio communications, including border control networks, as well as direction finding, and emission control and security. Location: Bureau headquartered in the southern Beijing suburb of Daxing. Bureau has at least 13 subordinate units. Third Bureau offices are based in Harbin, Dalian, Beijing (responsible for PLA emission security), Hangzhou, Ningdu County (Jiangxi), Xiamen, Shenzhen (responsible for coverage of Hong Kong/Macao wireless networks), Kunming (involved in counter-drug operations), Xian, and Urumqi.
- Fourth Bureau – Missions: focus on Japan and Korea. Location: headquartered in Qingdao, first office – Qingdo, Seventh Office – Hangzhou, other offices at Dalian, Beijing, Shanghai etc.
- Fifth Bureau – Missions: Russia related. Locations: Headquartered in Beijing's Daxing District Huangcun Village, Offices are located in Heilongjiang's Suihua City, Jiuquan and Xinjiang.
- Sixth Bureau – Missions: Taiwan and South Asia mission. Locations: headquartered in Wuhan's Wuchang District. Sixth Bureau offices stretch across central China from the eastern coastal city of Xiamen to the Yunnan city of Kunming. More specifically, offices are located in Xiamen, Nanchang (Seventh Office), Xiangfan; Ningdu County's Xiaobu Village [小布镇], Wuhan, Jingmen, and Kunming's Panlong District (Fourth Office).
- Seventh Bureau – Missions: Unclear. Locations: Headquartered in Shucun (树村) area of Beijing's northwest Haidian District. The bureau manages a satellite ground station in the northwest Beijing suburb of Shangzhuang and oversees at least one element in Urumqi area.

(Selected bureau engineers specialize in computer network defense and attack, and have conducted joint studies with the PLA Information Engineering Academy Computer Network Attack and Defence section. Divided into at least 10 offices, the Seventh Bureau employs English translators. One Seventh Bureau study examined support vector machine [SVM] applications for detecting intrusion patterns. Another study focused on psychological and technical aspects of reading and interpreting written foreign language.)

- Eighth Bureau (61046 Unit) – Missions: Based on language capabilities of members assigned, the Eighth Bureau appears to focus on Western and Eastern Europe and perhaps rest of world (e.g. Middle East, Africa, and Latin America). Locations: Nestled in Hanjiachuan (韩家川). It also has a presence in Wenquanzhen (温泉镇) in far north western Beijing. Among its 10 offices, at least one major office is located in the Hainan Island city of Haikou. The Seventh Office is based in Hubei Province's Xiangfan City. The Eighth Bureau satellite receiving station is in north western Beijing suburb of Xibeiwang (西北旺).
- Ninth Bureau – Missions: serve as the Third Department's primary strategic intelligence analysis and/or data base management entity. The Seventh Office appears to be involved in audio-visual technology (电子声像), and large scale data base management. Location: Not known. (Among all the bureaus, the Ninth is the most opaque.)
- Tenth Bureau (61886 Unit also known as 7911 Unit) – Missions: Central Asia or Russia-related mission, perhaps focused specifically on telemetry and missile tracking and/or nuclear testing. Locations: headquartered in Beijing's northwest suburb of Shangdi (上地) on Xinxi Road (信息路). First office – Beijing, Second Office – (also referred as 7911 Unit) Yining City, Xinjiang, near the Kazakhstan border, Third Office – Baren Village, Kashgar, Another 10th Bureau Office is in Urumqi.
- Eleventh Bureau (Unit 61672 also known as Unit 2020) – Missions: Russia related mission. (With Russian linguists assigned to both entities, differences between the 11th and Fifth Bureau missions differ is unknown). Location: headquartered in the Malianwa community (Beijing), just east of the Third Department headquarters compound. Offices are distributed throughout northern China. A 2020 Unit has had a presence in the far north western Heilongjiang county of Jiage Daqi (加格达奇) since 2005. Another office may be located in Urumqi's Anning (安宁) District.
- Twelfth Bureau (Unit 61486) – Missions: has a functional mission involving satellites, likely inclusive of intercept of satellite communications and possibly space-based SIGINT collection. Location: Headquartered in Shanghai's Zhabei (闸北) District. Subordinate offices and sites in the Shanghai area, and in southeast, northeast, southwest, and north western China. The 12th Bureau's Third Office is located in Shanghai's Baoshan (宝山) District and

has sponsored research into extracting synthetic aperture radar (SAR) satellite images. Other 12th Bureau offices are situated in Taicang (太仓), just outside of Shanghai, and Hangzhou's Daxiaogu Village. Its southwest site is situated outside Kunming in Songming (嵩明) County's Yuejia Village (月家村). The 12th Bureau's northeast station is said to be located in Changchun's Xinglongshan (兴隆山) Village. A southern site is situated within Guangzhou Huadu (花都) District. North western sites are located in Gansu and Xinjiang.

1.3.3 Beijing North Computing Center (BNCC)

Stokes and Hsiao (2012) assert, "BNCC, which is also referred to as the GSD 418th Research Institute, has a military cover designation of the 61539 Unit (previously was the 57370 Unit). BNCC may also be known as the Beijing North Commercial College (Beijing beifang shangye xueyuan[北京北方商业学院])." Regarding its location they say that BNCC is located adjacent to Beijing University and the Central Party School in the city's north western Jiaoziyang (哨子营) suburb. While discussing its missions, they emphasise:

Specific BNCC responsibilities are shrouded by a thick veil of secrecy. Initial indications of a role in cyber operations emerged in 2000, when Falungong authorities accused BNCC of launching denial-of-service attacks against the Organisation's mail servers. Among PLA entities involved in cyber operations, the GSD Third Department BNCC appears most capable of cyber reconnaissance architecture design, technology development, systems engineering, and acquisition. BNCC is one of China's earliest Organisations engaged in high performance computing under which at least 10 subordinate divisions appear responsible for design and development of computer network defence, attack, and exploitation systems. BNCC likely plays a leading role in command and control network management, code breaking, advanced malware development and acquisition, data storage, and vulnerability assessment. BNCC officers have experience in computer network attack and defence, network intrusion monitoring and control, and information collection. BNCC software source code has been made available to enterprises for commercialization. In addition to developing one of China's first stealthy RATs, BNCC fielded China's most advanced network intrusion detection system for analyzing threats and assessing vulnerabilities, including those associated with operating systems such as Android. BNCC's active defence software was certified in tests involving attacks against target networks. Its risk assessment function includes analysis of command and control systems. BNCC's advanced computing networks servers appear sufficient to handle vast databases containing collected electronic communications and files, including recorded phone calls, radio chatter, private emails, internet search records, passwords, password-protected computer files, as well as an abundance of personal data on individuals of interest. BNCC senior engineers also serve as advisors to the State Council Informatization Office, specifically the Information Security Working Group.

1.3.4 Other Organisations under the Third Department

According to Strokes *et. al* (2011), GSD Third Department is responsible for PLA CND and plays a central role within China's national-level information security community. CND-related Organisations managed by or affiliated with the Third Department include:

- The PLA Communications Security Bureau [通信机要局], China North Computation Center [北方计算中心], and the Third Department Computing Center [总参三部计算中心] in Beijing.
- Established in 2005, the National Research Center for Information Security Technology [国家信息技术安全研究中心] serves as the national authority on risk assessment for China's network security.
- The PLA Information Security Evaluation and Certification Center [解放军信息安全测评认证中心].
- Information Security Research Institute [信息安全研究所] and National Information Center [国家信息中心], which maintains a close affiliation with the Third Department S&T Equipment Bureau.
- The National Information Security Engineering Technology Center [国家信息安全工程技术研究中心] in Shanghai, managed alongside with the State Council's Ministry of Science and Technology, National Crypto Management Center, State Secrecy Bureau, and Ministry of State Security.

1.3.4.1 Training Institutes

Apart from the above mentioned organisations, there are a few training institutes (not necessarily functioning under the Third Department) as well:

- PLA University of Foreign Languages (解放军洛阳外语学院): Most linguists assigned to Third Department bureaus and TRBs receive language training at the PLA University of Foreign Languages in Luoyang, counterpart of the Defense Language Institute (DLI) in Monterey, California.
- PLA Information Engineering University (解放军信息工程大学): Technical training for electrical engineers, communications specialists, computer scientists, and network security

personnel is conducted at the PLA Information Engineering University in Zhengzhou, Henan Province.

1.4 GSD Fourth Department

The Fourth Department was established in 1990 (*Easton and Stokes 2011; Stokes 1999*), which is also known as Counter-Electronic Warfare Department (*Stokes 1999*) or Electronic Countermeasures Department (ECM) (*Sharma 2010*) or ECM and Radar Department (*Stokes 1999*). It was established, at the same level as the Second Department (or Intelligence Department [*Stokes also refer it as Foreign Intelligence Department*]) and the Third Department (Technical Department). Regarding the involvement of the Fourth Department in cyber issue, *Sharma (2010)* says:

The 4th Department's oversight of IW dates to at least 1999 and probably earlier. Recent scholarship notes that Dai Qingmin's seminal work, on Information Warfare, was vetted by the 4th Department prior to its publication in 1999 indicating that it had Organisational oversight of this topic even at that time. The GSD's decision in 2000 to promote Dai Qingmin to head the 4th Department vetting his advocacy of the INEW strategy further consolidated the Organisational authority for the IW and the CNA mission specifically in this group. Dai's promotion to this position suggests that the GSD probably endorsed his vision of adopting INEW as the PLA's IW strategy.

Mulvenon (2009) adds that the Fourth Department has operational responsibility of CNO in PLA especially after both the Communication Department and the Fourth Department presented their claims to acquire operational responsibility (in which the Fourth Department won because of Dai Qingmin's work on INEW). He also claims that during wartime personnel from the GSD Fourth Department will be the "trigger pullers" at both the national and warzone level.

Regarding its location *Stokes (1999)* says, "The headquarters of the Fourth Department was initially co-located with that of the Third Department (and that of the Second Department) at Xianghongqi, but in 1991 it was transferred to new facilities at Tayuan, southeast of the Summer Palace."

Regarding the missions of the Fourth Department, *Stokes (1999)* says, "The Fourth Department has the electronic intelligence (ELINT) portfolio within the PLA's SIGINT apparatus. This department is responsible for electronic countermeasures, requiring them to collect and maintain data bases on electronic signals." *Deepak Sharma (2010)* adds, "The Fourth Department oversees both operational ECM units and R&D institutes conducting

research on a variety of offensive IW technologies.” Stokes also predicts, “The Fourth Department could have possible computer network attack (CNA) responsibilities.” *Easton and Stokes* (2011) sum its missions as – “The Fourth Department holds the overall responsibility for electronic warfare (EW), including electronic intelligence (ELINT) and tactical electronic support measures (ESM).”

Apart from this, Stokes (1999) says:

The Fourth Department has two major Special Detachments located at Xibiewang and Yangfang, which are responsible for the electronic warfare (EW) defence of key state and military headquarters and facilities in Beijing. In addition to these two Special Detachments which are run directly from the Fourth Department headquarters, units of the Department manage and direct SIGINT and EW operations for the Army through Military Region to Divisional levels. There are, for example, several Counter-Electronic Warfare Department units in the Beijing Military Region, including a major unit at Xishan in the western mountain area which has a general responsibility for the EW defence of the Beijing region. The Department also manages and directs SIGINT and EW operations for the Air Force and Navy.

Easton and Stokes (2011) also argue that the Department not only plays a leading role in joint force planning and the development of requirements, but also oversees one or possibly two direct reporting electronic countermeasure (ECM) units. They say, “The first is a brigade level Organisation based in Langfang with subordinate elements in Anhui, Jiangxi, and Shandong. The other, located on Hainan Island, appears to have either operational or experimental satellite jamming responsibilities.”

Some R&D institutes are also allegedly operating under the Fourth Department. While discussing about R&D institutes, Sharma does not specify which R&D institutes are functioning under this Department, but Stokes (1999) points out one when he says, “The GSD 54th Research Institute supports the ECM Department in development of digital ELINT signal processors to analyze parameters of radar pulses. To augment its ground-based collection, China may be resurrecting an ELINT satellite program which has been dormant for over 20 years.” Some more institutes are pointed by Stokes et al (2011). They say, “The Fourth Department oversees the GSD 54th Research Institute, which most likely provides engineering support, and also maintains close links with a number of China Electronic Technology Corporation (CETC) entities, including the 29th Research Institute in Chengdu, the 36th Research Institute in Jiaxing, and the 38th Research Institute in Hefei.” One more institute pointed out by Easton and Stokes (2011) is PLA Electronic Engineering Academy (解放军电子工程学院), Hefei. They assert that the Fourth Department also oversees the

PLA Electronic Engineering Academy, an institution for professional military education and technical training.

1.5 Communication Department (通信部)

Sinodefence.com writes, “The Communications Department is the headquarters for the signal corps of the PLA, and a national-level organisation responsible for developing, constructing, operating, and maintaining the PLA’s nation-wide command, control, communications, computers, and intelligence (C4I) system. The department also works with civilian ministries and companies at the national and provincial levels to enhance PRC’s telecommunications infrastructure.” Though Mulvenon (2009: 273) elaborates that the Fourth Department won the operational responsibility of computer network operations (due to Dai Qingmin’s famous work on INEW) in a competition and its fierce competitor was none other than Communication Department, which was equally qualified.

While talking about its organisational structure sinodefence.com explains that the department is headed by a Director, a Political Commissar, and four Deputy Directors. The website claims it has following subordinate organs:

- Political Department (政治部)
- Science and Technology Bureau (科技局)
- Equipment Bureau (装备局)
- Communications Bureau (通信局)
- System Engineering Bureau (系统工程局)
- Mobile System Office (移动局)
- Factory Management Bureau (工厂管理局)

2. General Armaments Department (zong zhuangbei bu [(总装备部)])

According to Easton and Stokes (2011) the General Armaments Department (GAD) appears to be the key Organisation responsible for managing the acquisition of China’s space-based surveillance system and satellite tracking and control, most likely including electronic reconnaissance satellites. They also assert, “Within GAD, the Electronics and Information Infrastructure Department (总装电子信息基础部) Aerospace Equipment Bureau (航天装备

局) appears to be responsible for developing the technological requirements of the space-based sensor infrastructure supporting missile operations. It appears that the GAD may also manage the satellite tracking and control infrastructure supporting ELINT satellites.”

3. China’s Cyber Command

The *PLA Daily*, on 19 July 2010 reported that the GSD unveiled the establishment of the “Information Security Base” (信息保障基地) which the Chinese media referred to as the country’s first “cyber base”. It is operating under the GSD and Hsiao (2010) claims that the base may serve as the PLA’s cyber command. Hsiao turns our attention towards a ‘*Global Times*’ report published on 22 July 2010 which quotes an anonymous GSD officer. The report emphasises that the cyber base is a ‘defensive’ base for information security, not an offensive headquarters for cyber war. While discussing about its functions the report says, “The setup of the base just means that our army is strengthening its capacity and is developing potential military officers to tackle information-based warfare. Other tasks will include online information collection and the safeguarding of confidential military information by ‘build[ing] up walls’.”

What is worth paying attention here is its function of online information collection, which could range from publicly available free information to highly classified and sensitive information. So what actual functions China’s cyber base has, are not completely clear. This is also important as China’s foreign ministry spokesman Hong Lei, once responded that ‘gathering information’ is not ‘online spying’ while countering the cyber attack allegations imposed on China by the US.

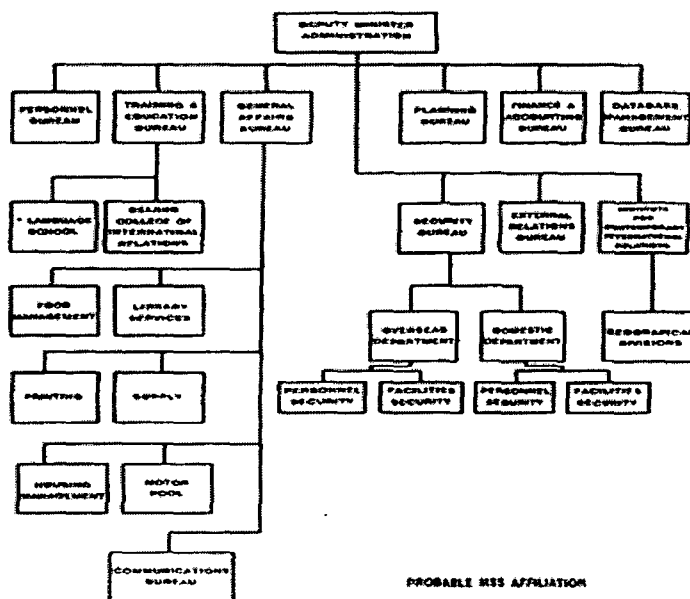
4. Ministry of State Security (MSS)

According to Wikipedia the Ministry of State Security is the security agency of the China. It is also probably the Chinese government’s largest and most active foreign intelligence agency, though it is also involved in domestic security matters. According to FAS, “The MSS was created in June 1983 by the Central Committee to centralize foreign intelligence and counterintelligence functions.” Regarding the structure and missions, the website explains, “The MSS is headed by the Minister of State Security, who reports to the Central Committee. It conducts counterespionage operations within China, and HUMINT and limited SIGINT operations both inside and outside of the PRC. The MSS centers its collection operations on

regional adversaries with which China has shared borders, including Russia, India, and Vietnam, and on nations that are militarily, politically, or economically important to China. The latter category includes the United States, Taiwan, South Korea, and Japan.” The website also claims that key intelligence collection objectives for the MSS include: acquiring foreign military and civilian high technology; collecting information on adversary military planning, foreign policy, and foreign trade positions concerning China; and monitoring Chinese dissident groups overseas. Carr asserts, “MSS is involved in: Counterespionage and Counterintelligence; Foreign Intelligence; and Domestic Intelligence. However they do not mention anything about its involvement in cyberwarfare, but according to Manuel, “The Ministry of State Security and other civil authorities have also become well-versed in cyberwarfare, partly through their attempts to establish a ‘great firewall’ around China’s computer networks and to strictly control Internet usage and because China is home to the most virulent non-governmental computer hackers in the world.”

The sub-ordinate organisations functioning under MSS is shown in the figure below. Since MSS is an intelligence organisation, its sub-ordinate Organisations are also supposed to be indulged in intelligence and espionage (including cyber espionage) activities.

Figure 17: China’s Ministry of State Security



Source: *Nicholas Eftimiades, China’s Ministry of State Security: Coming of Age in the International Arena, 1992 p.n. – 09.*

5. Ministry of Public Security (MPS)

According to Wikipedia, “The Ministry of Public Security (MPS) is the principal police and security authority of the mainland of the China and the government agency that exercises oversight over and is ultimately responsible for day-to-day law enforcement.” Regarding its missions the website asserts, “The Ministry operates the system of Public Security Bureau, which are broadly the equivalent of police forces or police stations in other countries. It also controls and administers the People’s Armed Police. Since the creation of the Ministry of State Security (in 1983), the MPS has lost much authority and does not undertake paramilitary functions, which are now within the province of the People’s Armed Police, nor does it generally conduct domestic intelligence which since 1983 has been a primary responsibility of the Ministry of State Security. Hong Kong and Macau have their own security bureaus/agencies and police forces.”

6. Commission for Science, Technology and Industry for National Defence (COSTIND)

According to Wikipedia, “The COSTIND (国防科学技术工业委员会) was formed in 1982 to centralize Chinese defence procurement and technology whose responsibility had been distributed among several agencies. It was a civilian ministry within the State Council, responsible for setting policy for defence procurement. It is considered as the Chinese counterpart of DARPA of the US.” Regarding its missions FAS says, “Together with the Military Intelligence Department (i.e. GSD 2nd Department), the COSTIND works to obtain military technologies for application to the Chinese military. Much of this technology is obtained through technological diversion and reverse engineering of products purchased from the West. The COSTIND is also responsible, in concert with the Military Intelligence Department, for the development of China’s space reconnaissance program.” Wikipedia asserts that name of the COSTIND has been changed. It says, “In March 2008 COSTIND was merged into a new super bureaucracy called the Ministry of Industry and Information Technology (MIIT) and renamed as the State Administration for Science, Technology and Industry for National Defence (SASTIND).”

7. Academy of Military Sciences (AMS [军事科学研究院])

According to Mulvenon (2009) AMS is one of the (other two are: NDU and CCA discussed below) CNO doctrinal and professional military education Organisations of China. Wikipedia also agree with Mulvenon that AMS is the PLA's premier military science research institution, reporting directly to the Central Military Commission (CMC), headquartered in Beijing. Regarding the functions of AMS, Mulvenon (2009) says, "The academy is the locus of development of PLA strategy and doctrine, and is also responsible for the coordination of various military research bodies, often at the behest of the CMC and the military leadership. While the majority of its work is academic, AMS's Campaign and Tactics Department (zhanyi zhanshu bu [战役战术部] also performs a similar function to the U.S. Training and Doctrine Command (TRADOC) in designing, attending, and assessing military exercises in the field." Regarding AMS's involvement in cyberwarfare, he asserts that AMS is also the principal institution responsible for exploring the future of military conflict, leading the analysis of the Revolution in Military Affairs (RMA) and cyber warfare. He also traces its research background and say, "Some of the earliest IO and CNO related research in the PLA was initiated at AMS, beginning with translation and analysis of foreign IW writings in the Academy's Foreign Military Studies Department. The first generation of AMS scholars included Wang Pufeng and Wang Baocun. Later, as information operations evolved and matured in the PLA, important work was conducted in the AMS Campaign and Tactics Department."

8. State Informatization Leading Group (SILG)

According to Chinese government website of Advisory Committee for State Informatization (ACSI), the State Informatization Leading Group (SILG) has been formed according to a decision taken in August 2001 by the Central Committee of the Communist Party of China (CPC) and the State Council with a view to providing stronger leadership to the promotion of informatiozation and to the safeguarding of state information security. Regarding the leadership of SILG, the website says, "Heading the SILG is Wen Jiabao (Even after Xi Jinping and Li Keqiang took over the website mentions Wen Jiabao's name), member of the Standing Committee of the Political Bureau of the CPC Central Committee and Premier of the State Council. Deputy leaders are Huang Ju, member of Standing Committee of the CPC Central Committee and Vice-Premier of the State Council, Liu Yunshan, member of the Political Bureau of the CPC Central Committee and Head of the Propaganda Department of

the CPC Central Committee, Zeng Peiyan, member of the Political Bureau of the CPC Central Committee and Vice-Premier of the State Council, Zhou Yongkang, member of the Political.”

Regarding the composition and missions of SILG, Strokes and Hsiao (2012) assert, “The State Informatization Leading Group (SILG), consisting of senior representatives of the CCP Central Committee Politburo, State Council, and PLA, establishes national informatization policies. With cyber security an important facet of informatization, the SILG’s Network and Information Security Working Group (网络与信息安全组) has advised senior leaders on CNO policy.” The government website also talks about two sub-ordinate organisations. One is the ACSI, established with the approval of SILG. It is a think-tank of SILG. The group of 55 experts has been appointed to the committee. They come from all disciplines including economy, technology and law. Among them are senior academicians who have long been in the area of information technology and noted economists. Another is the State Council Informatization Office (SCITO) which is an Organisation that does office work and handles routine affairs of SILG.

9. National Defence University (NDU)

According to Mulvenon (2009) NDU is one of the CNO doctrinal and professional military education Organisations of China. He further elaborates that the PLA’s most senior professional military education institution, training the best and brightest of the PLA for leading command positions. While discussing the difference between AMS (discussed above) and NDU, he asserts that the NDU does conduct some research, though its focus is much more near-term than the AMS. He also quotes Wang Baocun, who summarized the difference this way: “The NDU teaches officers, while the AMS writes papers and gives advice to the CMC. NDU must think about the current PLA and be practical (how to deal with IW now). AMS must think about the future, out 10-20 years.” He also talks about a sub-ordinate office at NDU responsible for examining information operations issues, which according to him is known as the Command Education Research Office (zhihui jiaoyan shi [指挥教研室]).

10. Joint Campaign Command HQ

According to Mulvenon (2009) Joint Campaign Command HQ is also involved in China’s cyberwarfare activities. He asserts, “While the GSD 4th Department is the locus for CNA planning during peacetime, some wartime responsibilities fall to the Joint Campaign

Command HQ under the Warzone.” While discussing about its sub-ordinate Organisations, he elaborates:

Within the Main Command Post (jiben zhihuisuo [基本指挥所]) of the HQ, various centres direct the IO and CNO-related functions. The most important of these is the Information Countermeasures Center (xinxi duikang zhongxing [信息对抗中心]). This unit is composed of relevant service commanders and their staff officers. It is responsible for providing advice on information countermeasure issues, planning and coordinating information systems, and guiding and coordinating the information countermeasures of every level of the operational group. The center is composed of comprehensive planning, electronic countermeasures (dianzi duikang [电子对抗]), network warfare (wangluo zhan [网络战]), information system defence, information security and secrecy, weapons and equipment support, and comprehensive support departments.

11. Wuhan Communications Command Academy (CCA)

According to Mulvenon (2009) Wuhan Communications Command Academy (CCA) is one of the CNO doctrinal and professional military education Organisations of China. He further explains that the Wuhan Communications Command Academy (CCA) is the senior professional military education institution in China for PLA communications and electronics personnel. While discussing its functions, he asserts:

It is responsible for training future communications and electronics unit leaders in doctrine, policy, technology, and leadership. In 1999, CCA hosted the first all-army collective training session for division and brigade chiefs of staff in IW theory, which has continued to this day. It is also the locus of PLA dissemination of doctrinal and teaching materials on information operations, and is the only institution certified to accredit information operations instructors for PLA educational institutions at every level and in every service. The CCA offers command and control related cross-disciplinary courses, with emphasis on IW at the core of undergraduate and graduate training. In December 1998, CCA established the PLA's first IW simulation experiment center. In the same year, the GSD Communication Department endorsed two CCA publications on IW for use as teaching materials, *Command and Control in Information Warfare* and *Technology in Information Warfare*. The textbooks were drafted by a task force of PLA IW theorists and instructors from CCA.

12. PLA Information Warfare Militia Units

According to Sharma (2010) the PLA has been creating IW militia units comprising of personnel from the commercial IT sector and academia since 2002. But according to Hsiao

(2010) the PLA has been developing PLA's information warfare (IW) units since at least 2003. One more source (Ming Zhou 2009) claims that China possessed the first official net militia unit with 40 professionals, long back in 1998. The same source also asserts that a large scale emergency order was given to form Net Militia Units in 2005. Regarding the composition and missions of PLA IW militia, Sharma (2010) says:

These IW militia units represent an operational nexus between PLA CNO operations and Chinese civilian information security (infosec) professionals. A political commissar for the Guangzhou People's Armed Police (PAP) garrison advocated in 2003 the direct involvement of urban militia units in information warfare, electronic warfare, and psychological warfare. He also proposed that militia reform efforts should focus on making information warfare as one of the Guangzhou militia's primary mission. PLA media reporting indicates that IW militia units are tasked with offensive and defensive CNO and EW responsibilities, psychological warfare, and deception operations, though the available sources do not explain the lines of authority, subordination or the nature of their specific tasking. A militia battalion in Yongning County (Ningxia Province, Lanzhou Military Region) established an IW militia group in March 2008 and tasked it to conduct network warfare research and training, and to "attack the enemy's wartime networks".

13. Technical Reconnaissance Bureaus (TRB)

According to Sharma (2010) the PLA maintains at least six Technical Reconnaissance Bureaus (TRBs) located in the Lanzhou, Jinan, Chengdu, Guangzhou, and Beijing military regions. On the other hand Stokes et. al (2011) argue that 12 operational bureaus are under the seven MR headquarters in Beijing, Chengdu, Guangzhou, Jinan, Lanzhou, Nanjing, and Shenyang. They also say that TRBs are separate and distinct from The Third Department's operational bureaus. Difference as well as similarity can be observed from following statement:

Each Military Region Headquarters Department Chief of Staff exercises authority over at least one TRB. However, senior Third Department authorities in Beijing likely issue policy guidance and general tasking for TRB collection, analysis, and reporting. TRB missions may parallel those of the Third Department, and include communications intelligence, direction finding, traffic analysis, translation, cryptology, computer network defence, and computer network exploitation. However, their primary role is to support the MR command (Stokes et al 2011).

Adding to this Sharma (2010) further explains the missions of TRBs as – “TRBs are responsible for SIGINT collection against tactical and strategic targets and have apparent CNO duties, though few details are available on the exact role or subordination of these units.” Stokes et al (2011) on the other hand discuss each one of TRBs in details (under each MRs):

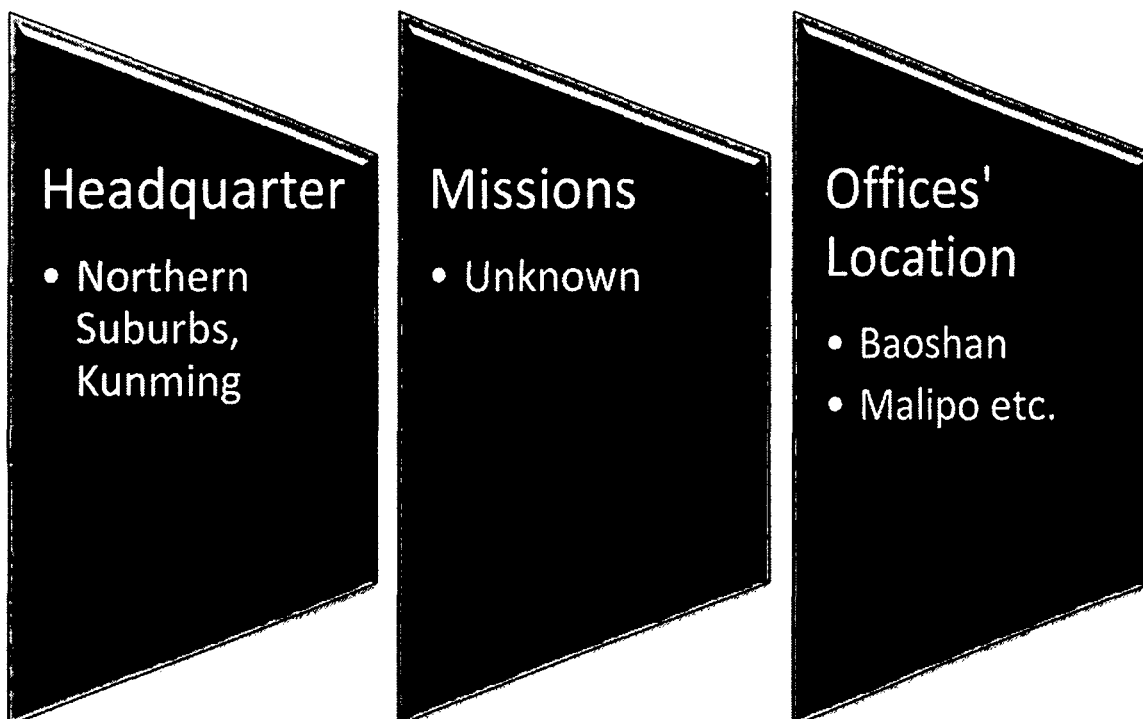
Beijing Military Region – The Beijing MR TRB (66407 Unit) is headquartered in Beijing’s Xiangshan Mountain area.

Headquarter	Missions	Offices' Location
<ul style="list-style-type: none"> • Xiangshan Mountain Area, Beijing 	<ul style="list-style-type: none"> • Russian (because of assigned Russian linguists) 	<ul style="list-style-type: none"> • Along the border of Inner Mongolia • In Hohhot (Unit 66196), Qiaobaozhen (巧报镇) • In Hailar (海拉尔 Unit 66367) area • In Neimeng Linhe (内蒙临河) etc.

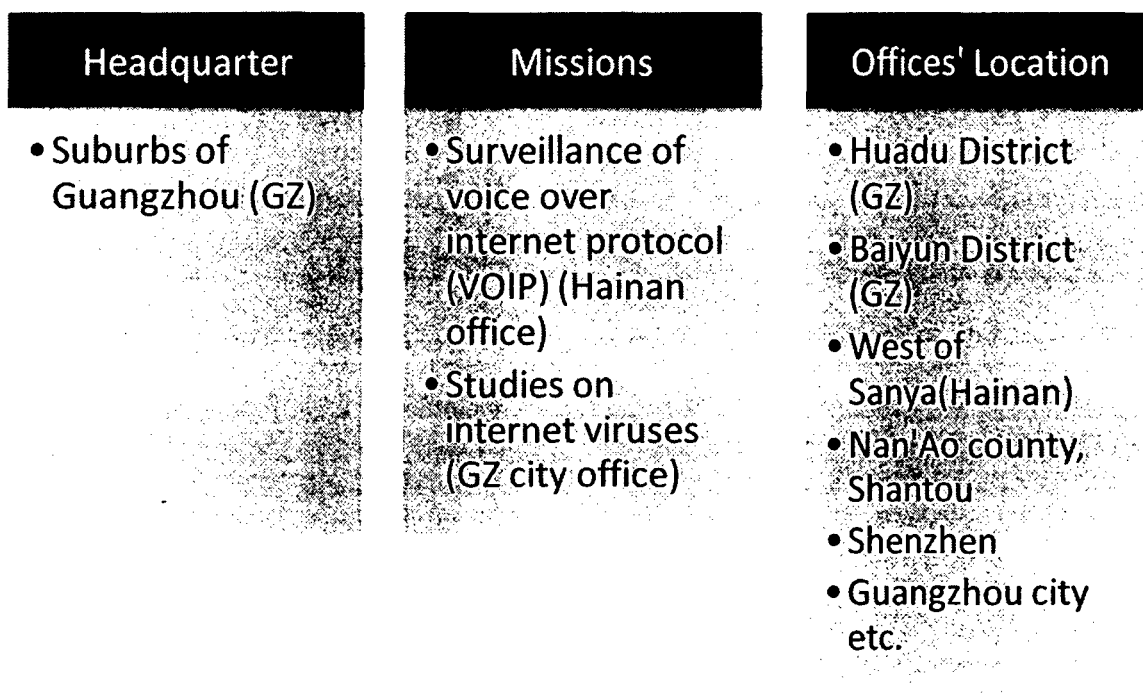
Chengdu Military Region – The Chengdu MR has two TRBs. The Chengdu MR First TRB (78006 Unit) is headquartered in Chengdu.

Headquarter	Possible Missions	Offices' Location
<ul style="list-style-type: none"> • Chengdu 	<ul style="list-style-type: none"> • CNE 	<ul style="list-style-type: none"> • Unknown

The Chengdu MR Second TRB (Unit 78020) is based in northern suburbs of Kunming.



Guangzhou Military Region (75770 Unit) – The Guangzhou MR TRB is headquartered in the Guangzhou suburbs and oversees at least eight offices operating in southern China.



Jinan Military Region – The Jinan MR TRB (72959 Unit) is located in Jinan City, and is said to oversee 670 technical specialists.

Headquarter	Missions	Offices' Location
<ul style="list-style-type: none">• Far Eastern End of Sushan Road, Jinan City	<ul style="list-style-type: none">• Microwave Relay Intercept• Korean• Japanese	<ul style="list-style-type: none">• Jinan City• Weihai etc.

Lanzhou Military Region – The Lanzhou MR oversees two TRBs. The Lanzhou MR First TRB (68002 Unit) is centered in the southern Lanzhou City's Qilihe District. Unlike other MRs, no subordinate offices under the Lanzhou MR First TRB could be identified. However, the Lanzhou MR's Second TRB (69010 Unit) appears to play an important and unique role in China's SIGINT community. The Lanzhou MR Second TRB has its roots in a section of the Third Department's Second Bureau based in Xinjiang. It merged with the Xinjiang MR, becoming the Lanzhou MR's second TRB in the mid-1980s.

Lanzhou MR's second TRB:

Headquarter	Missions	Offices' Location
<ul style="list-style-type: none"> • Shuimogou (水磨沟) village, Urumqi 	<ul style="list-style-type: none"> • SIGINT • Monitors military activities along China's borders with India, Pakistan, Afghanistan, Tajikistan, Kyrgyzstan, Kazakhstan, Russia and Mongolia 	<ul style="list-style-type: none"> • Shule County • Altay • Yining etc.

Nanjing Military Region – The Nanjing MR Headquarters Department, oversees two TRBs that are likely focused on Taiwan military and other communications and computer networks, as well as U.S. activity in the Western Pacific area of operations.

The Nanjing MR First TRB (73610 Unit):

Headquarter	Missions	Offices' Location
<ul style="list-style-type: none"> • Nanjing City 	<ul style="list-style-type: none"> • Taiwan military communications and computer networks • U.S. activity in the Western Pacific area 	<ul style="list-style-type: none"> • Zhuzhuang Suburbs, Nanjing • Songjiang District's Dongshi Village, Shanghai • Zhoushan Island • Minhang District, Shanghai • Zhuzhuang, Nanjing • Jianggan District or in Shangyu City Lihazhen

The Nanjing MR's Second TRB (73630 Unit):

Headquarter <ul style="list-style-type: none">• Zhenbancun (阵坂村), Fuzhou City	Missions <ul style="list-style-type: none">• Taiwan	Offices' Locations <ul style="list-style-type: none">• Hongshan Village, Fuzhou• Feifeng Mountain, Jianxin Village, Fuzhou• Gushan (鼓山), Fuzhou's eastern Jin'an District• Dongjing Mountain, Donghanzhen (东瀚镇)
--	--	---

Shenyang Military Region (65016 Unit) – The Shenyang MR TRB headquarters is situated in Shenyang's Dongling District.

Headquarter <ul style="list-style-type: none">• Donglian District, Shenyang	Missions <ul style="list-style-type: none">• Russian• Korean• Japanese	Offices' Location <ul style="list-style-type: none">• Harbing• Dalian• Jiamusi• Dongning County Heilongjiang• Fuyu County, Qiqihar• Hulunber, In. Mongolia• Hunchun City In. Mongolia
--	---	--

14. Hackers and Hacker Groups

In May 1999, after so called accidental bombing of Chinese embassy in Belgrade, Chinese hackers launched large scale hack attack on White House. Following the 1999's comments by then Taiwan President Lee Teng-hui that the model of relations between Taiwan and China is a "special state-to-state" relationship, stimulated numerous hack attack on Taiwan National Assembly, Presidential Executive Office and other government websites. Another incident known as EP-3 incident of 2001, mid air collision of a US Navy EP-3E ARIES II signal intelligence aircraft and a PLA Navy J-8II interceptor fighter jet, also known as Hainan Island incident, resulted in international dispute between China and the US. This incident also resulted in hacking of more than 1,000 US websites (American hackers also hacked same number of Chinese websites). Hacker groups have made their presence felt every time when such incidents have occurred in international arena. It is sometimes also referred as patriotic hacker groups (by Mulvenon and others).

There are numerous instances of such hacking activities (which would be analysed in next chapter) allegedly originating from China (though not all proved yet). But if these allegations are true, the number of hackers and hacker groups would be numerous. The details regarding these hacker groups are not available in open sources, however one author Marvel (2010: 36) has identified some of these hacker groups:

- ❖ NSFocus – It is an early and prominent hacker group active from 1997 through 2000 which evolved out of the Green Army Alliance. The group is now a prominent information security firm and whose website still retains the logo of the Green Army Alliance and enlists the name of its founding members (who were also some of the most prominent hackers of China).
- ❖ XFocus – It is a commercial information security company that grew from a hacker group. It co-sponsors 'XCon', one of the largest 'hacker conferences' in China in partnership with NSFocus and Venus Technology.
- ❖ Black Eagle Base – It was a patriotic hacker group whose members were arrested in February 2006, but the group was operational again six months later under the name of Black Eagle Honker Base. Its members released a statement claiming that the group vowed to focus its efforts on training people for the state and working to improve the state's network security industry, suggesting a possible cooperative relationship with state authorities as a condition of release. The group also thanked the State Security Bureau and COSTIND (now renamed as SASTIND) for their educational guidance they provided to its members while in custody.

- ❖ Javaphile Group – It was the group which led the first large scale attack on White House in 2009 just after the bombing of Chinese embassy in Belgrade.

Saporito and Lewis (2013), from Center for Strategic and International Studies, in an article write about another hacker group:

- ❖ Network Crack Program Hacker (NCPH) Group – This group is located in Zigong in the Sichuan Province. The group is believed to be comprised of students from the Sichuan University of Science and Engineering, led by Tan Dailin who uses the pseudonym ‘Wicked Rose,’ with KuNgBiM, Rodag, and Charles as members. The authors also identify WHG as a close affiliate, whose real name may be Zhao Jibing and is believed to be employed in the Sichuan province. During 2006, the group specifically targeted the Defense Department.

Hagestad (2012: 180) has also pointed out a few Chinese individual hackers who attended a Beijing Hacking show *Chinese Hackers Talk Hacker* in 2008. One of the attendees was Frankie Zie of Shenzhen, who is currently chief technology officer of a network security company located in China. Mr. Zie is a well known former black hat hacker, using the Hacker nom-de-guerre r00t, and claims to have hacked numerous websites in the US. Hagestad also points out another Chinese hacker ‘netcc’ who claims to possess the ability to hack a thousand websites per month.

Though these individual hackers and hacker groups are non-state actors but in some cases (like in the case of Black Eagle Base) it is evident that group has offered services to Chinese government agencies and departments, if not directly involved in Chin’s cyberwarfare. This might be helpful to Chinese government in two ways: Firstly, the government can use these individuals and groups for preparing and conducting cyber attacks on other nations during the period of both peace and conflict; secondly, if any finger is raised against China or somehow these attacks are traced to Chinese soil, the government can put the blame on some of these groups (and shut them down temporarily) to prove it’s innocence. The governments of other nations, even the US seems to follow the same practice. For instance many governments use the black market and other illegal source to buy zero day exploits or malicious code, and on the other hand claim that they have no relationship with those illegal sources.

15. National University of Defence and Technology (国防科学技术大学)

The latest Chinese supercomputer Tianhe-2 (on 16 June 2013) ranked as the fastest supercomputer in the world leaving behind supercomputers of the US, Japan and other countries. This huge achievement was all possible because of National University of Defence and Technology (NUDT). Wikipedia says that NUDT is a comprehensive national key university based in Changsha, Hunan Province, which is under the dual supervision of the Ministry of National Defence and the Ministry of Education. Regarding its missions the website asserts that NUDT is a leading institute in China's Supercomputer development and space program.

China daily report (*China Daily* 18 June 2013) asserts that this was not the first time when a Chinese supercomputer ranked as world's fastest. Tianhe-1A, earlier version of Tianhe-2, ranked world's fastest in 2010 and second fastest in 2011. The report also emphasises that China's supercomputing dream started in 1978 when then-Chinese leader Deng Xiaoping chose the National University of Defence Technology as one of the major institutions to develop China's own supercomputer. Originally, as Wikipedia points out, when NUDT was established in 1953, it was located in Harbin, the capital city of Heilongjiang Province, and was known as Harbin Military Academy of Engineering. In 1966 it was renamed as Harbin Academy of Engineering. In 1970 it was shifted to Changsha, capital city of Hunan Province, due to possibility of war with Soviet Union and was again renamed as Changsha Institute of Technology. Finally in 1978 this institute was named as National University of Defence and Technology.

16. PRC Military-Industrial Companies

A news report (*The Register* 13 May 2013) says that Chinese telecom firms like Huawei and ZTE were not allowed to enter the markets of various nation states like the US, Australia, India etc. because of security reasons. Another report published in DNA (on 26 June 2013) asserts, "The US House of Representatives intelligence committee urged US companies to avoid doing business with Huawei and ZTE, another telecoms firm, in case the Chinese government used their equipment for spying. It did not have firm evidence that this was the case, but the committee's 52-page report cited 'dozens and dozens' of calls about Chinese equipment behaving suspiciously." Huawei according to the report was forced to drop a joint \$2.2bn bid for Silicon Valley firm 3Com. The latest in the series is another Chinese firm Tencent whose famous mobile phone based application 'We Chat' faces a likely ban in India

(*The Times of India* 18 June 20013). The main reason provided by these nation states is – these Chinese firms pose threat to their national security, which is due to their alleged close links with PLA (though not proved yet). Huawei's founder was a senior engineer in PLA, which according to the DNA report provide a wealth of opportunities for Chinese intelligence agencies to insert malicious hardware or software implants into critical telecommunications components and systems. Even inside China these commercial firms do not only work in close ties with the PLA and allegedly also work for them. Marvel (2010) provides some useful insights on this issue. Huawei along with other firms like Zhongxing and Datang received direct funding from PLA for R&D on C4ISR systems (Marvel 2010: 43). Huawei and ZTE also provided certification training and related engineering training to PLA personnel assigned to communication and information warfare related positions (Marvel 2010: 43). Another firm called Venus Technologies Inc, which has close links with hacker groups, is also a provider of information security and computer network operations expertise to the PLA (Marvel 2010: 43). These examples easily prove that Chinese commercial firms offer services to the PLA which could be understood with this argument – if Chinese government is an autocratic one (as per Western thinking) how can any commercial firm refuse to provide services to them, but working for the State (or with State sponsorship against other nations- which autocratic government can easily do) has not yet been proved.

Conclusion

As available literature suggests there are many government and some non-government organisations that handle and are involved in information and cyber related activities. However the range of these activities is not completely known. Available literature also suggests that these organisations are not only based in capital city of Beijing rather spread all over China so that electronic warfare methods such as signal interception, jamming etc (which unlike computer network has limited geographical reach) could be used against strategically important nations (especially Taiwan) during the period of conflict and peace. This decentralization of cyberwarfare (and information warfare) related tasks to various specialized departments and bureaus, has made it difficult to understand functioning of command and control structure (Hagestad 2012: 35). The lower we go in the decentralised hierarchy list, it seems lesser information is available. However what is known is that the GSD with its sub-ordinate organisations like the GSD Fourth Department, Third Department, Communication Department and Information Security Base (Cyber Base) is the most eminent

military organisation involved in China's Cyberwarfare. Operational responsibilities of cyberwarfare and computer network warfare seem to lie with the GSD Fourth Department (as Mulvenon suggests so and available literatures do not claim otherwise), which also is the locus for CNA planning during peacetime and some wartime responsibilities fall to the Joint Campaign Command HQ under the Warzone. Other all organisations including both military and civilian (like the GSD Third Department, GSD Second Department, MSS etc.) which are involved in intelligence collection could also be involved in CNE. Organisations like Information Security Base (Cyber Base/ Cyber Command), MSS etc. as their names suggest are meant for providing security and defence. So, they could be involved in CND, but in many cases one organisation can be involved in many areas at the same time, for instance if cyber base would act as cyber command, it would not only be responsible for defensive missions but would also have to conduct offensive cyber operations if instructed. Hence this study is a speculative and subjected to change (with situation and time).

Chapter 5

Intentions and Capabilities of Chinese Cyberwarfare

China is blamed for most of the cyber attacks across the globe. If Chinese government is involved in or provides state sponsorship or if the Chinese government is working in collaboration with hackers to wage cyberwar against other nations (which is extremely difficult to say with certainty), the next question arises why is the government doing so, what are its intentions or objectives behind it? Are China's intentions same during the period of peace and conflict period or are they different? Another issue that comes up here is that if China is capable of exploiting high profile networks of many nations (including defence networks, finance networks etc.) and multinational companies then China possessing highly sophisticated cyber capabilities is really true or is it overblown? Or is it that these capabilities are just the tip of an iceberg and can multiply many folds during a period of conflict or war? The requirements of cyber skills for war period and for peaceful period are not different, so it is all up to the intent of the operator who operates the computer. The cyber skills available to an operator now, which is supposed to increase in future, can enable an operator to execute a host of cyber activities and cyber attacks. If the operator, in case of China, is being ordered by Chinese government what could be the intentions of the government then? These intentions of government can be understood from the kind of cyber activities it is involved in or from the kind of cyber attacks it has ordered. That's why all the cyber intrusions or hacking attacks attributed to China hold the key of understanding the intent of Chinese government. Also, by analysing these activities and by looking at some other factors (like China's cyber military drills, China's efforts and R&D in cyber domain, its cyber power etc.) one can also evaluate China's capabilities of conducting cyberwarfare. This chapter first looks into what available literature, especially Western literature, has to say about the intentions and capabilities of Chinese cyberwarfare and then it probes into the cyber attack incidents attributed to China. This chapter also analyses these cyber incidents so as to evaluate China's intentions and capabilities. In the end, chapter also looks into the China's response to these hacking allegations and analyses them in order to understand their views.

1. Intentions

The cyber skills can help Chinese government in many ways like collecting intelligence, identifying and understanding potential threats and adversaries, fighting against its adversaries in cyberspace in case of a conflict, exploiting other nations' computer networks,

taking their network down, enabling backdoor entry to others networks, stealing/destroying/degrading/denying information (like trade secrets, intellectual property rights etc.), conducting espionage activities, taking down critical infrastructures of other nations, implanting viruses and for a host of other purposes. But what are the purposes for which China has been using its skills and organisations is something that whole world wants to know.

Colonel Spade (2012), a scholar from US Army War College, argues, “U.S. government and think tank studies suggest that China has three primary national security objectives: sustaining regime survival (rule of the Chinese Communist Party [CCP]), defending national sovereignty and territorial integrity, and establishing China as both a regional and world power. Critical to those objectives are sustaining stable economic and social development, modernizing the military, and preventing Taiwan independence.” He again asserts:

China’s defence strategic framework includes four major provisions geared toward transforming their military and defence systems. First is the modernization of national defence and the armed forces through “informationization.” This includes a networked military and development of cyber capabilities. Second is the coordination of national defence spending and economic development, with an emphasis on ensuring ample resources for the military and dual-use industries and technology. Third is the reform of national defence and the armed forces. This includes science and technology, procurement, research and development, and manufacturing, again stressing integrated defence and civilian dual-purpose industry. Reform also includes an improved “national defence mobilization system.” The fourth provision is “leapfrogging” military science and technology development; that is, bypassing the gradual, developmental path the United States took to build a networked force in order to equal American capabilities by the mid-21st century.

The US Department of Defense Annual Report to the US Congress 2013 asserts:

Cyberwarfare capabilities could serve Chinese military operations in three key areas. First and foremost, they allow data collection for intelligence and computer network attack purposes. Second, they can be employed to constrain an adversary’s actions or slow response time by targeting network-based logistics, communications, and commercial activities. Third, they can serve as a force multiplier when coupled with kinetic attacks during times of crisis or conflict.

The report again emphasises:

China is using its computer network exploitation (CNE) capability to support intelligence collection against the U.S. diplomatic, economic, and defence industrial base sectors that support U.S. national defence programs. The information targeted could potentially be used to benefit China’s defence industry, high technology industries, policymaker interest in US leadership thinking on key China issues, and military planners building a picture of U.S.

network defence networks, logistics, and related military capabilities that could be exploited during a crisis.”

Scholars and government reports differ in their views on ‘what are the real intentions’ of Chinese government behind conducting cyberwarfare. They suggest various types of intentions and objectives, but are the real intentions of Chinese government known? Let us examine them one by one.

1.1. For Technology Leapfrogging and Economic Espionage

Cyberspace is an ideal option through which technology acquisition can be achieved without being detected. In words of M K Sharma (2011), “Espionage and technology transfer prosper in cyber warfare where being physically present is not required, and attribution becomes increasingly difficult. It also falls in line with China’s strategy of leapfrogging. By acquiring foreign military knowledge, China can quickly catch up and begin working at a comparable level, rather than investing the large amount of time and effort it would take to acquire this knowledge independently.” According to ‘The US Department of Defense Annual Report to the US Congress (2013),’ China utilizes a large, well-organized network of enterprises, defence factories, affiliated research institutes, and computer network operations to facilitate the collection of sensitive information and export-controlled technology, as well as basic research and science that supports U.S. defence system modernization. These, as per the report, include economic espionage, theft of trade secrets, export control violations, and technology transfer. This capability of the cyberspace, that Chinese are utilising extensively, bothers American government the most as the US cannot do the same with China. Since, the US is already a developed nation having advance technology and trade secrets, even if it steals China’s technology and trade secret (which is relatively low-tech) that won’t be useful for the US. On the other hand China is a developing nation that needs advance cutting edge technology and trade secret which could be stolen/ collected through cyberspace, without the fear of being detected. Sometimes, when these technologies or trade secrets are not available on computer system connected to internet or when it is classified information human intelligence personnel are also used to access those information or to implant backdoors/ malicious codes (as was done in the case of Stuxnet). The ‘The US Department of Defense Annual Report to the US Congress (2013)’ also cites some of the incidents in support of this argument:

- ❖ In August 2010, Noshir Gowadia was convicted of providing China with classified U.S. defense technology. This reportedly assisted China in developing a low-signature cruise missile exhaust system capable of rendering a cruise missile resistant to detection by infrared missiles.
- ❖ In September 2010, Chi Tong Kuok was convicted for conspiracy to illegally export U.S. military encryption technology and smuggle it to Macau and Hong Kong. The relevant technology included encryption, communications equipment, and Global Positioning System (GPS) equipment used by U.S. and NATO forces.
- ❖ In September 2010, Xian Hongwei and Li Li were arrested in Hungary and later extradited to the United States for conspiring to procure thousands of radiation-hardened Programmable Read-Only Microchips, classified as defence items and used in satellite systems, for the China Aerospace and Technology Corporation. Both defendants pleaded guilty and were sentenced in September 2011 to two years in prison.
- ❖ In January 2012, Yang Bin was arrested in Bulgaria and later extradited to the United States based on a December 2011 criminal indictment related to the attempted export of military-grade accelerometers used in “smart” munitions, aircraft, and missiles.
- ❖ In March 2012, Hui Sheng Shen and Huan Ling Chang, both from Taiwan, were charged with conspiracy to violate the U.S. Arms Export Control Act after allegedly intending to acquire and pass sensitive U.S. defense technology to China. The pair planned to photograph the technology, delete the images, bring the memory cards back to China, and have a Chinese contact recover the images.
- ❖ In June 2012, Pratt & Whitney Canada (PWC), a subsidiary of U.S. aerospace firm and defence contractor United Technologies Corporation (UTC), pleaded guilty to illegally providing military software used in the development of China’s Z-10 military attack helicopter. PWC “knowingly and wilfully” caused six versions of military electronic engine control software to be “illegally exported” from Hamilton Sundstrand in the United States to PWC in Canada and then to China for the Z-10.
- ❖ In July 2012, Zhang Zhaowei, a naturalized Canadian citizen, was arrested while entering the United States, based on a sealed January 2011 indictment alleging Zhang attempted to illegally acquire and export military gyroscopes used in unmanned aerial systems and for tactical missile guidance.

- ❖ In September 2012, Zhang Mingsuan was arrested in the United States and indicted after attempting to acquire up to two tons of aerospace-grade carbon fiber. In a recorded conversation, Zhang claimed he urgently needed the fiber in connection with a scheduled Chinese fighter plane test flight.
- ❖ In September 2012, Sixing Liu, aka “Steve Liu,” was convicted of violating the U.S. Arms Export Control Act and the International Traffic in Arms Regulations (ITAR) and possessing stolen trade secrets. Liu, a Chinese citizen, returned to China with electronic files containing details on the performance and design of guidance systems for missiles, rockets, target locators, and unmanned aerial vehicles. Liu developed critical military technology for a U.S. defense contractor.

Not all these incidents are related to cyberspace but all are classified information, which probably could not be accessed through cyberspace. This is where human intelligence is put into use. Thus cyberspace serves as a medium which provide access to high-technology (including cyber technology) and trade secret related information.

1.2. Anti Access/ Area Denial (A2/ AD) (Counter- intervention Operation)

The US Department of Defense Annual Report to the US Congress 2013 says, “As part of its planning for military contingencies, China continues to develop measures to deter or counter third-party intervention, particularly by the United States. China’s approach to dealing with this challenge is manifested in a sustained effort to develop the capability to attack, at long ranges, military forces that might deploy or operate within the western Pacific, which the Department of Defense (DoD) characterizes as ‘anti-access’ and ‘area denial’ (A2/AD) capabilities.” The report further explains that China’s A2/AD focus appears oriented toward restricting or controlling access to China’s periphery, including the western Pacific (which should be eastern Pacific when looked from China). It is mainly applicable in case of Taiwan (or may be in case of South China Sea region). If the US intervenes in these areas China might use its cyberwarfare capabilities to counter the US intervention by attacking American military network, logistics networks (NIPRNET- Non-classified Internet Protocol Router Network) etc. thereby delaying in deployment of troops. The case of Taiwan is discussed in detail by Libicki in his article “Chinese Use of Cyberwar as an Anti-Access Strategy- Two Scenarios,” written in January 2011.

1.3. For Buying Time

Buying time during the period of conflict is somewhat similar to above mentioned AA/AD strategy. In initial period of the conflict, Chinese military might use cyber attacks against an adversary's computer networks and electronic equipments etc. This would cut off the soldiers, who would be waiting for orders (either in battlefield or in their camp), from the central commanding authority or from other fellow soldiers of other areas. By the time the adversary looks for other ad-hoc means to communicate, this would certainly buy some time for China to choose best option in the last moment or may be for some other purposes. This would also provide China with the best opportunity to attack the adversary and finish the war as the enemy remain isolated and uninformed. China can also use the same method to cause delay in the deployment of adversary's troops or the troops of any third party as discussed above.

During the period of peace, M K Sharma (2011: 178) asserts, "While China tries to match its military power with the US, it is buying time by keeping a low profile and depending on cyber reconnaissance. Cataloguing adversary weaknesses not only provide asymmetric advantage in the event of a conflict, it also acts as a deterrent while China catches up in traditional military might. By utilising cyber reconnaissance, China can also accelerate its advancement in hi-tech weaponry."

1.4. Supplement to Conventional Forces

During a wartime scenario, 'The US Department of Defense Annual Report to the US Congress (2013)' writes, "The PLA GSD Fourth Department (Electronic Countermeasures and Radar) would likely use information operations (IO) tools, to include jamming/EW, CNO, and deception to augment counter-space and other kinetic operations." On 6 September 2007, Israel hacked (*NYT* Oct 14, 2007) Syria's air defence system (bought from Russia) through cyber or electronic means, which facilitated Israeli Air Force (IAF) fighter aircrafts (F-15Is, F-16Is and an ELINT aircraft, according to Wikipedia- altogether 8 aircrafts participated but at least 4 of them entered Syrian airspace) in entering inside Syrian airspace undetected and in bombing Syrian nuclear site located at Dayr as-Zawr. This whole operation known as "Operation Orchard," is still a mystery in term of how did it successfully hacked in the air defence system created by Russians? Speculations (*The Register* Nov 22, 2007) of 'sky-hacking' and 'air-to-ground network penetration' were being made. Another report (Weinberger Oct 04, 2007) wrote, "The U.S. developed 'Suter' airborne network attack system developed by BAE Systems and integrated into U.S. unmanned aircraft by L-3 Communications was used by the Israelis. The technology allows users to invade

communications networks, see what enemy sensors see and even take over as systems administrator so sensors can be manipulated into positions so that approaching aircraft can't be seen." This could be a possible explanation but the truth remains that these technologies can act as huge supplement for conventional forces.

While talking about use of new technologies by Chinese military, the 'The US Department of Defense Annual Report to the US Congress (2013)' asserts, "New technologies allow the PLA to share intelligence, battlefield information, logistics information, weather reports, etc., instantaneously (over robust and redundant communications networks), resulting in improved situational awareness for commanders. In particular, by enabling the sharing of near-real-time ISR data with commanders in the field, decision-making processes are facilitated, shortening command timelines and making operations more efficient." Information operation and cyberwarfare are products of 'Information and Communication Technology,' which is increasingly becoming an integral part of modern militaries of most of the countries including PLA. Regarding PLA's emphasis on use of these technologies against adversaries, 'The US Department of Defense Annual Report to the US Congress (2013)' asserts:

PLA authors often cite the need in modern warfare to control information, sometimes termed "information blockade" or "information dominance," and to seize the initiative and gain an information advantage in the early phases of a campaign to achieve air and sea superiority. China's "information blockade" likely envisions employment of military and non-military instruments of state power across the battlespace, including in cyberspace and outer space. The PLA would likely rely on IO to disrupt the U.S. capability to use navigational and targeting radar. The *Science of Strategy* and *Science of Campaigns* detail the effectiveness of IW and CNO in conflicts and advocate targeting adversary C2 and logistics networks to affect their ability to operate during the early stages of conflict. They also identify information warfare (IW) as integral to achieving information superiority and an effective means for countering a stronger foe.

2. Capabilities

The former vice-chairman of the U.S. Joints Chiefs of Staff and a notable cyber expert, General James Cartwright, has said that a full-scale Chinese cyber attack potentially has the same effect as weapons of mass destruction (Magnus Hjortdal 2011). Another scholar, Hagestad (2012 118) claims that the PLA offensive cyberwarfare capabilities appear to be fairly elementary. Desmond Ball (2011) asserts that China has the most extensive and most practiced cyber-warfare capabilities in Asia, however he also claims that China's demonstrated offensive cyber-warfare capabilities are fairly rudimentary. He again says, "China's cyber-warfare capabilities are very destructive, but could not compete in extended

scenarios of sophisticated IW operations.” His own argument seems to be contradictory, not to speak of other authors. He again argues that there is no evidence that China’s cyber-warriors can penetrate highly secure networks or covertly steal or falsify critical data. But, when sensitive information regarding F-35 fighter was stolen, a news report (*WSJ* April 21, 2009) claimed, “The spies inserted technology that encrypts the data (several terabyte of data) as its being stolen; as a result, investigators can’t tell exactly what data has been taken.” This report serves as one of the evidences that Ball was searching for. And the report also confirmed China’s involvement in this incident as it reported, “Investigators traced the penetrations back with a ‘high level of certainty’ to known Chinese Internet protocol, or IP addresses and digital fingerprints that had been used for attacks in the past.” One more incident that could serve as an evidence is the recent incident (May 2013 - mentioned above) in which news reports claimed that China ‘stole’ the US missile system designs and details of fighter jets, navy ships, helicopters etc. These types of information are highly sensitive and classified information and only those, who are confident enough of their sophisticated capabilities, go after such information. Hence, if attribution of these incidents to China is true, Chinese capabilities must be highly sophisticated. One more probability could be involvement of third party (country or organisation) which might be exploiting and stealing details of the US government re-routing through Chinese IP addresses because Chinese computer networks are also as vulnerable as that of the US. And this can serve as a pretext which Chinese government can always use, if blamed by any other nation for hacking and cyber intrusions.

In this way, different views of various authors can be either supported or negated and thereby capability can be predicted based on various factors like analysis of incidents; analysis of various components of cyber domain; analysis of government’s efforts and investment; number of cyber military drills; R&D in cyber domain etc. Hence, in order to predict and evaluate the capabilities that China possesses many elements have to be studied and factored in.

2.1. Cyber Power – The New Component of CNP

In the process of prediction and evaluation of cyberwarfare capabilities, the term ‘Cyber Power’ can be pretty helpful. According to M K Sharma (2011: 18), “It’s the belief of many that in the ‘information age’, information is becoming major resource of power. The power is passing from the capital-rich to information-rich. This reasoning implies that one country that can best lead the information revolution will be more powerful than any other.” He (2011: 15)

again argues that as a consequence of the development of ICT, a new source of power is gaining momentum and Henry Kissinger's notion that 'relations among state are determined by raw power and the mighty will prevail. He (2011: 167), while discussing the components of Comprehensive National Power (CNP), also emphasises, "In the dynamics of CNP, the cyber power component is becoming increasingly dominant as it would not only enhance military power but is a prerequisite for economic development. Also, through cyber power, states' soft power can have deeper reach. China's 'informatisation' process can be seen as realisation of this new component of CNP." Thus, it can be observed that cyber capabilities are also linked with CNP.

Spade (2012) defines 'cyber power' as – "Cyber power is the ability of a nation-state to establish control and exert influence within and through cyberspace, in support of and in conjunction with the other domain-elements of national power. Attaining cyber power rests on the state's ability to develop the resources to operate in cyberspace." Another definition by M K Sharma (2011: 08) says, "Cyber power is that intangible virtual asset which exists in cyber space and is directly proportional to the degree of control an individual or a group or a non-state actor or a state could exercise over cyber space in its favour." While evaluating the cyber power of China, Spade (2012: 10) asserts:

If cyber power is the ability of a nation-state to establish control and exert influence within and through cyberspace, then China has demonstrated that it is a strong cyber power. Most recently, in April 2010, China Telecom – a PRC-owned Internet service provider – introduced erroneous network traffic routes into the Internet. In an event lasting only 18 minutes, these instructions propagated across the World Wide Web causing foreign Internet service providers to route 15 percent of the world's Internet traffic through Chinese servers. Affecting 37,000 networks, this re-routing included traffic to and from U.S. government and military sites, including the U.S. Senate, Departments of Defense and Commerce, and others, as well as commercial websites, including Dell, Yahoo, Microsoft, and IBM.

Spade also puts forward, "The U.S. military refers to applications of cyber power as Computer Network Operations (CNO) and subdivides them into three categories: Computer Network Defence (CND), Computer Network Attack (CNA), and Computer Network Exploitation (CNE). These categories are analogous to thinking within China's PLA. The offensive capabilities of cyber power are CNA and CNE." Hence cyber power can also be understood as power of a nation state to conduct CNO (including CNA, CND and CNE).

2.2. Intelligence (SIGINT/ ELINT/HUMINT)

Regarding the role of intelligence in modern warfare, some Chinese observers assert, “Warfare in the information era is a test of strength between intelligence capabilities of combat forces (Stokes 1999).” Thus, intelligence has a crucial role to play in China’s cyberwarfare and hence before predicting China’s cyberwarfare capabilities, Chinese intelligence capabilities have to be understood as well.

Ever since Gulf War (i.e. from 1990) and later on during Iraq War, Chinese intelligence had been keeping an eye on the US actions. One of the reasons was that China has no recent experience of war. And secondly Iraq was fighting with China’s weapons and equipments, so it was a period of quality testing of their weapons. That’s why the US and allied military troops’ activities were examined so closely that Chinese intelligence predicted the beginning of ground phase of war few days beforehand. Manuel, in his online article, writes, “The intelligence and EW aspects of the Gulf War were closely monitored by a special SIGINT unit located in Kashi, 1,700 miles from Baghdad that intercepted large amounts of US and Allied military communications. Special SIGINT units in the Chinese Embassies in Turkey and Iraq also intercepted communications and collected electronic intelligence on US and Allied military activities. For example, these units reportedly intercepted intelligence that the ground phase of the war was about to start five days beforehand.” Chinese intelligence and espionage units, established in Chinese embassies in various countries served as an excellent source of identifying the capabilities and weaknesses of the US and allied forces. It was discovered by the US later on and according to Manuel that was the reason why Chinese embassy in Belgrade was bombed by the US in May 1999. He argues:

Chinese strategists and military planners thoroughly analysed the NATO air war against Yugoslavia in March-June 1999 (Operation Allied Force), which forced the Serbian forces from Kosovo, and were again impressed by the efficacy of precision air strikes, often targeted with real-time intelligence (including imagery and SIGINT provided by UAVs), against the Yugoslav C3ISR (command, control, communications, intelligence, surveillance and reconnaissance) systems, and by the uselessness of the Soviet-made air defence systems against NATO’s EW capabilities. A special ‘high-tech electronic espionage unit’ was reportedly established in the military attaché’s office in the Chinese Embassy in Belgrade to collect electronic intelligence on US and Allied military activities (until it was bombed by the US on 7 May).

Regarding the SIGINT capabilities of China, Stokes (1999) emphasises, “China maintains the most extensive SIGINT network of all the countries in the Asia-Pacific region. SIGINT

systems include several dozen ground stations, half a dozen ships, truck-mounted systems, and airborne systems.” Manuel adds on, “China is actively and extensively engaged in the whole realm of signals Intelligence (SIGINT), electronic warfare (EW) and cyber-warfare activities. It ranks as the leader in Asia, at least according to some more quantitative measurements, in some important information warfare (IW) areas. China maintains by far the most extensive SIGINT capabilities of all the countries in Asia.” As far as human intelligence is concerned, it helps the Chinese government in accessing what is not accessible through cyberspace for example the information stored in air gapped computer system and network which is not connected to internet. All the incidents mentioned above in the section of ‘For Technology Leapfrogging and Economic Espionage’ are ample example to show how HUMINT help in illegal technology acquisition.

2.3. Supercomputers

Tianhe-2, the latest supercomputer of China, ranked fastest (*BBC* June 17, 2013) in the world on 16 June 2013 leaving behind the US’ supercomputer ‘Titan’. It was not the first time when a Chinese supercomputer got the top slot. Tianhe-1A, earlier version of Tianhe-2, ranked world’s fastest (*China Daily* June 18, 2013) in 2010 and second fastest in 2011. Another earlier version Tianhe-1, the predecessor of Tianhe-1A revealed in October 2009, ranked the fifth fastest supercomputer in TOP500 list. China’s early supercomputers include: Yinhe-1 (YH-1) built in 1983; Yinhe-II built in 1992; Yinhe-III built in 1996.

Though the US still dominated with more number of supercomputers in the TOP500⁵ list of the fastest supercomputer in the world, but the top slot went to China. Out of these 500 supercomputers, the US has 252 and China has only 66. Here gap in terms of numbers is huge but China has second largest number of supercomputers in the world after the US. The project Tianhe-2 was originally scheduled for completion in 2015, but was instead declared operational in June 2013. As of June 2013, The Supercomputer has yet to become fully operational. It is expected to reach its full computing capabilities by the end of 2013. With completion of this project before the scheduled time, Chinese (as usual) have once again proved their high level of commitment towards their work. And if the supercomputer is not yet fully functional, still became the fastest in the world, what would happen if it becomes fully functional? There is a probability that it might become consecutive winner for 2-3 years in one go. Chinese experts believe that the supercomputer would lose the edge by 2015.

⁵ TOP500 project, initiated in 1993, publishes an updated list of names of 500 fastest supercomputer twice a year (Once in June and in November)

2.4. Cyber Security Experts

In a recent report in *The Hindu* dated 19 June 2013 claims that China has the maximum number of cyber security experts in the whole world. According to the report China has 125,000 cyber security experts, which is much more than what the US has (91,080). The report further elaborates, “China’s cyber workforce is composed of various components of military, national security, public security, propaganda militia and academia. It now has an estimated strength of 125,000 personnel which includes regular troops (30,000), specialists from various universities, research institutes and states enterprises (60,000), and militia (35,000).”

2.5. Military Digital (Cyber) Drills

Tracking the past records of China’s digital drills, Ball (2011) writes, “From the late 1990s until 2005, the PLA conducted more than 100 military exercises involving some aspect of IW, although the practice generally exposed substantial short-falls. A similar number was probably conducted in the period from 2005 to 2010.”

‘The US Department of Defense Annual Report to the US Congress (2013)’ also asserts:

PLA EW units have conducted jamming and anti-jamming operations testing the military’s understanding of EW weapons, equipment, and performance, which helped improve their confidence in conducting force-on-force, real-equipment confrontation operations in simulated electronic warfare environments. The advances in research and deployment of electronic warfare weapons are being tested in these exercises and have proven effective. These EW weapons include jamming equipment against multiple communication and radar systems and GPS satellite systems. EW systems are also being deployed with other sea and air-based platforms intended for both offensive and defensive operations.

Ball (2011) also provides some examples of China’s cyber drills:

- 500 soldiers took part in a network-warfare exercise in Hubei province in 2000 in which simulated cyber-attacks were conducted against Taiwan, India, Japan and South Korea.
- Another incident of June 2000, “a series of high-technology combat exercises” was to be conducted by the PLA, which according to Ball, “had to be suspended” when they were attacked by “a computer hacker.”
- In an exercise in Xian, ten cyber-warfare missions were rehearsed, including planting (dis)information mines; conducting information reconnaissance; changing network

data; releasing information bombs; dumping information garbage; releasing clone information; organising information defence; and establishing „network spy stations.

- In Datong, forty PLA specialists were reported in 2001 to be “preparing methods of seizing control of communications networks of Taiwan, India, Japan and South Korea”.
- In October 2000, an exercise presided over by the PLA Chief of Staff simulated cyber-warfare and EW “with countries south and west of the Gobi desert”.

Spade (2012) also claimed:

Between October 1997 and July 2000, the PLA conducted multiple army and military region cyber warfare training exercises, with cyber detachments conducting CND and CNA against one another. Their tactics and techniques included “conducting information reconnaissance, planting information mines, changing network data, releasing information bombs, dumping information garbage, disseminating propaganda, applying information deception, releasing clone information, organizing information defence, and establishing network spy stations.”

In a recent event, an *Economic Times* article of 29 May 2013 claims, “Ahead of President Xi Jinping’s maiden meeting with his US counterpart Barak Obama, China said it will conduct the first ever exercise to test new types of combat forces, including units using digital technology to practice cyber war.” The report further clarifies that the drill will be carried out in late June at the Zhurihe training base in north China’s Inner Mongolia Autonomous Region, the country’s largest military training field. This incident was reported by Chinese media themselves which was not a common practice earlier. Previously drills were conducted but not necessarily reported (which meant China followed Deng’s policy of ‘Bide for your time’), but the recent reporting by Chinese media (and that also before Obama-Xi meet when China was being blamed for most of the hacking incidents across the globe and Obama was supposed to deal the cyber issue with China very strictly) proves that China has gained enough confidence and is not afraid of US. It seems China’s time has come that Deng asked China to wait for.

2.6. Chinese President Xi Jinping’s US visit and Snowden’s Disclosure

The Chinese president Xi Jinping visited the US president Barack Obama for the first time ever since he became president. Before this visit the US strongly criticised China for its alleged involvement in cyber-theft of intellectual property rights, trade secrets and other

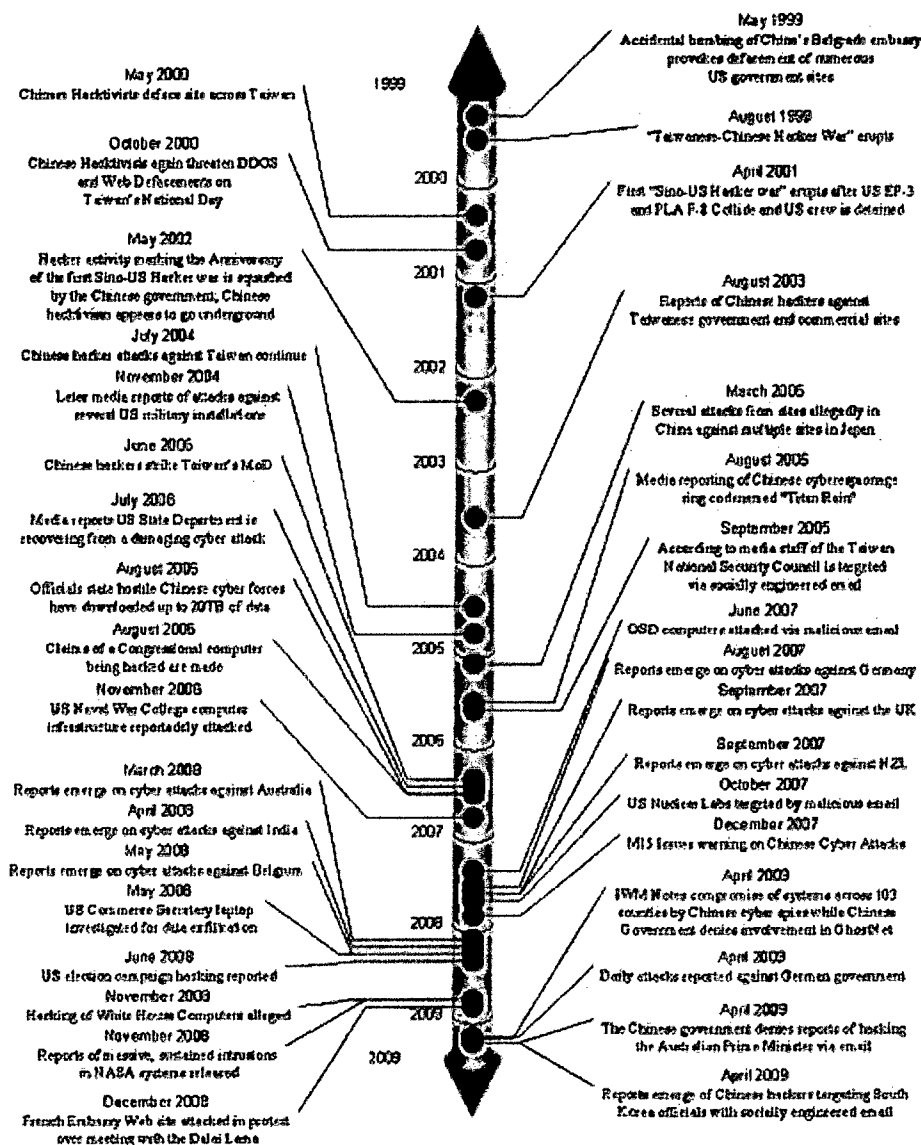
cyber attacks. A report published by Mandiant, a private cyber security firm based in Virginia (US), also claimed to expose Chinese military unit 61398, which according to Mandiant has stolen hundreds of terabytes of data from at least 141 companies spanning 20 major crucial industries. Even the US government claimed it had plenty of evidence against China. During this visit cyber issue was supposed to be discussed in details. But the day (6 June 2013) on which Xi Jinping arrived in the US, a classified electronic surveillance program named “PRISM,” operated by American National Security Agency (NSA), was disclosed by NSA contractor Edward Snowden. The classified program was used by the American government to spy on people all over the world. The US government initially claimed that it was meant for foreign national (meaning non-Americans), but later on news report claimed that even Americans were not forbidden. According to Snowden (*IB Times* June 17, 2013) NSA had been hacking Hong Kong and China since 2009 and NSA has also hacked civilian infrastructure networks in other countries such as “universities, hospitals, and private businesses” And the time when this news came into light Snowden was already in Hong Kong. One might speculate ‘Chinese hands’ behind the disclosure of US classified programme not just because the timings of Xi’s visit and the disclosure coincided but also because of the fact that the US president Obama, who was supposed to take strong measures against China for its conduct in cyberspace, lost his upper hand. How can Obama government, who is itself indulge in electronic surveillance and hacking incidents against its own people and the government of other nations, can criticise other nation state or take strong measures against them. Nobody knows this speculation of ‘Chinese hands’ has some ground or not but grant of political asylum to Snowden by Chinese government could have provided speculators with some more reasons. Reasons could also be seen in the fact that China allowed Snowden to board flight from Hong Kong airport to Moscow. However, Chinese government is playing safe and does not want to confront the US.

3. Incidents attributed to China

China has been blamed for most of the cyber intrusions and hacking activities going on around the globe. Most of these allegations are being made by Western countries especially the US. The US government show their serious concern about these cyber issues and have also worked extensively on cyber issues. They have published plenty of works especially on China’s cyber skills and capabilities. One of such work is “Capability of People’s Republic of China to Conduct Cyber Warfare and Computer Network Exploitation,” prepared for. “The

US-China Economic and Security Review Commission,” authored by Bryan Krekel. This report was prepared by Northrop Grumman Corporation, one of the main defence contractors of the US. Since the report was published in 2009, it enlists all major cyber and hacking incidents attributed to China from 1999 to 2009. The figure below is the timeline that contains all major cyber and hacking incidents attributed to China from 1999 to 2009 and it is followed by the explanation of the incidents mentioned in the timeline (as explained in the original report). Post 2009 incidents are mainly based on news reports; article by James A Lewis and Laura Saporito; book by Hagestad (2012). List of these incidents has been attached in ‘Appendices A’.

Figure 18: Cyber Incidents Allegedly Attributed to China from 1999 to 2009



Source: Bryan Krekel, "Capability of PRC to Conduct Cyber Warfare and CNE," (2009), p -

3.1. Trend Analysis

If these cyber attacks attributed to China are true, it can be observed that most of the initial incidents (starting from 1999) were patriotic hacking incidents driven by the feeling of nationalism. The biggest target of these patriotic hacking was Taiwan; the US was the next. In 2002, after the Communist Party of China (CPC) issues a strongly worded condemnation of patriotic hacking against foreign networks most of the patriotic hacking incidents stopped, but attack against Taiwan continues, which cannot be carried on against the will of CPC. CPC must have shown tolerance or might have allowed hacker groups deliberately to target Taiwan. One more possibility is that CPC might have ordered hacker groups to do so or hacker groups might have been functioning under Chinese government. One argument in support of this can be observed in the fact that the Chinese computer network exploitation operation codenamed "Titan Rain" dates back to 2003. It is just one year after CPC strongly condemned patriotic hacking. Chinese government might have provided state sponsorship to these patriotic hacker groups or individual hackers for developing the operation "Titan Rain." Since then PLA and hacker groups might have been working together or PLA might have recruited some talented hackers. Otherwise, it would not have been possible for hackers and hacker groups to operate after CPC's strong condemnation of patriotic hacking activities, especially the hacking of government networks and websites of Taiwan. Even after 2002 the patriotic hacking activities persist though only against Taiwan but majority of the cyber activities attributed to China constitute cyber espionage activities against countries like the US, UK, Germany, New Zealand, Australia etc. The targets were non-classified but sensitive information like operational details of the space shuttle including performance and engine data, war game information on the networks, database at the nuclear weapons laboratory etc. The patriotic hacking incidents again took place against Japan in 2005 (due to omission of key historical facts pertaining to Japan's actions in World War II) and against France in 2008 (due to French President Sarkozy's meeting with the Dalai Lama). Chinese hackers also installed backdoor applications on government computers and computer networks of the US, Germany and Taiwan, so as to ensure stealth future entry. Why this future entry is ensured? The computers and computer networks, where backdoor applications had been installed by Chinese hackers, must be of their use in future. Probably that's why major powers like the US and Germany were chosen (may be because of their advanced technologies). And since Taiwan is permanently under attack of PRC future entry had to be ensured. After 2006, the number of target countries has been increasing (initially from the US and Taiwan to UK,

Germany, Belgium, S. Korea, New Zealand, India, Australia etc), which reached to 103 countries in March 2009 (though not known it was intentional or unintentional to reach 103 countries). With the increase in the number of target the level of sophistication of attacks has also increased – from initial patriotic hacking, website defacement, denial of service attacks to the use of sophisticated malwares and softwares like ‘Titan Rain,’ ‘Ghost-net’ etc. Most of the cyber incidents listed above seem to be acts of cyber espionage. The targets of espionage activities included both government and private networks. Most of the government targets were ministry of defence and foreign ministry of various nations. The targeted private firms belong to the category of energy sector (oil and gas companies), defence sector (the US defence contractors like Lockheed Martin, Northrop Grumman etc.), chemical industries (like Dow Chemical etc.) and other sectors like aerospace, engineering and military research etc. This list is quite similar to the target list prepared by Mandiant (mentioned above) and coincidentally it is similar to the priority list of “The National Medium- and Long-Term Program for Science and Technology Development (2006-2020),” published by the State Council of China, categorised under the sub-heading of ‘Main Areas and Priority Topics’ and ‘Frontier Technology.’ It includes energy, water and mineral resources, environment, agriculture, manufacturing industries, transportation sector, information industry and modern service industry, population and health, urbanization and city development, public security, national defence, biotechnology, information technology, advanced materials technology, advanced manufacturing technology, advanced energy technology, marine technology, laser technology and aerospace technology. So, either it is a co-incidence or a deliberate effort by Chinese government to use cyberspace to leapfrog in certain key technologies. Another motive of the Chinese government could be collection of intelligence information by scanning military and government networks, understanding the vulnerabilities, exploiting those vulnerabilities, implanting backdoor applications etc. This could also be considered as preparation of future cyberwar. In case of conflict or war already known vulnerabilities can be exploited (to implant viruses like Stuxnet capable of carrying out kinetic effects) or already implanted deadly backdoor applications/viruses/malware can be activated, which can result in either communication interference or in physical damage of computer system, shutting down the entire network. These cyber capabilities can also be used by Chinese government to supplement its conventional warfare capabilities. However, recent trend of Chinese cyber intrusions seem to have shifted from non-classified information to classified information, which can be easily observed in recent incident in which China allegedly stole the US weapon system and aircraft related information (which won’t be available in non-

classified category). One more incident in support of this argument could be hacking of fighter jet F-35 related information earlier in 2007 or 2009. With increase in the sophistication level of cyber skills, Chinese have gained confidence and have even gone for classified information. It suggests that China is enhancing its capabilities in all domains – cyber domain and all other conventional domains. Chinese government is using cyber domain to enhance its conventional capabilities as well as cyberwarfare capabilities.

4. China's Response

Chinese government have always denied all the allegations of hacking and cyber intrusions against them. Geng Yansheng, a spokesman for the Ministry of National Defence, said (NYT Feb 20, 2013) that China had been the victim of cyber attacks. China had replied (NYT Feb 20, 2013) several times that Chinese government does not support any form of hacking, rather China is itself a victim of hacking and cyber intrusions. In this context, Ventre (2009: 210) argues:

The victimised nations have all denounced their guilty party: Estonia denounced Russia as did Georgia. The US and European countries (France, Germany, UK and Belgium) have all accused China, without really checking first before acting. Do we really have victims on one side, a group made up of Western and European nations or their allies, and on the other side the culprits, a group of China and Russia?

He (2009: 211) quotes a report by Ripstech, published in 2002, which concluded that in 2002 most of the cyber attacks came from the US and Israel, not China or Russia. Dong Niao (东鸟, 2010), a Chinese scholar who has written extensively on 'cyberwar', argue that ever since the evolution of internet, the US has always controlled it (both technologically and politically). He cites following examples:

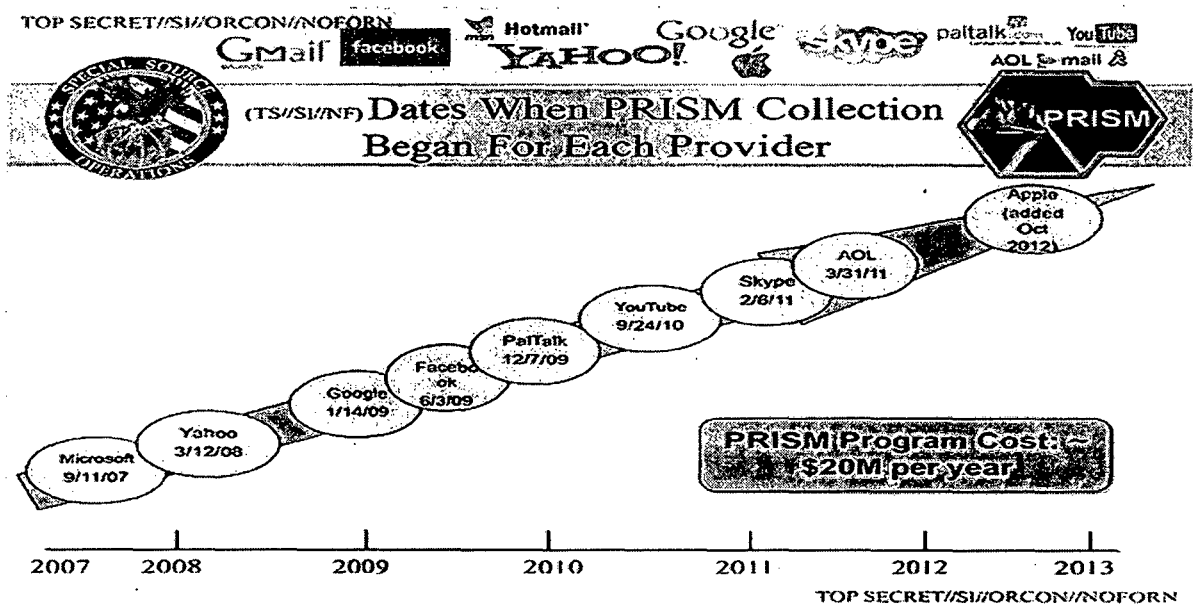
- On 30 May 2009, when people from countries like Cuba, Iran, Syria, Sudan and North Korea tried logging in MSN Messenger a message was displayed: "810003c1: We are unable to provide you the services of .NET Messenger". Other service providers like Google, Yahoo etc. also adopted similar policy. Microsoft declared that it was in accordance with the American government guidelines for software export and services to countries on which sanctions have been imposed by the US.
- The US has controlled the aorta of internet and crucial internet technologies for more than 40 years. The US has been controlling developing countries and their politics,

economy, military etc. through monopolizing the crucial internet technologies like microchips, micro processors etc. (that developing countries are bound to use, as no other option is available). The special advantageous position that the US has gained through technological advancements, serves as a 'thorn in the neck' for other countries.

- On 01 April 2009, in order to protect the internet from assault of hackers or terrorists, the US senate proposed 55 paged bill called 'Internet Kill Switch'. According to the bill, in case of network or cyber security emergency the President of America reserves the right to cut off any federal government network or American critical information system or any network.

These examples elaborate that the US is much more dominant player in the field of cyberspace and internet than that of China. One more incident that proves the US dominant player is the recent surveillance program 'Prism' exposed by Snowden, in which all major private companies like Google, Yahoo, Microsoft, Skype, Facebook, Youtube, Apple etc were involved.

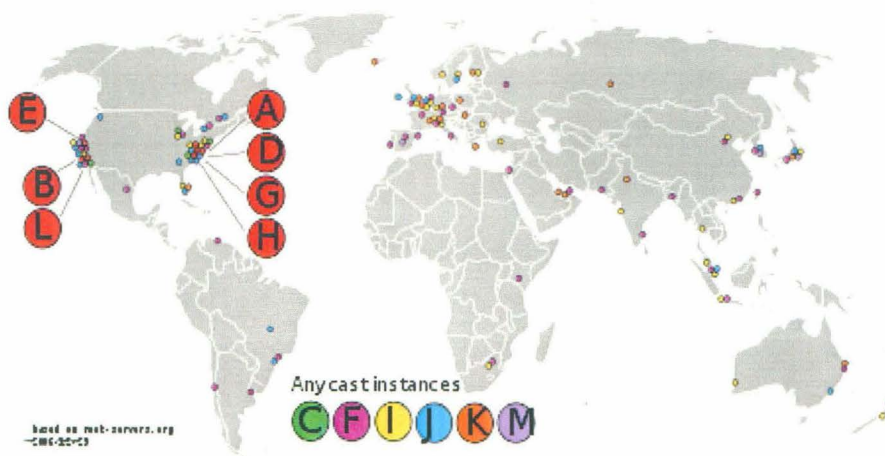
Figure 19: Companies Involved in Classified Surveillance Programme 'PRISM'



Source: "NSA Slides Explain the PRISM Data-collection Program," The Washington Post, 10 July 2013

One more point, raised by most of the Chinese scholars including Dong Niao, is that who owns and control the internet? In order to answer this question they look at the location of the root servers. From the following figure can be observed that most of the root servers are clustered together in the US or Europe. Thus according to Chinese scholars control and ownership and even the switch to operate internet (the kill switch) is there in the hands of the US government, how can China compete with the US in cyberspace?

Figure 20: Locations of Root Servers



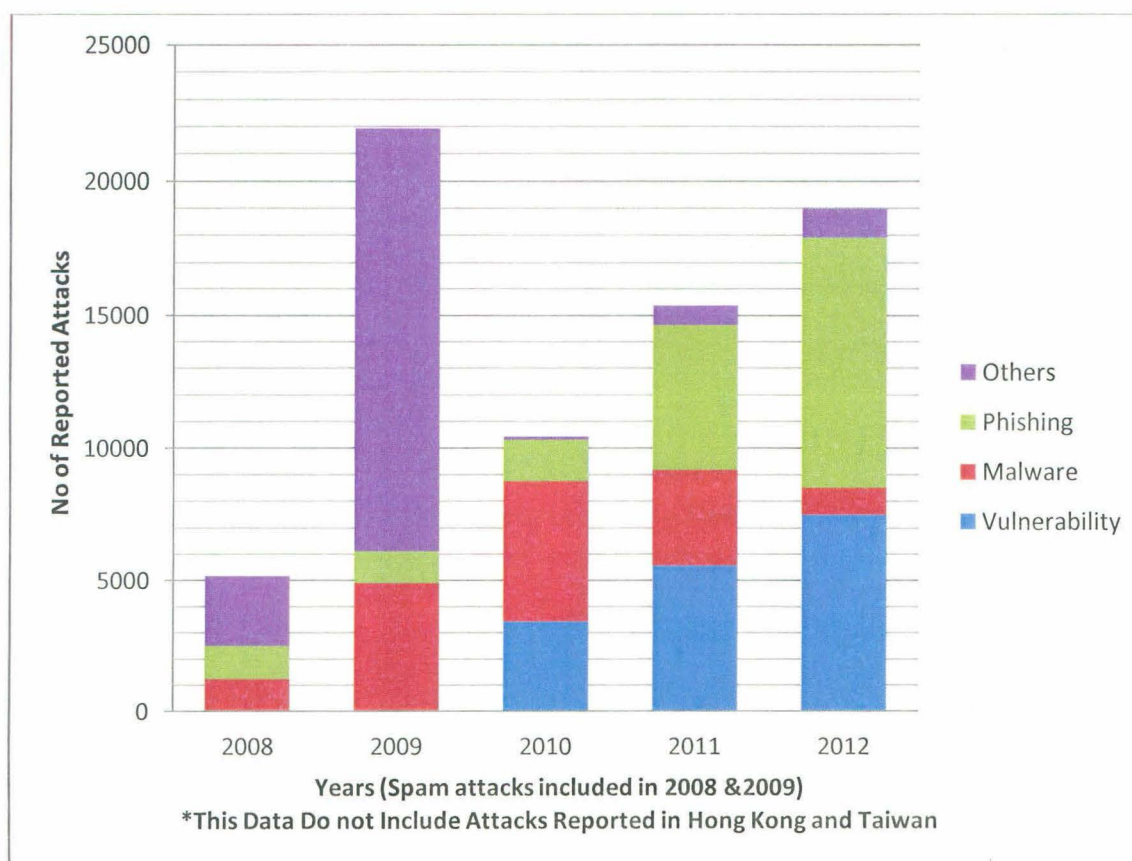
Source: Wikipedia (http://en.wikipedia.org/wiki/Root_nameserver)

Thus it can be observed that the US is a more dominant player than China and internet is mostly controlled by the US, but still allegations are made against China. As far as China's claim of being a victim is concerned data provided by the 'National Computer Network Emergency Response Technical Team/Coordination Centre of China' (CNCERT/CC)⁶ can be helpful. The following graph presents the number of reported cyber attacks on China (excluding Hong Kong and Taiwan). It can be observed from the graph that number of attacks against China has been increasing from 5167 attacks (excluding scanning attacks) in 2008 to 19,000 in 2012. The only exception is the year 2009, where number of attacks seems

⁶ CNCERT/CC was created in October 2000 and has been a member of Forum of Incident Response and Security Teams (FIRST) since August 2002, as well as being on the Steering Committee of the Asia Pacific Computer Emergency Response Team (APCERT). It is under the responsibility of the Chinese Domestic Ministry. Some 31 branches of CNCERT/CC cover 31 provinces of continental China.

to be maximum till date. It is because spam attacks, which were largest in number that year (67.38 percent), were also included in 2009 (also in 2008), but were not included in subsequent years. Ventre (2009) also studied the data provided by CNCERT/CC from 2003 to 2006 and claimed (Ventre 2009: 217), “A study if the most frequent attacks recorded 220,000 foreign computers launching regular attacks against Chinese websites. Attacks came from the United States (40 percent), Japan (11 percent), Taiwan (10 percent) and Korea (8 percent).” However, Ventre (2009: 214) also emphasizes, “These statistics do not pretend to display, by themselves, a faithful picture of the situation in terms of insecurity/security of the networks of a given country. They cannot be because the data is only based on the incident that were known and reported to CERTs. These statistics may only be the tip of the iceberg, showing only a small part of the danger to the ship’s captain; the worst might be hidden under the water.” It means number of cyber attacks on China is much more than what is presented here, if not all incidents of attacks are reported. Thus, the claim, that China itself is a victim of cyber attacks, is not false.

Graph 1: Reported Cyber Attacks on China*



Source: Based on Annual Reports of APCERT

5. Conclusion

As the available literature and analysis of cyber incidents suggest, China's focus during the period of peace seems to be 'technology', 'trade secrets' and 'industrial espionage' so that China's economic growth rate could be maintained. China seems to use cyber and information technology to leapfrog in all fields of technologies including military technologies, industrial technologies etc. Industrial espionage is not something new; it had been going on ever since nation state came into existence, it's only the methods and means that have changed. And since international law does not address the legality of peacetime espionage (Spade 2012: 08), it provides an open opportunity for all nation states especially to close competitors to compete with each other without going to war. Therefore, almost all nation states, especially major powers exploit this opportunity and pursue espionage activities and China is no exception to it. Cyberspace serves as the best medium for conducting espionage activities as no life of secret agent has to put in danger, rather agents can access any corner of the world without being physically present there through remote access and other software. Cyber espionage in the commercial sector allows China the opportunity to skip generations of research and development efforts, levelling the playing field in science and technology, and by association boosting economic and military might (Fritz 2008: 57). However, espionage during peacetime is not only limited to peace time rather it also serves as an opportunity to prepare for situation of conflict or war. For example networks can be scanned, vulnerabilities can be identified and exploited, backdoor applications, malware, and viruses etc. can be implanted in the network during peacetime which can be activated to achieve pre-planned objectives during the period of conflict. As China has no recent experience of war, it is difficult to predict how China would use cyberspace during the period of conflict? Given the kind of advantage cyberspace provides, it seems China would use cyberwarfare in initial phase of conflict/war and would try to make adversaries blind and deaf by disrupting their command and control; by denying them the required information; by disseminating misinformation and thus would try to achieve information dominance/superiority. Information superiority, say Chinese commentators, is not necessarily determined by technological superiority, but by new tactics and independent creativity of commanders in the field (Stokes 1999). However, how much creative Chinese commanders are it could be known only after battle starts.

China would try its level best to develop its hacking abilities to such a level of sophistication which can allow it to hack adversaries' air defence system and conduct Israel style air strike

or conventional warfare with the support of cyberwarfare skills. It is because this type of attack goes along with Chinese characteristic: attacking silently and covertly so that nobody knows who actually was behind the attack. Chinese analysts and researchers are well aware of the fact that cyberwarfare technologies like 'Suter', the technology which enabled Israel style attacks in 2007, can enhance the lethality of the conventional forces many folds. Chinese government act as an intervening actor which provides with the required resources for carrying our R&D to develop technologies like 'Suter' and other key technologies to enhance China's defensive and offensive capabilities. China's white paper on defence also asserts, "Priority is given to R&D of new and high-tech weaponry and equipment, and endeavours to achieve breakthroughs in a number of key technologies and leapfrogging technological progress, thus speeding up weaponry and equipment modernization" (China's National Defence 2006). Example of one of such research is the publication of an article (*NYT* March 20, 2013) titled "Cascade-Based Attack Vulnerability on the U.S. Power Grid" in an international journal called Safety Science last spring. The author of the article Wang Jianwei, a graduate engineering student of Liaoning Province, was wrongly portrayed (*NYT* March 20, 2013) as China's cyber warrior by well known China specialist Larry M Wortzel. Author's goal, with which independent American scientists also agree, was to find a solution to make the network safer and better protected. There could be one more aspect of these researches – the unpublished findings, which could serve as classified document. This points out one more intention that China could be aiming at: learning from the US vulnerabilities, strengthening China's own networks by eliminating those vulnerabilities and finding ways to exploit those vulnerabilities so that they can be used during period of conflict.

As far as China's cyberwarfare capabilities are concerned it can be observed that Chinese government has put in a lot of efforts to enhance its cyberwarfare capabilities. The number of cyber security experts and cyber military drills suggest that Chinese government is leaving no stone unturned to become a major cyber player. The government, instead of sitting and waiting for cyberwarfare to come, is confidently and no longer covertly, strengthening defensive and offensive cyber skills. The trend analysis of the incidents attributed to China makes us believe that China's cyber skills' sophistication level has increased tremendously. China's sophisticated espionage activities like 'Titan Rain', 'Ghost Net', theft of classified weapons' details etc. clearly indicates that China's capabilities have grown enormously. Even the success story of China's supercomputers, which moved from fifth fastest in 2009 to the fastest in 2010, shows the kind of efforts government would have put in. These efforts still

continue and continue at a greater than normal pace as if war is going to start soon probably because Chinese scholars don't see much difference between peace and conflict period. Again the way China confidently announces publically its cyber military drills, just before the Xi's first visit to the US, in the backdrop of China being blamed for most of the hacking incidents, presents the confident China has gained as a major cyber player. And the way China transferred the blame ball in the US court at Xi's meeting with Obama in California, suggest that China has not only become a major cyber player but also a major cyber power in international arena.

Thus, if the attribution of above mentioned cyber incident to China is true, it is evident that sophistication level has increased tremendously – from patriotic hacking, website defacement, denial of service attacks etc. to sophisticated malware attacks, theft of classified information. Therefore it can be observed that China's cyberwarfare skills are no longer rudimentary and have increased tremendously in sophistication level. However, if sophistication level of these activities are compared with sophistication level of 'Stuxnet', 'Flame' etc. it can be clearly said that there is still a lot of difference in the level of sophistication. The US level of sophistication is still very high and it still dominates in cyberspace as no any cyber incident, attributed to China, has been reported till date which could result in kinetic effect as 'Stuxnet' did. This difference seem to be decreasing with time, but China still has to go a long way, which China would most probably travel without going into conflict with the US and by exploiting the cyberspace for its own benefits, until no international convention or legal framework is put into effect.

Chapter 6

Conclusion

1. Concept of Cyberwarfare – Global and Chinese Discourse

In international arena the concept of cyberwarfare remains a contested concept. Every nation state has its own set of rules for cyberspace domestically, but when it comes to the international platform, forget about the set of rule, they widely vary on the definition of cyberwarfare. UN is the only international organisation which provides an official international definition, however no nation follows it as it is just a definition and not international law. One more effort at international level has been recently witnessed in the form of a publication called 'The Tallinn Manual on International Law Applicable to Cyber Warfare' by NATO established 'Cooperative Cyber Defence Centre of Excellence', which emphasises on the effect caused by cyber attack to decide whether an act in cyberspace can be considered as cyberwarfare or not. Most of the nation states define cyberwarfare as per their own convenience and keeping in view their own benefits. Some nations do not even bother to define it but are always ready to exploit it for their benefits. Among nation states it is the US which has done most of the research work and has published maximum numbers of government reports and documents. Others might not have invested so much, but almost all major powers have attached great importance to the issue of cyber attacks as cyber threats have emerged as huge national security threats especially for those nations that are more dependent on ICTs. The UK has declared hostile cyber attacks on UK's cyberspace and cybercrime as tier one priority risk to national security. Russia seems to be one of the most active players in cyberspace as it has been reportedly blamed twice of waging cyberwarfare against other nations: once in 2007 against Estonia; and another in 2008, supplemented by conventional forces against Georgia. Since, there is no universally agreed international law or organisation which could guide the conduct of nation states in cyberspace and could determine the rule of engagement in cyberwarfare, it is all up to nation states to decide how to behave in cyberspace: whether to act responsibly; aggressively; or to exploit the loopholes of cyberspace covertly?

'Cyberwar' as a term was first used by *John Arquilla* in 1993, which has after going through two decades of global debates and discussions, has established itself as a rich concept. However, on the one hand it is still being debated and is still being referred as 'incipient

concept' and on the other hand threat of 'Cyber Pearl harbour' and 'Cyber 9/11' is being speculated. The available literature suggests that cyberwarfare is related to IW/IO but is not its synonym. The concept of cyberwarfare has evolved from the concept of IW/IO. Initially cyberwarfare was a small sub-set of IW/IO but with time it has incorporated many elements of IW/IO. As of now, EW and use of electromagnetic spectrum all belong to cyberwarfare. Cyberspace, located in information environment and composed of information and physical dimensions, was one of the operational areas of IW/IO, which now belongs to cyberwarfare. Hence it can be said that IO can be conducted in cyberspace but not all cyberspace operations are IO. Another element of IW/IO called CNO, composed of CNA, CND and CNE, is now a part of cyberwarfare. IO can take forms of physical attack against tangible information infrastructures but as per existing definitions cyberwarfare cannot. As far as cyberwarfare's relationship with other form of warfare is considered not much of study has been done so far. Whatever little study has been done suggests that the content and the range of cyberspace have been increasing. When link between cyberspace and other traditional war fighting domain is probed it is observed that cyberspace is closely related to other domains. Even after declaration of cyberspace as a separate domain it is evident that it is not completely separate from other domains, rather they are interlinked and cyberspace has its presence in all domains. Hence, other domains are accessible through cyberspace and can be easily exploited by anyone (nation state, terrorist organisations, corporations, hackers etc.) wants to.

Cyberwarfare as a concept is still highly controversial as a group of scholars argue that war is characterised by violence which does not seem possible if war is waged in or through cyberspace. They believe past incidents of cyber attacks are not qualified to be called as examples of cyberwar. They even declared that cyberwar has never happened in past, that cyberwar does not take place in the present, and that it is unlikely that cyberwar will happen in future. However, it is countered by another group of scholars who provide ample amount of evidence to prove their point. Apart from that the recent 'Stuxnet Incident', 'Exodus Incident of South India' and 'The Metro (Subway) Train Failure due to Software Malfunction' prove that cyberspace has the potential to carry out physical destructions; result in violence; and has the capability to derail trains. Thus it can be said that the current ongoing conflict between nations in or through cyberspace might not have reached the level of war but if exploited properly cyberspace has the potential to convert the ongoing conflict into war.

Chinese Concept

The official Chinese concept of cyberwarfare is difficult to trace as official documents (mainly white paper on defence) do not explicitly mention the term 'cyberwarfare'. However, official concept can be understood in terms of 'informatisation' and 'networkisation' of Chinese defence forces which cannot be possible without the help of ICT. China's emphasis on both 'informatisation' and 'networkisation' indirectly shows the importance being attached to cyberwarfare. The most recent white paper on defence (2013), which explicitly mentions the term 'cyberspace', confirms the importance being attached by current Chinese government in present context, yet the official definition of cyberwarfare is not provided by Chinese government. As far as Chinese scholars are concerned they have worked extensively on cyberwarfare and cyberspace. They went ahead of Western scholars in tracing the first use and the origin of cyberspace. They have done an in depth study on the development process of cyberspace and hence have presented the incident and time when cyber started being associated with computers. Chinese scholars and military strategist has always laid great emphasis on asymmetric mode of warfare as they know it is extremely difficult for China to compete with developed countries in terms of conventional military strength as the support of all latest sophisticated technologies, is there with the developed nations. If a situation of conflict or war arises (may be in case of Taiwan proclaiming independence, or in case of 'Diaoyu Island Dispute' with Japan, or in case of 'South China Sea Dispute' etc.) the US is expected to intervene, and China just cannot afford to sit back and wait for being defeated. In this quest for asymmetric means, cyberwarfare suits China's requirement of overcoming a militarily stronger and technologically more advanced adversary. Chinese scholars and military strategists have studied various characteristic features of cyberwarfare so that optimum utilisation of the cyber means could be ensured whenever required in whichever situation. Though China has not yet declared cyberspace as a separate war fighting domain, however Chinese literature devoted to the study of cyberspace are in plenty. Available literature, like Western literature also suggests that cyberspace is closely related to other domains and other modes of warfare. Almost all other domains and modes of warfare are dependent on cyberspace and almost all of them are accessible through one means of cyberspace, which if exploited well can provide the opportunity to achieve information superiority.

When Chinese concept of cyberwarfare is looked for, available literature suggest that the original concept is of Western origin and it was borrowed, used and studied by Chinese military strategists, thinkers and scholars. In this way, the study of the Western concept by Chinese people and China's age old long history and tradition of military resulted into development of new ideas that further enriched the original concept. Just like the Western concept of cyberwarfare the Chinese concept also evolved from IW/IO. China has also been using the similar terms and expressions (like CNO, CNA, CND, cyberspace, IW/IO etc.) as used by their Western counterparts. However, owing to the different military tradition and culture, Chinese concept of cyberwarfare has developed its own flavour, which can also be referred as 'Cyberwarfare with Chinese Characteristics'. The first and the most basic difference lies in the very concept of warfare, in which war is seen as a means to defeat the enemy without actually fighting and the 'use of force' had always been considered the last resort. This thought of 'killing less people but still achieving victory' in complete accordance with the nature of cyberwarfare. Another nature of cyberwarfare, that complements China's nature is the 'attribution issue'. Traditional Chinese culture promotes modesty which says, 'even if you are good you do not say it yourself'. Similarly when according to attribution issue it becomes extremely difficult to locate or trace the origin of cyber attacks, China, even if involved in the attacks, would be modest and would say, 'no no we have not done this'. Second prominent difference is that most of the Chinese strategists do not see much difference between war, conflict, crisis or peace period and emphasise that the benefit of cyberspace and hacking should always be taken whether it is conflict, crisis, war or peace period. The third prominent difference, which could be observed in the definitions provided by Chinese scholars, is that almost none of the Chinese scholars talk about role of nation state. They talk about two adversaries and two sides involved in cyberwar but do not mention whether the two sides or adversaries could be nation state or not. Thus it seems that China does not want its government to be involved directly in cyberwarfare, rather other options like hackers, hacker organisations, corporations etc should be considered. This indirect involvement of Chinese government provides them the advantage of denying their involvement if in case the origin of cyber attack is somehow located to China and China is blamed for cyber attacks. The fourth difference is that there is no evident difference between Chinese civilian cyberspace and military cyberspace, rather integration of both is emphasised. And it is here where Mao's concept of 'People's War' comes into effect, which advocates that both soldiers and civilians, who have technical knowhow of network security and advance cyber skills can serve as cyber warrior and participate in China's cyberwarfare. Fifth

and the most important difference is the integration of modern cyberwarfare skills with China's traditional military practices. For example use of strategies from Sun Zi's *Art of War*, Sun Bin's *Art of War*, 36 Stratagems, etc. in contemporary cyberwarfare. This 'Cyberwarfare with Chinese Characteristics' could serve as an element of surprise to the adversaries of China as they are not well aware of China's military tradition and China, which take pride in its glorious military tradition, would certainly take advantage of these surprise elements.

2. Threats, Intentions and Capabilities of Chinese Cyberwarfare

There are numerous organisations involved in China's cyberwarfare including both government and non-government organisations. The government organisations are located all over China, however all of them are controlled from Beijing. At the central level GSD, with its sub-ordinate organisations like the Third Department, the Fourth Department and Information Security Base (Cyber Command), is one of the most prominent organisations. Operational responsibilities of China's cyberwarfare seem to lie with the GSD Fourth Department. The regional locations of cyberwarfare units are area specific and their functions are also area specific as electronic warfare, a component of cyberwarfare has limited geographical reach. The central organisations are complemented by many regional organisations like TRBs, research institutes and universities. In case of many of the regional organisations command and control structure is not known.

The non-government organisations are basically the hacker organisations, private (cyber) security firms, corporations etc. which operates under the strict surveillance of Chinese government as Chinese cyberspace may also fuel up domestic unrest and present huge threats to the survival of CPC regime. Chinese government has shown a certain level of tolerance to the non-government organisations which have been involved in patriotic hacking against other nations, same would not be tolerated if carried out against CPC. Chinese government has already shown that they can restrict the conduct of Chinese hackers whenever required. After the recent Mandiant report, number of cyber attacks originating from China reduced tremendously. Thus it can be observed that Chinese hackers operate at the will of Chinese government. Even the private telecommunication companies like ZTE, Huawei etc are blamed to be working in collaboration of Chinese government, however these allegations have not yet been proved.

Cyberwarfare skills can be used for a host of purposes. It can be understood in two different time periods: peace time; and conflict or war time. And between these two time periods there lies a grey area as the demarcation line between peace and war time is not clearly defined and hence this grey area is the place where both problems and opportunities lies. This grey area can be exploited by any organisation or nation state for their benefit without going too far in the area or crossing the vague demarcation line, which might not be accepted by victim nation or victim organisations of another nation. Sometimes, when significant cyber skills and enough confidence is gained, which seem to be the case with China, even crossing the vague demarcation line in grey area would not result in military retaliation as the attribution issue comes to the rescue. Thus China is playing safe by exploiting cyberspace as much as possible for its benefit and is confident of not being punished as attributing these cyber attacks is extremely difficult. If somehow cyber attacks are traced back to China, as recently happened, China has the option of denying the allegations or putting blame on some hacker organisations or if possible diverting the international attention towards another nation by showing that others are also doing the same. The US's, along with all major software service provider giants, indulgence in classified surveillance programme 'PRISM' initiated the argument that if almost all major powers are doing the same thing how can they blame others?

As far as China's intention during peace time, which is also the immediate intention of China, seem to be the 'technology leapfrogging' and 'economic espionage'. Cyberspace has provided China with an ideal opportunity of leapfrogging in certain high technologies through illegal means on the one hand and not getting caught on the other hands. Economic espionage and acquisition of trade secrets can enable China to maintain it pace of economic development and technology acquisition would help China in becoming self reliant and innovation based society, which is China's future target.

Since China has no recent warfare experience it seems difficult to predict China's war time intentions. However owing to the advantage cyberspace provides, it seems China's intention would be to use cyberspace pre-emptively so as to gain initial advantages and achieve information domination. China would also intend to use its cyberwarfare skill to disrupt adversary's command and control structure, which would cut off the adversary's soldiers from their commanding office. This would render them clueless without any guidance of what to do and what not to, which is equivalent to Mao's motive of making the enemy deaf and blind. China's intention would be to use 'Cyberwawrfare with Chinese Characteristics' as an element of surprise for adversaries, as most of China's adversaries do not understand

the true essence of Chinese age old military culture. China would also take advantage of its cyberwarfare skills to delay the deployment of adversary's troops by attacking logistics and command and control networks. In the beginning phase of war, China would use its cyberwarfare skills for supporting its conventional forces, so that the lethality precision of attacks could be increased. China's intentions during wartime is speculative and futuristic, however present intentions of China seem to be intelligence collection, scanning the vulnerabilities in adversaries' network, implanting backdoor applications and viruses so that these could be exploited in future wars.

As the indicators discussed in chapter five indicates that China, after closely examining the US activities since Gulf war and realising the importance of IT in modern warfare, has focused on improvising its IT and cyber capabilities. The indicators suggest that China has enhanced its intelligence collection capabilities to such a level that the US had to bomb China's intelligence collection unit. Other indicators like supercomputers and number of cyber security experts suggest that China has invested hugely in cyber domain and the investments have started giving returns as well. The maximum number of cyber security that China has, itself shows the priority attached to cyberwarfare by Chinese government. These achievements in cyber domain has not only enhanced Chinese cyber skills but has also boosted the confidence of China. This confidence is also visible in the cyber drills conducted by China, which initially used to be conducted covertly that recently has been conducted publicly. This confidence was again visible in Snowden's case and Xi's first meet with Obama. This confident new China has made significant advancements in cyber capabilities. The trend analysis indicates that China is capable of intruding into both classified and non-classified networks. Even the highly sensitive and classified information of the US have been targeted by China several times. The involvement in cyber espionage with the help of highly sophisticated tools like 'Titan Rain', 'Ghost Net' etc. also reaffirms that China possesses sophisticated cyberwarfare capabilities. However, the level of sophistication has to be analysed comparatively. The level is quite low if compared with the US and Israel as no cyber incident attributed to China has resulted in kinetic effect or physical damage as 'Stuxnet' did. The level of sophistication goes up if compared with Asian nations. Given the kind of cyber incidents that China has been involved it can be observed that China's cyberwarfare capabilities are no longer rudimentary.

As far as perceived threat from China's cyberwarfare is concerned it depends on a lot of factors like intentions, capabilities of China's cyberwarfare. It has already been observed that

China's cyberwarfare capabilities have improved significantly. Hence it seems that China poses a significant threat to other nations, especially to those whose networks are not secure and whose network in spite of being secure has information relevant to China's growth and development. However, it is also overblown sometimes by other nations in order to get higher budget allocations. The threat of 'Cyber Pearl Harbour' and 'Cyber 9/11' seems to be overblown at present, however it is not that these are not possible in future. China does not agree with the fact that higher sophistication level means greater threat. Going by the fact that the US's cyberwarfare capabilities are more sophisticated, the US should be a bigger threat, but no other nation raise eyebrows towards the US. China is right when it claims to be a victim of cyber attacks, however it is also an aggressor in cyberspace. Same is the case with the US, or with any other major powers. Thus, unless and until the grey area exists the cyberspace would always be exploited. Unless universal definition is not agreed upon by various nation states, no international legal framework can be conceived of. And unless no legal framework is drafted no international organization, devoted to cyber security and prevention of cyberwarfare can be thought about. Hence, the need of time is international collaboration and not allegation. Various nations need to work out together to demarcate the line clearly in the grey area so that a common standard can be used globally, which would discard the emerging cyber threats.

This work studied cyberwarfare as independent variable, conventional warfare as dependent variable and Chinese government / CPC/ hacker communities as intervening variable. In course of the work indicators like Israel attack (2007) and the US war on Iraq suggest that cyberwarfare has the potential to increase the lethality of conventional warfare drastically. This study also suggests that Chinese government i.e. CPC is intervening into China's cyberspace and using China's resources to compete with other nations and to strengthen its conventional warfare capabilities. China is exploiting cyberspace by developing world's fastest supercomputers and by recruiting maximum number of cyber security personnel. Chinese hacker communities, sometimes acting on behalf of state, also act as intervening variable by launching cyber attacks against other nations, stealing classified information.

This work started with the hypothesis that the ongoing conflicts in the cyberspace carry full potential to convert itself into a total warfare. Based on analysis of the concept of cyberwarfare, both Chinese and global, and analysis of the controversies related to the term in chapter two it can be safely said that ongoing conflicts in the cyberspace carry full potential to convert itself into a total warfare. Thus first hypothesis of the work stand substantiated.

This work also had a second hypothesis that China's cyberwarfare capabilities are fairly limited and rudimentary. On the basis of the discussions about organisations, intentions and capabilities in chapter four and five it can be safely said that China's cyberwarfare capabilities are no longer limited and rudimentary. Thus, as a result this study negates the second hypothesis.

REFERENCES

----- (2012), *PLA General Staff Department*, [Online: Web] Accessed 14 March 2013, URL: <http://www.sinodefence.com/overview/organisation/gsd.asp>

----- (2010), *Advance Persistent Threat*, [Online: Web] Accessed 06 March 2013, URL: <https://www.mandiant.com/resources/m-trends>

----- (2012), *Annual Reports of APCERT*, [Online: Web] Accessed 16 November 2012, URL: <http://www.apcert.org/documents/pdf/>

----- (2013), *APT1: Exposing One of China's Cyber Espionage Unit*, [Online: Web] Accessed 06 March 2013, URL: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

*----- (1988), JP 3-13, *Joint Doctrine for Information Operations*, [Online: Web] Accessed 11 October 2012, URL: http://www.c4i.org/jp3_13.pdf

*----- (1998, 2001, 2011, 2012), JP 3-13, *Doctrine for Joint Operations*, [Online: Web] Accessed 25 October 2012, URL: http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf & http://www.fs.fed.us/fire/doctrine/genesis_and_evolution/source_materials/dod_joint_ops_doctrine.pdf

*----- (2000), JP 2-01.3, *Joint Tactics, Techniques and Procedures for Joint Intelligence Preparation of the Battlespace*, [Online: Web] Accessed 11 April 2012, URL: <http://ids.nic.in/Jt%20Doctrine/JOINT%20INTELLIGENCE%20PREPARATION%20OF%20THE%20BATTLESPACE.pdf>

*----- (2001, 2008, 2010), JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*, [Online: Web] Accessed 11 April 2013, URL: http://ra.defense.gov/documents/rtm/jp1_02.pdf

*----- (2003), *National Strategy to Secure Cyberspace*, The US Department of Homeland Security, [Online: Web] Accessed 16 November 2012, URL: http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf

*----- (2005), AFDD 2-5 or AFDD 3-13, Air Force Doctrine Document, [Online: Web] Accessed 24 October 2012, URL: <http://www.au.af.mil/pace/epubs/afdd3-13.pdf>

*----- (2006), National Military Strategy for Cyberspace Operations, [Online: Web] Accessed 24 October 2012, URL: http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf

*----- (2010), *Military Doctrine of the Russian Federation*, [Online: Web] Accessed 12 October 2012, URL: http://carnegieendowment.org/files/2010russia_military_doctrine.pdf

*----- (2010), *Securing Britain in an age of Uncertainty: The Strategic and Security Review*, [Online: Web] Accessed 12 October 2012, URL: http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191634.pdf

*----- (2011), UN Security Council, Resolution 1113, 5 March 2011.

*----- (2013), US Department of Defense Annual Report to the US Congress, [Online: Web] Accessed 16 June 2013, URL: http://www.defense.gov/pubs/2013_China_Report_FINAL.pdf

* Hildreth, Steven A. (2001), *Cyberwarfare*, CRS Report to Congress, [Online: Web] Accessed 12 October 2012, URL: <http://www.fas.org/irp/crs/RL30735.pdf>

*China's White Paper on National Defence (2006), [Online: Web] Accessed 20th August 2012, URL: <http://www.China.org.cn/english/features/book/194421.htm>

*China's White Paper on National Defence (2013), [Online: Web] Accessed 20 April 2013, URL: http://news.xinhuanet.com/english/china/2013-04/16/c_132312681.htm

*Department of Defense, USA, *Department of Defense Strategy for Operating in Cyberspace*, July 2011.

*Melzer, Nils (2011), "Cyberwarfare and International Law", UNIDIR Resources, [Online: Web] Accessed 21 November 2012, URL: <http://www.unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf>

*Military power of People's Republic of China, Annual report to the U.S. Congress (2007), [Online: Web] Accessed 20th August 2012, URL: <http://www.defencelink.mil/pubs/pdfs/070523-China-Military-Power-final.pdf>

*Military power of People's Republic of China, Annual report to the U.S. Congress (2007), [Online: Web] Accessed 20th August 2012, URL: <http://www.defencelink.mil/pubs/pdfs/070523-China-Military-Power-final.pdf>

*Northrop Grumman Corporation (2009), *US-China Economic and Security Review Commission Report on the Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*. [Online: Web] Accessed 12th March 2012, URL: http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Aproved%20Report_16Oct2009.pdf

*PRC State Council Information Office (1998), *White Paper on National Defence*, [Online: web] Accessed 10 August 2012, URL: <http://www1.China.org.cn/e-white/5/index.htm>

*PRC State Council Information Office (1998), *White Paper on National Defence*, [Online: web] Accessed 10 August 2012, URL: <http://www1.China.org.cn/e-white/5/index.htm>

*Steven A. Hildreth (2001), *CRS Report for Congress on Cyberwar*. [Online: Web] Accessed 05 August 2012, URL: <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA398642>

*Wilson, Clay (2004), "Information Warfare and Cyberwar: Capabilities and Related Policy Issues," *CRS Report for Congress*, [Online: Web] Accessed 11th April 2012, URL: http://www.rtna.ac.th/article/Information%20Warfare%20and%20Cyberwar_Capabilities%20and%20Related%20Issues.pdf

Agency (2012), "Exodus of NE people continues; govt issues 15-day ban on bulk SMSes", *The Indian Express*, Bangalore, August 17, 2012.

Andress, Jason and Winterfeldt Steve (2011), *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, USA: Syngress.

Arquilla, John (1997), "Cyberwar is Coming," in Arquilla, John and Ronfeldt David F. (eds.) *In Athena's camp: Preparing for conflict in the Information Age*, RAND Corporation.

Arquilla, John and Ronfeldt David F. (1997), *In Athena's camp: Preparing for conflict in the Information Age*, Santa Monica: RAND Corporation.

- Ball, Desmond (2011), "China's Cyber War Capabilities", *Security Challenges*, Vol. 7, No. 2.
- Barboza David (2013), 'China Says Army is Not behind Attacks in Reports', *The New York Times*, 20 February 2013.
- Barnes, Julian E (2012), "Pentagon Digs in on Cyberwar Front", *The Wall Street Journal*, New York, 06 July 2012.
- Carr, Jeffery (2011), "Clausewitz and Cyberwar", *Digital Dao*, 23 October 2011, [Online: web] Accessed 12 October 2012, URL: <http://jeffreycarr.blogspot.in/2011/10/clausewitz-and-cyber-war.html>
- Carr, Jeffrey (2011), *Inside Cyberwarfare: Mapping the Cyber Underworld*, USA: O'Reilly.
- Cereijo, Manuel P.E. (--), "China And Cuba And Information Warfare (IW): Signals Intelligence (SIGINT), Electronic Warfare (EW) And Cyber-Warfare", [Online: Web] Accessed 14 March 2013, URL: <http://camcocuba.org/html/ADDITIONAL%20PAGES/CEREIJO%20E/cereiyo-1/CEREIJO-48-E.html>
- Chen (陈) *et. al.* (2001), "21 shiji zhanzheng xin gainian - wangluozhan (21 世纪战争心概念 – 网络战) Cyberwar – New Concept of 21st Century Warfare", *Journal of Military Communications Technology*, 22 (4): 73-76.
- Chen Zhong (陈钟) (2010), "wangluozhan bu dengtongyu junshi zhanzheng (网络战不等同于军事战争) Network Warfare is not same as Military Warfare", *xinxi anquan yu tongxin baomi (信息安全与通信保密) Information Security and Communication Secrecy*, -- (--)
- Clark Richard A. and Knake Robert (2010), *Cyberwar: The next Threat to National Security and what to do about it*, USA: Harper Collins.
- Dai Qingmin (2002), "On Integrating Network Warfare and Electronic Warfare," *Academy of Military Sciences (中国军事科学院 Zhongguo junshi kexueyuan)*.
- David Betz and Tim Stevens (2011), "Cyberspace and the State", London: *The International Institute of Strategic Studies*, p. 95-97.

Dong, Niao (东鸟) (2010), *zhongguo shubuqi de wangluozhan* (中国输不起的网络战) China Cannot Afford to Lose Cyberwar, Changsha: Hunan People Publishers.

Eftimiades Nicholas (1992), "China's Ministry of State Security: Coming of Age in the International Arena", *Contemporary Asian Studies*

Franklin, Kramer D. *et. al.* ed. (2009), *Cyberpower and National Security*, Washington D.C.: National Defense University Press.

Gorman Siobhan and Dreazen Cole (2009), "Computer Spies Breach Fighter-Jet Project", *The Wall Street Journal*, 21 April 2009, [Online: web] Accessed 20 June 2010, URL: <http://online.wsj.com/article/SB124027491029837401.html.html>

Hagestad, William T. (2012), *21st Century Chinese Cyberwarfare*, UK: IT Governance Publishing.

Heickero, Ronald (2010), *Emerging Cyberthreats and Russian Views on Information Warfare and Information Operations*, Stockholm: FOI (Swedish Defence Research Agency).

Hjortdal, Magnus (2011), "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence", *Journal of Strategic Security*, Volume IV (2): 1-24.

IDSA Task Force (2012), *India's Cyber Security Challenge*, New Delhi: Institute for Defence Studies and Analyses

Jason, Fritz BS (2008), "How China Will Use Cyber Warfare to Leapfrog in Military Competitiveness", *Culture Mandala*, 8 (1): 28-80.

K. Santhanam, Srikant Kondapalli (2004), *Asian security and China 2000-2010*, New Delhi: Shipra Publications.

Larry M. Wortzel (2011), China's Approach to Cyber Operations: Implications for the United States, in Elisabette M. Marvel (eds.) *China's cyberwarfare Capability*, New York: Nova Science Publishers. [Online: web] Accessed 7 April 2012, URL: <http://www.internationalrelations.house.gov/111/wor031010.pdf>

Liang Yan (2008), "Development of Computer Network Operation Concepts", *Ship Electronic Engineering*, 28 (4):--

Libicki, Martin C. (2009), *Cyberdeterrence and Cyberwar*, Santa Monica: RAND Corporation
Libicki, Martin C. (2011), "Chinese Use of Cyberwar as an Anti-Access Strategy- Two Scenarios", [Online: web] Accessed 7 April 2012, URL: http://www.rand.org/content/dam/rand/pubs/testimonies/2011/RAND_CT355.pdf

Lu Daohai (1999), *Information Operations* (信息作战), Beijing, China: PLA Arts and Literature Press.

Man Kaiyan(满凯艳) and Di Xin (狄鑫), "shijie wangluozhan xiaoyan siqi (世界网络战硝烟四起) Global Cyberwar Transcends Everywhere", zhiku baogao (Zhiku Report).

Marquand Robert and Arnoldy Ben, (2007), "China emerges as leader in cyberwarfare", *The Christian Science Monitor*, [Online: web] Accessed 15 August 2012, URL: <http://web.mit.edu/gssd/cyberspace/Weekly%20Article/China%20emerges%20as%20leader%20in%20cyberwarfare.pdf>

Marvel, Elizabeth M. (2010), *China's Cyberwarfare Capability*, New York: Nova Science Publishers.

Mattis Peter (2012), "The Analytic Challenge of Understanding Chinese Intelligence Services", *Studies in Intelligence*, 56(3): --

McGhie, Ian A (2012), *Cyber-Warfare: Vital ground, 'Emperor's New Clothes' or Strategic Paralysis?*, U.K: Royal College of Defence Studies.

Meng, Fansong and Han, Yining (2011), "Concept Differentiation and Analysis on U.S. Military's Cyber Operations", *Scientific Research*, Vol. 13, Wuhan (China): PLA Communication command Academy.

Mezzofiore, Gianluca (2013) "NSA Whistleblower Edward Snowden: Washington Snoopers are Criminals", *International Business Times*, June 17, 2013, [Online: Web] Accessed 28 June 2013, URL: <http://www.ibtimes.co.uk/articles/479709/20130617/nsa-whistleblower-edward-snowden.htm>

Michaels, Jim (2013), "Pentagon Develops Rules of Engagement for Cyberwar", *USA Today*, Virginia, 5 April 2013.

Mondal, Sudipto (2012), "Mischievous Potential of Social Media in Full Play", *The Hindu*, Bangalore, August 17, 2012.

Mulvenon, James (2009), "PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability," in Roy Kamphausen, David Lai, Andrew Scobell (eds.) *Beyond the Strait: PLA Missions Other Than Taiwan*, Strategic Studies Institute.

Mulvenon, James C. and Yang Andrew N D (2002), *The People's Liberation Army as Organisation*, Santa Monica: Rand Corporation.

n. a. (2013), "China Bytes Back with Fastest Supercomputer", *China Daily*, 18 June 2013, [Online: web] Accessed 20 June 2013, URL: <http://english.people.com.cn/202936/8288009.html>

n. a. (2013), "China's Tianhe-2 Retakes Supercomputer Crown", *BBC*, 17 June 2013, [Online: Web] Accessed 18 June 2013, URL: <http://www.bbc.co.uk/news/technology-22936989>

n. a. (2013), "Cyber Security is New Battlefield as US-China Tension Grows", New Delhi, 26 June 2013, [Online: Web] Accessed 28 June 2013, URL: <http://www.dnaindia.com/scitech/1853195/report-cyber-security-is-new-battlefield-as-us-china-tension-grows>

n. a. (2013), "NSA Slides Explain the PRISM Data-collection Program", *The Washington Post*, 10 July 2013, [Online: Web] Accessed 12 July 2013, URL: <http://www.washingtonpost.com/wp-srv/special/politics/prism-collectiondocuments/?hpid=z1>

n.a. (2013), "China opposes hacking allegations: FM spokesman", *Xinhua News*, Beijing, 19 February 2013, [Online: web] Accessed 21 February 2013, URL: http://news.xinhuanet.com/english/china/2013-02/19/c_132178666.htm

Nelles, Mattia, (2012), "China's Growing Cyber War Capacities: A Threat to US Interests in Cyberspace?", *E-International Relations*, [Online: web] Accessed 15 August 2012, URL: <http://www.e-ir.info/2012/07/29/chinas-growing-cyber-war-capacities/>

Nu Li, Li Jiangzhou, and Xu Dehui (2000), "Strategies in Information Operations: A Preliminary Discussion," *Military Science*.

Nye, Joseph S. (2012), "Cyber War and Peace," *Project Syndicate*, [Online: web] Accessed 11 April 2012, URL: <http://www.project-syndicate.org/commentary/cyber-war-and-peace>

Page Lewis (2007), 'Israeli sky-hack switched off Syrian radars countrywide', *The Register*, 22nd November 2007, [Online: Web] Accessed 28 June 2013, URL: http://www.theregister.co.uk/2007/11/22/israel_air_raid_syria_hack_network_vuln_intrusion/

Qiao, Liang and Wang Xiangsui (1999), *Unrestricted Warfare*, Beijing: PLA Literature and Arts Publishing House.

Rid, Thomas (2012), "Cyberwar: Think Again," *Foreign Policy*, [Online: web] Accessed 11 April 2012, URL: <http://www.foreignpolicy.com/articles/2012/02/27/cyberwar#6>

Riley, Charles (2013), "China's Military Denies Hacking Allegation", *CNN*, Hong Kong, 20 February 2013, [Online: web] Accessed 21 February 2013, URL: <http://money.cnn.com/2013/02/20/technology/china-cyber-hacking-denial/index.html>

Saporito Laura and Lewis James A. (2012), *Cyber Incidents Attributed to China*, Centre for Strategic and International Studies, [Online: web] Accessed 7 April 2012, URL: http://csis.org/files/publication/130314_Chinese_hacking.pdf

Schmitt Michael N. (2013), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, NATO Cooperative Cyber Defense Centre of Excellence, Tallinn: Cambridge University Press, [Online: Web] Accessed 05 April 2013, URL: <http://www.ccdcoe.org/249.html>

Schneider, Bruce (2010), "Threat of 'Cyberwar' Has Been Hugely Hyped", *CNN*, 07 July 2010, [Online: web] Accessed 27 November 2012, URL: <http://edition.cnn.com/2010/OPINION/07/07/schneider.cyberwar.hyped>

Sharma, Deepak (2011), "China's Cyber Warfare Capability and India's concern", *Journal of Defence Studies*, Vol. 5, No 2.

Sharma, MK (2011), *Cyber Warfare: The Power of Unseen*, New Delhi: KW Publishers

Shi *et. al.* (2010) "Comprehension for cyberspace and cyber-war for Information Warfare", *hangtian dianzi duikang* (航天电子对抗) *Aerospace Electronic Countermeasure*, 26 (4): --

Shu Zhi'an (舒治安) (2011), "*saibo kongjian yu hai zhanchang wangluozhan jishu fazhan yanjiu* (赛博空间与海战场网络战技术发展研究) Research on the Development of Cyberspace and Navy Battlefield Network Warfare Techniques", *Proceedings of Electronic Information Technology in Naval Battlefield*, -- (--):--

Sowmiya, Ashok (2013), "Delhi Metro Train Breaks Down in Tunnel", *The Hindu*, New Delhi, 12 June 2013.

Spade, Jayson M. (2012), China's Cyber Power and America's National Security, [Online: Web] Accessed 28 January 2013, URL: <http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB424/docs/Cyber-072.pdf>

Staff,Reporter (2012), "9 held for targeting N-E students", *The Hindu*, Pune, August 14, 2012.

Stallone, Martin (2009), *Don't Forget the Cyber!*, Naval War College, New Port.

Stokes, Mark A. (1999), *China's Strategic Modernisation: Implications for the United States*, US: ----

Stokes, Mark A. and Hsiao, L.C. Russell (2012), "Countering Chinese Cyber Operations: Opportunities and Challenges for U.S. Interests", *Project 2049 Institute*.

Stokes, Mark A. et. al. (2011), "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure", *Project 2049 Institute*.

Sun (孙) et. al. (2012), "Conception Analysis and Thought on the term Cyberspace", *Fire Control & Command Control*, 37 (4):--

Tharoor, Shashi (2012), "Living With the Reality of Virtual Threat," *The Hindu*, New Delhi, 23 August 2012. [Online: web] Accessed 24 August 2012, URL: <http://www.thehindu.com/opinion/lead/article3808398.ece?homepage=true>

Thomas Timothy L. (1996), "Russian Views on Information Based Warfare", *Airpower Journal*, Special Edition.

Trias, Eric D. and Bell, Bryan M. (2010), "Cyber This, Cyber That . . . So What?", *Air and Spacepower Journal*, Spring, U.S.

Ventre, Daniel (2011), *Cyberwar and Information Warfare*, New York: John Wiley & Sons.

Wang Houqing, Zhang Xingye (2000), *The Science of Military Campaigns (战役学)*, Beijing: NDU Press.

Wang Pu Feng (1995), xinxizhanzheng yu junshi geming (信息战争与军事革命), *Academy of Military Sciences (军事科学院)*.

Wei, Jincheng (1996), "New Form of People's War," *Jiefangjun bao*, 25 June 1996.

Weinberger, Sharon (2007), "How Israel Spoofed Syria's Air Defense System", *Wired*, 04 oct 07, [Online: web] Accessed 20 June 2012, URL: <http://www.wired.com/dangerroom/2007/10/how-israel-spoof/>

Yuan (袁) *et. al.* (2010), "shijie wangluozhan fazhan zhuangkuang de chubu yanjiu(世界网络战发展现状的初步研究) Preliminary Research of Current Situation of Global Cyberwarfare", *Informatization Research*, 36 (8): 20-21.

Zhang Mingzhi (张明智) and Hu Xiaofeng (胡晓峰) (2012), "wangluo kongjian zuozhan ji qi dui zhanzheng fangzhen de yingxiang (网络空间作战及其对战争仿真建模的影响) Cyberspace Operations and its Influence on Warfare Simulation Modelling", *Military Operations Research and Systems Engineering*, 26 (4): 10-14.

Zhang, Yong (张勇) and Ding Jianlin (丁建林) (2012), "Study on Cyberspace Structure and the Methods of Attack and Defence", *Netinfo Security*.

Zheng Kun(郑坤) and Tian Xiaopeng (田晓朋) (2009), "jisuanji wangluozhan jieshao (计算机网络战介绍) Introduction to Computer Network Warfare", *Science & Technology Information*, Vol. --, No. 35

Annexure A

Cyber Attacks Attributed to China

1999

May 1999: The accidental US bombing of China's Serbian embassy in May 1999 draws angry protest from China's hacker community and leads to a series of defacements of US government websites by Chinese hackers.

August 1999: The "Taiwan-China Hacker War" erupts after then-President of Taiwan Lee Teng-hui recommended Taiwan's relationship with the People's Republic of China be on a "state-to-state" basis. Chinese hackers defaced numerous Taiwan government, university and commercial sites. Taiwan hackers attacked back, defacing Chinese government Websites with pro-Taiwan language.

2000

May 2000: Chinese hackers deface Taiwan government Websites with anti-Taiwan political statements in protest over the swearing in of Chen Shui-bien.

October 2000: Chinese hackers threaten a denial of service attacks and Web defacement against Taiwan government and private Websites in protest over Taiwan's celebration of National Day.

2001

April 2001: The collision of a US Navy EP-3 reconnaissance plane and a People's Liberation Army Navy (PLAN) F-8 fighter and the subsequent detention of the EP-3 crew members for eleven days on Hainan Island sparked the first "Sino-US Hacker War," with denial of service attacks and Web defacements launched from both sides against government and private sites.

2002

May 2002: To mark the one year anniversary of the first Sino-US Hacker War, Chinese civilian hackers begin to plan a large scale attack of US Websites. Their planned attacks end after the Communist Party issues a strongly worded condemnation of patriotic hacking against foreign networks.

2003

August 2003: Hackers operating from sites in mainland China's Hubei and Fujian Provinces penetrate thirty Taiwan government agencies and at least twice as many Taiwan companies. The attacks focus on the Defense Ministry, Election Commission, and the National Police Administration among others. This is part of an ongoing series of attacks against the Taiwan government and private industry that continue through 2004 against other notable Websites such as Taiwan's Ministry of Finance and the Kuomintang Party.

2004

June-July 2004: Attacks against Taiwan continued in 2004 targeting Websites belonging to Taiwan's Ministry of Finance, the Kuomintang Party, the Democratic Progressive Party (DPP) and the Ministry of National Defense's (MND) Military News Agency.

November 2004: US media reports that Chinese hackers attacked multiple unclassified US military systems at the U.S. Army Information Systems Engineering Command at Fort Huachuca, Arizona, the Defense Information Systems Agency in Arlington, Virginia, the Naval Ocean Systems Center in San Diego, California and the United States Army Space and Strategic Defense installation in Huntsville, Alabama.

2005

May 2005: A series of attacks believed to have originated from China and South Korea hit numerous Japanese university and industrial Websites. The attacks may have been caused by a rise in tensions between the countries over the Japanese Education Ministry's alleged omission of key historical facts pertaining to Japan's actions in World War II and China's opposition to Japan's attempt to be a permanent member of the UN Security Council.

August 2005: Media reporting first covers the story of a Chinese computer network exploitation operation codenamed "Titan Rain," alleging the intrusions into DoD systems date back to 2003.

September 2005: According to Taiwanese media, the Taiwan National Security Council is targeted via socially engineered emails containing malicious attachments, infecting the recipient hosts and possibly installing a backdoor through which the intruders can return undetected. Subject lines include "arms procurement" and "freedom."

2006

June 2006: Taiwan media reports that Chinese hackers attacked Taiwan's Ministry of National Defense (MND) and the American Institute in Taiwan (AIT). The attacks may have been launched using socially engineered email and attempted to spread misinformation about the MND in an apparent smear campaign. Attackers also stole account login credentials from Chunghwa Telecom's Web mail system, the MND's telecommunications provider.

July 2006: US media reports that intruders penetrate the US Department of State (DoS) networks, stealing sensitive information and user login credentials, and install backdoors on numerous computers, allowing them to return to the systems at will. DoS systems administrators are forced to limit Internet access until the investigation is completed. While China's involvement is not obvious, problems were especially acute at the Bureau of East Asian and Pacific Affairs, responsible for policy coordination on China, North Korea and Japan.

August 2006: Pentagon officials state hostile civilian cyber units operating inside China have launched attacks against the NIPRNET and have downloaded up to 20 terabytes of data.

August 2006: A Member of Congress who is a vocal critic of China's human rights record claims Chinese hackers penetrated his office computers and those of their staff.

November 2006: Chinese hackers attack the US Naval War College computer infrastructure, possibly targeting war game information on the networks. The College's Web and emails systems are down for at least two weeks while the investigation takes place.

2007

June 2007: Media reports indicate approximately 1,500 computers are taken offline following a penetration into the email system of the Office of the Secretary of Defense (OSD).

August/September 2007: German media reports that Berlin authorities believe Chinese hackers, with ties to the PLA, installed backdoor applications in various systems using Microsoft Word and PowerPoint documents. Targeted German government entities include the Federal Chancellery, the Ministry of Economics and Technology and the Federal Ministry for Education and Research. German officials estimate that 60 percent of cyber attacks hitting Germany emanate from China, many from the cities of Lanzhou, Guangdong, and Beijing.

September 2007: UK media reports on Chinese hacker attacks against government offices of the United Kingdom, including the Foreign Office. The attacks did not lead to major adverse effects, according to officials, though the constant, ongoing activity of China's cyber attackers is acknowledged as a constant problem.

September 2007: New Zealand's secret service suggests possible Chinese government involvement in the recent cyber attacks. China's government denies any involvement. This follows similar reporting regarding attacks against United States allies.

October 2007: US media reports that China is suspected as the source of at least seven versions of socially engineered email targeting 1,100 employees at the Oak Ridge National Lab in Oak Ridge, Tennessee. Eleven staff possibly opened the malicious attachment, allowing the attackers to gain access to, and potentially steal sensitive data, including a database at the nuclear weapons laboratory housing personnel records going back to 1990.

December 2007: The British domestic intelligence service, MI5, issues a confidential alert to 300 chief executives, accountants, legal firms and security chiefs warning of cyber attacks and electronic espionage sponsored by Chinese state organizations. Included is a warning that the PLA is targeting businesses working in China and using the Internet to steal confidential business information.

2008

March 2008: Australian security agencies acknowledge that they have been the victim of ongoing cyber attacks, but stop short of accusing China.

April 2008: Indian officials claim China is behind "almost daily attacks into the networks belonging to the government and Indian's private sector."

May 2008: The Belgian Government reports government systems have been targeted multiple times by hackers operating from China.

May 2008: U.S. authorities investigate claims that Chinese officials surreptitiously copied the contents of a US government laptop during then- Commerce Secretary Carlos Gutierrez' visit to China.

November 2008: Media sources report that Chinese hackers penetrate the White House information system on numerous occasions, penetrating for brief periods before systems are patched.

November 2008: Business Week magazine publishes a report on significant cyber intrusions dating back several years at some of NASA's most critical sites including the Kennedy Space Center and Goddard Space Flight Center. The operations to prevent the attacks from China are codenamed, "Avocado." Attacks included socially engineered emails launched at top officials. Among the data stolen are operational details of the Space Shuttle including performance and engine data.

December 2008: Chinese hackers associated with hack4.com stage politically motivated Web defacements on French Embassies in the US, United Kingdom, China, and Canada after French President Sarkozy's December 2008 visit with the Dalai Lama.

2009

March 2009: A Canadian research team publishes a study of the 'GhostNet' cyber espionage network that targeted over 1,300 hosts around the world including those at the German, Indian, Pakistani and Portuguese embassies around the world and the Tibetan Government in Exile in India. The Canadian-based Information Warfare Monitor (IWM) notes the compromise of numerous government and private information processing systems across 103 countries. The operators responsible for the network all operated from Hainan Island in China. The Chinese government denies all accusations of responsibility or state sponsorship.

March 2009: The Philippine Daily Inquirer publishes a report citing the 'GhostNet' study's assertion that the computer network of the Philippines' Department of Foreign Affairs (DFA) has been hacked by cyber spies based in China.

April 2009: Media reports the German government records daily attacks against its networks, many from Chinese based operators. The German Foreign Office is heavily targeted the reports note and are penetrated via socially engineered email.

April 2009: Australian media reports that Chinese cyber spies are targeting the Australian Prime Minister via email and mobile phones. The Chinese government denies all accusations.

April 2009: Media sources report that hackers based in China infiltrated the Intranet of South Korea's Finance Ministry, causing concern over the potential theft of sensitive government

data. The cyber attackers used socially engineered emails to target ministry staff. The email, disguised to look as though sent from one or more trusted officials, executed malicious software when opened allowing the attackers to access the systems.

Post 2009

2010

- In January 2010, India's National Security Advisor, M. K. Narayanan, asserted that Chinese hackers had attempted to penetrate computers in some of India's most sensitive government offices, including his own, on 15 February 2009.
- On 10 June 2010, South Korea claimed that a government website was attacked the previous day from Internet addresses in China. The intrusions involved a Distributed Denial-of-Service attack, and were launched from 120 IP addresses. The targeted website reportedly provided "information on administrative services and government policies".
- The Web-site of Taiwan's National Security Bureau (NSB) was reportedly attacked from China about 590,000 times from January to October 2010, or an average of about 2000 times a day. The Taiwanese media have reported that some Chinese hackers utilise Taiwan to practice their skills. Others route their attacks through Taiwanese servers, mainly because of the common language. For example, six Internet addresses in Taiwan were used in attacks on Google in January 2010.
- In November 2010, a US Congressional advisory group reported that a Chinese state-owned telecommunications company had hijacked US Internet traffic. The incident occurred on 8 April 2010 and lasted for 18 minutes, during which time traffic was re-routed by China Telecom from major US Government and military Web-sites (including those of the US Senate and the Office of the Secretary of Defense) to China, where Chinese officials were able to monitor the traffic. The re-routed traffic amounted to about 15 percent of global Internet traffic.

2011

- On 4 March 2011, South Korea's National Cyber Security Center said that about forty South Korean government and private websites had been attacked the previous day, including those of "the presidential office, the Foreign Ministry, the National Intelligence Service, U.S. Forces Korea, and financial institutions", and that these attacks originated in China. The attacks involved a more sophisticated form of Denial-of-Service operation, in which two peer-to-peer file-sharing Web-sites were initially

infected with malware, from which up to 11,000 PCs were then taken over and used in the DOS attack.

- South Korean officials claimed in March 2011 that China targeted Seoul's plans for acquisition of *Global Hawk* unmanned aerial vehicles.
- Taiwan's Ministry of National Defense announced in April 2007 that Chinese Net Force hackers had used Trojan Horses to obtain information on two particularly sensitive matters, the *Po Sheng* (Broad Victory) project (involving cooperation with the United States on C4ISR—command, control, communications, computers, intelligence, surveillance and reconnaissance) and the *Han Kuang-23* (Han Glory-23) defence exercise.
- US officials involved in talks with China at the Copenhagen climate change summit in 2009 were “subject to a cyber attack containing the ‘poison ivy’ remote access tool (RAT) intended to give hackers almost complete control over the victim’s system”.
- In March 2011, it was reported that the “parliamentary computers” of a least ten Federal Ministers of Australia had been hacked into by Chinese intelligence agencies in February, including those of Prime Minister Julia Gillard, Foreign Minister Kevin Rudd and Defence Minister Stephen Smith, and that “several thousand emails may have been accessed”
- In February 2011, Canadian media reported that “Chinese government hackers” had penetrated the computers of the Finance and Defense Departments and the Treasury Board in Canada in January. They reportedly “also infiltrated computers in the offices of senior government officials in a bid to steal passwords providing access to key government data”.
- In the case of France, the chief of the Network Security Agency stated in March 2011 that a cyber attack occurred in France in November-December 2010 in which around 150 computers in the Finance Ministry were penetrated and documents relating to the G-20 were accessed by sources believed to have originated in China. A further 10,000 computers had to be taken off-line in March 2011 and “inspected for traces of the Trojan Horse responsible, which was apparently introduced via an email attachment”.
- Bugged computers were detected “in the foreign ministries of several countries, including Iran and Indonesia, and in the embassies of India, South Korea, Taiwan, Portugal, Germany and Pakistan”. Investigators tracked the virus to “a group of servers on Hainan Island”, and to “other servers ... based in China’s Xinjiang Uyghur

autonomous region, where intelligence units dealing with Tibetan independence groups are based”.

- February 2011: The computer security firm McAfee alleged that Chinese attackers had made “coordinated, covert and targeted” intrusions into the systems of five major oil and gas firms to steal proprietary information. It reported that “the hackers could be traced back to China via a server leasing company based in Heze city of Shandong province that hosted the malware”, as well as to Beijing IP (Internet Protocol) addresses, and that the attacks, which it called Operation *Night Dragon*, “focused on financial data related to oil and gas field exploration and bidding contracts”. It also claimed that the hackers had “copied proprietary industrial processes”.
- A targeted attack campaign primarily directed at private companies involved in the research, development and manufacture of chemicals and advanced materials occurred in 2011. A total of 29 companies in the chemical industry saw the longest sustained attacks, but another 19 companies in various other sectors (primarily defence) were affected as well. Symantec traced the attacks back to a computer system that was a virtual private server (VPS) located in the United States, but the system was owned by a 20-something male living in the Hebei region in China. The cost of the VPS (RMB200 a month) as well as its US location is suggestive, but Symantec was unable to determine if the hacker was operating as part of a larger organization.

2012

- Trend Micro’s Report released findings regarding their tracking of the Luckycat campaign. The Luckycat campaign attacked diverse targets including aerospace, energy, engineering, shipping, and military research industries as well as Tibetan activists and organizations in Japan and India using a variety of malware, some of which have been linked to other cyber-espionage campaigns. Using open source research, Trend Micro mapped an email address back to its QQ number and linked the number to a hacker in the Chinese underground community. Although the Trend Micro report does not link the attacks directly to government-employed hackers, the techniques and victims targeted point to a state-sponsored campaign. From his nickname and the hacker’s published posts, The New York Times (<http://www.nytimes.com/2012/03/30/technology/hackingin-asia-is-linked-to-chinese->

ex-graduate-student.html?pagewanted=all) traced the alias to Gu Kaiyuan. Located in Chengdu, Gu was a former student at Sichuan University, which receives funding for computer network defence research and indicates the Chinese government sponsorship of hackers.

- Dubbed 'Operation Aurora' for the use of the Hydraq (Aurora) Trojan horse, Symantec monitored this group's activity and their utilization of the 'Elderwood platform,' so named for a source code variable (originates from China). The targeted industry sectors include defense, various defense supply chain manufacturers, human rights and NGOs, and IT service providers, with Google, Adobe Systems, Juniper Networks, Yahoo, Symantec, Northrop Grumman, Morgan Stanley, and Dow Chemical all documenting attacks. The scale of the attacks (both number of targets and duration) as well as the resources required to gather intelligence and intellectual property indicate that a large criminal organization, attackers supported by a nation state, or a nation state itself were responsible. The New York Times reported from a source involved in the investigation that Jiaotong University in Shanghai and Lanxiang Vocational School in the Shandong Province were traced back to the attacks.

2013

- Mandiant's Intelligence Report¹ identifies APT1 (Advance Persistent Threat) as a persistent Chinese cyber threat actor with operations that are likely government-sponsored. APT1 is believed to be the 2nd Bureau of the People's Liberation Army (PLA) General Staff Department's (GSD) 3rd Department, commonly known as Unit 61398. Activity has been traced to Shanghai. Also known as 'Comment Crew' and 'Byzantine Candor,' operations can be traced back to beginning in 2006. There are 141 known victims across multiple industries, with targets including the information technology, aerospace, public administration, satellites and telecommunications, scientific research and consulting, energy, transportation, construction and manufacturing, international organizations, engineering services, hi-tech electronics, legal services, media, advertising and entertainment, navigation, chemicals, financial services, food and agriculture, metals and mining, healthcare, and education industries. In an effort to stress the human agency behind cyber attacks, the report identifies three online personas: 'Ugly Gorilla,' a screen name attributed to Wang Dong, 'DOTA,'
-

and 'SuperHard,' attributed to Mei Qiang. All three individuals have connections to the Chinese military.

- February 2013: Bloomberg's investigation² into a hacker targeting government ministries in Vietnam, Brunei, and Myanmar, as well as oil companies, a newspaper, a nuclear safety agency, an embassy in mainland China, and personal computers in Taiwan and Philippines was traced to a QQ (QQ is popular instant-messaging software in China) and email address belonging to Zhang Changhe. Located in Zhengzhou, Zhang is a teacher at PLA Information Engineering University where professors train junior officers to serve in operations throughout China. Zhang is also affiliated with the Beijing Group, consisting of programmers, the people handling the infrastructure of command centres, and translators of stolen data.
 - May 2013: A news report³ titled "China 'stole' the US missile system designs" published in *The Hindu* on 28 May 2013, The report claims, "In the latest twist to the cyber-war between China and the US, a high level defence group here has accused Beijing of hacking into US system and stealing designs of advanced weapons described as the backbone of the Pentagon's regional missile defence for Asia, Europe and the Persian Gulf." The Washington Post in its report⁴ on the same day wrote, "Among more than two dozen major weapons systems whose designs were breached were programs critical to U.S. missile defences and combat aircraft and ships. The designs included those for the advanced Patriot missile system, known as PAC-3; an Army system for shooting down ballistic missiles, known as the Terminal High Altitude Area Defence, or THAAD; and the Navy's Aegis ballistic-missile defence system." According to the report vital combat aircraft and ships, including the F/A-18 fighter jet, the V-22 Osprey, the Black Hawk helicopter and the Navy's new Littoral Combat Ship, which is designed to patrol waters close to shore." Even the F-35 Joint Strike Fighter (the most expensive weapon system ever built), according to the report was also targeted. The details of F-35 were also targeted earlier in 2009 (or 2007) and origin of the attack was also allegedly from China.
-

Annexure B

Equivalent Organisations – At a Glance

	CHINA	U.S.
1	General Staff Department (GSD)	Joint Chiefs of Staff
2	GSD Third Department	National Security Agency (NSA)
3	PLA University of Foreign Languages (解放军洛阳外语学院), Luoyang	Defense Language Institute (DLI), Monterey, California
4	Central Military Commission (CMC)	National Command Authorities (NCA)
5	AMS's (Academy of Military Science) Campaign and Tactics Department (战役战术部)	U.S. Training and Doctrine Command (TRADOC)
6	COSTIND (Commission for Science, Technology and Industry for National Defence) (国防科学技术工业委员会) OR SASTINND (State Administration for Science	DARPA