China's Cyber Warfare:
The Strategic Value of Cyberspace and the Legacy of People's War

Ji-Jen HWANG

A thesis submitted in fulfilment of requirements for the degree of Doctor of Philosophy

School of Geography, Politics and Sociology
University of Newcastle upon Tyne

March 2012

Table of Contents

List of Acronyms

ARPANET	Advanced Research Projects Agency Net [in USA]
BBC	British Broadcast Company
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
C2W	Command and Control Warfare
CCP	Chinese Communist Party
CCDCOE	Cooperative Cyber Defence centre of Excellence [in NATO]
DDoS	Distributed Denial of Service
DoS	Denial of Service
DoD	Department of Defense [USA]
DNS	Domain Name System/Server
EW	Electronic Warfare
FNC	Federal Networking Council [USA]
GCSQ	Government Communication Headquarters [in the UK]
GIG	Global Information Grid
IANA	Internet Assigned Number Authority
IETF	Internet Engineering Task Force
INEW	Integrated Network Electronic Warfare
IO	Information Operations
ISP	Internet Service Provider
IT	Information Technology
IW	Information Warfare
LAN	Local Access Net
MOOTW	Military Operations Other Than War
NATO	North Atlantic Treaty Organisation
NCW	Network Centric Warfare
NCIRC	NATO Computer Incident Response Capability
OSI	Open System Interconnection
PLA	People's Liberation Army [PRC]
PO	Psychological Operations
PRC	People's Republic of China [in Mainland of China]
RFC	Request for Comment
RMA	Revolution of Military Affairs
ROC	Republic of China [in Taiwan]
SACT	Supreme Allied Commander of Transformation [in NATO]
SLD	Second Level Domain
TCP/IP	Transmission Control Protocol/Internet Protocol
TLD	Top Level Domain
USA	United States of America
USCC	US-China Economic and Security Review Commission
WWW	World Wide Web
W3C	World Wide Web Consortium

Glossary

Asymmetric Warfare
This is the warfare of 'acting, organising and thinking differently from opponents to maximise relative strengths, exploit opponents' weaknesses or gain greater freedom of action. It can be political-strategic, military-strategic, operational or a combination, and entail different methods, technologies, values, organisations or time perspectives.' (Cassidy, 2003:8)

Botnet
A botnet, also known as a zombie net, is a group of computers infected with the malicious kind of robot software, known as bots, which present a security threat to the computer owner. Once the robot software (malicious software or malware) has been successfully installed in a computer, this computer becomes a zombie or a drone, unable to resist the commands of the bot commander. (Carr, 2009:13)

Cache
This is a hardware component that improves computer performance by transparently storing data so that future requests for that data can be retrieved faster. The data that is stored within a cache might be values that have been computed earlier or duplicates of original values that are stored elsewhere.

C4ISR
This acronym stands for Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance, which means a computer-based combat system able to command and control military troops from various services engaged in joint operations.

Comprehensive National Power
'Comprehensive National Power' (CNP) (綜合國力, *zonghe guoli*) is a term employed by the PRC's leadership to represent the evaluation of possible variables for China's national power, which includes 'natural resources, population, economy, military, and science and technology.' (Li and Wang, 2010:257)

DDoS / DoS
This acronym stands for Distributed Denial of Service, also known as 'Denial of Service' (DoS). This kind of attack is characterised by an explicit attempt by attackers to prevent legitimate users of a service from utilising it. Attacks can be directed at any network device, including attacks on routing devices and web, electronic mail, or Domain Name System (DNS) servers. (Carr, 2009:27)

DNS
This acronym stands for Domain Name System/Server. Technically, the internet Domain Name System (DNS) is a set of databases containing IP addresses and their corresponding domain names. Since each domain name is mapped to a particular numeric address, the DNS performs the transformation back and forth between the domain names and the numbers of the respective IP addresses.

OSI
This acronym stands for Open System Interconnection, a world-wide standard which defines a networking framework for implementing protocols in seven layers. These are, from top to bottom, the Application, Presentation, Session, Transport, Network, Data Link, and Physical Layers.

People's War
The term People's War (人民戰爭, *renmin zhanzheng*) was coined by Mao in the 1920s. It is a strategic concept originally formulated to oppose the enemy during China's civil war, which then became a general doctrine of mobilising the massive Chinese populace to achieve a political goal and to defeat a militarily superior opponent despite military inferiority.

Strategic Culture
Strategic culture is a conceptualisation for understanding the way that countries formulate and implement military-security policies. (Collins, 2010:171) Culture is viewed as a value-added explanation of strategic behaviour.

TCP/IP
This acronym stands for Transmission Control Protocol/Internet Protocol. This is a functional transmission to correctly disassemble and reassemble data through small packages on the internet from the side of delivery to the side of reception. The function of IP is to arrange and lead the flows of information to their exact destination through the networks' physical layers, namely OSI.

Unrestricted Warfare
This term is derived from a book on military strategy written in 1999 by two colonels in the PLA, Qiao Liang (乔良) and Wang Xiangsui (王湘穗). Its primary concern is how a nation such as China can defeat a technologically superior opponent such as the USA through a variety of means.

Chapter One: Introduction

In recent years, the dramatic growth of internet usage has triggered an increasing interest in cyberspace, not only in terms of personal business but also on a governmental level. From 2000 to 2010, global internet usage increased from 360 million to over 2 billion people. (US Department of Defense, 2011) According to a 2011 report of China's Internet Network Information Center (CINIC), in 2010, Chinese netizens[1] numbered 457.3 million in total, up 73.3 million from just one year before. (CINIC, 2011:13) Aside from users, the scale of cyberspace[2] itself has also expanded exponentially: for example, the number of distributed TCP/IP addresses[3] in China reached 278 million in 2010 – an increase of 19.4% when compared with the year before. (CINIC, 2011:23) This steep rise in internet usage and scale means people are quickly becoming accustomed to dealing with their affairs in virtual cyberspace rather than in a physical environment. This may cover banking, marketing, shopping, or communication; the range of functions relying on cyberspace multiplies with each passing day. Furthermore, fundamental sectors of state such as agriculture, electricity and water supply, defence, government administration, information and telecommunication, public transportation, banking and finance, mail systems and goods supply chains all already operate via cyberspace.

Cyberspace has the potential to bind together the civil, government, and even military sectors as they are all constructed on this same intangible, indispensable information network platform. The network platform of cyberspace is physically structured by combining a large amount of hardware such as computers, servers, routers, converts and cables. The continuing growth of networked systems, devices, and platforms means that 'cyberspace is embedded into an increasing number of capabilities.' (US DoD, 2011) However, as the Chinese idiom states: 'while water can carry a boat, it may also capsize it'. That is to say, while a state may benefit enormously from a heavy reliance on cyberspace, in doing so, it becomes more vulnerable to being 'capsized' by the many attacks, crimes and terrorist acts generated through this medium. The task of securing cyberspace rates as one of the most serious challenges for national

[1] The term 'netizen' is defined in the report as people who are able to access the internet via broadband including both cable and/or wireless, and mobile devices. (CINIC, 2011:13-16)
[2] The definitions and concepts of cyberspace will be addressed in detail in Section 2.1.
[3] Please refer to Section 2.1.1 for a definition of IP addresses.

security, public safety, and the economy in modern times. Coping with the impact of a rapidly expanding cyberspace is an issue that states must unavoidably address in the digital era.

Traditionally, a state is protected inside its geographic territory by physical borders, often consisting of natural barriers such as rivers, oceans, straits, mountains, and special terrain. However, the geographical protection of a state is far removed from cyberspace. Research points out that any fresh meat passing a physical border into a country will undergo inspection, but a malicious attack via cyberspace could be transmitted across 20 borders by the click of just one button. (Nykodym and Taylor, 2004) Traditional physical borders cannot protect a state against attacks arising from cyberspace. Instead, each state must formulate new strategic approaches to meet such threats.

Historically, a state's power has largely been in direct relation to its territory, which, though land is a fixed resource with limited supply, could be expanded through competition and the occupation of other countries (Luke 1997). Once the territory of a state had been established, its power could be presented to the world. However, the digital age is transforming this tradition, manifested not only in civil society but also on the military field. As recent evidence suggests, the growth of the internet has transformed cyberspace from a societal platform into a potential battlefield in which states contest power. This will influence state security as government bodies no longer dominate communication systems and techniques in cyberspace. (Schwartz, 2001)

This raises the question of how exactly cyberspace can be defined as a potential battleground and what differences there are with traditional battlegrounds in terms of warfare. Since the invention of the World Wide Web (WWW), states have built up their information infrastructure to cope with both domestic and international affairs. States have now begun to compete with one another for dominance in this potential battleground. A 'virtual landscape' parallel to a state's geographic territory may thus be drawn in cyberspace, representing a metaphorical territoriality that differs from that of the physical world. This new virtual structure challenges traditional doctrines of military strategy; further to this, any new developments in military strategy will inevitably bring about a re-formulation of state policy regarding warfare and security. As such, research into the effect the development of cyberspace as a potential battleground plays on existing military doctrine is becoming increasingly crucial.

It is thus of global significance that China, a rising world superpower, is currently expending great effort on the development of cyber warfare. This research will investigate how China's fundamental strategic doctrine, People's War[4] – which is traditionally based upon geographical battlegrounds – can be integrated into the concept of cyberspace as a battlefield. Through a case study of China's rapidly developing cyber warfare, this research aims to generate potential responsive guidelines, as well as underlining the importance of cyber security to a state's national security as a whole. Traditional military strategy based on geographic battlegrounds must be re-considered in light of insights arising from Strategic Studies and Security Studies, in order to tackle new strategic issues relating to warfare conducted in cyberspace. Another consideration for this research is how relevant discourses of international relations approach the prospect of cyberspace as a new arena in which states compete to expand their power through the application of new military strategy. States may deploy strategies of cyber warfare to accomplish decisive campaigns outside of their own territory, potentially fulfilling the ancient Chinese maxim: '*subduing the enemy without fighting is the acme of skill*.' (Sun Tzu, *The Art of War*)

Research Questions

What is the relationship between cyberspace as a potential battleground and existing doctrines of modern Chinese strategy?

Expanding on the primary research question, this research further encompasses three secondary research questions:

1. How is cyberspace developing into a potential battleground?
2. How has People's War remained the guiding principle throughout the many transformations of modern Chinese strategy?
3. How does China develop and conduct cyber warfare through the strategy of People's War?

In order to answer these research questions, this research aims to construct an analytical framework, which comprises of Chapters Two, Three, and Four, so that four theoretical propositions are produced as follows:

1. The strategic values of cyberspace make it an intangible arena in which states contend for predominance over one another.

[4] The concept of People's War will be examined comprehensively in Section 3.2.

2. China's cyberspace is constructed based on an integrated platform consisting of computer networks, telecommunications, and electromagnetic environments in order to enlarge the strategic value of cyberspace.
3. Cyberspace as a potential battle space is particularly suited to the tradition of People's War. This means that this strategic tradition remains an up-to-date doctrine in modern Chinese strategy.
4. China's cyber warfare is a strategic warfare that adopts the principle of People's War. In so doing, internet control and monitoring are also likely to be an element of China's cyber warfare in order to control and command civilians into disciplined cyber warriors for military purposes.

Following the analytical framework, the research presents a case study as an empirical investigation to further elaborate these propositions empirically. In the case study, three distinct types of evidence are collected as follows, which may also form a methodological validity of triangulation:

1. Interviews with representatives of ROC's military, government and civilian sectors, which presents Taiwanese perceptions of the cyber warfare strategy of the People's Republic of China (PRC). This data collection is analysed as shown as Section 5.2 to Section 5.5.
2. Analysis of recent cyber incidents which suggest actual implementation of PRC cyber warfare strategy. This data collection is presented in Section 5.6.
3. Documentary evidence of China's cyber warfare from the PRC. This data collection is presented in Section 5.7.

One might argue that the fieldwork in Taiwan will have some bias against the PRC. As noted in the methodology section 5.1, one limitation of interview data collected in Taiwan is that it might only reveal Taiwanese perceptions of China's threat and Taiwanese officials may have their own agenda so distort the threat. However, conducting interviews inside China, particularly in this sensitive military-oriented area, is imposible because respondents within the Chinese military would likely be extremely reluctant to be interviewed, let alone to give politically unacceptable answers, for fear of putting themselves at risk.[5] Therefore, though the fieldwork in Taiwan might have inevitable bias against the PRC, conducting fieldwork and interviews in Taiwan can

[5] As Bryman (2008:150-152) indicates, researchers need to have keen perception on whether respondents are reluctant to give socially unacceptable answers for fear of being judged, which can break down the validity of data collection.

nevertheless be an effective alternative measure. In addition, the opposing position of the Taiwanese military should still provide a good understanding because their judgments are conceptually sophisticated and insightful, since Taiwanese military and officials have obtained plentiful experience in exercises against China's cyber warfare. Of course, the information derived from the interviews must be subject to critical examination by the researcher. Validation of the interviews is undertaken in Section 5.1, which follows the interviews with empirical case studies in order to highlight areas of agreement with the interviews and counteract any bias. Ultimately the aim is to reach a valuable research outcome by answering the research questions via the examination of the analytical framework through the presentation of empirical case studies backed by interviews with those who know the area well.

This research is premised on the assumption that China conducts cyber warfare based on Chinese military documents discussed in Section 5.7. The interviews are therefore a means to collect additional data in order to further investigate the significance and implications of Chinese documentary evidence on cyber warfare and alleged incidents in which China is believed to engaged in cyber attacks. For this reason, rather than proving whether China conducts cyber warfare or not, the interviews were focused on obtaining valuable insights into modern Chinese strategy and some possible methods of China's cyber warfare from the Taiwanese perspective. Political confrontation between the Taiwan and China heightens the interest of Taiwanese officials in Chinese strategy and policy in this area and makes them highly aware of Chinese activities in the field. Bias might be a problem in the interpretations of Taiwanese officials but the interviews have also provided valuable empirical information and validation of other sources in explaining how China implements its strategies in cyberspace.

1.1 The disciplines of cyber warfare: Military Studies and Strategic Studies

The key issue of this research is cyber warfare. Research indicates discovery of several cases of cyber warfare within recent years, carried out not only by states but also by non-state actors[6] (Arquilla and Ronfeldt, 2001:17). Denotatively, cyber warfare can refer to warfare conducted in cyberspace, regardless of the actors involved. Aside from investigation into the nature of cyberspace, this research will involve explorations into Military Studies, including aspects such as strategy and

[6] Section 5.2 will further examine how such incidents in cyberspace demonstrate that both state and non-state actors could implement cyber warfare strategy within military conflicts.

warfare. For some critics, the value of Military Studies can be somewhat questionable, as relevant works are often written 'for a professional audience rather than an academic one.' (Freeman, 2010:392) However, Military Studies may well provide conceptual guidance for the study of warfare, including its nature and principles, comprehension of its regularity and development and the application of further strategy and tactics, and even predictions and corresponding guidelines for future warfare. Military Studies can be interpreted as the study of any activity directly or indirectly related to war. Alternatively, it may be the study of any activity related to military affairs, the study of the relationship between armed forces and war, or even the characteristics of soldiers. In short, Military Studies involves the exploration and epistemology of military knowledge. Though such knowledge can be generally extended yet further to certain cross-border fields like crime-fighting, smuggling, trafficking and piracy (Baylis and Smith, 2005:2-4), the traditional focus of Military Studies is conventional warfare. In Wang Pufeng's (1998) view, Military Studies encompasses two interconnected dimensions. The first dimension is warfare, implying the investigation of the use of the military to present a state's power. The other dimension is national defence, tackling the problems of constructing this military power. These two dimensions are closely interrelated due to mutual cause and effect.

Since military affairs are by nature highly concerned with functionality and practicality, Military Studies must surpass purely theoretical conjecture; instead, related investigations must closely correspond with military practice, such as how to conduct and win a war, to ensure fulfilment of actual requirements. From a functional perspective, the primary purpose of Military Studies is to analyse past precedents to extract relevant factors of warfare which can be systematised into useful knowledge. In this way, the gap between current military capabilities and guidance for future warfare may be removed; it may even make it feasible to overcome time limitations to quickly collect accurate necessary information to prepare the national defence, perhaps via cyberspace. (Cheng, 2003) However, though military planning and the construction of military power may be based on such rational thinking, this does not necessarily infer certain military victory: the outcomes of warfare are influenced by many variables, not least by the uncertainty in situation awareness experienced by participants in military operations referred to

by Carl von Clausewitz as the 'fog of war'. (Clausewitz, 1976:140)[7] Doubts may include, for example, what the extent of the discrepancy is between theoretical probabilities and the true readiness of the national defence. Or, how many variables exist which have been overlooked or not correctly calculated? What conclusions have the enemy drawn in terms of military guidance? How well prepared is the enemy's national defence? These multiple factors are all associated with the process of warfare – from preparation to operation. The results of warfare will accordingly reflect these factors. Military Studies hopes to create the most appropriate military strategy based on historical experience, in order to narrow as much as possible the distance between prior theoretical thinking and the subsequent result. This directly corresponds to Sun Tzu's aphorism in *The Art of War*: '*careful planning will lead to a victory; careless planning will lead to a defeat*'.

Another discipline relevant to cyber warfare is Strategic Studies. Strategy is indispensable for states to provide effective inter-communication between civil society, defence policy and military forces. Strategy has never been easily defined, as its exact meaning and derived notions can be confusing due to their ambiguous nature. Before further exploration of the concept, it would thus be useful to clarify the term. Baron de Jomini explained comprehensively that strategy is 'the art of directing the great part of the forces of an army onto the most important point of a theatre of war, or of a zone of operations.' (Howard, 1965:34) His contemporary Carl von Clausewitz defined strategy as 'the use of engagement for the object of war.' (Clausewitz, 1976:128) In the words of the British critic Liddell Hart, 'strategy is the art of distributing and applying military means to fulfil the end of policy.' (Hart, 1991:321) General André Beaufré stated that 'strategy is the art of dialectic of force or the art of the dialectic of two opposing wills using force to resolve their dispute.' (Freeman, 1992:282) These different definitions by eminent pioneers of Strategic Studies, though reflecting somewhat abstract elements of strategy, establish the fact that the aim of strategy is to link military power to political purpose. Despite the periodic modification of the application of strategy and the occasional redundancy of traditional frameworks in examining modern strategic details, the fact that certain political purposes guide military force has never changed. Although the fundamental concept of strategy has never undergone

[7] Clausewitz's eminent work, entitled *Vom Kriege [On War]*, was translated into English by Michael Howard and Peter Paret and published in 1976.

a monumental shift, the academic investigation of strategy is currently expanding greatly compared with the eras of Clausewitz and Sun Tzu.

Nevertheless, the concept of strategy is still primarily focused upon the field of warfare, which also encompasses security, national defence, and military discipline. However, Clausewitz, in his work *On War*, stresses that strategy contains a diverse range of features such as ethics, supply, mathematics, geography and statistics. (Clausewitz, 1976:183) Michael Howard (1965) also points out that strategy should consist of dimensions of society, logistics, operations and technology. This not only reflects the extensive themes and approaches of Strategic Studies but also indicates that exploration across the various disciplines is necessary to comprehend, evaluate and produce strategy. As a result, it is undeniable that the diversity of demands, from philosophy to science, theory to practice, and civil to military, makes the nature of Strategic Studies exceedingly complex. Additionally, there is no clear boundary between different subject areas. As Kenneth Booth (1997:96) points out, 'strategic theory helped to constitute the strategic world, and then Strategic Studies helped to explain itself reverentially and tautologically.' From this point of view, in order to form this strategic world, any one of the variety of intellectual concepts in human life can be regarded as an element of Strategic Studies. The features of diversity and complexity prevalent in this field of study will inevitably lead to further research developments.

Though much relevant research has been conducted in the field, critics still claim that existing Strategic Studies remain academically wanting. Philip Green, for instance, asserts that aspects of the field, such as deterrence theory, are 'pseudo-scientific,' using apparent scientific methods to give it a 'spurious air of legitimacy.' (Green, 1966:225) These criticisms stem from doubts concerning not only the miscellaneous, seemingly random, features of strategy but also the methods of scientific investigation involved in the field. Clausewitz commented that everything in strategy is very simple, but this does not mean that everything is easy. (Clausewitz, 1976:656) As Baylis et al.(2007:9) investigate, critics have stated that: 'Because strategists focus on the role of military power, they tend to be preoccupied by violence and war,' and that Strategic Studies neglects the 'more cooperative, peaceful aspects of world politics' as it chiefly regards the world as a 'conflict-oriented' space. That is to say, states traditionally present their power through the

military, and Strategic Studies is accordingly state-centric and obsessed with conflict and force.

However, in the digital age, the progress of information technology (IT) and the rapid development of cyberspace into a potential battleground have blurred the boundary between military and civil power, as both sectors function on the same information network platform. As a result, this platform, cyberspace, potentially binds together the civil, government, and military sectors of a state. Therefore, the formulation of cooperative and peaceful inner state, inter-state, or even transnational strategies among these three sectors will be indispensable when attempting to resolve conflicts occurring within the battleground of cyberspace.

1.2 Understanding warfare

In addition to interpretations arising from Military and Strategic Studies, it is necessary to comprehensively understand the concept of warfare in order to devise relevant strategies relating to cyberspace. Historically, changes in human behaviour have caused transformations in warfare, and civilisations in different time eras have evaluated warfare in myriad ways. In general, warfare indicates armed conflict between different political groups. However, many regard warfare as merely a risky approach to gain benefits, which may or may not be useful, legal or necessary. The consequence of these different approaches to warfare over time is the wide extension of definitions of warfare, which may even contain metaphorical meanings. For example, the American concept of 'Cultural War' can be seen as a metaphorical take on warfare. (Steinert, 2003)

Clausewitz (1976:75) defines war as 'an act of force to compel our enemy to do our will.' In Clausewitz's view, a 'true war' is still defined as armed combat provoked by enmity. Crucially, then, the establishment of the existence of an enemy is the key to distinguishing between true warfare and metaphorical or agonistic war. As a result, it is essential for doctrines of defence strategy to identify the enemy in the battleground of cyberspace. Basically, the enemy is 'the other', 'the stranger' and existentially deemed to be something 'different.' (Schmitt, 1996)[8] 'The enemy is solely the public enemy, because everything that has a relationship to such a collectivity of men, particularly to a whole nation, becomes public by

[8] The works of Carl Schmitt, a German political theorist, are widely controversial, but this research refers analytically – not normatively – to his definition of enemy, which does not imply support of his general political philosophy.

virtue of such a relationship. The enemy is *hostis*, not *inimicus* in the broader sense.' (Schmitt, 1996:28) This perspective posits that hostility towards the public enemy is an essential fact within the concept of warfare. Schmitt additionally asserts that 'Every religious, moral, economic, ethical, or other antithesis transforms into a political one if it is sufficiently strong to group human beings effectively according to friend and enemy.' (Schmitt, 1996:37) Therefore, in addition to the existence of an enemy, recognising a conflict of antithesis may also help discern and classify true warfare. This theoretical concept of distinguishing between friend and enemy may support this study in establishing guidelines for differentiating between true warfare, antagonistic attacks, or merely non-malicious provocations on the cyber battlefield. This research will also explore whether the traditional method of relying solely on physical military action to counter hostility or make distinctions between friend and foe can be applied successfully to cyberspace.

So how will it be possible to identify true warfare in cyberspace in order to justify defensive action? In terms of international law, Article Two of the Charter of the United Nations explicitly states, 'All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.' (Charter of the United Nations, 2009) Nevertheless, there remains a discrepancy between legal warfare and the reality of war. The former is a war declared according to justifiable standards of international law; the latter may be a war which is not only undeclared, but may also be a conflict of force which is, by definition, not true warfare. A well-known example is the Korean War from 1950 to 1953. The countries involved in this war number as many as fifteen, and the casualty figures run into the hundreds of thousands (though the total numbers of casualties suffered by all parties involved may never be known). (Singer, 1972:68) However, since it was not declared, the Korean War was criticised as a mere conflict of armed forces, not legalised warfare. (Singer, 1972)

Due to the needs of quantitative research, the definition of warfare also relies on the statistics of war, such as the number of people involved, the time period, the type of actors (*state or non-state; military or non-military*), and the number of casualties. For instance, the Encyclopaedia Britannica defines warfare as a large-scale conflict of armed forces – a definition established through the number of people engaged in the situation, which must number no fewer than five hundred

thousand. Singer (1972) defines an international war as a military conflict occurring between national entities, so one of the actors therefore must be a state. He further makes explicit that the number of deaths must be no fewer than one thousand. It is also very important to identify who initiates the war and who is the victim. For example, in the physical world, a state could claim to be a victim when its territory is invaded by others.

The potential battleground of cyberspace does not fit neatly into the definitions of conventional warfare. Warfare changes and adapts in pace with the progress of technology, which is itself often astonishingly rapid. (Creveld, 1991:312) Advances in weapon technology increasingly erode the significance of sovereign territorial boundaries, so that traditional state borders might not be the only factor influencing a state's defensive strategy against attack or invasion. In other words, warfare reflects the development of technology; to a large degree, the possible achievements of strategy depend on technological capabilities. For instance, when humans entered the age of the atom, the transformation of warfare took place much faster than ever before. In modern times, the speed, scale, and potential damage of cyber attacks could be much more severe than even nuclear weapon attacks, as nuclear ballistic missiles are technically controlled by computer-based combat systems. (This will be discussed in more detail in Section 4.2) As a result of such developments, strategic concepts and policies of national defence must be adjusted accordingly; otherwise, it will be impossible to meet the rapidly changing challenges to state security.

1.3 The transformation of warfare

It is possible to identify three main historic transformations of warfare in world politics, based upon the three different phases of military evolution: Machiavellian, atomic, and digital. The first two phases are examined below according to the views of John Herz (1962), the latter by taking into account the work of many scholars.

1.3.1 *The Machiavellian age*

As John Herz (1962:39) suggests, in the Machiavellian system, states were heavily influenced by power politics and it was possible for a state to become dominant by establishing a relatively higher law and authority. At that time, states protected their own interests and territoriality by employing military force or economic approaches to threaten one another. Upon the emergence of the modern state system, concepts

of ‘international anarchy’ and ‘collective security’ appeared. Modern territorial states were protected by a so-called ‘hard shell’, which acts like a cell wall protecting a small unit within a larger body. This ‘hard shell’ established features of a state such as ‘impenetrability’ and ‘territoriality.’ (Herz, 1962:40) In Herz’s view, the features of modern territorial states can be condensed into the terms ‘independence, sovereignty, non-intervention, equality, and international law’. (Herz, 1962:48)

The ‘impermeability’ of modern territorial states relied upon maintenance of sovereignty and control of territory. Throughout history, powerful states broke the ‘hard shell’ of smaller states, previously considered impermeable, and even wiped out their sovereignty. This revealed the limitations of impermeability and peaceful co-existence in the world. Therefore, within international relations, nation-states adopted a certain standard for actions and behaviour regarding principles of territoriality to ensure the continuing functionality of the state. For a state, the nature of territoriality included its impermeability, state power, and maintenance of sovereignty. (Herz, 1962:60)

1.3.2 *The atomic age*

Following World War II, warfare moved into the atomic age. Due to nuclear weapons’ feature of massive-scale destruction, geographical boundaries became more and more ambiguous. Some countries, like the United States of America, Russia, or China possess a vast geographic territory including continental land and ocean. The ocean could previously act as a natural barrier, reminiscent of a moat, to protect the state from attacks arising outside the area. However, nuclear weapons such as interstate missiles can now be deployed by military forces, resulting in the erosion of the boundary between the battlefront and the rear. The previous impermeability of the ‘hard shell’ of territoriality thus no longer exists, unless the state is able to deploy an effective anti-missile defence system to defeat threats from the edge of the ‘shell.’

States, based on rationality and self-control, are nevertheless forced by the devastating nature of nuclear weapons to ensure effective deterrence against atomic war. Attacks on enemies with such destructive weapons could also be regarded as a threat to the aggressor itself, as all humans inhabit the same fragile planet. (Herz, 1962:13-14) Though technological discoveries in the new atomic age were unpredictable, meaning state military planning and policy making could not always

match the pace of development, nuclear developments effectively resulted in the reduction in importance of military superiority, as destructive weapons such as atomic bombs, even in tiny amounts, boasted results massive enough to destroy entire territorial states. Inferior powers were thus able to mount an offence against traditionally more powerful adversaries, and states competed with one another to develop these destructive weapons, leading to the vicious circle of the international arms race. In the atomic age, geographical territory and state sovereignty were no longer guarantees of power, since the 'impermeability' of the territorial state would be easily obliterated by weapons like the atomic bomb. Therefore, as Herz indicates: 'Before we undertake to study in more detail how the principal new factors affect the structure of statehood and the system of international relations, we must glance back at where we have come from: […….] the era of territoriality.' (Herz, 1962:36) The atomic age was an era in limbo between the past and future.

Despite the dawn of the atomic age, even taking into account rational approaches to disarmament and arms control, states have not been able to transcend the restraints of pursuing national interests, leading to inevitable security dilemmas. Herz proposes the idea of the mutual dilemma to: 'kill or perish, of attacking first or running the risk of being destroyed.' (Herz, 1962:231-232) The solution to this dilemma could be represented metaphorically as two sides choosing to stay in the same boat, as any explosion would cause both sides to sink together. Despite this collective concern, human nature does not facilitate easy mutual trust, as people cannot predict the actual plans of the enemy. Feelings of perceived insecurity may well occur even if both sides remain in the same virtual boat. Herz poses the question: 'How could [a nation] trust in the continuance of good intentions in the case of collective entities with leaders and policies forever changing?' (Herz, 1962:235) The most significant example is of course the Cold War, in which the phenomenon of bipolarity was clearly manifest. At this time, the motivation for states to maintain national security was generally driven by the dread of being attacked, not by the hope of pursuing peace. (Herz, 1962:242) In the face of destructive atomic weaponry, states' national interests suddenly included the need to build up offensive power, as well as the simultaneous maintenance of the constraints of collective security. In Herz's (1962) view, 'holding operations,' which refers to the halting of arms races amongst states, might be the most efficient solution for resolving the security dilemma. But once again, would states be willing

to implement holding operations without the prior reduction of perceived insecurity and fear?

1.3.3 *The digital age*

In the present digital age, also known as the information age[9], techniques of IT are advancing at an astonishing pace. The concept of warfare is undergoing an evolution of strategy due to developments in computer devices, network systems, and telecommunication. Historically, information technology is not the first new development to cause a revolution in military strategy, as there have been similar experiences with audio and video broadcasting. From Machiavelli to the atomic age, many new technologies have entered the world and subsequently affected the existing doctrine of military strategy and warfare. (Paret, 1986:21-31) In terms of scale, however, information technology is the deepest and broadest revolution. It is also believed that the most important progression in weapon technology is currently in the realm of electronics. (Creveld, 1991:267) In addition, as Barry Buzan and Lene Hansen (2010:54) point out, the technology of cyberspace has 'a military as well as a civil side that can be difficult to differentiate.' Warfare in the digital age is consequently very different to warfare in the previous two ages.

In the digital age, cyberspace has emerged as a potential domain in which to wage war. Dimensions of cyber warfare must therefore be applied to military strategies in order to protect states' interests against cyber threats. Threats of cyber warfare, which may affect critical infrastructure, are referred to as non-traditional threats, as they do not result from conventional violence or traditional weapons. The target of a conventional attack is usually a regime or a state. However, the actors who produce non-traditional threats and launch attacks do not necessarily identify with a regime or a state, and their targets are located all over the world. This means that cyber warfare is an issue beyond the previous international scope. It is therefore necessary to develop new strategies through cooperation not only with states but also with private sectors which own information infrastructures in order to construct mechanisms for prevention of cyber threats and attacks.

[9] The term has been identified as an era when 'ideas about the computer, the internet, or digital resources seem to influence policy decisions more than social concerns about access, privacy or preservation.' (Weller, 2011:18) The term is often applied in relation to the use of mobile electronic devices, digital music, high definition television, digital cameras, the internet, cable TV, and other items that have come into common use in the past 30 years. (Castells, 2000)

One might well ask: would such cooperation match a state's interests and defence policy? What are the constraints on cooperation with private sectors or even with other states? Lewis (2003:xii) points out that there are indeed constraints, but that: 'Cooperation in cyber security is crucial because there are no national solutions to transnational problems.' Therefore, unlike traditional state-centric conduct in international politics, it is now essential that private sectors take precedence in transnational cooperation to protect states' common interests.

1.4 Features of warfare in cyberspace and existing doctrines

Following the definition of warfare and its three transformations, it is possible to interpret cyber warfare simply as any kind of warfare waged in cyberspace by both state and non-state actors. In 2001, the US Congress released a government report regarding research into cyber warfare. This report notes that 'Cyber warfare can be used to describe various aspects of defending and attacking information and computer networks in cyberspace.' Also: 'It can include *offensive* information operations mounted against an adversary, or even *dominating* information on the battlefield.' (Hildreth, 2001:16; emphasis mine)[10] That is to say, compared with warfare conducted on traditional battlefields or even the deployment of atomic bombs, the distinction between offence and defence in cyber warfare is even more ambiguous. However, this research debates that the ideas of a 'hard shell' and impermeability in the territorial state system may still remain somewhat applicable in cyberspace. This will be examined further in Section 2.2 through an investigation into the features of cyberspace.

Forms of cyber warfare may be categorised into various types, such as Information Warfare (IW), Electronic Warfare (EW), and even cyber terrorism, all of which are performed against enemies in cyberspace. Information Warfare, also known as Information Operations (IO), was proposed by a team of strategists led by Andrew Marshall, director of assessments in the US Department of Defense. It can be defined as warfare designed to affect the enemy's networks or information-based systems via cyberspace. This information may include text, image, audio, and video. (Libicki, 2007) Electronic Warfare, according to existing US doctrine relating to information communication, is any military action using electromagnetic approaches to control the electromagnetic spectrum or to attack an enemy. Cyber

[10] This research report may be regarded as one of the earliest official documents that points to the concept of cyber warfare. (Hildreth, 2001)

terrorism is now popularly discussed in the arena of politics. Research states that it is defined by the National Conference of State Legislatures as: 'The use of information technology by terrorist groups and individuals to further their agenda to organise and execute attacks against networks, computer systems and telecommunications infrastructures or making threats electronically.' (Gorge, 2007:9)

What existing doctrines of military strategy relate to information communications in cyberspace? Evidence shows that Chinese military doctrines are likely to draw closely from those of the US military, as will be seen in Section 5.4.2. Due to this fact, though China is the primary case in this research, it is possible to glean relevant information from US military documents, which are more readily available. According to the latest documents released by the US Department of Defense (DoD), there are two existing doctrines related to information communications, which fall under operations of the Joint Forces. The first is the doctrine of Information Operations (IO), and the other is the doctrine of Electronic Warfare (EW). The scope of the former is to 'provide doctrine for information operations planning, preparation, execution, and assessment in support of joint operations,' and in this doctrine, cyberspace is regarded as 'the notional environment in which digitized information is communicated over computer networks.' (Doctrine of IO, 2006:111) The applications of the latter 'in support of homeland defence are critical to deter, detect, prevent, and defeat external threats such as […..] hostile space systems, and cyber threats.' (Doctrine of EW, 2007:20) These two doctrines provide some general guidelines for the purposes of training and exercise, but they do not provide guidelines of cyber warfare strategies, tactics of protection, detection, and reaction, or coordination between governmental and private sectors.

Cyber warfare has become a problematic yet crucial challenge for states worldwide, and more research is necessary. For example, further to the principal duty of protection, what strategies for detection and reaction should a state's national defence implement in terms of cyber warfare? Also, as mentioned previously, strategy involves inter-communication between civil society, defence policy and military forces. It is thus important to consider how states coordinate the governmental and private information infrastructure to reinforce defence strategy with regards cyber warfare. Eriksson and Giacomello (2006) point out that any new

defence strategy brought about by developments in cyber warfare may challenge the realist camp in International Relations, which traditionally practices state-centric and military-oriented Strategic Studies.

It is important to identify why China's cyber warfare is a particular cause for concern. The Chinese government recently released a White Paper entitled *China's Peaceful Development*, in which it declares to the world that China has made the strategic choice of peaceful development. (PRC State Council, 2011) However, China's rise as a world power is not merely economic in nature; there are regular developments and advancements in China's military. As such, despite the PRC's insistence that its rise is peaceful, it has become both essential and valuable to study the development of China's cyber warfare, particularly the incorporation of cyber warfare into existing Chinese strategy and doctrine, as well as to understand China's way of thinking regarding cyberspace as a potential battleground.

1.5 The nature of this research and thesis structure

This research can be categorised as Strategic Studies even though, as investigated previously, the true boundary between the fields of Military Studies/War Studies and Strategic Studies is uncertain. Therefore, the consideration of ethical, legal, and moral issues occurring in cyberspace is informed by Strategic Studies. Furthermore, military-related research may differ from more general studies due to the rare opportunities for the testing of conclusions in real-world situations. For general studies of any subject, such as Science and Engineering, it is possible to test out conclusions and subsequently adapt theoretical recommendations as necessary. However, for research associated with military affairs, the circumstances are not the same. The factors of war are uncertain and there are no opportunities for theoretical alterations in the real world. Any verification of the efficacy of conclusions can only appear in a situation of war, which may then make any revision irrelevant, or even impossible. The reality is that there are high risks to such research when applied to the real world. If it were to fail, it may lose the chance for correction once and for all. This research must therefore be as prudent and objective as possible, but even so, certain limitations may still exist. For instance, one might argue that China's cyber warfare is still at the conceptual level as there is not a substantial body of evidence and groundwork to precisely prove the operation of

cyber warfare by a state, even though this warfare has been clearly visible within global politics for many years.

The primary aim of this research is to investigate how the development of cyberspace as a potential battleground challenges existing doctrines of military strategy through a case study of China's cyber warfare. The secondary research questions will be answered comprehensively through an in-depth, longitudinal examination of previous research as well as the study's own empirical case study. The common contentious limitation of a case study is to what extent the results can be generalised. The methodological details of the case study in this research will be explained further in Chapter Five.

For the ease of identifying any new findings, this research is divided into two main parts: an analytical framework and an empirical section, comprising six chapters in total. Firstly, the analytical framework of this research starts from a theoretical examination of cyberspace in Chapter Two, which lays out conceptually how cyberspace is developing into a potential battle space. Here, the nature of cyberspace and its features are presented and examined, and the four principles of cyber-territoriality are set out. It is hoped that these principles can form a theoretical tool to offer cyber actors a justification for dealing with disputes in cyberspace. Chapter Three focuses on modern Chinese strategy. The chapter proceeds from an investigation into the basis of strategy and an outline of traditional Chinese strategic culture, and leads into a discussion of the three transformations of Chinese strategy in the modern era. The constant guiding doctrine of People's War is explained in detail in this chapter, as well as its suitability for adaptation to cyber warfare. Chapter Four links the two previous chapters into an analytical framework, which will allow explorations of how China's cyber warfare is challenging existing modern strategy and how the doctrine of People's War can be adopted in the digital age. The case study is analysed empirically in Chapter Five, to indicate the current developments and deployment of China's cyber warfare. Finally, Chapter Six presents the conclusions of this research.

Through the examinations and analyses of the following chapters in this research, it is argued that:

1. The features of cyberspace present a strategic value for both state and non-state cyber actors. Actors are therefore likely to contend for the

dominance of cyberspace, which is accordingly transformed into a potential battleground.

2. The government of the PRC, a rising power in international politics, strategically shapes the integrated platform of cyberspace, consisting of various electronic environments, in order to enlarge its strategic value.
3. China's cyber warfare adopts the doctrine of People's War, a constant guideline of Chinese modern strategy that is perfectly suited for the potential battleground of cyberspace.
4. As a result, internet control and monitoring in China is not only employed for political purposes to prevent the Chinese people from accessing sensitive political information and to suppress opposition, but could also be a method of preparing and conducting cyber warfare by creating 'cyber warriors' and accumulating important information for the Chinese government. Meanwhile, the strategic value of cyberspace offers a condition far superior to any other medium for the rapid dissemination of information, conducive to the mobilisation of the Chinese people into 'online nationalism'.[11] However, online nationalism can be employed not only by the Chinese government for external political purposes, but also by the Chinese people themselves for internal purposes.[12]

[11] This term refers to nationalism communicated via various electronic media, such as emails, websites, instant messages, SMS, and mobile devices, and is employed in China's cyberspace to mobilise people and disseminate information on certain political issues. This will be discussed in Section 4.3.5 and Section 5.5.1.

[12] This argument will be developed in Section 5.5.1.

Chapter Two: Cyberspace as a Potential Battleground

The term cyberspace[13] was first coined by William Gibson in 1982 and came into wide use after the publication of his 1984 science-fiction work *Neuromancer*. (Benedikt, 1991:335) The term has been used frequently ever since. It seems, however, that what Gibson invented was not merely a single new word, but in fact a reference to a whole new world.[14] Unlike physical geographical battlegrounds, such as those of land, sea and air, cyberspace has become a virtual space in which states may present military power in a different manner. A recent US government report clearly emphasises the importance of security in cyberspace as a current critical issue of national security for all states worldwide.[15] Moreover, according to Ian West (2010), head of the Technical Centre at the NATO Computer Incident Response Capability (NCIRC), even though it has been acknowledged that the security of cyberspace is imperative for state security, existing research into cyberspace primarily focuses on the technical side, but fails to investigate more strategic aspects. It is evident, then, that academic resources still lack supportive theoretical concepts relating to cyberspace. In order to devise a comprehensive state strategy to secure cyberspace, it is first essential to comprehend both the features of cyberspace and how these features shape cyberspace as a potential battleground. This in turn is impossible to do without first assessing the nature of cyberspace. As Gregory Rattray (2001:79) points out, the nature of cyberspace as a battlefield must be understood in order to prevent or handle malicious attacks in this new realm of information systems.

Cyberspace is established upon a universal platform of information infrastructure which creates an unprecedented strategic condition by blurring the boundaries between the government sector, civil society, and private industry. Conducting operations on such an ambiguous battleground requires efficient

[13] Cyberspace refers to the virtual space in which communication occurs via computer networks. The term 'cyberspace' is a portmanteau of the words cybernetics and space. It can also be written as two separate words: cyber space.

[14] Interestingly, William Gibson's inspiration for the term 'cyberspace' came from watching youngsters playing video games. He observed that 'video game kids and computer users seem to develop a belief that there is some kind of actual space behind the screen, some place you cannot see but you know is there.' (Barnes, 1996:195)

[15] According to the US Congressional Research Report, published in 2009, cyber security is regarded as 'one of the most urgent national security problems facing the new administration.' (Rollins and Henning, 2009:1)

information capabilities to cope with the challenges of the uncertainty of combat. As Lance Strate (1999:3) highlights, cyberspace is a 'collective concept,' which can be defined by the diverse applications of a space associated with computers and telecommunications.

Cyberspace can be defined in a variety of ways through different dimensions and angles of analysis. However, though the dimensions of cyberspace may be altered, the intrinsic nature of cyberspace has not been changed since its creation. Compared with geographical fields, cyberspace is a relatively new realm, which represents not only a physical theatre but also a virtual domain with associated abstract concepts. Even though a large number of studies about the internet or cyberspace have been compiled, it can still be asserted that little is known about how cyberspace is structured and how it operates. Therefore, this chapter takes as its premise that there is a need to define and illustrate the features of cyberspace inherent across the government, civil society, and military sectors, which should begin with an examination of the nature of cyberspace to establish how its features may shape it into a potential battleground.

2.1 The nature of cyberspace

Although the term 'cyberspace' originally came from science fiction, for many of us cyberspace now forms part of our everyday routine. Since 1990, rather than considering cyberspace to be a manifestation of a video game, academia has begun to take cyberspace more seriously. This development is certainly closely related to the rapid commercialisation of the internet in the 1990s. Michael Benedikt (1991:122) defined cyberspace as a structure formed by an amalgamation of computer technologies such as both 2D and 3D graphic user interfaces, internet technology, virtual reality, multimedia, databases, and hyperlinks. He also ascribes a broad domain of physical space to the nature of the computer-sustained virtual world.[16]

Along with the technical development of computers and the internet, cyberspace seems to be becoming more concrete and the concept of cyberspace is continuously expanding. Cyberspace is not only a physical body of machines or

[16] Michel Benedikt also indicates that cyberspace is 'a new universe; a parallel universe created and sustained by the world's computers and communication lines. A world in which the global traffic of knowledge, secrets, measurements, indicators, entertainments, and alt-human agency takes on form: sights, sounds, presences never seen on the surface of the earth blossoming in a vast electronic night.' (Benedikt, 1991:1)

computer networks which store and exchange data via computer media, but is also a conceptualised space. Tim Jordan (1999:26) attests that 'Cyberspace has been conceptualised as a net, matrix, metaverse and, universally, as a place constructed out of information.' Mark Slouka (1996:2-6) claims that the critical impact of information techniques infiltrating society has led to the creation of a whole new society, namely cyberspace. He also stresses that cyberspace brings about the development of the so-called 'global brain' which generates a 'global sense,' referring to a manner of geographically unrestricted thinking.

In practical terms, according to the US governmental report *Cyberspace Policy Review 2009*, cyberspace is the 'interdependent network of information technology infrastructures, and includes internet, telecommunication networks, computer systems, and embedded processors and controllers in critical industries.' Some experts believe that 'Cyberspace is a domain characterised by the use of electronics and the electromagnetic spectrum to store, modify and exchange data via networked systems and associated physical infrastructures' (Hansen, Williams, Mills, and Kanko, 2008). Furthermore, Rattray (2001:17) argues that 'Cyberspace is actually a *physical domain* resulting from creation of information systems and networks that enable electronic interactions to take place.'

In terms of communication technology, as Eduard Babulak (2009:142) suggests, in the digital generation, cyberspace is 'collaborative', allowing us to communicate over long distances through sharing 'emotions' and 'non-verbal communications', and will feature what he terms advanced 'tele-commuting.' In Strate's theoretical discourse (1999:382-412) three conceptual orders of cyberspace are proposed. Within the second order of the three, he identifies three specific aspects: physical, conceptual and perceptual. According to these definitions, physically, cyberspace is 'the material base of computers, monitors, disk drives, modems, wires, and their users.' Strate (1999:412) indicates that, conceptually, some scholars claim cyberspace is 'the sense of space generated within the mind as we interact with computer technology', or more perceptually as 'the sense of space generated by the computer-user interface, through one or a combination of our senses.'

In summary, it can be argued that cyberspace is created upon a physical platform and forms a conceptual space via the spatial flows of information transmitted. Put another way, cyberspace is a space comprising telecommunication

networks which use either electronics or electromagnetic transmission and the internet to form a conceptualised space.[17] In order to comprehensively understand cyberspace, this research will address both its physical and conceptual aspects.

2.1.1 *Physical aspects: cyberspace as a technical field*

In recent years, the dramatic growth of internet usage has triggered an increasing interest in cyberspace, not only in personal business but also on a governmental level. Both the internet and cyberspace can be seen as social, cultural constructions, but it could be argued that there is a key difference between them in that the internet has a clear technical definition whilst the term cyberspace has become increasingly vague and drained of meaning. Cyberspace is a virtual world with different dimensions to the physical world. For example, previous physical state borders are largely meaningless and non-existent for internet users in cyberspace, which creates a certain strategic value, addressed in detail in Section 4.1. In addition, it has been stated that: 'Cyberspace is the total interconnectedness of human beings through computers and telecommunication without regard to physical geography,' and also: 'Cyberspace started to become a *de facto* synonym for the *Internet*, and later the *World Wide Web*, during the 1990s.' (Hildreth, 2001:1) Accordingly, cyberspace can be considered physically to be a combination of the internet and the World Wide Web (WWW); the former being a network which transmits information; the latter being storage which presents information. Historically, the internet is the extension of a government project in the Advanced Research Projects Agency (ARPA)[18] in the United States. The earliest ideas for a computer network, in 1962, were intended to allow general communications among computer users. The ARPA network (known as ARPANET) was first used by the US military and government in 1969. After the Cold War, the US government released the technique of ARPANET to academia and civil society as a whole. In the 1980s, Transmission Control Protocol/Internet Protocol (TCP/IP) became the standard protocol of communication for the

[17] This argument will be elaborated in the case study of China's cyber warfare through relevant empirical evidence presented in Section 5.4.

[18] ARPA (Advanced Research Projects Agency), under the Defense Advanced Research Projects Agency (DARPA) of the United States Department of Defense, was the world's first operational packet switching network, and the predecessor of the contemporary global internet. The packet switching of ARPANET was based on designs by Lawrence Roberts.

network. By 1994, only 8 countries had joined this network, but in 2009[19] the internet could be accessed in 195 countries. The internet has become the overwhelming backbone to global society, and is now a complex spatial system without obvious boundaries. The following statement reflects the definition of the term internet since 1995 according to the US Federal Networking Council (FNC):

> Internet refers to the global information system that:
>
> 1) is logically linked together by a globally unique address space based on the Internet Protocol (IP) or its subsequent extensions/follow-ons;
> 2) is able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite or its subsequent extensions/follows-ons, and/or other IP compatible protocols; and
> 3) provides, uses or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described herein.

It can be additionally noted that the function of TCP is to correctly disassemble and reassemble data through small packages on the internet from the side of delivery to the side of reception, and the function of IP is to arrange and lead flows of information to their exact destination through the networks' physical layers.[20]

In 1989, the British scientist Tim Berners-Lee developed the technique of the hyperlink. In a manner reminiscent of the complexity of a spider's web, this technique combines a diversity of formats such as text, image, audio and video into a document which can be requested and submitted by different functional

[19] World internet usage in 2009 is illustrated below:

Geographical regions	Internet users (million)	% of population
World total	1,734.0	25.6 %
Asia	738.3	19.4 %
Europe	418.0	52.0 %
North America	252.9	74.2 %
Latin America	179.0	30.5 %
Africa	67.4	6.8 %
Middle East	57.4	28.3 %
Oceania/Australia	21.0	60.4 %

This table is generated based on online information available from <http://www.internetworldstats.com/stats.htm>

[20] The 'networks' physical layers' refers to the Open System Interconnection (OSI) model, which defines a networking framework for implementing protocols in seven layers. Control is passed from one layer to the next, starting at the application layer in one station, and proceeding to the bottom layer, over the channel to the next station and back up the hierarchy. The seven layers, from top to bottom, are the Application, Presentation, Session, Transport, Network, Data Link, and Physical Layers. TCP/IP is the radical protocol for the Transport and Network Layers. (Edwards, 2009:346-349)

servers on the internet via the location of its web address. This crucial technique quickly became the foundation of the global information infrastructure. Since 1994, many facilities and techniques have been invented by private sectors, and accordingly governmental control faded away from this realm. (Castells, 2000:394-402) Currently, the relevant official standards and technical specifications governing the operation of the World Wide Web and the internet are organised by the World Wide Web Consortium (W3C), which is a non-governmental organisation. Given that W3C may be able to function without any state influence, a further question is raised regarding the manner in which a state may coordinate its governmental and private information infrastructures to exploit necessary strategy and reinforce security ability in the potential battleground of cyberspace.

As Lennard Kruger (2005:7) points out in his research report for the US Congress, 'To navigate the internet requires using addresses (and the corresponding names) that identify the location of individual computers.' Cyberspace, however, is a very interesting creation. Unlike the physical world, no one can certify how big cyberspace is, as its scale is dependent on different measurements, such as, for example, IP addresses, nodes, or the amount of information online. In cyberspace, each place is coded by one unique IP address. No matter whether there are computers connected to it or not, these so-called niches still exist per se. The terminal computers which are connected to an IP address are referred to in technical terminology as 'hosts', which can be clients or servers. In addition to this, there are two other kinds of niche. Those already assigned IP addresses but not connected to a terminal computer, such as those in an empty classroom on campus, are known as niches without cyberspace. Those which have not been assigned IP addresses are referred to as niches without geographical place. An IP address consists of four sets of numbers ranging from 0 to 255, each number set separated by a full-stop. Every computer on the internet has a unique IP address. However, there is also a textual address for locating a computer on the internet; the Domain Name, which corresponds to the numerical IP address. Even though IP addresses, such as 128.240.229.7 for example, provide a convenient and compact representation to specify a source and destination, it can be presumed that users still prefer to assign each computer a pronounceable and

memorable name, such as proxy.ncl.ac.uk[21] for example, which is the equivalent domain name. The internet Domain Name System (DNS) is a set of databases containing IP addresses and their corresponding domain names. Since each domain name is mapped to a particular numerical address, the DNS performs the transformation back and forth between domain names and IP address numbers. This is located in the uppermost layer, the Application Layer, in the networks' physical layers.

It is important to note that without IP addresses, the internet would simply not match its definition. However, it could function perfectly well without the use of the DNS. The existence of the Domain Name System is not because computers need it for any technical reason, but rather that the users – people – prefer such a format. Therefore, compared to the IP address system, the Domain Name System carries a characteristic of sociality, making it more significant for analysis. Technical development makes up only a small part of the whole history of the Domain Name System; instead, the primary focus, especially since 1990, has been on how to manage the system and who should have the authority to police its operation. Thus cyberspace cannot merely be analysed on a technical level, but must also be considered socially and politically.

Cyberspace is a space physically constructed by the Domain Name System, which combines the assigned IP addresses, servers, routers, and cables into a system which links up computers to form a critical infrastructure. Therefore, it is necessary to know how IP addresses and the DNS operate and how this affects cyberspace as a battlefield. As will be seen, this research argues that the domain identified by IP addresses can form a virtual territory, and a line connected by nodes of IP addresses can draw a boundary acting as a virtual border. This virtual border can be a real functional border dividing different 'territories' in cyberspace, so that the users inside a 'territory' cannot cross the functional border to go outside of this cyber-territory, and vice versa.[22] That is to say, computers and their

[21] In this domain name, 'uk' means the country of the United Kingdom; 'ac' means this address is related to academia (some countries use 'edu' instead); and 'ncl' is an abbreviation for Newcastle University. Using the alphabet to represent numbers is not a new idea. Before the Domain Name System, people had already used the alphabet to individualise telephone numbers, such as '1-800-THECARD.' Its history can be traced back to the 1920s when the US telephone system relied on local-exchange telephone numbers, though the alphabet was then used in a slightly different context.

[22] An IP address can be allocated to a geographical location via relevant information such as longitude and latitude. Therefore, a network domain, which might be a virtual cyber-territory, can in fact be related to geographical territory.

users could be protected from threats arising outside their cyber-territory; indeed, people inside one cyberspace territory may even be prohibited from connecting to outside networks.[23]

As described above, the Domain Name System relies upon the system of IP addresses. Before the use of TCP/IP, which began in 1983, every computer had its own name or nickname, and every host on the net had its own name-address table. As Cricket Liu and Paul Albitz (2006:11-32) explain, foreseeing that not every host would be able to include all internet hosts in its name-address table in the future, in RFC 799[24] D. L. Mills (1981) proposed a hierarchical name-space partitioning, based on the geographic locality of hosts, which would solve this issue and also geographically re-territorialise cyberspace. He invented a topological map covering the space of all internet addresses with a set of so-called 'name domains.' Later, in RFC 819[25], Zaw-Sing Su and Jon Postel (1982) proposed that internet names should form a tree-structured administrative dependent, rather than a strictly topological hierarchy depending on geographic locations. In addition, they proposed to establish a Name Service, which would be a network service providing name-to-address translation, and a naming authority which could assign simple names and ensure proper distinction between these names. Furthermore, in RFC 882 and 883, Paul Mockapetris (1983) suggested further technical developments in the construction of cyberspace to resolve three crucial problems in the network system. Firstly, as the application of the network grew, the number of resources, the number of locations for resources, and the diversity of such an environment caused formidable problems. Secondly, the ARPANET illustrated these size-related problems. ARPA internet was a large system and was likely to grow much larger. The need to map between host names and ARPA internet's addresses was beginning to pressure the existing mechanisms. The final and most serious problem was related to computer mail.

[23] For instance, as Jens Damm and Simona Thomas (2009, 120-121) point out, the Chinese government can technically prohibit the internet users inside the network domain (cyber-territory) of Mainland China from surfing some outside websites through the use of a censorship mechanism.

[24] RFC is the abbreviation of Request for Comment. RFC is a series of documents published by the Internet Engineering Task Force (IETF) describing methods, behaviours, research, or innovations applicable to the working of the internet and internet-connected systems. These documents discuss many aspects of computing and computer communication focusing upon networking protocols, procedures, programmes, and concepts. Even though RFC is offered as suggestions rather than requirements, the IETF adopts some of the proposals published in RFCs as internet standards. (Bradner, 1996)

[25] RFC 819 is noted as a key development in the structure of computer addressing for the internet.

When mail system technicians realised the impossibility of centralising mailbox names, they created an increasingly large and irregular set of methods for identifying the location of a mailbox. Some of these methods involved the use of routes and forwarding hosts as part of the mail destination address, forcing the mail user to comprehend multiple address formats, the capabilities of various forwarders, and ad hoc tricks for passing address specifications through intermediaries. In order to solve these problems, RFC 882 pinpointed the conceptual framework of the domain system. RFC 883 discussed further the implementation of domain name servers and specified the format of transactions.[26] Both of them outlined the indispensable principles associated with domain names and their use for further network designs.

Another significant document is *Domain Requirements* RFC 920. In RFC 920, J. Postel and J. Reynolds (1984) suggest an initial top-level domain name. Rather than a suggestion, Postel and Reynolds (1984) indicate that 'this memo is a policy statement on the requirements of establishing a new domain in the ARPA-Internet and DARPA research community.' The top-level domain name was divided into three: 'Temporary,' 'Categories,' and 'Countries' as below:

Temporary:

ARPA = current ARPA-Internet hosts.

Categories:

GOV = Government; any government-related domains meeting the second level requirements.

EDU = Education; any education-related domains meeting the second level requirements.

[26] The solution has three major components: (Mockapetris, 1983)

1. The *Domain Name Space*, which is a specification for a tree structured name space. Conceptually, each node and leaf of the domain name space tree represents a set of information. Query operations are attempts to extract specific types of information from a particular set. A query names the domain name of interest and describes the type of resource information that is desired.
2. *Name Servers* are server programs which hold information about the domain tree's structure and sets of information. A name server may cache structure or information about any part of the domain name tree, but in general a particular name server has complete information about a subset of the domain space, and can point to other name servers that can be used to lead to information from any part of the domain tree. The parts of the domain tree for which name servers have completed information are called 'zones;' a name server is an 'authority' for these parts of the name space.
3. *Resolvers* are programs that extract information from name servers in response to user requests. Resolvers must be able to access at least one name server and use that name server's information to answer a query directly, or pursue the query using referrals to other name servers.

COM = Commercial; any commercial-related domains meeting the second level requirements.

MIL = Military; any military-related domains meeting the second level requirements.

ORG = Organisation; any organisation-related domains meeting the second level requirements.

Countries:

A two letter code identifying a country according to the ISO 3166 Standard of 'Codes for the Representation of Name of Countries.'

These divisions are very important. According to RFC 920's specifications, domain names are available from network service providers, and are organised in accordance with the different categories. The change, using the name of categories defined by different aggregations of similar organisations and 'free of undesirable semantics,' (Postel and Reynolds, 1984) is a critical point, which made cyberspace a social territoriality open to the development of the DNS.[27] In addition, for people, a domain name, such as www.ncl.ac.uk, reads from left to right, and also from most specific to least specific. The first field 'www' is the name of the host computer. The next field, here 'ncl' is the third level domain name. The third field 'ac' is the Second Level Domain (SLD) name. The very last field 'uk' is the Top Level Domain (TLD) name, which in this case is also a country code domain name. However, for computers operating under the Domain Name System, it is interpreted from right to left and from least specific to most specific. Thus the country code will be identified first and so on.

There are five main components in the Domain Name System. They are: local user's computers, local Internet Service Provider (ISP) Name Servers, Root Name Servers, Top Level Domain Name Servers, and Second Level Domain Name Servers. The whole process can be schematised as follows: (Bayne, 2008:631)

[27] As Postel and Reynolds (1984) define: 'Domains are administrative entities. The purpose and expected use of domains is to divide the name management required of a central administration and assign it to sub-administrations. There are no geographical, topological, or technological constraints on a domain. The hosts in a domain need not have common hardware or software, nor even common protocols. Most of the requirements and limitations on domains are designed to ensure responsible administration.'

Local computer → Local ISP Names Server → Root Name Server → Local ISP Names Server → TLD Name Server → Local ISP Name Server → SLD Name Server → Local ISP Name Server → Local computer → Destined Host (www.ncl.ac.uk)

In addition, with the help of Cache[28], after the query of the destined Host (www.ncl.ac.uk), the local ISP Name Server will, within a certain period of time, help any local ISP Name Server to quickly resolve any similar queries from other computers within the same local ISP. However, Cache is a double-edged sword, since this benefit also provides space for manipulation by computer viruses.

On the other hand, as mentioned previously, the Domain Name System cannot be seen as a purely technical field. The processing time of the DNS is not faster than that of using an IP address. Under the structure of the DNS, in order to connect to a host which is located in a different Top Level Domain, it is necessary for the system to make queries four times and inter-communicate eight times before the local computer can finally connect to the remotely located destined Host, unless this information already exists in the Cache. Certainly, not every connection needs to undergo such a complicated process. Connecting to a destined Host in the same TLD is much simpler. However, in other cases, for example, if connecting to a remote destined Host through the Third Level Domain as well as a different TLD, there could be even more complicated inter-communications. Though the entire process normally take just a few seconds, if there were no Domain Name System and each computer were connected to other machines only through the use of IP addresses these 'few seconds,' could be saved, not to mention the social costs for maintaining the stability of Name Servers. Performance and efficiency do not seem to have been the first priority here.

There are further networks in cyberspace other than the internet: according to the definition of cyberspace, there are three more networks, which are the telecommunication, electronic and electromagnetic networks. Due to the latest developments in technology, these communication infrastructures are also constructed upon the TCP/IP system, regardless of whether they are space-based,

[28] Cache is a hardware component that improves computer performance by transparently storing data so that future requests for that data can be retrieved faster. The data that is stored within a cache might be values that have been computed earlier or duplicates of original values that are stored elsewhere. However, this means that a client who is requesting data from a system is not aware that the cache exists, and also does not know exactly where the provided data comes from.

airborne, or wireless networks. Thus different weapons systems, such as ballistic missiles on land, warships in the sea, and aircraft in the air, can be integrated into this infrastructure in order to control and command them with first-hand information. According to the *US Global Information Grid Architectural Vision*[29], for instance, the newest version of the Global Information Grid (GIG) will integrate the telecommunication, electronic and electromagnetic networks in accordance with the primary interface, standards and guidelines of networks such as TCP/IP, Physical Communication Links, Access Protocols and Routing Protocols. Through cooperating with satellites, this GIG architecture can provide advanced communication, control, and command through different formats, such as voice, metadata, imaging, and data exchange, in order to deploy further operational actions. On the one hand, this is undoubtedly a military advantage as it can reinforce military capability in the future battlefield by integrating different weapon systems into one information system. On the other hand, it could also become a vulnerable area and an attractive attack target for adversaries. In addition, this military system shares the same information and telecommunication infrastructure with civil society in cyberspace.

For the security of cyberspace, as Postel and Reynolds (1984) point out, 'An individual must be identified who has authority for the administration of the names within the domain, and who seriously takes on the responsibility for the behaviour of the hosts in the domain, plus their interactions with hosts outside the domain.' IP addresses in cyberspace are allocated by the Internet Assigned Numbers Authority (IANA), which is the body responsible for coordinating some of the key elements that keep the internet running smoothly. (Edwards, 2009:353) While cyberspace has become a potential battleground in terms of international politics, there are some private organisations, such as W3C IANA, and ICANN[30],

[29] 'Global Information Grid Architectural Vision' describes the aims – and, thereby, provides the direction – for the development of the Global Information Grid (GIG) capabilities that will support the strategy of the US Department of Defense for their missions, operations, and functions in future cyber warfare. (Global Information Grid Architectural Vision, 2007)

[30] ICANN, the Internet Corporation for Assigned Names and Numbers, was established as a Californian not-for-profit public benefit corporation in 1998. Its creation was invoked by the US Department of Commerce during a public proceeding in 1997–1998 that invited international participation. ICANN took over the centralised coordination of the internet's domain name and address assignments. (Mueller, Mathiason, and Klein, 2007:237-254) In addition, this institution also cooperates with private sectors for technical support.

serving as transnational political actors[31] to police the global operation of cyberspace and secure its functions. However, as long as the internet functions as an information network inextricably linked by technical complexities, the conditions for actors to pose a threat will remain. In addition, the feature of anonymity in cyberspace still remains even though the TCP/IP is traceable to a geographical location. This will be discussed in greater detail with regard to China's case in Chapter Five.

2.1.2 *Conceptual aspects: cyberspace as a social field*

Instead of relying on a simple dichotomy of the physical and conceptual aspects of cyberspace, many scholars have begun to focus on the relationship and interaction between cyberspace and real society. For instance, as Castells (1996) points out, the network is not only an organisational principle of cyberspace, but also the principle of organisation overall, even though this principle is still unable to integrate the world in which we live as a whole. He further argues that what we are trying to understand is not the culture of virtual reality but the culture of real virtuality in the post-modern world. David Hakken (2003:11) uses the new term 'cyborgs@cyberspace' to link the abstract concept of cyberspace with real society by its material basis or carriers, namely cyborgs.[32] Hakken also points out that the wide belief that there is a computer revolution in our world is just a myth, arguing that the role of advanced information technology in societal formation is better understood symbolically or ideologically than in technological terms. In terms of human history, information in cyberspace which can be transformed into knowledge for humans is more important than the computer technology of cyberspace. (Hakken, 2003:141-142) For example, Deleuze (1990) noticed that after the Second World War, a new kind of power emerged and rapidly began dominating our societies; this new power is based on information technology and computers. He terms this new form of society 'control society' that 'no longer

[31] States and governments in the world have equality of statehood by law. However, due to the lack of political similarity between countries, transnational actors must exist and must now increase their authority in order to deal with disputes between states. In addition to state and non-state actors, it could be suggested that private groups, companies, and national minorities in each country should engage with transnational actors. (Baylis and Smith, 2005:427-430)

[32] Cyborg is a portmanteau of cybernetic and organism. The term was coined in 1960 when Manfred Clynes and Nathan Kline used it in an article about the advantages of self-regulating human-machine systems in outer space. However, David Hakken uses the idea of 'cyborgs@cyberspace' (cyborgs at cyberspace) to refer to the fact that a computer-based information infrastructure with named automated information technologies can reproduce information in cyberspace into knowledge for people. (Hakken, 2003:141)

operates by confining people but through continuous control and instant communication.' (Deleuze, 1990:174) As referenced by Manuel Castells (2000:15-18), Michel Foucault points out that power and social forces are incorporated obscurely into practices or structures which everyone takes for granted. It can be argued that it is the same for cyberspace. As Lawrence Lessig (1996) claims in his *Reading the Constitution in Cyberspace*, cyberspace is governed by three sorts of constraints. Just as in the ordinary physical world, cyberspace is constrained by law, social norms, and rules. However, there is another set of peculiar constraints in cyberspace: rules and laws which are embedded into the software itself. 'Rules, for example, that require a password upon entry into a system; or that require a filename no longer than thirty characters; or that require a verified returned address on a particular e-mail message; or that allow the places one's web browser has visited to be reported to another web browser.' (Lessig, 1996:869-910) These constraints are not constraints that one can choose to follow or ignore, regardless of whether or not they are welcome. As Lessig (1996:32) further indicates, 'While regulation in real space is primarily regulation that relies upon cooperation of the individuals who live under the regulation, regulation in cyberspace can be something different. The code in cyberspace – the software – can enforce its control directly.' Indeed, a cooperative mechanism behind the software itself is necessary in order to secure cyberspace, an arena in which civil society, the government, and the military are all mixed together. This cooperative mechanism not only involves extensive negotiations between government and private sectors; the security of cyberspace also rests on 'active cyber citizenship as a resilient model that can manage this new and challenging security environment.' (Harknett and Stever, 2009) Internet users thus play a crucial role in cyberspace.

The first level of Strate's (1999:382-412) classification of the three levels/orders of cyberspace, mentioned previously, is concerned with the ontology of cyberspace composed of 'paraspace' or 'nonspace' and 'spacetime.' While paraspace, or nonspace, refers to a fictional, imaginary, or unrealised space – a seemingly paradoxical space that is a fake space or a simulation – cyberspace can be seen instead via different dimensions, which involve relationships between humans and computers, between humans via computers, and between computers themselves. However, instead of asking what cyberspace is, a more profound

thing is to understand what kind of environment cyberspace produces; in what precise environment something may exist or occur. Interestingly, both the 'virtual' and the 'real' in cyberspace can actually be defined as either real or virtual, but the true main issue should be how they connect and interact with one another, as well as under which precise conditions cyberspace is considered to be real, and under which conditions virtual. Cyberspace is not totally independent from the world in which we live. Perhaps, cyberspace is a different environment from our 'real' society, but the events in cyberspace are still, in fact, events occurring in the real world. As Bayne (2008:629) stresses, 'cyberspace is the operating environment,' and 'through exchange of information, goods, and services, this environment is simultaneously physical (tangible and real) and present in geospace.'

Castells (2000) further proposes the concept of 'a space of flows' to replace the former notion of 'a space of place'; conceptually, cyberspace is formed by spatial flows of information. Castells (2000) also claims that society is constructed from certain flows, including flows of information and flows of technology which form a 'network society.' He (2000:442-445) defines the space of flows as having three different layers: 'The first layer, the first material support of the space of flows, is actually constituted by a circuit of electronic exchanges (micro-electronics-based devices, telecommunications, computer processing, broadcasting system, and high speed transportation – also based on information technologies),' and the second layer is a 'space of flows constituted by its nodes and hubs.'[33] These nodes and hubs coordinate all the local places integrated into the network. Consequently, the concept of cyberspace can also be represented in layers of spaces of flows. Information flows through cyberspace, making use of the hardware network to form a vital infrastructure of flows based in the physical world. Finally, the third layer of 'the space of flows refers to the spatial organisation of the dominant, managerial elites.' Castells (2000:446) believes that 'elites are cosmopolitan, people are local.' The space of power and wealth is thus reflected all over the world, but people's life and experience are rooted deeply in

[33] 'The space of flows is not placeless, although its structural logic is. It is based on an electronic network, but this network links up specific places, with well-defined social, cultural, physical, and functional characteristics.' (Castells, 2000:443) As Castells (2000) also indicates, some places are information exchangers, i.e. communication hubs which mutually coordinate. Some places are the nodes of network society which link up the locality with the whole network.

local places through culture and history. However, due to the 'nodes and hubs' linking local people, the populace in cyberspace has become a crucial power which can generate, distribute, and receive information in cyberspace's network society. In addition, people can be mobilised in this space to produce an influence based on a political purpose, as will be discussed in further detail in later chapters.

As a result of this network society, a virtual world can be formulated which represents the number of internet hosts[34] distributed worldwide. This virtual world may present a wholly different terrain to the geographical one, since the number of internet hosts is not necessarily in equal proportion to the size of the territories of their respective states, nor the extent of the state's power. It may thus be assumed that information will flow from regions with a high density of information to regions with a low density, representing a flow of information as a moving power based on constant requests for information, made due to the intrinsic curious nature of human beings. Timothy Luke (1997:9) claims that the human will express 'its bit forms on cyberspace/infoscape/mediascape of telemetricality,' as a result of natural human nature; humans imprint their personal nature onto the virtual flows of cyberspace through demand for this digital information. Alongside this flow of information from state to state via cyberspace, invisible impacts and intrusion may also be encountered since this flow can possibly form a type of power.[35] Information flows are processed and distributed by internet hosts. According to the ranking of the number of internet hosts per state, it can be concluded that a small state is not necessarily equal to a small power in cyberspace if information can represent power. In addition, recent research identifies a partial map of the internet (Figure-1, OPTE 2005) based on data from 2005 by the OPTE Project. In this graph, each line is drawn between two nodes which represent two IP addresses. This graph can visually portray the potential virtual battlefield of

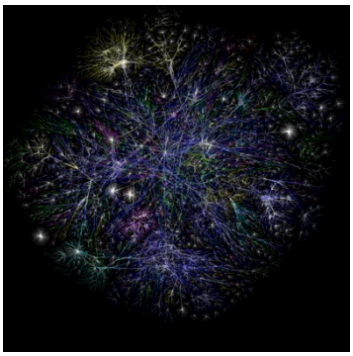

Figure-1 (OPTE, 2005)

[34] The ranking of the number of internet hosts (an Internet Service Provider's (ISP) computer Server is a host) per state has been generated as statistics. In the 2009 rankings, for example, in terms of geographic territory, Taiwan is very small at 138th in the world; however, its internet hosts ranking is 15th in the world. If information can be harnessed into power in cyber-territory, this reinforces the strategic value for states of asymmetry in cyberspace.

[35] This power means a state is potentially able to influence the ideology of another state's people via disseminated information , such as propaganda.

cyberspace. Furthermore, Figure-1 is a scale-free graph,[36] and recent research points out that 'a focused attack on a scale-free network is the most productive.' This scale-free graph may therefore show where the points of vulnerability in cyberspace might lie. (Repperger, Haas, McDonald, and Ewing, 2008) Meanwhile, in order to understand the changing of the 'world political map', O'Tuathail (1999) investigated the impact of instant communication and information flows. His research has contested various discourses associated with the transcendence of territory during the growth of cyberspace due to the features discussed in the next section. It is therefore worth investigating how relevant theories of international relations contend that cyberspace will be a new arena where states compete to expand their power, replacing geographical battlegrounds.

2.2 The features of cyberspace as a potential battleground

The actors in the potential battleground of cyberspace are not necessarily only states, but may also be non-state actors such as non-government organisations and even private companies. Unlike the modern state system, in which a war is usually waged by a state, it is possible that an attack in cyberspace may be conducted by just one individual. If traditionally a war could be identified based on whether a state's territoriality is intruded, the same proposition can be reflected onto cyberspace. That is to say, war could be defined based on encroachment onto virtual territory in cyberspace. In order to examine how this 'cyber-territory' can be invaded, it is indispensable to establish some principles of cyber-territoriality for further investigation.

The digital age is manifested not only in civilian circumstances, but also on the military field. Recent research indicates that 'the sophisticated information technologies on which the best armed forces, and all modern societies, now rely pose an attractive target to potential adversaries.' (Moran, 2010:139) It is consequently highly likely that cyberspace is developing into a potential battleground in the digital age. The internet, rapidly expanding in scope, constitutes a new theatre for belligerent politics, further transforming cyberspace from a societal and political platform into a potential battleground. This will affect national state security as traditional borders cannot protect a state's territory from cyber

[36] A scale-free graph such as Figure-1 means that a power-law relationship would exist for the same plot. As new links are added, the most highly connected nodes are more likely to gain additional links, which somewhat reflects the concept of the 'rich getting richer.'

threats, and government bodies no longer dominate communication systems and relevant techniques in cyberspace. (Schwartz, 2001) So why exactly is cyberspace considered a potential battleground? And what differences are there with traditional battlegrounds in terms of warfare? To begin with, it is contestable whether military strategy based on geographical battlegrounds can fit the battleground of cyberspace. After the invention of the internet and the World Wide Web, states began to build up their information infrastructure for both domestic and international affairs. States have started to compete with one another for dominance in this potential battleground, and it can be expected that a parallel virtual landscape will be drawn in cyberspace which will represent state territoriality differently to that of the physical world. Traditional thinking about the existing doctrine of military strategy will consequently be challenged based on this new proposition. In addition, state policy regarding warfare and security will need to be re-formulated, to respond to new military strategies which may well be generated to match this new battleground. Therefore, states need to seek a comprehensive strategy to formulate the best approach to secure cyberspace, which may be identified through investigation of several of its key features.

2.2.1 *The permeability of cyberspace*

In the territorial state system, in addition to natural barriers, fortification and fortresses constituted important elements in the border surrounding a state's territory. Correspondingly, servers and routers also play the same role as functional borders in cyberspace to prevent malicious attack from outside. Geographical barriers, borders and fortification, acting as a hard shell, would formerly have represented the impermeability of the state. However, this cannot be said for the equivalent functional borders in cyberspace due to the key feature of infiltration. Conceptually, cyberspace is formed by spatial flows of information reminiscent of liquid, resulting in the key feature of infiltration. Through an examination of the characteristics of cyberspace, Cahill (2003:101) concludes that all systems allowed input are vulnerable since theoretically any computer network can be infiltrated and attacked; geographical distance from the target is almost irrelevant. Consequently, any computer system allowing input can be a target of attack for cyber infiltration, and the feature of infiltration in cyberspace will therefore challenge defensive approaches at a strategic level.

A cyber attack is essentially the use of computer viruses to intrude upon the computer systems of an adversary target. Vice versa, the defensive approach is to prevent such viral infections from entering the computer systems which support state information infrastructure. Cyber attacks are conducted based on certain dimensions: one such dimension is information infrastructures such as TCP/IP and network structures; the other is techniques used in cyberspace such as firewalls and encryption/decryption. In addition, an attack may include various purposes of offence, defence, and even deterrence. It is thus essential to investigate features such as permeability and impermeability, which would influence functional borders in the battleground of cyberspace. Regardless of whether or not an approach is offensive or defensive, all approaches pertain to certain operational actions associated with tactical level methods and techniques, such as tracing a hacker, decrypting a code, reinforcing a firewall against attacks, even conducting counter-attacks, and so on and so forth. However, in addition to existing doctrines at a tactical level, relevant guidelines at a strategic level are indispensable to tackle the issue of cyberspace as a battleground. Traditional warfare carries risks because all humans inhabit the same planet, and any attack across a state's borders may endanger them. In terms of cyber warfare, humans do not just exist alongside one another inside state borders, but are actually all making use of the same cyberspace which may potentially become a battleground. Cyberspace combines many different computer networks which are all inter-connected. These computer systems are susceptible to infection from computer viruses whenever the systems are not restricted to read-only. Once a computer virus has been created it will exist in cyberspace to automatically infect computer systems from one state to another state without purpose or discrimination, since these different states share the same cyberspace as the transmitting medium. It may thus mirror the way some biological viruses can transmit mutually between humans and animals as both biological bodies are susceptible to infection.

2.2.2 *Three sectors sharing cyberspace: civil society, government and military*

Historically, civil networks are derived from ARPANET, which was a research network for military purposes. Cyberspace, which technically comprises transport and physical layers and was also derived from ARPANET, potentially binds together the military, government and societal sectors, as they are all constructed

on the same virtual information platform. This has caused the boundary between the battlefront and the rear to disappear. In addition, though attacks in cyberspace are waged by actors in a state's territory, these actors are not necessarily acting for that particular regime or state. In sum, cyberspace manifests itself not only in the military field but also in civilian circumstances, as both share the same information platform. This feature of cyberspace means that as a battlefield, it falls into the category of irregular warfare, as Freedman (2008) stresses in his research. He also points out that the battlefield is transformed from one which is separated from civil society to one which is combined with civil society. (Freedman, 2008:597) Furthermore, as Thomas Cahill (2003:100) reports, Chinese senior Colonel Wang clearly stated that conducting an attack against a state's civilian network, including, for example, financial transactions, telecommunications, media networks, and traffic dispatching systems, could entirely paralyse the enemy, causing social panic which can lead to political disaster. Thus, in terms of cyber attacks, the division between the battlefront and the rear is no longer clear; as such, existing military doctrines based on this division must be challenged.

Though the design of information infrastructure may vary across states, the so-called Open System Interconnection (OSI) model is a world-wide standard which defines a networking framework for implementing protocols in seven layers, which are, from top to bottom, the Application, Presentation, Session, Transport, Network, Data Link, and Physical Layers. In addition, TCP/IP is the radical protocol for the Transport and Network Layers of the OSI in all sectors. Therefore, for instance, both the US Network-Centric Warfare[37] and Global Information Grid, which are the most advanced information architecture for military operations in the world, operate on a so-called 'Convergence Layer,' which is established upon the same Transport Layer and Network Layer shared by civil infrastructure, in order to connect various networks and telecommunications. (Department of Defense, 2007) In this way, dominant capability in this battlefield can be increased whilst the ability of securing the civil information infrastructure can be reinforced. The relations between civil society, government, and military are shown in Figure-2 below.

[37] Network-Centric Warfare (NCW), though originally coined by the US military, is now also a new concept in European military affairs.

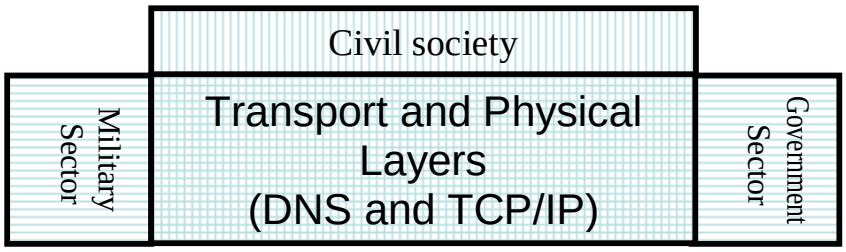

Figure-2: Researcher's own

In this figure, the bold lines between the different areas can be assumed to be servers, such as proxy servers and web servers with firewall or encryption/decryption, acting as an inspection mechanism in order to monitor communication and information exchange between the three sectors. However, all of them share the same infrastructure: the Transport and Physical Layers constructed by the DNS and TCP/IP.

2.2.3 *Asymmetry and vulnerabilities of cyberspace*

Cyberspace has become indispensible for modern human lifestyles across the world, but the features of cyberspace mean conditions of asymmetry and vulnerability are created.

On traditional battlegrounds, the scale of warfare, identified by the size of the battlefield, the manpower involved, and the causal destruction, may be limited geographically, whereas the exponential growth of cyberspace presents a very different scenario. For instance, according to The Office for National Statistics in the UK, in 2008 65% of households in Great Britain had internet access, numbering 16 million in total – up 1 million from just the year before.[38] Due to this steep rise in internet usage, people are already becoming accustomed to dealing with their affairs in virtual cyberspace instead of in a physical environment. This covers banking, marketing, shopping, communication and suchlike. The Office for National Statistics (2008) also points out that: 'Use of the Internet by both consumers and businesses has expanded rapidly in recent years. For example, the latest National Statistics Omnibus Survey shows that in July 2005 over 60 per cent of adults in Great Britain used the Internet, and results from the e-commerce survey show that in 2004 over 64 per cent of all UK businesses had Internet access. Together with this expansion in Internet use, there has been an

[38] If internet use in a relatively developed country like the UK can rise so substantially, as the trend for expansion of cyberspace continues, developing countries have even more potential for a massive rise in usage.

increase in spending over the Internet.' (Wallis, 2006:2) The range of functions relying on cyberspace is expanding with each passing day. For instance, the fundamental sectors of state such as agriculture, electricity and water supply, defence, government administration, information and telecommunication, public transportation, banking and finance, mail systems and goods supply chains and so on all operate via cyberspace.

However, as the Chinese proverb states: *while water can carry a boat, it may also capsize it*. That is to say, whilst a state gains great benefits from relying heavily on cyberspace in terms of these critical national infrastructures, thus being 'carried', this very reliance means there is more risk of being 'capsized' if cyberspace is adversely affected. State reliance on cyberspace offers an attractive target for adversaries, since many attacks, crimes and terrorist acts can be generated through the medium of cyberspace. Due to the reach of information technology in the digital age, any individual may be able to conduct cyber attacks or simply spam junk emails to cripple computer servers. This makes the virtual field of cyberspace much more vulnerable than a traditional territory, which is protected by physical borders which enemies cannot overcome so easily. Cyber attacks can leap over state border inspections to create damage to information infrastructure. Put simply, cyberspace offers a feature of asymmetry beneficial for cyber attackers. As this asymmetry and vulnerability are caused by the technical features of cyberspace, it is essential to understand the physical construction of cyberspace in order to prevent potential threats.[39] Furthermore, as Paul Virilio (2000) indicates in his discourse on dromology, the speed at which something happens may change its essential nature, and that that which moves with speed will come to dominate that which is slower. 'Whoever controls the territory possesses it. Possession of territory is not primarily about laws and contracts, but first and foremost a matter of movement and circulation.' (Virilio, 2000)[40] This view reinforces the argument that the speed of movement in cyberspace leads to further vulnerability.

[39] Please see Section 2.1.1.

[40] This is from an interview with Paul Virilio entitled '*The Kosovo War Took Place in Orbital Space*' in 2000. He believes that the Kosovo War largely bypassed geographical territories. This war is generally acknowledged as the first war ever fought in cyberspace. (Cavelty, 2007:73)

2.2.4 *A non-state space: anonymity of actors*

As recent research indicates, the speed and anonymity of cyber attacks make the actors indiscernible, whether they are terrorists, criminals, nation states or even just individuals carrying out random malicious attacks. (Kelly, Raines, Baldwin, Mullins, and Grimaila, 2008) In traditional warfare, an enemy can be recognised by its visible hostile military action, and the target of attack is usually a regime or a state. According to Schmitt's (1996) definition, mentioned in the Introduction, in human history enemies could generally be identified as unknown people or strangers, and existentially deemed to be something 'different'. Moreover, in a conventional war, the enemy becomes the public enemy, because everything that has a relationship to a collectivity of humans, particularly to a whole nation, becomes public by virtue of such a relationship. This perspective posits that hostility and the public enemy are crucial prerequisites in the concept of warfare. Even in the atomic age, the threatened use of nuclear weapons was an obvious presentation of certain hostility towards other states. However, in cyberspace, for any individual or group, the existence of the enemy is indiscernible. Thus, identifying hostility or the enemy is a crucial factor when attempting to secure cyberspace. In addition to the existence of an enemy, recognising a conflict of armed forces also makes it possible to discern what can be classed as a war. However, the actors who produce threats or even launch attacks in the battleground of cyberspace do not necessarily identify with a regime or a state. Cahill (2003:101) proposed two categories of actor in cyberspace, which are 'intentional cyber actors (I-actors)' and 'unintentional cyber warfare attack (UA).' He interpreted that the former intentionally wage war in cyberspace, affecting national security, and may be identified as cyber troops or cyber forces; the latter refers to non-malicious provocations which may not be intended to attack states through cyberspace. (Cahill, 2003:101) The features of cyberspace increase the ambiguity of hostility in such a battlefield. This research will argue that the way in which the existence of an adversary is discerned challenges modern strategy in the potential battleground of cyberspace.

It is thus very difficult to identify an attack waged in cyberspace, and it is just as difficult to define it according to the international legal environment. Singer (1972:19) stresses that international war is a military conflict occurring between national entities. In war, one of the actors must be a state and the number of deaths

no less than one thousand. In terms of an attack in cyberspace, a problem thus arises as there could be no immediate physical 'casualties' in a cyber attack. Existing definitions, based on the features of conventional war, may not easily match the battlefield of cyberspace in the digital age. The world is faced with a 'legal vacuum'[41]: national or international laws cannot impose justice or prevent transnational hostile actions in cyberspace; a further problematic issue is how it will be possible to define a true war based on existing law in order to justify legal defensive action in cyberspace.

2.3 The metaphorical 'territoriality' of cyberspace

Traditionally a state is protected inside a geographic territory surrounded by physical borders – natural barriers such as rivers, oceans, straits, mountains, and special terrain. These boundaries also distinguish the state's territory and determine its territoriality. In general territory in the modern state system was protected by borders lined with fortresses and fortifications to form a 'hard shell' (Herz, 1962).[42] However, in the atomic age, destructive weapons perhaps changed such territorial thinking as nuclear power shattered all previous conceptions. This may well occur again as a result of cyber warfare in the digital age, since the geographical protection of a state is far removed from cyberspace. For instance, research points out that any fresh meat passing the physical border into a country will be inspected, but a malicious attack via cyberspace could be transmitted unchecked across 20 borders by the click of just one button (Nykodym and Taylor, 2004). As the virtual 'territory' of cyberspace is shaped differently to the physical world, traditional borders cannot ensure state security against cyber attacks; instead, each state needs to formulate new strategic approaches to guard its relevant surroundings. However, cyberspace is also a space like land, sea and air. States or non-state actors can interact and communicate with one another through these spaces, and share the resources arising from them. As David Fahrenkrug (2008:135) argues, strategists often make the big mistake of erroneously focusing just on information, and not on cyberspace itself – the platform which bears the information. Fahrenkrug provides

[41] Since the onset of cyber-terrorism, it has been questionable who is responsible for the content of policy in cyberspace. (Cavelty, Mauer, and Krishna-Hensel, 2008:101-108)

[42] In addition, Herz also provides an example from Mencius, an ancient Chinese philosopher, to reflect the condition of territorial security. Mencius provided guidance for the governor of a small state about a thousand years ago, advising: 'Dig deeper your moats; build higher your walls; guard them along with your people.' (Herz, 1962:107)

the example of sea as a modern line of communication for states. It is far more important to securely maintain this line of communication than to protect the goods transported through it. He goes on to extrapolate that instead of protecting the information itself, securing cyberspace as a domain, where information is stored, transferred, and modified via a computer system, should be the aim of theory and strategy. (Fahrenkrug, 2008:141) Unfortunately, according to Hansen (2008:43), although the US Joint Chiefs of Staff approved the definition of cyberspace and recognised that it was a potential battleground as early as October 2006, military doctrines relating to cyber warfare still remain uncertain. It is therefore crucial to create guidelines for the identification of cyber warfare in order to clarify operational doctrine for the battlefield.

What's more, conceptual boundaries, such as proxy servers acting as functional borders, are essential in cyberspace for actors to recognise respective ownership, as actors may include states, non-state organisations, private companies and even individuals. In other words, it could be constructive to establish a conceptual 'territory' for each actor in cyberspace, so that the actors can demarcate their zone of responsibility and proclaim their 'authority', which may imply equivalence to 'sovereignty'. Servers, routers and network protocols can be employed technically as functional borders to form this corresponding 'territory', as well as protecting against attacks in cyberspace. This research argues that cyberspace could be conceptually territorialised by the Domain Name System, TCP/IP, and functional borders, creating a new virtual realm. This new conceptualised territory also leads to a virtual territoriality[43], which could be dubbed *cyber-territoriality*, where in addition to states, non-state organisations and private companies are also actors in cyberspace. In other words, it is not necessary that owners of cyber-territoriality be only states, but can also be private actors who have the authority of managing the 'functional borders' created by IP addresses and the DNS.

Moreover, definitions of territory[44] seem to assume that territory exists innately, and in a general sense involves not merely an actual and already existing

[43] Territoriality is a term associated with nonverbal communication, referring to how people use space to communicate ownership/occupancy of areas and possessions. (Beebe, Beebe, and Redmond, 2008:209)

[44] The word 'territory' is defined in Merriam-Webster's Collegiate Online Dictionary as:

1. a: a geographical area belonging to or under the jurisdiction of a governmental authority.

geographical area, but the relation of this area to either humans or animals. Wolfgang Kleinwächter (2000) put forward the concept of 'territory of cyberspace,' conceptually constructed upon the Domain Name System and IP addresses, but he did not go so far as to explain the potential territorialisation of cyberspace. As Robert Sack argues, 'Territories are socially constructed forms of spatial relations and their effects depend on who is controlling whom and for what purpose,' and 'Territoriality in humans is best understood as a spatial strategy to affect, influence, or control resources and people, by controlling area; and, as a strategy, territoriality can be turned on and off.' (Sack, 1986:216) As a result, a territory is not merely a geographical space, but also a conceptual space such as cyberspace. These discourses, proposed from the field of philosophy, construct the argument that territory is not confined to a geographical area; it can also be something abstract: a concept, rather than a geographical zone. In other words, though the word 'territory' is derived from geography, the concept of territory can also be conceptually regarded as a sphere of autonomy in accordance with its ownership. As discussed in depth in Section 2.1, cyberspace, constructed of interconnected computer networks, provides an infrastructure for information exchange and communications based on the Domain Name System (DNS) and the mapping of IP addresses. This indispensable information platform is structured by combining a large amount of physical hardware, such as computers, servers, routers, converts, and cables, with conceptual interactions, such as information exchange and communications. The authority to control these individual physical systems and to access their information potentially constitutes a virtual territory of cyberspace, leading to the 'territorialisation' of cyberspace. As Ian Buchanan and Adrian Parr (2006:194) examine, the concept of the virtual territory has already been applied to cyberspace in the work of Deleuze and Guattari[45].

---

b: an administrative subdivision of a country. c: a geographical area (as a colonial possession) dependent on an external government but having some degree of autonomy.

2. a: an indeterminate geographical area; b: a field of knowledge or interest.
3. a: an assigned area; especially: one in which a sales representative or distributor operates; b: an area often including a nesting or den site and variable foraging range that is occupied and defended by an animal or group of animals.

[45] In the book, *Thousand Plateaus*, 'the territory is the product of a territorialization of milieus and rhythms…A territory borrows from all the milieus; it bites into them, seizes them bodily…It is built from aspects or portions of milieu…There is a territory precisely when milieu components cease to be directional, becoming dimensional instead, when they cease to be functional to become expressive…What defines the territory is the emergence of matters of expression.' (Deleuze and Guattari, 1988:314-315)

The main achievement of the Domain Name System is to create a conceptual space which regulates dispersed IP addresses into a well-organised and strictly individual hierarchy: a name space under a certain domain. However, if the DNS were temporarily ignored, only the relation between assigned IP addresses and their connected hosts would be considered. It could be judged that the geographic mapping between the space constructed by IP addresses and the geographic space constructed by these host computers becomes meaningless, since there is no rational or regular relation between them. In other words, without the DNS, IP addresses would just be a series of numbers, and their allocation would be arbitrary, especially in terms of geographic distribution. Therefore, if the DNS were somehow removed and then brought back, the map of cyberspace would be totally different. Under this new DNS framework, cyberspace would have a meaningful and hierarchical structure; thus, in contrast to the chaotic image of cyberspace established by IP addresses only, the DNS would create a well-defined construction. Cyberspace would be reconstructed as a hierarchical realm by the DNS and IP address system. In this hypothetical example, the Domain Name System (DNS) would not merely rebuild the system ruptured by use of IP addresses alone, but also deconstruct itself from its technical field and then reconstruct itself. In addition, this issue cannot be described only from a technical point of view; it must also be considered from social and cultural dimensions, since the difference between ‘dajkjw23ds.org’ and ‘cybersecurity.org’ or ‘chinese-web.org’ cannot be answered in terms of technical orientation, as their functions are all the same from the DNS’s point of view. Certainly, technology causes some structural limitation, but the motivation of matching domain names with popular terms used in real life or special meanings goes far beyond technology itself. The DNS reconstructs the relationship between distributed IP addresses and well-structured domain name spaces to establish a virtual territory of cyberspace, which also obtains symbolic values and names which can only be noticed in the social environment in which they are used. In addition, each computer has a name assigned by an Internet Service Provider (ISP) when connecting to the internet to identify its position in the whole hierarchical name space. In the real world, it is possible that two people may have exactly the same names, which is not a problem as people are identifiable through other means. However, this is impossible in the virtual territoriality of cyberspace even if two machines are identical. The name space is exclusively at any time under the

principle of universal response, according to which the same query always gets the same answer no matter where it was asked or what server name was required. Unlike in real life where one's name and space or location are separate, under the Domain Name System, a name represents space and location. There is no possibility for the identical, and that creates an extremely rigid territoriality. In the next chapter this research will generate a theoretical tool, equivalent to the principles of the territorial state system, in order to identify whether or not the virtual territoriality of cyberspace is being intruded upon.

2.4 General concepts of cyber warfare

The current importance of cyber warfare is clear and obvious to observers, as it has been addressed recently by many government and media reports.[46] However, the explicit conceptual identification of cyber warfare remains uncertain. From historical experiences of human warfare, it can be found that the more advanced the military technology, the more the spatial range of wars will expand. Battlefields have transferred from jungle to plain and from plain to ocean, and then out yet further to air and then space. Regardless of whether a space is tangible or intangible, if it is accessible to human reach, warfare may, perhaps inevitably, occur therein. Operationally, conceptual definitions indicate the essence of traditional warfare: 'war has historically been (a) a struggle involving the use of armed force; (b) between opposing sovereignties, nation-states in the last few centuries, sovereign cities, tribes, and groups before that.'[47] However, due to its inherent features, cyberspace is not necessarily subject to the same warfare as traditional theatres. In the information age, as indicated by Alvin Toffler (1993), humans have shifted focus on the influence of information from the social to the military arena.[48] Further to that, as Dong Zifeng (2006:127) stresses, since 1957, battlefields have broken

[46] Roughly 648,000 results are called up by a Google search of the keyword 'cyber warfare' on 1st December 2010. These results include government reports, news and articles of events associated with cyber warfare.

[47] Traditionally, conventional warfare is defined as having 'four essential constituent elements: (a) there must be a contention between at least two nation-states; (b) the nation-states must use their armed forces in the contention; (c) each nation-state's goal must be to overpower the opposing state(s) [the enemy] and impose peace on the victor's terms; and (d) the contending states will have symmetrical, although diametrically opposed, goals.' (Brenner, 2009:54)

[48] Alvin Toffler believes that the types of warfare can be categorised by the cultural background of the era, such as the agricultural age [First Wave], the industrial age [Second Wave], and the information age [Third Wave]. (Toffler, 1993) In the 'Third Wave' – the information age – Toffler believes that the forms of war rely on telecommunication systems and computer networks, where information can be mastered efficiently. (Toffler, 1993:65-72)

through the limit of the Earth's gravity and entered universal space. Battle space has now transferred from tangible territories (air, land, and sea) to an intangible territory (cyberspace).[49] The contest over this virtual space has begun.

In addition to traditional warfare, Martin Libicki (1995) proposes that there are seven forms of warfare in the 21st century, namely 'Command and Control Warfare (C2W), Intelligence-Based Warfare, Electronic Warfare (EW), Psychological Operations (PO), Hackerwar, Information Economic Warfare, and Cyberwar.' Alongside the development of information technology, nearly all information related activities are carried out and conducted via electronic infrastructures – cyberspace. As a result of this, the previous situation of overlap in the definitions of the different types of warfare has become dramatically more pronounced. It may be argued, though, that strategic thinking on cyber warfare may cover Libicki's seven new types of warfare, since these forms of warfare effectively share the same battle space. Divergences arise instead through different media, implements, and devices, and through outcomes, such as information, intelligence, electronic equipment, psychological effects and so on. In terms of establishing a defensive strategy, establishing as wide a defensive shell as possible is perhaps the best catch-all strategy to deal with the range of threats. Cyberspace is defined in the latest military doctrine of cyber operations, released in 2010, as 'a 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.'[50] This is the clearest definition of the concept of cyberspace published so far. As stated, it is possible to argue that Libicki's seven different forms of warfare are all carried out and deployed on the same battleground, namely cyberspace. Based on this argument, cyber warfare can be classified as the primary strategy to secure the potential battlefield of cyberspace, forming a common conceptual strategy for the different types of warfare. Cyber warfare can be regarded simply as a strategy related to wars or threats in cyberspace.

[49] Since the first satellite was launched in 1957, humans' battle arenas have been transformed from the dimension of ground to the dimension of space. Furthermore, in the information age, the conquest of territory has shifted from tangible to intangible territory. (Dong, 2006)

[50] As seen in the US Doctrine Document 3-12 named '*Cyberspace Operations*', published 15th July 2010. This is a significant indication of cyber warfare, since relevant military training and exercises will be carried out according to this doctrine. The US Doctrine of Joint Operations also notes, 'Cyberspace is a domain that requires man-made technology to enter and exploit. The difference is that it is easier to see and sense the other domains [such as land, sea and air]' (U.S. Air Force, 2010:51)

In the physical world, the threats for human beings and state or non-state actors can traditionally be classified into three categories: crime, terror, and war. (Brenner, 2009) Each category has its own different legitimate players and attack targets, and so they are grouped separately. However, as Susan Brenner (2009) points out, in the digital age, as these three categories of threat could all be carried out via cyberspace, the boundary between them is becoming indiscernible. Furthermore, due to this situation, it may be argued that threats from each of these three different categories, when they are conducted in cyberspace, can be re-classified as applications of cyber warfare, so that action against such threats can be carried out legitimately. This is an additional reason why it is so important to definitively and academically interpret the concept of cyber warfare by examining principles of cyber territoriality.

Following the explanation of the concepts of cyberspace and warfare/strategy presented in previous sections, it is possible to interpret cyber warfare as warfare performed in cyberspace by either state or non-state actors which poses any threat to the security of cyberspace. As investigated, cyberspace is an electronic infrastructure combining the internet, computer networks, and telecommunication systems. Conceptually, cyberspace is also formed by the information that it contains, which includes any form of communication contributed by people.

Thus, regardless of the precise type of cyber warfare, of which there are many, conceptually they all touch on one identical principle, which is that all are based upon the electronic infrastructure of cyberspace. Cyber warfare, then, is the core and vital strategy shared by these different forms of warfare to secure (or even compete for) the same battlefield. Cyber warfare may be inferred to be a strategic contest of actors against one another, carried out in order to gain dominant power in cyberspace. As Shen Weiguang[51] stresses, the approach of cyber warfare can destroy adversaries' computer systems to distress or even obliterate information delivery in many sectors such as financial systems, telecommunications, power supplies, and transportation services. (Shen, 1996) Actors can also implement

[51] Shen Weiguang is known as a pioneer in the field of China's information/cyber warfare. His book, entitled *新戰爭論 [Xin zhanzheng lun, Theory of New War]* was published in 1990 (before the Gulf War). In his book, he proposed conducting asymmetric warfare through cyber warfare, and predicted that future wars will focus on information carried by computer networks. (Shen, 1990) At that time, Shen was regarded as a futurologist, as the military power of information technology was only unveiled for the first time in the Gulf War.

harassment attacks, falsify information, steal data, and monitor their enemies. Furthermore, in terms of the military, cyber warfare can be considered a strategy for dealing with operations in cyberspace. According to US military doctrine, operations in cyberspace are defined as 'the employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace.' (US Air Force, 2010:51)

Cyber warfare does not necessarily match the characteristics of conventional warfare outlined in the Introduction. Similarly, the criticism is often made that a cyber war might not meet the requirements which define a true war, since there are no physical casualties or damages in cyberspace. In the digital era, as Libicki (2009:179) points out, 'what constitutes an act of war may be defined one of three ways: universally, multilaterally, and unilaterally.' He explains that 'a universal definition is one that every state accepts.'[52] An alternative hypothetical way in which a cyber attack could be identified as an act of war is if a group of states agrees on a specific definition of cyber war, identifiable by certain named characteristics. (Libicki, 2009) In order to identify a general concept of cyber warfare which may be accepted by states as a universal definition, it is valuable to review and borrow some principles of the traditional territorial state system (even though actors in cyberspace are not necessarily just states). When compared with the territorial state system, cyberspace is more metaphoric, acting as a conceptual world, as there are many remarkable social behaviours, norms, and communications in this space. That is to say, cyberspace may be regarded as a metaphor of an intangible territory.

2.5 The impact of the growth of cyberspace on international security

It has been pointed out that Strategic Studies is part of International Security Studies (ISS), since ISS is focused on 'the use of force in international relations,' which also distinguishes ISS from the general field of IR. (Buzan and Hansen, 2009:16) In human nature, the desire for security is a basic need. In a state, security must be stable and comprehensive, and no threats should be perceptible. True security means that an identity (region, state, group, or individual) maintains its existing value, including benefits for the people (Buzan, 1991). However, this 'value' is an abstract concept because threats to it might not actually exist. This value can be identified, in

[52] The closest international equivalent to 'every state' is the United Nations. Thus if the United Nations regards something as an act of war, this would fall into the universal definition. (Libicki, 2009)

reality, as interests. The concept of national security is therefore to assert the state's interests and to avoid war and threats from outside of the state.

As Lene Hansen (2009) argues, a crucial issue of cyber security is the identification of networks or cyber actors and their link to a nation/state or regime. Attacks occurring in cyberspace must therefore be investigated through a transnationally cooperative mechanism that goes beyond traditional state authority. Existing related cooperation must also be re-examined in the light of the features of cyberspace in order to best tackle new challenges. What's more, as recent research points out, private individuals and groups are never far from the frontlines in the potential battlefield of cyberspace – the actors in cyberspace are largely non-state rather than state. (Cavelty, Mauer, and Krishna-Hensel, 2008:108) In terms of cyber-territoriality, though it can also be argued that it may be difficult to identify exactly who actors are, based on the Domain Name System (DNS), it is fairly simple to identify through which Internet Service Provider (ISP) a private actor accessed the internet. Furthermore, cyberspace can be a virtual world, which contains many cyber-territories in which functional borders can be employed. Thus, existing strategy also has to be reconsidered through these features of cyberspace in order to generate a new comprehensive strategy to guide cyber warfare in the near future. However, due to the intrinsic features of cyberspace, such as anonymity, asymmetry, and shared information infrastructure, everyone and anyone can be a warrior; as such, the populace in cyber-territory has become a crucial factor in terms of cyber security, and accordingly a civilian-based defensive strategy may well be the best security strategy for cyberspace.

Historically, information technology (IT) is not the first new development to cause a revolution of military strategy, as there have been similar experiences with audio and video broadcasting. From Machiavelli to the nuclear age, many new technologies have entered the world which have affected existing doctrines of military warfare and strategy. (Paret, 1986:21-31) However, information technology is the deepest, widest and most recent revolution. Dimensions of cyber warfare must be applied to states' military strategies in order to protect a state's interests from enemies' cyber threats. Threats of cyber warfare affecting critical infrastructure are referred to as non-traditional threats, as they do not result from conventional violence or traditional weapons, even if the target of an attack is a regime or a state. However, the actors who produce non-traditional threats and launch attacks do not

necessarily identify with a regime or a state, and their targets are all over the world. This means that cyber warfare is an issue beyond the international landscape, and it is therefore necessary to develop new strategies not only through cooperation between states, but also with the input of private sectors which own information infrastructures and facilities.

However, it is questionable whether such cooperation would fit neatly with states' interests and defence policies. There would no doubt be constraints on cooperation with private sectors or even with other states. Lewis (2003: xii) points out that these constraints do indeed exist, but he specifies that 'Cooperation in cyber security is crucial because there are no national solutions to transnational problems.' Therefore, unlike the traditional state-centric conduct in international politics, it is consequently now essential that private sectors take precedence in transnational cooperation in order to create strategies to protect common interests in the future.

Military strategy also directly affects security issues. The military approach is traditionally regarded as the foundation of protection and cornerstone of national security. However, there is concern about the threats caused by non-traditional factors such as ethnicity, religion, economics, environmental resources, and informatics. After the conclusion of the Cold War, Buzan (1991) further expanded security study from simple military study to a five-dimensional concept. These dimensions, in addition to military security, are environmental security, economic security, social security, and political security. These new levels of threat are multi-level and pluralised. They are very different from the traditional approach, which constitutes threats generated mainly by armed forces, but their impacts on sovereignty, state security and social development are just as profound. In addition, such impacts usually need to be dealt with not only by transcending inter-state relations but also by incorporating transnational relations. Since 1970, there has been an increase in the amount of non-state groups which process world affairs such as global currency exchange, health, oil supply, mail and transportation. These activities could not be performed across states as easily if they were based on traditional politics. A theory known as transnational politics, which goes beyond traditional inter-state theory, was proposed to explain the interactions between different transnational societies (NGOs). As some non-state actors may also challenge security (Eriksson and Giacomello, 2006), security has become a critical component in both the international and the transnational sector.

How can relevant theories of international security inform analyses of the growth of the potential battleground of cyberspace in the digital age? Due to the difficulties of cooperation, 'Trust is often difficult between states, according to realists, because of the problem of cheating,' (Baylis and Smith, 2005:304) capabilities in cyberspace can shift the balance of power among states quickly. In addition, based on the assumptions from neo-realism, it is inevitable that a state will develop some offensive military strategies in order to protect itself and defend its sovereignty, and that its power will be expanded in so doing. Therefore: 'Uncertainty, leading to a lack of trust, is inherent in the international system.' (Baylis and Smith, 2005:302) Consequently, the development of a strategy of coordination with other states, as well as non-governmental actors in cyberspace, is crucial for national security.

As a result, state and non-state actors need to cooperate in order to develop a useful defensive strategy against threats occurring in the intangible territory of cyberspace. In addition, it is necessary to certify the efficacy of relevant military doctrines through conducting exercises and implementing necessary modifications in order to create practical comprehensive sets of guidelines for involved actors, as well as encouraging interaction between close allies to expand international defences. A significant recent example shows that this approach has already been adopted by some countries. According to an official report (US Department of Homeland Security, 2010), a joint military exercise of cyber warfare, known as 'Cyber Storm,' was conducted by 12 international state actors and 60 private companies (non-state actors). This exercise, first carried out in 2006 and later repeated in 2008 and 2010, aimed to train governmental and private sector understanding and implementation of relevant concepts and processes. Though the results of the exercises still remain classified, the specific objectives were published as follows:[53] (US Department of Homeland Security, 2010)

- Examining the capabilities of participating organisations to prepare for, protect from, and respond to the potential effects of cyber attacks;

[53] As the report indicates, Cyber Storm is intended to act as a catalyst for assessing communications, coordination and partnerships across critical infrastructure sectors. To accomplish this, Cyber Storm II, in 2008, served as a distributed exercise that allows players around the world to exercise from their own office locations. The exercise control centre was located at a Department of Homeland Security facility in the Washington, D.C. metropolitan area. The scenario progressed as players received "injects" from the control centre via e-mail, phone, fax, in person, and websites set up specifically for the exercise. These injects simulated adverse effects through which the participants exercised their cyber crisis response systems, policies and procedures. (US Department of Homeland Security, 2010)

- Exercising strategic decision making and interagency coordination of incident response(s) in accordance with national level policy and procedures;
- Validating information sharing relationships and communications paths for the collection and dissemination of cyber incident situational awareness, response and recovery information; and
- Examining means and processes through which to share sensitive information across boundaries and sectors, without compromising proprietary or national security interests.

Compared to the mature concept of international security, the concept of cyber security is still not fully understood due to the lack of relevant ground theories. In addition, it is technologically complex and the network environment in which it operates changes at lightning speed. Therefore, a feasible solution for cyber security will be proposed in Chapter Five through a case study of China's cyber warfare.

Chapter Three:
Modern Chinese Strategy

It is impossible to know what is unique to a state's strategy without first assessing what aspects of strategy are common to other states in the international system (Ross, 2009:1). Though a state's strategy is formed by its own strategic culture, a state presents itself to the international system through these common aspects of strategy, and as a result, these common aspects are necessary for examination and illustration of strategy as a whole. Therefore, this chapter takes as its premise the argument that any effort to explain modern Chinese strategy should begin with an analysis of the sources of strategy that are common to all states in international politics. Compared with some classic theories in the field of International Security, the study of military theory, including such fields as War Studies and Strategic Studies, is a relatively new realm which still lacks essential fundamental theories to offer support for further research into strategy. Therefore, in order to eventually explore modern Chinese strategy by comprehensively interpreting the unique nature of Chinese culture, it is first indispensable to examine the sources of strategy in the international system on a theoretical basis. This chapter will hence not only provide the foundation for a deeper understanding of modern Chinese strategy, but also simultaneously link modern Chinese strategy to the international system.

In addition, the West has been the dominant civilisation in the modern age, and all other civilisations have been forced to absorb its impact, regardless of whether this influence is welcome or not. We can see this trend within the field of Strategic Studies. For this reason, in this chapter the first section, which invesitgates on traditional Western strategic thinking contextualised with relevant ancient Chinese thinking, will create a theoretical basis of strategy in order to be contrast next with traditional Chinese strategic culture. These two sections will be linked up together in a discussion of the strategy of People's War in modern Chinese strategy. The final section on China's Revolution in Military Affairs will follow on for China's cyber warfare.

3.1 The theoretical basis of strategy [‘戰略’ (*Zhan lüe*)]

The Chinese term ‘戰略’, transliterated as ‘*zhan lüe,*’[54] refers to ‘strategy’ as it is known in the modern era. In ancient China, the two Chinese characters as a term first appeared in 306 A.D. as a book title, but the context of the book was not related to ‘strategy’ per se.[55] Instead, the concept of ‘strategy’, which can be seen as the ‘art of war’, was represented in ancient China by the term ‘兵法’ (*bing fa*) from about 512 B.C.[56] This Chinese term literally means ‘method of the military.’ Through Western influence on the modern era, the term ‘戰略’ (*zhan lüe*) came about and can be seen as a translation of the English word ‘strategy’. It not only directly represents the concept of ‘strategy’ imported from Western strategic thought[57] but also replaces the term ‘兵法’ (*bing fa*), which originally referred to the ‘art of war’. Nevertheless, the precise definition of strategy is highly contentious regardless of whether it stems from Western or Eastern culture. In addition, with regards to the evolution of modern Chinese strategy in the 20th century, core strategic thoughts such as the concept of ‘People’s War’, which will be discussed in depth subsequently, remain in an indiscernible and vague position between the tactical and strategic level. Thus, in order to comprehensively elaborate the concept of ‘戰略’ (*zhan lüe*) in modern Chinese strategy, it is indispensable to first understand the nature of ‘strategy’. The essential definitions of ‘strategy’ and its origins will help identify where the term ‘*zhan lüe*’ originated from in the philosophy of ancient China as well as appropriately pinpoint ‘People’s War’ at a strategic level.

---

[54] From now, words in brackets ( ) are transliterations of the preceding Chinese characters.

[55] The book entitled *戰略*’ (*Zhan lüe*) was written by Si-Ma in 306A.D., and was the first ancient Chinese book to use these two Chinese characters together in the title. (Niu, 2003) ‘戰’ (*zhan*) means ‘warfare’ and ‘略’ (*lüe*) means ‘strategy.’ The term ‘戰略’ (*zhan lüe*) is thus a Chinese translation of strategy that links together Western strategy with Chinese strategic thought.

[56] The earliest recognised Chinese military work is Sun Tzu’s *The Art of War*. Its Chinese title is ‘*孫子兵法*’ (*Sun Zi Bing Fa*). Sun Tzu began to use ‘*bing fa*’ to present the concept of strategy in about 512 B.C. (Sawyer, 1993:149) In other words, ‘*bing fa’* represented the concept of ‘戰略’ (*zhan lüe*) from 512 BC onwards until the term 戰略 (*zhan lüe*) became established.

[57] According to General Beaufré, strategic thought must continuingly take the facts of change into account and can predict probable changes many years ahead. Strategic thought must work on hypotheses and generate solutions by truly original thought. (Collins 1973:235)

3.1.1 *The origin of strategy*

Before the early modern period, the Roman Frontinus wrote a book entitled '*Strategemata*'[58] in the 1st century A.D. The Byzantine emperor Maurice, who was also a well-known strategist, followed with '*Strategicon*' in the late 6th century A.D. *Strategemata* is the first book to make a connection between strategy and warfare by using 'strategy' in the book title to represent the art of war. '*Strategicon*' meant the discipline of the General.[59] Much later, in 1777, Maizeroy, in his work titled '*Théorie de la Guerre*', used '*stratégie*' to define 'the conduct of operations.' This book was published and distributed to the extent that the term strategy was gradually used in military terminology not only in France but all over Europe. Though the word '*strategy*' has been used for only about two hundred and thirty years, the concept of strategy already existed during the ancient period, but was referred to by different terminology, such as '*taktike lechne*' in Greek and '*ars bellica*' in Latin. The former has the original meaning of tactics; the latter means 'art of war.' In the Eastern world, first to use '戰略' (*Zhan Lüe*), the modern Chinese translation of strategy, as the title of his work was the Chinese historiographer Si-Ma in 306 A.D. (Niu, 2003:18) However, the most famous masterpiece and earliest military work in relation to strategy is *The Art of War* written by Chinese strategist Sun Tzu in approximately 500 B.C.[60] In both the Western and Eastern world strategy was regarded as a method with which to pursue victory on the battleground through military force. Liddell Hart called this strategy 'pure or military strategy.' (Paret et al., 1986:35) This traditional interpretation presents the primary principle of strategy.

---

[58] The term '*Strategemata*' is originally from the Greek '*strategama*', which has been translated as 'stratagems' in English. (Polyaenus et al., 1994)

[59] '*Strategicon*' was the title of a manual of war written by Maurice, and was also the term for the title of commander of a military region in the Byzantine Empire. By the late 6th century, the Byzantine Empire incorporated about 30 military regions, and Maurice wrote the book in order to educate the commanders of these regions.

[60] Sun Tzu, respectfully known as Sun Wu, is the author of *The Art of War* (*Sun Zi Bing Fa*) which is an essential text of traditional Chinese military philosophy and strategic thoughts. The book contains 13 chapters and was written in about 500 B.C. (Griffith, 1971) The first foreign language edition was published in French in 1772. Collins clearly states that Sun Tzu was the first great figure in ancient times to build up a complete structure of strategic thought, stating that the 13 chapters of his masterpiece could doubtlessly rival almost all the military writings in the world, including that of Karl von Clausewitz. (Collins, 1973) However, very few scholars have examined Sun's existence. (Yan, 2011:70) One might still argue that Sun might be a mythical figure. Nevertheless, the book of *The Art of War* is the most significant work for Chinese strategic thinking since the work has been an essential reading in studying Chinese strategy. Thus, this research is going to examine the ideological influence of the work itself for Chinese strategy in modern era, rather than arguing for or against Sun's existence and who the author may have been.

Machiavelli, writing in the 16th century, was one of the most important Western strategists of the early modern era. His tremendous achievement was to propose a concept of hierarchy of ranks as a normative standard, which remains the foundation of the modern command structure. His work, *The Art of War*, also became the primary instructional material at the military academy established by Maurice of Nassau at that time. In his military thought Machiavelli regarded discipline as the key element to reinforce military capability. He stressed that discipline could be accomplished by drill and training through a certain command structure. As Max Weber also asserted in his essay titled 'The Origins of Discipline in War,' 'It [war] is discipline and not gunpowder,' 'which initiate[s] transformation,' and 'gunpowder and all the war techniques associated with it became significant only with the existence of discipline.' (Paret et al., 1986:35) In addition to weapons technology, Paret believes that social and moral dimensions are very important for a war. This important concept of the existence of discipline became the foundation of professional military ethics in the future. Machiavelli also emphasized that battle and combat were very important approaches in strategy. This point of view seems to be an antecedent to that of Clausewitz. It could be also argued that such a strategy may lack a peaceful element as it focuses solely on the defeat of opponents in campaigns. Furthermore, Machiavelli claimed that a state's security is its first priority of consideration. A state's military power must be able to resist against threats arising from outside its borders; otherwise, it will not be able to retain security inside the state. Such a concept is similar to Sun Tzu's statement that 'War is a matter of vital importance to a state.' (Sun, 1971:91)

Like Machiavelli, Justus Lipsius, who also deeply influenced Maurice of Nassau, emphasized that citizens had a military obligation to serve their country and stressed that native soldiers were more trustworthy than foreign mercenaries. However, some authorities still believed that only mercenaries were sophisticated enough to control advanced weapons and perform more complicated tactics. (Paret et al., 1986) This instance of conflict between rulers and strategists demonstrates that policy-making may well dominate the development of strategy.

Another strategist, Raimondo Montecuccoli, a famous Lieutenant General in Austria in the 17th century, was in disagreement with the bureaucratic hierarchy when he endeavoured to revolutionise the military. He tried to integrate all the knowledge acquired through experience to generate a 'universal paradigm' for

strategy. Though it was not the only strategic approach he supported, his experiences of the battlefield led him to state that attrition should be adopted after a series of defeats. He also stressed that war cannot be waged without battle and 'conquests and decisions can only be achieved by combat and battle.' (Paret et al., 1986:56) In terms of strategy, his brilliant contribution was to advocate 'manoeuvre warfare' which was used successfully in his campaign against the French army in 1678. In the 18th century, manoeuvre warfare became very popular as many generals tried to achieve victory without engagement. In his strategic thoughts, Montecuccoli regarded strategy, operations and tactics as an 'indivisible identity' and he claimed to use an active defence to weaken the enemy. (Paret et al., 1986:62)

In conclusion, concepts of strategy in the early modern era mainly incorporated categories such as military personnel, military organisation, and military operations. Strategists also believed that command and control were fundamental components to succeed in war; in terms of command, every soldier must follow orders from superiors through the hierarchical structure. After a command is received, the actions of soldiers must be in coherence, which is known as 'control.' Sun Tzu said that in an organised war, 'When the men have been unified the courageous will not be able to advance alone, the fearful will not be able to retreat alone. This is the method for employing large numbers.' (Sawyer, 2007:170) However, the larger the scale of a war, the more difficult command and control become. Command and control are closely linked with appropriate communication in war to enable enormous numbers of soldiers to follow command and control on a huge battlefield.

3.1.2 *Defining strategy*

Historically, strategy referred to military theory or the art of war. In modern society, however, strategy is a well-known term and has been widely used not only in military studies but also in business management. Some eminent pioneers of strategic studies defined strategy through military thinking. For example, Baron de Jomini explained comprehensively that strategy is 'the art of directing the great part of the forces of an army onto the most important point of a theatre of war, or

of a zone of operations.'[61] His contemporary Carl von Clausewitz defined strategy as 'the use of engagement for the object of war.'[62] In the words of the British critic Liddell-Hart 'Strategy is the art of distributing and applying military means to fulfil the end of policy.'[63] General André Beaufré stated that 'Strategy is the art of dialectic of force or the art of the dialectic of two opposing wills using force to resolve their dispute.'[64] These different definitions, though reflecting somewhat abstract elements of strategy, establish the fact that strategy aims to link military power to political purpose. However, strategy is still a highly contentious subject due to the diversity of political orientation from one age to another. The study of strategy may well provide conceptual guidance for warfare, which includes the nature and principles of warfare, comprehension of its regularity and development, application of further defence policy for state security, and even the prediction of how warfare will transform in the future. Therefore, strategy can be regarded as a theory for any activity which includes offence and defence directly or indirectly related to operations, tactics and various type of warfare. Alternatively, it may be a theory for any activity related to military affairs, including the study of the relationship between armed forces and warfare. In short, strategy involves the exploration and epistemology of military knowledge. Such knowledge can be generally extended yet further to certain cross-border fields such as crime-fighting, smuggling, trafficking and piracy. (Baylis and Smith, 2005:2-4) Admittedly, strategy was applied to different dimensions by strategists depending on the purpose of warfare and the political situation of the time. Establishing a general or common principle of strategy running through various phases from one generation to another, however, is worth investigation as it may facilitate tackling varied challenges in the future.

Historically, aspects of warfare have often been changed as a result of human behaviour. Different civilisations in different eras have been inclined to evaluate warfare in myriad ways. In general, warfare indicates armed conflict between different political groups. However, many people regard warfare as

---

[61] Howard, M., B. H. S. and E.Liddell Hart (1965) *The Theory and Practice of War.* Essays presented to Captain B. H. Liddell Hart. Editor: Michael Howard. [By various authors.]. pp. x. 376. Cassell: London.

[62] Clausewitz, C. v., Howard, M. N., Paret, P. and Brodie, B. (1976) *On War.* Princeton; Guildford: Princeton University Press. (Edited and translated by Howard and Paret)

[63] Baylis, J., Wirtz, J. J., Gray, C. S. and Cohen, E. (2007) *Strategy in the contemporary world: an introduction to strategic studies.* 2nd ed. Oxford: Oxford University Press. p. 5

[64] Ibid

merely a risky approach to gain benefits. Different approaches to warfare over time have consequently caused the definition of warfare to be widely extended. From a functional perspective, the primary purpose of strategic study is to extract relevant factors from previous experiences of warfare so that these factors can be systematised as useful knowledge. In so doing, the distance between current military capability and guidance for future warfare could be narrowed and it would be feasible to overcome time limitations to correctly prepare the national defence. (Cheng, 2003) However, though military planning and the construction of military power may be based on such rational thought, this does not necessarily infer certain military victory because the result of warfare is influenced by many variables. For example, what is the extent of the discrepancy between theoretical probability and the true readiness of the national defence? How many variables exist which have been overlooked or not correctly calculated? What conclusions has the enemy drawn in terms of military guidance? How well prepared is the enemy's national defence? All these factors are associated with the process of warfare; from preparation to operation. The result of warfare will accordingly reflect these factors. Thus the function of the study of strategy is to investigate the most appropriate strategic approach based on not only historical experience but also current calculations of the enemy, in order to narrow the distance between advanced theoretical thinking and the subsequent result.

Furthermore, it is indispensable for states to address strategy in order to provide effective communication between civilian society, defence policy, and military forces. Strategy has never been easily explained, as its exact meaning and derived notions are confusing due to their ambiguous nature. Before further exploration of the concept, it would thus be useful to clarify the term. Despite the periodic modification of the application of strategy and the occasional redundancy of traditional frameworks in examining modern strategic details, the fact that certain political purposes guide military force has never changed. Although the fundamental concept of strategy has never undergone a monumental shift, the academic investigation of strategy is currently expanding greatly compared with the eras of Clausewitz and Sun Tzu.

Strategic Studies is primarily focused on research into warfare, which is also addressed by the study of security issues within the field of International Relations. In his work *On War*, Clausewitz stressed that strategy contains a

diversity of features such as ethics, supply, mathematics, geography and statistics. (Clausewitz, 1976:183) Michael Howard (1965) also mentions that strategy should consist of dimensions of society, logistics, operations and technology. This not only reflects the extensive themes and approaches of Strategic Studies but also indicate that exploration across the various disciplines is necessary to comprehend, evaluate and produce strategy. As a result, it is undeniable that the diversity of demands, from philosophy to science, theory to practice, and civil to military, makes the nature of Strategic Studies exceedingly complex. Additionally, in terms of Strategic Studies, there is no boundary between different subject areas. Any one of the variety of intellectual concepts in human life can be regarded as an element of Strategic Studies. The features of diversity and complexity prevalent in this field of study will doubtless lead to further research developments.

Nevertheless, although much research has been conducted in the field, critics still claim that existing Strategic Studies is too new an academic discipline to have developed a fundamental theoretical base. Philip Green, for instance, asserts that Strategic Studies are 'pseudo-scientific, using apparent scientific methods to give the subject a 'spurious air of legitimacy.' (Green, 1966:225) These criticisms stem from doubts concerning not only the miscellaneous, seemingly random, features of strategy but also the methods of scientific investigation involved in the field. Clausewitz commented that everything in strategy is very simple, but this does not mean that everything is easy. (Clausewitz, 1976:656) As Baylis et al. (2007:9) investigate, critics have stated that: 'Because strategists focus on the role of military power, they tend to be preoccupied by violence and war' and that Strategic Studies neglects the 'more cooperative, peaceful aspects of world politics' as it chiefly regards the world as a 'conflict-oriented' space.

Briefly, strategy can represent different approaches and different applications due to its inherent variety. These approaches are mutually related and may even be sub-categories of one another. For instance, one approach is based on various levels of strategy such as total strategy, overall strategy and operational strategy according to French General Beaufré's strategic pyramid. (Niu, 2003:33) Another approach is based on the uses of military force such as defence, deterrence, compellence, posturing and offence. (Jordan et al., 2008:49-54) However, these two approaches contain a spectrum of multidimensional factors, just as Clausewitz and Howard initially suggested. In Clausewitz's strategic

theory, outlined in his work *On War*, he indicates five dimensions of strategy, which are ethics, supply, mathematics, geography and statistics. (Clausewitz, 1976:183) Michael Howard also identified four dimensions in his 1979 article '*The Forgotten Dimensions of Strategy*.' Later scholars provided a more developed theoretical concept of those dimensions. (Jordan et al., 2008:29)

3.1.3 *The concept of strategic culture*

In terms of a state's strategy, it is arguable that the development of a state's strategy is deeply influenced by the national culture. Basically, a state aims to find ways to maintain national security by employing various levels of strategy. However, the strategy of a state also contains characteristics of that state's culture and social trends, as culture influences the philosophy of both war and peace. As John Baylis and Steven Smith (2005:543) point out, 'a culture is composed of the customs, norms, and genres that inform social life.' In addition, culture is especially important in a state like China which has an ancient civilisation and strategic tradition spanning thousands of years. Consequently, cultural thinking has merged with strategic thinking to form a strategic culture. Even though the application of a state's strategy is not completely determined by it, strategic culture can, however, influence the choices of strategic operation. In addition, the process of shaping a strategic culture is associated with the concepts of security, interests, and threats. In terms of Chinese strategic culture, as Gong Yuzhen (2005:160) points out, there are several influencing factors, such as the distinctiveness of the civilisation, the geographical environment, and historical experiences. Furthermore, Andrew Scobell (2002:1) puts forward two motivations for trying to understand modern Chinese strategy through the dimension of strategic culture. The first reason is that national culture is widely regarded in China as a key point in strategy. The second reason is that the strategic actors and policymakers in the People's Republic of China (PRC) itself have claimed that their behaviours are conditioned by deeply ingrained traditional Chinese philosophy regarding international relations.

The term 'strategic culture' was coined by Jack L. Snyder who studied the Soviet limited nuclear war doctrine of 1977. This concept was first used to predict the likelihood of the Soviet leadership accepting the policy of limited nuclear war. (Johnston, 1995:5) Snyder (1977:8) defines strategic culture as 'the sum total of

ideas, conditioned emotional responses, and patterns of habitual behaviour that members of a national strategic community have acquired through instruction or imitation and share with each other.' Since then, studies of strategic culture have been developed. Ken Booth (1990:121) argues that strategic culture is 'a way of adapting to the environment and solving problems with respect to the threat or use of force.' As Yitzhak Klein (1991:5) indicates, strategic culture is 'the set of beliefs held by strategic decision-makers regarding the political object of war and the most effective means of achieving it.' He goes on to write: 'Strategic cultures can be a hierarchy of concepts on several levels: political, strategic, and operational.' Furthermore, Alastair Johnston (1995:46) believes that strategic culture is 'an integrated system of symbols (e.g. argumentation structures, languages, analogies, metaphors) which acts to establish pervasive and long-lasting strategic preferences by formulating concepts of the role and efficacy of military force in interstate political affairs, and by clothing these conceptions with such an aura of factuality that the strategic preferences seem uniquely realistic and efficacious.' Rosita Dellios' research into Chinese strategic culture led her to state (1997:203) that strategic culture 'pertains to a people's distinctive style of dealing with and thinking about the problems of national security.' As former US military attaché to China Andrew Scobell defines, strategic culture is 'the fundamental and enduring assumptions about the role of war (both interstate and intrastate) in human affairs and the efficacy of applying force held by political and military elites in a country.' (Scobell, 2002:2)

Strategic culture can thus be regarded as the way of thinking of the members of the community responsible for producing a state's strategy. Consequently, one aspect of research into strategy may be the analysis of the strategic behaviour of members of this community. On a state level, these actors are strategists or the political elite, a group of people considered to be the best in the political arena because of their power and educational background. These people are the usual decision-makers for a state's strategy and they form the 'community' that develops a state's strategic behaviour. Therefore, in addition to cultural influence, strategic culture is also heavily affected by this political community and environment. Wars are, in fact, political issues, and a war will remain in the realm of politics until the aims behind starting the war are achieved. It could be suggested that the culture of this political community and a state's

strategic culture mutually affect each other, especially if the government is a dictatorship, which is akin to the one-party system of China.

3.1.4 *Summary of strategic concepts*

A state's strategy can be roughly classified into two levels: national and military. The former is the highest strategic level for a state as it forms guidance not only for the national defence but also for the development of the whole country. The latter is the deciding principle behind various tactics and methods of warfare to guide military operations in both offence and defence. Furthermore, regardless of the type of warfare, there is no doubt that weapons technology reinforces strategic approaches and expands the scope of state strategies. However, the expansion or reinforcement of strategies due to developments in technology will still derive from fundamental strategic thought as a result of a state's strategic culture. This is especially the case in China, where philosophies are deep-rooted due to the particularly long cultural tradition. Strategic culture essentially emphasises that a state's strategic thinking is influenced by its culture; thus, a state's strategic behaviour from one generation to another may well reflect its constant strategic culture. (Johnston, 1995:4-5) Thus, it will be argued in this research that even though warfare itself has transformed through the different ages, and battlefields have changed from land, sea and air in geographical space through to virtual cyberspace because of revolutions in weapons technology, modern Chinese strategic thought regarding warfare has fundamentally never changed as a consequence of the continuing and constant influence of strategic culture.

Chinese strategic culture is guided by traditional Chinese ideology, which has primarily been shaped by the Confucian-Mencian paradigm and the ancient Chinese philosophy of war.[65] Through investigating a range of literature on 'People's War', which has not only inherited the military thought of ancient Chinese strategists but also links to the modern era and continues to guide modern Chinese strategy, this chapter will produce a relevant theoretical discourse. This discourse, generated principally from the angle of defence, will clarify the ambiguous image of modern Chinese strategy. The structure of Section 3.2 is organised chronologically in order to clearly present how People's War has been a

[65] This argument will be further elaborated upon in Section 3.3.

constant doctrine throughout strategic shifts in modern China from one age to another.

3.2 Chinese strategic culture: a radical factor in shaping Chinese strategy

In terms of Strategic Studies, it is argued that western strategic thinking and discourses may well play the leading role in the world since the western technology of warfare is dominant in the modern era. However, the basic tenets of every evolutional stage of China's People's War all hark back to the work of ancient Chinese strategists. Along with China's rising in these decades, revealing the impact of traditional Chinese strategic culture on modern Chinese strategy is therefore highly valuable in order to investigate how the traditional thinking shapes the unique modern Chinese strategy. Embracing the possibility that non-Western cultures may exhibit different ways of thinking and acting in international politics, it is pertinent to recognise the impact of Chinese strategic culture on its modern strategy, especially when considering security in the 21st century. Chinese strategic culture continues to play an important role in modern Chinese strategy, and is likely to guide China's cyber warfare in the digital age. It is arguable that the idea of cyber warfare perfectly fits into Chinese strategic thinking which has been formed through traditional Chinese strategic culture.

As Scobell (2002:1) believes, it is important to interpret Chinese strategic culture for two reasons: firstly, culture is regarded as a critical part of strategy; secondly, the PRC's scholars, analysts, and policymakers admit that their thinking and behaviour is often influenced by traditional Chinese culture relating to international relations. Thus, Chinese strategic culture is not merely formed by China's contemporary strategic conditions, its national interest, and specific experience of wars, but also shaped by its historical culture and traditional relations with neighbouring nations. As Johnston argues, Chinese strategic culture is mainly cultivated through traditional Chinese thoughts associated with strategy, namely the Confucian-Mencian paradigm and the philosophy of war represented by Sun Tzu's work '*The Art of War*.' (Johnston, 1995:252-254) Meanwhile, Dellios (1989:204) also states that Chinese strategy combines characteristics of the People Liberation Army's (PLA) heritage with characteristics of contemporary warfare. However, her work does not comprehensively examine the specific strategic principles which shape this PLA heritage. In sum, it can be concluded that modern Chinese strategy,

namely People's War, is profoundly influenced by Chinese strategic culture, which mainly comprises of the Confucian-Mencian paradigm and the ancient philosophy of war.

3.2.1 *The doctrine of the Confucian-Mencian paradigm*

In Chinese traditional culture, the Confucian-Mencian paradigm[66] is a leading ideological model. Chinese traditional culture represented by this paradigm has been very influential in shaping the mental and social value of all Chinese people. Though the Confucian-Mencian paradigm was oppressed by the Cultural Revolution from 1966 to 1976, the paradigm remains deep-rooted in the thinking of Chinese people. It therefore may well be believed that policymaking in China is influenced by this Chinese tradition, as borne out in certain examples.[67]

In addition, as Gao (2003:122-129) explores, since the Warring States Period[68] in China, Chinese ideology has integrated the Confucian-Mencian paradigm and the philosophy of war for more than two thousand years, so the development of military theory is quite potentially influenced by these factors. The Confucian-Mencian paradigm claims that virtuous governance is the foundation of a sovereign, and that warfare is only one of the ways to accomplish

---

[66] The Confucian-Mencian perspective, which Alastair Iain Johnston terms the Confucian-Mencian paradigm, regards the world as harmonious rather than conflictual. (Johnston, 1995) Harmony and order can be maintained through virtuous and exemplary behaviour on the part of the ruler. In addition, as Yan Xuetong (2011:259) probes, many Chinese scholars believe that 'traditional Chinese thought [mainly Confucian-Mencian paradigm]' to IR should be and will be recognised as the 'Chinese school' of IR. In other words, it is shown to be a widespread set of beliefs in the Chinese community in a way that is similar to that argued by Johston as this research investigates in the section.

[67] As Xu Keqian (2009) points out, the Confucian-Mencian paradigm has been the basis of Chinese cultural value for Chinese people from one generation to another. In addition, evidence shows that this paradigm is influential in China's policymaking , such as in the following examples:

1. Wang Zaibang (2011) points out that the white paper *China's Peaceful Development* reflects the traditional Confucian-Mencian paradigm in guidelines for foreign policy.
2. 'Chinese traditional thought becomes very influential in the thinking of policymakers.' (Yan, 2011) For instance, the Chinese government has begun to regard 'social welfare' as essential for people through reference to the teaching of the Confucian-Mencian paradigm.
3. Though the Chinese Cultural Revolution (1966-1976) oppressed the Confucian-Mencian paradigm, China's 12th Five-Year national planning in 2010 promotes the teaching of the Confucian-Mencian paradigm in the national educational system in order to refine the moral behaviour of Chinese people. (People.com, 2011)
4. China's foreign policy employs certain Chinese traditions, such as the ancient thought of 'being neighbourly', as a diplomatic approach to coterminous states. (Yang, 2011)
5. On 6th April 2010, President Hu Jintao, China's paramount policymaker, clearly stressed the importance of Chinese traditions in China's policies in a public speech, encouraging the CCP leadership to follow such traditions. (XinHua News-1, 2010)

[68] The Warring States Period (戰國時代, *Zhanguo Shidai*), also known as the Era of Warring States, covers the period from 476 B.C. to the unification of China by the Qin Dynasty in 221 B.C. (Brooks, 1998:4)

virtuous governance. Accoring to *The Analects of Confucius*[69], Confucius considers war with a very prudent mindset, writing: 'It is only once a truly efficacious person has instructed the people for seven years that the subject of battle can be broached.' (Confucius, 1998:170) and 'To go into battle with people who have not been properly trained is to forsake them.' (Confucius, 1998:170) In other words, virtuous government and teaching of the people must precede leading them into war. This involves long-term training and should not be rushed, lest the people be harmed or even destroyed. Confucius recognises the importance of the military in defending against outside threats, protecting the people and maintaining state security. When asked by Zi Gong how to govern effectively, 'Confucius replied: make sure there is sufficient food to eat, sufficient arms for defence, and that the common people have confidence in their leaders.'[70] This demonstrates the emphasis on both the military and the people which is reflected in Chinese strategic culture. In addition, in terms of international relations, Gong (2002:153-155) points out that historically the Chinese regarded their country as the centre of world, naming it '中國' (*Zhongguo*), which literally means 'middle kingdom.' In ancient times, the small states surrounding China had to pay tribute if they were conquered. Chinese empires complimented this by giving gifts back to these small states in a system known as 'moralisation' from the view of the Confucian-Mencian paradigm. This was followed in order to maintain harmonious relations with other nations, as opposed to using force. Li (1998:240) argues that the soul of Chinese strategy created by Chinese civilisation is a strategic culture of seeking peace, pursuing unification, and emphasising defence. These three basic points are the issues of focus for the study of Chinese strategic culture. In fact, the conservative concept of waging a war with prudent consideration represents the manner of controlling the forces in traditional Chinese military theory. Another influence giving prominence to the concept of peace in Chinese strategic culture is the idea of conducting a righteous war. In *The Analects of Confucius*, 'Confucius

[69] This is from an English edition of '*The Analects of Confucius: A Philosophical Translation.*' translated by Ames and Rosemont Jr in 1998. (Confucius, 1998) In addition, Confucius's sayings were emobodied by his disciples in this book, which comprises twenty chapters. The sayings attributed to Confucius quoted in this research accordingly reflect the arguments and debates of his early followers.

[70] With regards the relations between a ruler and his people, in *The Analects of Confucius* Confucius also said, 'If a superior man loves propriety, the people will not dare not to be reverent. If he loves righteousness, the people will not dare not to submit to his example. If he loves good faith, the people will not dare not to be sincere.' (Confucius, 1998:154)

said, when the way (道, *Dao*) prevails in the world, ritual propriety (禮, *li*), music (樂, *yue*), and punitive campaigns are initiated by the empire (天下有道，則禮樂征伐自天子出, *tianxia you dao, ze liyue zheng fa zi tian zi chu*).'(Confucius, 1998:196) This shows that Confucius insisted that conquering other nations must rely on 'refinement and excellence.'[71] In other words, in the sense Confucius regarded 'civil culture and virtue' as more prudent than waging war. Mencius also wrote that using military force with the pretence of benevolence cannot make other states submit with sincerity.[72] In fact, all of these ideas convey the idea of righteous war[73] in Chinese traditional culture. As Johnston (1995:68) points out, a 'righteous war' is the only situation in which armed forces can be legitimately employed. This is known in Chinese as 'A campaign must have a name (師出有名, *shi chu you ming*).'[74] This means a war must be conducted for a righteous reason, using armour and weaponry to punish unrighteous violence. (Johnston, 1995:69) In this way, military action will earn the full support of the populace. This has been one of the critical fundamental principles of Chinese strategic culture.

However, in modern conditions, Swaine (2000:21) argues that the choice of adopting moralisation or military force will depend on levels of military capability and the necessity of using force. That is to say, superior military ability is a realistic backbone to 'moralisation,' allowing a state to adopt 'moralisation'

---

[71] According to Confucius 'If distant populations are still not won over, they persuade them to join them through the cultivation of their refinement (文, *wen*) and excellence (德, *de*).' (Confucius, 1998:195-196)

[72] 'He who, using force, makes a pretence to benevolence is the leader of the princes. A leader of the princes requires a large kingdom. He who, using virtue, practises benevolence is the sovereign of the kingdom. To become the sovereign of the kingdom, a prince need not wait for a large kingdom. ….. When one by force subdues men, they do not submit to him in heart. They submit, because their strength is not adequate to resist. When one subdues men by virtue, in their hearts' core they are pleased, and sincerely submit….' (Mencius, 1970:190-207)

[73] Righteous war, first used by Mencius, is a revolutionary war waged with the purpose of benevolence to overthrow a non-benevolent sovereign. As Mencius said, 'In the "Spring and Autumn" there are no righteous wars. Instances indeed there are of one war better than another. "Correction" is when the supreme authority punishes its subjects by force of arms. Hostile states do not correct one another.' (Mencius, 1970:477-478)

[74] This term originates from *Liji[The Classic of Rites.* In 475-221 B.C., Wu made an incursion into Chen, destroying the (places of) sacrifice, and putting to death those who were suffering from a pestilence (which prevailed). When the army retired, and had left the territory, Pi, the Grand-administrator of Chen, was sent to the army (of Wu). Fu Chai (king of Wu) said to his internuncius, 'This fellow has much to say. Let us ask him a question.' (Then, turning to the visitor), he said, 'A campaign must have a name. What name do men give to this expedition?' The Grand-administrator said, 'Anciently, armies in their incursions and attacks did not hew down (trees about the) places of sacrifice; did not slay sufferers from pestilence; did not make captives of those whose hair was turning. (Niu, 1997:63)

rather than using military force. Bill (1996:6-7) indicates that the traditional Chinese economic principle of 'self-reliance' is also reflected in the PRC's military, especially with regard to developing its own military technology. Modern Chinese strategy demonstrates an eagerness to gain the ability of self-reliance in order to secure superior military capabilities. In addition, due to the influence of Confucian-Mencian paradigm, it is argued that China chooses to wage war based on justice. Making a war acceptable to the people must depend on legal justifications. However, war does not necessarily have to be defensive; it can also be castigatory, such as the Sino-Vietnamese War. Scobell (2002:3) points out that, not only does China have a 'cult of defence', consistently announcing a policy of peaceful, non-expansionist, defensive strategy for the national defence, but the justice of using military force is also stressed, under the 'name' of adopting an offensive or pre-emptive attack. This 'stealthy' aggression has become one of the features of Chinese strategic culture apparent in modern Chinese strategy.

3.2.2 *Ancient Chinese philosophy regarding the importance of war*

In addition to the Confucian-Mencian paradigm, there are a number of Chinese ancient discourses on strategy. Some great ancient Chinese philosophers, such as Lao Zi and Mozi, advocated peace based on the ancient philosophical concept that loving everyone is benevolent. Lao Zi thought highly of the 'Benevolent Governance' in the Yao and Shun Ages, and his teaching of 'Benevolent Governance' passed from one generation to another. Lao Zi also fostered the Chinese Doctrine of Kingcraft. In most cases, ancient warfare was intended to ensure the survival of a nation; its purpose was to protect the people in as benevolent a way as possible. Such wars could be considered just, as the aim was to save people in crisis. Often, the army labelled itself the army of victory. The idea of preventing invasion, promotion of justice and the launch of warfare for acceptable reasons stems from the concept of just warfare. The legacy of these ideas is that Chinese strategic culture is characterised by the thinking that one should not invade others, nor should one be invaded. The best example of this concept might be the Great Wall. Since ancient times, China placed emphasis on the importance of agriculture. However, nomadic Northern nations attempted invasion at various times throughout the Chinese dynasties. Therefore, Emperor

Qin Shihuang ordered the building of the Great Wall to prevent invasion by the nomads. Militarily, this strategic culture does not reflect a passive defence; rather, it combines defence with attack. This allows for the preparation of warfare whilst simultaneously reducing the enemy's combat capability. Once the upper hand is gained, warfare would turn from defence to attack.

In Ralph Sawyer's (2007:2) view, the seven military classic monographs[75] in ancient China are the textual foundation for official examinations of both tactical and strategic conceptualisation, providing a common ground for the ancient Chinese philosophies of war. These monographs include Sun Tzu's *The Art of War*, which is the most significant work to represent ancient Chinese strategic thought. It is referred to intensively by Mao Zedong in his theory of People's War.[76] As Taiwanese scholars Shen and Wan (2006:3) argue, two points can be extrapolated from these seven classic monographs: the first is the importance of making a state wealthy, and reinforcing military capability; the second is to focus on the flexibility and diversity of the art of war. In addition, it can be concluded that the philosophy and principles of People's War originate from Sun Tzu's strategic thought. Sun Tzu said, 'Warfare is the greatest affair of state, the basis of life and death, the Way [Dao] to survival or extinction. It must be thoroughly pondered and analysed.' (trans. by Sawyer, 2007:157) This implies that warfare is very important for nations and accordingly the importance of the populace cannot be neglected, a key aspect of People's War. In addition, Mao's 16 character formula '*Enemy progresses, we retreat; Enemy halts, we harass; enemy tires, we attack; enemy retreats, we pursue*' reflects Sun Tzu's strategic thought. The mobile wafare maxim '*Enemy progresses, we retreat*' is reminiscent of Sun Tzu's 'If they [enemy] are strong, avoid them' in the chapter Initial Estimations, and 'One who excels at employing the army avoids their ardent *chi* [life force]' in the chapter Military Combat. (trans. by Sawyer, 2007:158, 170) '*Enemy halts, we harass*', referring to guerrilla warfare, relates to Sun Tzu's 'If they are rested, force them to exert themselves.' (trans. by Sawyer, 2007:158) '*Enemy tires, we attack*' mirrors Sun Tzu's 'Create disorder [in their forces] and

[75] The seven military classics are: 'Tai Kung's Six Secret Teachings,' 'The Methods of the Ssu-ma,' 'Sun Tzu's Art of War,' 'Wu Zi,' 'Wei Liao Zi,' 'Three Strategies of Huang Shih-kung' and 'Questions and Replies Between Tang Tai-tung and Li Wei-kung.' (Sawyer, 2007:vii-viii)

[76] According to Mao's personal letter of the 22nd October 1936, 'Those military collections being bought are not suitable, since most of them are related to tactics. What we need is related to commanding of battles and strategy. Based on this requirement, please buy Sun Tzu's "*The Art of War*".' (Mao, 1936)

take them.' (trans. by Sawyer, 2007:158) Finally, '*enemy retreats, we pursue*' is similar to Sun Tzu's 'Strike when it [the enemy] is indolent or exhausted.' (trans. by Sawyer, 2007:170) Furthermore, the concept of 'active defence' in People's War can be seen in Sun Tzu insistence on the necessity of pre-emption in a campaign: 'Whoever occupies the battleground first and awaits the enemy will be at ease; whoever occupies the battleground afterward and must race to the conflict will be fatigued. Thus one who excels at warfare compels men and is not compelled by other men.' (trans. by Sawyer, 2007:166) In terms of mobilisation of the people, as Sun Tzu points out, 'The Dao [way] causes the people to be fully in accord with the ruler,' (trans. by Sawyer, 2007:157) He thus believes that it is very important to earn the full support of the people. What's more, it can be argued that the concept of asymmetric warfare, including guerrilla warfare and information warfare, also manifests a connection between People's War and Sun Tzu's thought. For instance, in Mao's '*Problems of strategy in China's Revolutionary War*' and '*On Protracted War*,' as Johnston (1995:255) indicates, some precise references can be associated with Sun Tzu's military thoughts. As Peng (2008:31) points out, Mao is inclined to consider a war through dialectics, such as big and small, far and near, before and after, weak and strong, war and peace, old and current, which can also be found in Sun Tzu's writings. For example, Sun Tzu (trans. by Sawyer, 2007:179) wrote: 'to keep the enemy's forward and rear forces from connecting; the many and few from relying on each other; the upper and lower ranks from trusting each other….' in the chapter Nine Terrains, which is a guideline on the strategic mastery of terrain as a tactic of protracted warfare. However, the most classic concept of asymmetric warfare extracted from Sun Tzu is the idea of defeating the enemy without actually fighting. He argues that 'One hundred victories in one hundred battles [physical conflicts] is not the pinnacle of excellence.' 'Subjugating the enemy's army without fighting is the true pinnacle of excellence.' (trans. by Sawyer, 2007:161) Thus, under such a heritage, the PLA's devotion to developing special warfare, such as cyber warfare, can be easily understandable as the desire to reach 'the true pinnacle of excellence' in the digital age.

Though the maxim of subduing the enemy without fighting is perhaps the most important for asymmetric warfare, it is arguable that the most important idea of all in Sun Tzu's work might be the 'war to end all wars.' Johnston (1995)

considers the 245 wars between the Ming Dynasty and great powers near its Northern boundary as proof that the diplomatic policies of the Ming government were characterised by realist values, advocating the notions of 'making good use of every opportunity to achieve victory', 'sustaining the war by means of war', and the 'war to end all wars.'

In summary, modern Chinese strategy is shaped by its strategic culture which is primarily formed from both traditional culture and the ancient Chinese philosophy of war. However, this does not mean that this strategic culture will never change, as Chinese strategic culture does not only rely on its origins, but is also significantly influenced by the political ideology of the Chinese Communist Party (CCP). During China's modern time era, Chinese strategic culture has been greatly modified by Chairman Mao due to the impact of China's Cultural Revolution from the 1960s up to the present, as this kind of 'generational change' is also regarded as an important source of strategic culture. (Lantis and Howlett, 2010:89) As Mao (1991) famously said, 'Political power grows out of the barrel of a gun,' and 'With guns the whole world can be transformed.' These sayings have indoctrinated the Chinese people and their political leaders since as early as 1927, and accordingly continue to influence Chinese modern strategy. From this view, it may be argued that Chinese modern strategy does not truly call for peace as it has done in ancient times, despite the claims of many Chinese theorists. As a result, it may be that China's cyber warfare includes the significant addition of threats and specific attacks to discourage adversaries from waging a war, channelling the concept of a 'war to end all wars.'

Further to this, the PRC is one of the few Communist states, with the largest number of Communist Party members in the world. The PRC's Constitution regulates that the CCP leads the state's armed forces and the government simultaneously in a 'one-party state'[77]. Though the PRC has conducted a policy of economic opening since Deng Xiaoping's era, reforming the societal sector and establishing many private enterprises, the deep-rooted one-party system has not been altered. As analysed previously, strategic culture is not just influenced by traditional culture, but also by the political elite, the primary actors formulating state

[77] Shambaugh points out that China's political system is that of a one-party state, and the source of this one-party dominance is the close link between the military and the ruling party. He also suggests that this one-party state must study the transition from authoritarianism to democracy, so that the regime can build social bases of support and form other political parties. (Shambaugh, 2009:96-97)

strategy and carrying out strategic behaviour. In China, the political elite are the members of the CCP and are heavily influenced by the tenets of the CCP. As Shambaugh (2009:144-145) indicates, the CCP has a Party school system to cultivate the political elite. Undergoing this training programme has become an essential experience for an advanced career in China's political system. The ideology of the political elite, who heavily influence Chinese strategic culture, is formed in this party school system.[78]

Undoubtedly, in accordance with traditional Chinese culture such as the Confucian-Mencian paradigm, Chinese strategic culture traditionally seeks peace and pursues defence rather than offence.[79] However, the strategic culture in the PRC is certainly influenced by the ideology of the CCP. As pointed out by Shen Weiguang, known respectfully as the 'father of Chinese Information Warfare', socialism with Chinese characteristics exhibits features of Leninism, Mao Zedong Thought, Deng Xiaoping Theory, and the Three Represents. (2005:168) These ideas consistently shape the ideology of the CCP, even though current PRC policies diverge from the origins of Communism and do not advocate dictatorship of the proletariat. In addition, nationalism and active defence are considered useful approaches against imperial invasion in the PRC, which still regards powerful Western states, such as the USA, as imperialists. Chinese strategic culture has thus differentiated from traditional Chinese culture. Furthermore, Johnston (1996:217) argues that China has presented a consistent '*realpolitik*' or '*parabellum*' strategic culture. He moreover indicates that 'Chinese decision makers have internalised this strategic culture such that China's strategic behaviour exhibits a preference for offensive uses of force.' (Johnston 3, 1996:217) In this case, the PRC's development of asymmetric warfare as a strategy of pre-emption under the auspices of active

[78] This school system is called the 'Central Party School.' Several key functions are fulfilled through a variety of training programmes, including: (Shambaugh, 2009:144)

1. Marxist-Leninist ideology and the latest party policy documents.
2. Mechanisms and methods of party organisational control.

In addition, the Central Party School is a national-level party school, divided into several different sub-levels, such as provincial party schools, county party schools and even overseas party schools, and also including several cadre academies.(Shambaugh, 2008:829-838) The structure of this nationwide school system is fairly complex.

[79] Wang Hongxu, Director of the Institute for International Strategic Studies at the CCP Party School, argues that Chinese leaders from Mao to Hu have been influenced by the ideology of Chinese traditions upon their strategic thinking. Leaders potentially apply such aspects as the Way (道, *dao*) and ritual propriety (禮, *li*) [investigated earlier in section 3.2.1], to China's policy-making. (Wang, 2011)

defence, despite justifications of righteousness when waging war, would come as no real surprise.

3.3 People's War: a critical doctrine in modern Chinese Strategy

As examined later in Section 3.3.1, the term 'People's War' originally coined in Egels' work in 1849. Egels' idea inspired Mao Zedong (also written as Mao Tze-Tung) to carry out the concept of China's People's War in 1927, which gradually became the most significant strategic thinking in modern Chinese strategy and has been well-known in the world for decades. In addition, Mao first read Clausewitz's work '*On War*' in 1937, and subsequently applied the concepts put forward by Clausewitz in his claim that warfare is the most typical form of political struggle. (Mao, 1991:171) In fact, some ideas of People's War are similar to the concepts put forward by Clausewitz. Clausewitz (2001:170)[80] argues that war relying on a normal army is general warfare and war waged by the power of the masses is an authentic 'people's war'. The countries that best employ the approach of people's war will draw more advantages than countries which neglect the idea. (Clausewitz, 2001:464-465) As a result, it is therefore arguable that Mao's military though, primarily a People's War, is actually a hybrid of Western strategic thinking and Chinese traditions.

Furthermore, strategy is a highly contentious concept, and there is no exception to this in the case of modern Chinese strategy. Tactics of warfare may be changed due to the development of military technology, but a state's strategy, which is beyond the level of tactics, is always bound to a state's interests. The state will guide any approach to warfare in line with these interests. In this way, strategy not only influences policy making but is also the guideline for development of military power, including military organisations, tactics, doctrine, national defence expenditure, logistics, and weapons technology. Some Western research considers People's War to be an outdated, redundant concept with no research value.[81] For

[80] This is a Chinese edition directly translated from '*Vom Kriege*' which is the original German work of Clausewitz. The Chinese edition is titled '*戰爭論 (Zhanzheng Lun, The theory of war).*' (Clausewitz, 2001)

[81] Godwin claims that if the concept of Mao's People's War is not dispensed with, it will impede the modernisation of the People's Liberation Army. (Godwin, 1987:589) Joffe indicates that, in practice, the Chinese army has abandoned the concept of People's War, though due to ideological and political reasons, they still claim to be following the military doctrine of People's War derived from Mao's original conception. As an operational guide to fighting and force-building, 'Maoist doctrine has not been developed by China's post-Mao leaders; it has been almost completely abandoned.' (Joffe, 1987:571)

example, Shambaugh (1999:663) asserts that Western researchers pay too much attention to the threats of China instead of the meaning behind the threats. In terms of a different strategic culture, most recently Pillsbury (2008:181-183) has indicated that Western research of Chinese military affairs neglects the traditional stealth of the Chinese military and any methods potentially adopted to deceive the enemy. Taiwanese scholar Luo Chin-Bo (2005:26) also implies that Western strategists would rather study Sun Tzu's *Art of War* than investigate why the People's Republic of China (PRC) continues to insist on the concept of 'People's War' as the guideline of modern Chinese strategy. However, if underlying misapprehensions about modern Chinese strategy can be clarified and eradicated, it will be understood why China in fact still insists on the legitimacy of People's War. This is therefore a vital research direction.

Since the initial proposal of the idea of People's War, modern Chinese strategy has through time undergone three key stages: 'People's War' (1927-1977), 'People's War under Modern Conditions' (1978-1991) and 'Local Wars under High-Tech Conditions' (1992-present). These transitions were due to the influences of the different time periods, Chinese leaderships, and related circumstances.[82] Recent research concludes that the Chinese scholars who guide warfare mainly pertain to three schools of thought, namely the school of People's War, the school of local war, and the school of military revolution.[83] Furthermore, Michael Pillsbury (2000:268) argues that these three schools potentially reflect the current structure of Chinese defensive power and the development of military doctrines and theories. In accordance with his research, 80% of his 55 interviewees, who are Chinese scholars, strategists, or military officers, believe that the People's Liberation Army should follow the school of People's War, even though Western researchers generally conjecture that modern Chinese strategy now merely follows the current doctrine of 'Local War under Hi-Tech Conditions', and that People's War is now an outdated

[82] The timeframe of the key stages in the transformation of Chinese military strategy from 1927 to the present day remains contentious and different scholars put forward different dates. This research refers to the timeframes identified by Burles and Shulsky (2000:21-36)

[83] Michael Pillsbury, a leading US scholar of China Studies, led a research team to study and evaluate Chinese military power in 2000 in terms of various aspects influencing future national security, thus identifying the three schools of thought. (Pillsbury, 2000:269) Pillsbury is a consultant to the US government in Washington DC and has advised the Pentagon for more than three decades, including a year as Special Assistant for Asian Affairs at the Net Assessment Office, two years as Assistant Undersecretary of Defense for Policy Planning, and several years at the RAND Corporation and the National Defense University. His book incorporates more than 600 quotations from over 200 Chinese authors since 1994.

concept. As the school of People's War still dominates the senior level of Chinese leadership, it can accordingly be concluded that the ideas of People's War will continue to influence modern Chinese strategy. In addition, as Pillsbury (2000:292-296) points out, though the three schools decline to accept each other's views, there is one concept common amongst all three. This is that the strategy of asymmetric warfare will inevitably continue to be developed in China. The most significant form of asymmetric warfare is cyber warfare, a type of warfare which mainly deals with the control of information in cyberspace, a potential battlefield beyond the scope of land, sea and air. Chinese military leaders strongly believe that dominance of information is an effective asymmetric approach in which 'the inferior can defeat the superior.' According to Pillsbury's interviews, it is believed that Information Warfare has been linked with People's War.[84]

At each stage of modern Chinese strategy, the concept of People's War has been an invariable characteristic of state strategy, and its principles to this day still underlie the fundamental ideology of Chinese military thought despite the passing of time. It is thus essential for a true understanding of modern Chinese strategy that the principles of People's War be examined, as well as the application of People's War in each of the three key stages identified above. In addition, it will be suggested that the principles of People's War have always been, and remain, the constant guideline of modern Chinese strategy, but that they have switched from an operational guideline on a tactical level, applied in the 19th century, to conceptual principles on a strategic level behind the development of Comprehensive National Power (CNP)[85] in the 21st century. In order to interpret this argument, the following sections investigate the origins and legacy of People's War. Firstly, since 1927, how did the concept of People's War originate and develop from Mao's military thought? Secondly, the concept of People's War continued after 1978 when Deng Xiaoping

[84] According to an example given in Pillsbury's research, the interviewee clearly points out that 'The concept of People's War of the olden days is bound to continue to be enriched, improved and updated in the information age to take on a brand-new form. . . . only by bringing relevant systems into play and combining human intelligence with artificial intelligence under effective organisation and coordination can we drown our enemies in the ocean of an information offensive. A people's war in the context of information warfare is carried out by hundreds of millions of people using open-type modern information systems.' (Pillsbury, 2000:292)

[85] 'Comprehensive National Power' (CNP) (綜合國力, *zonghe guoli*) is a term employed by the PRC's leadership to represent the evaluation of possible variables for China's national power. Its concept basically means the sum of total powers and resources for a state to be survived. It is evaluated through five factors: natural resources, population, economy, military and technology. China values population as the most important factor. (Li, 2010:257-260)

took over the Chinese leadership. This period was an important turning point in the history of the PRC because the reforms started at this time still continue in China at present. During the process of modernisation led by Deng, how did the concepts of People's War continue to be developed alongside Deng's military theory? Although the Four Modernisations[86] of the Chinese Communist policy were conducted very successfully, in relative terms the pace of military modernisation was significantly slow. Thirdly, how did the concept of People's War under the leadership of Jiang Zemin in 1992 transform into the new concept of 'Local War under High-Tech Conditions'? Finally, how will the concept of People's War develop in order to tackle future challenges in China? The different periods are shown in Figure-3 below.

<table>
<tr><th>1927-1977</th><th>1978-1991</th><th>1992-present</th></tr>
<tr><td>People's War</td><td></td><td></td></tr>
<tr><td rowspan="2"></td><td>People's War under Modern Conditions</td><td></td></tr>
<tr><td></td><td>Local Wars under Hi-Tech Conditions</td></tr>
<tr><td>Tactical Level</td><td colspan="2">Strategic Level</td></tr>
</table>

Figure-3: Transformation of Modern Chinese Strategy

The figure above presents the fact that 'People's War' has constantly been a doctrine of modern Chinese strategy from 1927 to present. In the first stage, from 1927 to 1977, People's War was a principle at the tactical level of military operations on the massive battleground of Mainland China. In the following two stages after 1977 (though the term itself does not appear in the title of the latest stage) People's War was transformed into a national strategic level principle. In this regard, it is also used to address international affairs, and has become a primary principle reinforcing state strategy in different dimensions; not only in the military, but also in economics, the societal sector and national construction (key aspects of China's Comprehensive National Power (CNP)[87]. The principle of People's War itself has not changed, but has instead been applied to different levels and fields, for

[86] The Four Modernisations are the goals of Deng Xiaoping's reforms. They were first announced by Zhou Enlai in 1975 at the Fourth National People's Congress in one of his last public acts. After his death and Mao's soon thereafter, Deng Xiaoping assumed control of the party in late 1978. In December 1978 at the Third Plenum of the 11th Central Committee, Deng Xiaoping announced the official launch of the Four Modernisations, formally marking the beginning of the reform era. The Four Modernisations were in the fields of agriculture, industry, technology and defence. (Finkelstein, 1999:103)

[87] Please refer to the definition in Glossary.

example by shifting from campaigns on domestic battlefields to the conduct of foreign affairs.

3.3.1 *Origins of People's War (1927-1977)*

The term 'People's War' originally appeared in Engels' works in 1849.[88] He stresses that a people which pursues independence should not solely use general methods of military operations. Instead, those that are weak in military terms should employ guerrilla warfare and enter revolutionary war to defeat those stronger than themselves. Two theoretical components feature in Engels' definition of People's War. The first is that the party using People's War should strive to reach the enemy's limits of strategic offence. The other is that relying on a populace striving for resistance speeds up the process of attaining the enemy's limits of strategic offence. In 1927, Mao Zedong applied Engels' theory to the revolutionary war in China. Mao's own experiences of the Chinese Civil War shaped and cultivated his military ideology, leading to the development of 'People's War,' which he later officially affirmed in the 7th National Congress of the Communist Party of China (CPC) in 1945. 'People's War' originally began as a special method of using the masses in a societal exercise. It could be argued that Mao's People's War applied military discipline to the masses in order to mobilise them for a political purpose. However, due to differing social conditions throughout history, People's War has taken on different forms since its creation. When evaluated theoretically from a military perspective, the concept of People's War can be raised from a tactical level to a strategic level. The *Chinese Military Encyclopaedia*,[89] states that '*People's War is to seek the liberation of class or against foreign aggression, and organise and arm the masses for war. The People's War is in accordance with the fundamental interests of the oppressed*

[88] The term 'People's War' originated in Engels' work '*The defeat of the Piedmontese*' written in 1849 and first published in the *Neue Rheinische Zeitung* No. 260-263, March 31, April 1 and 4, 1849 in Germany. This work is based on the battle of Novara between Italy and Austria in 1848. Engels believed that the reason behind the defeat of the Piedmontese is that, due to his personal weaknesses, the King of Piedmont naïvely chose to rely on his limited regular army to protect against Austrian attack rather than mobilising the oppressed masses to fight. Engels extrapolates that a revolutionary war must rely on the masses and employ the style of people's war, so that oppressed peoples can be liberated. This idea inspired Mao's conception of People's War in China. The English edition of Engels' works can be found on '*Engels in Neue Rheinische Zeitung March/April 1849*' on the website of Marxists Internet Archive accessed via: http://www.marxists.org/archive/marx/works/1849/03/31a.htm#263.

[89] The Chinese Military Encyclopaedia 1997 was co-edited by many Chinese military organisations and institutions. The quotation is translated by the author of this research.

classes and the oppressed nations.' (Zhang Zhen, 1997:547) People's War can also be the subject of scientific studies into the features and rules of war, which may eventually apply as a guideline to the decision of either waging or preventing a war. (Zhang Zhen, 1997:1)

Some strategists regard People's War as a military doctrine as well as a principle of the use of the armed forces. However Taiwanese scholar Shuh-Fan Ding (1996:35-43) argues that such a point of view actually refers only to the tactical level of People's War. Thus, in order to truly comprehend People's War, the military philosophy behind it must be examined. As Ding (1996:43) points out, some Chinese scholars may consider People's War to be akin to a military theory in its own right, as it contains three elements which could elevate this idea to such a level. Firstly, People's War meets the criteria of being a philosophy, providing theoretical guidance for military actions; secondly, People's War employs an army, which serves it in practice; and thirdly, People's War has a clear set of tactics, for use by its military forces. (Ding, 1996:43) In addition, the concept of People's War can be found in Chinese military philosophy, the construction of the Chinese national defence and the principles of Chinese operational tactics. Ding (1996:19) also points out that the concept of People's War could in the future evolve into a complete military science as it currently heavily dominates the study of Chinese military science. (Ding, 1996:19) Two of the PRC's strongest leaders have backed the practice of People's War: during the Chinese Civil War, Mao stressed that 'our strategies and tactics are established upon the basis of People's War' (Mao, 1991:1248) Deng additionally acknowledged that Chinese strategy was formed by Chairman Mao and Mao's key strategic principle was People's War. (Peng, 2000:173) Furthermore, Chinese academia shows that the military thought first proposed by Mao consists of three elements: the notion of People's War, the idea of constructing a 'people's army' and the operational approaches of People's War. In 2002 Chinese scholar Pan Zhaohuan reported that the senior generals then in office regarded the philosophy, strategy and tactics of People's War as the core of Mao Zedong's thought. (Pan, 2002:13) As Pan (1992:7-8) indicates, the Japanese Defence Report 1962 states that 'respecting the thoughts of soldiers and people' is included in the military thought of Chairman Mao. The report also indicates that Mao's People's War combines the concept of total militarisation with the development of military meritocracy. It has been clearly

indicated that in terms of contemporary Chinese strategy, the concept of People's War already formed China's national defence doctrine in Mao's time. (Baylis et al., 1987:132-135) Mao's tactics of deterrence against threats from 'imperialists', such as the US and the USSR, were based on the fact that at that time China was vulnerable and weak. Mao advocated the idea that 'everyone is a soldier' in order to conduct 'Protracted War' as an operational guideline for guerrilla warfare. (Baylis et al., 1987:133) Thus, the concept of People's War was clearly a key element in Mao's military thought. Mobilisation of the masses, total militarisation, and harnessing of the people's will to defeat the enemy were the goals of People's War. The core and critical ideas of People's War were formulated from these three goals.

Moreover, in terms of a people's army, Mao drew conclusions from previous experiences of armed struggle and decided that the first issue of People's War for the Chinese armed struggle was to organise peasants' armed forces into a people's army. Mao said that 'To struggle for the creation of an army of the Chinese people is the task of the whole nation. Without an army of the people there will be nothing for the people.' (Mao III, 1954:291) The principle behind the construction of the people's army may be founded on the Marxist guideline of a revolution of the proletariat. The proletariat in China at that time were peasants, as China was a country established upon the agricultural industry, and according to Mao: 'The armed struggle of the Chinese Communist Party is peasant war under the leadership of the proletariat.'[90] (Mao, 1991:609) Furthermore, according to ancient Chinese works on warfare, the scale of peasant uprising and peasant war in Chinese history had been extremely large and virtually unmatched in the rest of the world. Only in Chinese semi-feudal society can such a large-scale uprising be found. (Mao, 1991:630-635)

In order to successfully construct the people's army, it was necessary to provide and follow a theoretical approach and strict guidelines, so that the armed forces, made up mostly of peasants, could be transformed into a people's army with strong discipline and high military attainment, whilst still retaining the character of the proletariat and a close association with the masses. As the army would originally be drawn from the masses, the army can be impelled to be ready

[90] The English is translated from the Chinese version of 'Selected Works of Mao Tse-Tung III' (Mao, 1954:60)

for battle at all times in order to securely maintain their own fundamental interests. In addition to being ready for battle, the army must also shoulder the responsibility of organising the masses, arming the people, and constructing a new regime through revolution. (Mao, 1991:86) Mao indicated that to establish a strong national defence, the Chinese people must rely on themselves. (Mao II, 1993:524) Mao told the people that, with regards the construction of a people's army, 'What we are doing and investigating is how to industrialise socialism and how to modernise national defence, and then how to cope with the new challenges in the atomic age' (Mao, 1977:144) Mao hoped to build up an army from scratch, take it from a low level of quality to a high level, and in doing so reinforce the modernisation and normalisation of the armed forces. In terms of modernisation, Mao stressed that 'The latest military equipments must be acquired and the latest tactics must be studied alongside them.' Regarding normalisation, Mao required the 'execution of unified command, unified institutionalisation, unified organisation, unified discipline and unified training, in order to carry out perfect joint operations throughout the different services.' (Mao III, 1993:103; 337; 374; 314)

In summary, at the time of origin, it can be concluded that People's War contained the following features, which gave People's War the potential to transform from a tactical to a strategic level. In addition, these features may continue to apply to other forms of warfare in the digital age.

1) **The army and the people are the foundation of victory:**

   Both the people and the army are the main actors conducting warfare. In Mao's '*On Protracted War*,' he states succinctly that 'The army and the people are the foundation of victory.' (Mao & Lawrence, 1954:237) In addition, in terms of both offence or defence, the potential to conduct warfare is deep-rooted in the masses. (Mao, 1991:511) Through his experiences of the Chinese revolution, Mao came to believe that the people are the primary actors in warfare and manpower is the main resource for a successful war.

2) **Conducting/defending against a war must rely on the mobilisation of the people:**

   Mao perceived that it is not enough to simply recognise the importance of the people in a war. It is also vital to know how to mobilise the people to engage in and support warfare. Mao claimed that in order to mobilise the people

effectively and collectively, the political purpose behind the war must be clearly outlined so that the armed forces have a clear understanding of their own actions; the political steps and policies for achieving the final purpose must be illustrated so that the people know how to reach these goals; the propaganda encouraging the people to join up must cater to the masses so that mobilisation can achieve maximum success; and the political motivation behind the armed struggle must be upheld so that the armed forces can be retained. (Mao, 1991:480-481) In addition, the implementation of solutions to the practical problems of the people, as well as consideration of the people's interests, are imperative, so that the masses can see visible benefits and be willing to be mobilised for war. (Yuan, 2000:141)

3) The approach of three combinations of forces:

In order to achieve mobilisation of the people, one of the most significant elements is the approach of three combinations of forces. The first combination is that of the main troops with local troops; the second is the regular army with the guerrilla army; and the third is armed masses with non-armed masses. The integrated power of the people can thus be exerted seamlessly. Local troops can liaise between the main troops and the armed masses, so that each force can provide support to the others. (Mao, 1991:1041)

4) Creation of new battlefields[91]:

According to Mao, a battlefield is a geographical space for opponents to accomplish the purposes behind their warfare and to compete with each other in a certain time limit through operational organisation, format of combat, and operational approaches. (Mao, 1950:58-59) Based on this principle, in the Chinese Civil War Mao harnessed geographical advantages in the battlefield to the greatest extent, so that his inferior army could defeat a relatively superior opponent and play off the enemy's vulnerability by evading their strength in order to gain the final victory.

5) The primary tactics of People's War:

(1) Mao integrated his understanding from past military experiences to propose his tactical concept of guerrilla warfare, which forms the basis of

[91] This involves the deliberate tactic of leading the enemy to new battlefields. This can reflect tactics of manoeuvre warfare, protracted warfare, or attrition warfare, if the military power of the enemy is superior.

People's War theory. The concept is manifested in a 16 character formula from his work of 1928: '*Enemy halts, we harass; enemy tires, we attack; enemy retreats, we pursue.*'[92] (Mao, 1954:212) This formula was produced in accordance with the principle of luring the enemy, but also contains levels of tactical offence and defence. In addition, the formula also interprets the tactical retreat and counterattack. The operational tactics of People's War were developed based on this short formula. (Mao, 1950:54)

(2) Further to that, the concept of People's War emphasises two military methods: 'Mobile Warfare'[93] and 'Positional Warfare.'[94] The former is a basic form of eliminating the opponent by taking advantage of familiarity with the geographical space of the military theatre. The latter involves building up a solid fortification as a hard defensive shell to delay the enemy's attack. (Mulvenon and Yang, 2001:137) Mao indicates that mobile warfare was the major form of combat during the Anti-Japanese War and that guerrilla warfare should be regarded as the secondary form. (Mao II, 1954:224) As James C. Mulvenon and Andrew N.D. Yang (2001:136) state, mobile warfare, positional warfare, and guerrilla warfare are the three basic tactics of People's War put forward by Mao. They can additionally be further developed and applied to modern hi-tech warfare.

(3) There are two 'effects' of People's War in terms of attrition warfare tactics: the first is the 'swarm effect' which involves taking advantage of plentiful manpower to exhaust the enemy on the battlefield; and the second is the 'sting effect': using mobile weaponry equipment to sneak up on the enemy. (Dellios, 1989:205) The purpose of the employment of these two effects is to achieve the measured destruction of the enemy through the use of the masses in the battlefield.

(4) In addition, there are ten principles of operations.[95] These principles had been successfully implemented in Mao's past experiences of military

---

[92] This is taken from the English translated text '*Selected Works of Mao Tz-Dong.*' (Mao and Lawrence, 1954:212)

[93] Mobile Warfare, larger in scale than guerrilla warfare, is the English term for one of Mao Zedong's operational tactics. For the general topic of military mobility, however 'manoeuvre warfare' is the term generally being used in the Western military orthodoxy.

[94] As Mulevnon and Yang (2001:137) point out, the PLA interprets and applies the concept of positional warfare as'digging tunnels and hardening shelters on the battlefield.'

[95] According to the 'Selected Works of Mao Tse-Tung IV,' these ten principles are: 1. Attack dispersed, isolated enemy forces first; attack concentrated, strong enemy forces later. 2. Take small and medium

conflict. Thus, they were viable military approaches to accomplishing the principles of People's War, and could also provide a doctrine for People's War under conditions of different warfare in the future, whilst maintaining the basis of solidarity between the people and the armed forces.

6) Active defence as a deterrence strategy:

Mao stresses that tactics of defence must adopt active, not passive, approaches. (Mao I, 1993) The army and the people should be consolidated for defensive purposes through various methods such as mobilisation of the people, organisation of the militia[96] and the 'three combinations' mentioned previously. Furthermore, this solidarity not only applies to military conflict against the outside threats of imperialists, but also extends to the construction of society and development of the economy to reinforce Comprehensive National Power in the future. Once defensive approaches in a state become active in nature, this may result in the outcome of deterrence.

3.3.2 *The continuing strategic guideline of People's War under Deng (1978-1991)*

Following Mao, Deng took over the leadership of China in 1978. From this time, there was no occurrence of any significant war, so Deng shifted the emphasis of military strategy to focus on a principle centred on national interest. Deng's guideline was entitled 'People's War under Modern Conditions', so titled because Deng believed that Mao's doctrine should be continued and adapted to fit into the new conditions brought about by the advent of the modern era. (Deng I, 1994:10)[97]

This shift further affected Chinese foreign policy, in particular state policy towards the USA. In 1989, at a meeting with former US President Nixon, Deng

---

cities and extensive rural area first; take big cities later. 3. Make wiping out the enemy's effective strength our main objective; do not make holding or seizing a city or place our main objective. 4. In every battle, concentrate an absolutely superior force, encircle the enemy forces completely, strive to wipe them out thoroughly and do not let any escape from the net. 5. Fight no battle unprepared; fight no battle you are not sure of winning; make every effort to be well prepared for each battle. 6. Give full play to our style of fighting – courage in battle, no fear of sacrifice, no fear of fatigue, and continuous fighting. 7. Strive to wipe out the enemy through mobile warfare. 8. With regard to attacking cities, resolutely seize all enemy fortified points which are weakly defended. 9. Replenish our strength with all the arms and most of the personnel captured from the enemy. 10. Make good use of the intervals between campaigns to rest, train and consolidate our troops. (Mao, 1967:161-162)

[96] Militia means a military force that is raised from the civil population to supplement a regular army under certain conditions.

[97] The 'Selected Works of Deng Xiaoping' is divided into three volumes. Volume I records Deng's works from 1938 to 1965; volume II is from 1975 to 1982; and volume III is from 1982 to 1992. Volume III was published in 1993, and afterwards volume I and II were published in 1994.

clearly expressed that both China and the USA recognised the principle that each state would choose to look after their own interests above all else. (Deng II, 1993:79) In addition, Ross (2009:15) points out that during the time of their respective leaderships, both President George H. W. Bush and Deng Xiaoping sought to stabilise relations between China and the USA. As Mi (2004:308) states, Deng's strategic theory was not merely the guidance for military operations, but also concentrated on the importance of national construction and development. Deng himself proclaimed that the most important interest for China was national stability. (Deng II, 1993:284) This stability would have to be established upon the foundation of China's continuing modernisation, so Deng was keen to promote his agenda of domestic military reforms and 'opening and reform policy' to open the doors of China to the international economic market. (Ross, 2009:16) Mao's leadership was established in wartime, when the primary task of the Chinese Communist Party was the overthrow of the Nationalist Party regime. However, after World War II and the conclusion of the Chinese Civil War, Deng believed that there would not be any more large-scale wars for at least a few decades to come. (Deng I, 1994:77) In addition, O'Dowd (2007) claims that China's lack of success in the Sino-Vietnamese War of 1979 revealed the poor quality of the manpower, equipment and logistics of the Chinese military at the time. As Scobell (2003:411-415) argues, after the Second World War there was a phase of intense technological development throughout the world, including military technology, potentially causing a deep concern about the quality of the soldiers who would be required to master such modern equipment in the future. Deng's military theory therefore not only made sure to follow the doctrine of People's War, but also provided new related guidelines on waging 'local wars'[98] under modern conditions. In 1978, Deng shifted military theory from 'People's War' to 'People's War under Modern Conditions'. (Joffe, 1987:557) Joffe (1987:559) claims that the People's Liberation Army (PLA) had to add some new ideas to the traditional concept of People's War in order to effectively tackle the new challenges raised by the change of Chinese leadership. He indicates, for instance,

[98] According to Chinese national strategy, as identified by Burles and Shulsky (2000:31), there are five types of 'local war': '(1) small-scale border conflicts, (2) contention for territorial seas and islands, (3) surprise air attacks, (4) resistance against partial hostile intrusions, and (5) punitive counterattack.'

that the idea of luring the enemy in[99] may not be applicable to future warfare, and so it would be imperative to study new methods of warfare and adjust the role of the guerrilla troops and the militia. (Joffe, 1987:560)

How, then, was the concept of People's War continuingly developed alongside Deng's military theory? Firstly, Deng inherited the basic concept of mobilising the people, but used this for the purpose of the construction of the national defence rather than for carrying out military operations, as in Mao's era. As Liu (2000:113) points out, 'People's War under Modern Conditions' still emphasises mobilising people in various sectors to reinforce the ability of China's national defence. The data of Comprehensive National Power (CNP)[100] can provide quantitative statistics on the potential for mobilisation of the people. Secondly, in terms of application and construction of armed forces, Deng maintained the concept of the 'three combinations', though in 1987 he refined the combinations to field troops, local troops, and militia.[101] The guiding principle for the establishment of the militia was to control quantity, refine quality, place emphasis only on what is truly important, and construct a strong foundation. (Liu, 2000:115) In addition, Deng stressed that the army must be able to cope with a sudden outbreak of war on a local scale and be prepared for a war on a large scale. (Peng, 2000:174) Crucially, People's War must be adjusted to fit the features of modern warfare. Future warfare would be conducted in modern conditions. Therefore, in addition to development of military technology and weaponry, cultivation of military manpower, militia and soldiers would be necessary to strengthen the effectiveness of People's War. (Deng-2, 1993:46) As much as 90% of the PLA is considered to be a 'junkyard army' by some Western scholars, but as Bitzinger (2001:41) insists, they must not be overlooked. He emphasises that extensive manpower is far from being useless in local wars under modern conditions, and that superior weapons technology is not the be-all and end-all.

[99] 'Lure the enemy in' is a tactic of 'strategic retreat' from Mao's military thought. Facing invasion from outside imperialists, it would have been unlikely to successfully prevent the enemy from encroaching on territory, and so it would in fact be better to let the enemy enter further into the territory where the CCP would be more likely to win struggles. (Wang, 1999:94) As Elleman (2002) argues, the idea of luring the enemy in was a way of using geographical space to buy time.

[100] Comprehensive National Power is a thorough indication of the Chinese state's politics, economy, military, technology, diplomacy, education, and culture.

[101] The three combinations of Mao's People's War involved normal troops, guerrilla troops and militia. (Deng Xiaoping, 1993:46) In 1983 the PRC rebuilt the system of the reserve forces and organised tens of reserve military divisions in order to reinforce military power after a massive downsizing of the regular army. (Liu, 2000:115)

Collins (1973:18) also argues that a fundamental struggle is for the consolidation of the people's will.[102] This is the key issue in any military conflict and other issues like superiority of weapons are in fact not as crucial.

In conclusion, Deng's military strategy was inherited from Mao's People's War. Despite the changes in strategy, Deng believed that wars under modern conditions could still be fought through the practice of People's War. Modern conditions merely changed the materials used, but did not affect the true essence of war. In addition, Deng insisted that due to these modern conditions, the concept of People's War must be combined with a modernisation of the national defence and armed forces. It could therefore be argued that in Deng's era, People's War had attained an advanced level. People's War at this level used Deng's policy of the 'Four Modernisations' to allow more power to be released from all societal sectors, so that the power of the people could be combined with the regular army to prepare for or even prevent a war. Comparatively, People's War in Mao's era was at a more basic level. Deng further claimed that the tactical thought of his military strategy was that of 'active defence.' (Deng, 1992:97) Though this was the guiding idea at a strategic level, at an operational level necessary offensive approaches must also be adopted. Deng (1992:98) stressed his four basic intents: to embed defence into offence and merge the two; to be prepared for war at any time; to defeat the enemy with a well thought out plan[103]; and to follow the tactic of protracted war.[104]

3.3.3 *The guideline of 'Local War under Hi-Tech Conditions' (1992-present)*

Jiang Zemin took over the Chinese leadership in 1989. His military experience was not as abundant as Mao's or Deng's, and as a result, his military thought basically rested upon the military theories of his predecessors, as well as being influenced by domestic and international factors during that time[105]. Jiang

---

[102] According to Collins' interpretation of strategic thought, revolutionary warfare (such as People's War) falls into a different category of warfare to that merely waged in land, sea and aerospace. He believes that revolutionary war goes beyond geographical territory into the realms of politics, society, and psychology. (Collins, 1972:18)

[103] According to Deng's theory, if war is inevitable, it is best to focus on good preparation in peace time to achieve victory on the battlefield in wartime. (Liu, 2000:26, 91)

[104] Deng's guidelines emphasised that the PLA must strive for the goal of being constantly prepared for a long drawn-out war. (Liu, 2000:93)

[105] Domestic factors include the Tiananmen Square protests of 1989, disadvantages caused by economic reform, and the return of Hong Kong and Macao to China. International factors include economical sanctions against China for human rights abuse following the 1989 Tiananmen Square protests, the terrorist attacks of September 11th 2001 in New York, the 1991 Gulf War, the conflict in Kosovo, and

therefore changed China's strategic guideline from being based on the battleground to focusing on the development of national power, causing the transformation in China's strategy to 'Local War under Hi-Tech Conditions.'

It can be argued that the Chinese leadership would invariably regard the massive Chinese populace as a fundamental basis of strategy throughout time, from the period of traditional battlefields to any new developmental stages. Thus, the idea of People's War was retained by Jiang with regards the development of national power. Jiang proclaimed two basic changes: military strategy would shift from local wars under 'general conditions' to local wars under 'hi-tech conditions'[106]; secondly, the army must begin to follow a model of qualitative efficiency rather than one of mere quantitative scale (Xiao, 2004:141-142) These two basic changes formed the direction of military development during this period. Additionally, in order to strengthen the political loyalty of the populace, Jiang (2001:2) announced the 'Three Represents.'[107] According to the 2002 China National Defence report, the 'Three Represents' have since been written into the Constitution of the PRC (as the 'important thought of Three Represents') so that the PLA is required to learn and implement them by law. These 'represents' are not only designed to re-assert the exclusive leadership of the Chinese Communist Party in China but also to stress the goals of revolutionising, modernising, and normalising the PLA. As Shambaugh (1996:274) states, due to these changes, since 1989 the PLA have gained more and more influence in the higher echelons of the Chinese political environment. In addition, according to Taiwanese researcher Wong (2007:272), Jiang realised that the assurance of efficient logistics was an essential factor in winning a local war under hi-tech conditions, since the scale of consumption of resources can be extremely unpredictable in operational forms of modernised warfare. As the Congressional Report of the United States (2003:21) points out, despite the PRC having the largest army in the world, the Chinese military would not have been able to successfully wage a war

---

the Third Taiwan Strait Crisis in 1995-96. All served to convince Chinese leaders that they had to re-assess how they should prepare for future conflicts. (Scobell, 2008:34)

[106] Jiang announced his military strategy of 'winning local wars under hi-tech conditions' at the PRC Central Military Commission in 1993.

[107] The 'Three Represents (三個代表, *Sange Daibiao*)', a socio-political ideology of the Chinese Communist Party (CCP), was first introduced officially by Jiang Zemin at the 16th Party Congress in 2002. The 'Three Represents' are: The CCP represents advanced social productive force; the CCP represents the progressive course of China's advanced culture; the CCP represents the fundamental interests of the majority. (Jiang, 2002)

outside the Chinese territory due to the lack of supportive technology and logistics at the time. Shambaugh (2004:10) also argues that the Chinese army was at this point around 20 years behind the US army in terms of development of military technology. Therefore, it became necessary to reform China's military affairs and distribute strategic resources more effectively.

Finkelstein (2004:11-13) claims that since 1995, the PLA has presented its determination to standardise and legalise army modernisation. New defence law and relevant regulations have been generated in order to reform military affairs, including military personnel, logistics, acquisition, and technology R&D.[108] Institutional reform of the military has thus become the core issue of the army's development. The PLA's Revolution in Military Affairs (RMA)[109] is based on the inherent characteristics of China's military. According to the 2004 China Defence Report, China's armed forces were reduced by 200,000 soldiers alongside a simultaneous reinforcement of the navy, air force and 2nd artillery troops. In addition a boost was given to the information infrastructure and weaponry modernisation was accelerated. In addition, the PLA began to conduct a strategic scheme to identify talent. This is a crucial scheme in the institutional reform which emphasises that high quality in the military is vital to achieving the aims of People's War under hi-tech conditions. As stated in the 2004 China Defence Report, Jiang devised a plan to implement the scheme in 2003, in order to cultivate the military elite in the long-term. This plan is divided into two stages: firstly, the quality of military manpower will be visibly refined by 2010; and secondly a vast leap in quality of the military elite will be made between 2011 and 2020. [110] Jiang also clearly indicates that within 10-20 years the PLA will have 'informationised' troops which can, through training, easily master information warfare.

During his leadership, Jiang generated the military theory of 'Winning Local Wars under Hi-Tech Conditions' and devoted himself to reforming the PLA by carrying out a RMA with the Chinese characteristics outlined by People's War.

[108] For instance, in 1999 PLA Civilian Regulations were enacted and in 2000, the PRC Military Officer Law was enacted. In addition, the PLA also established the Professional Military Education System and a professional corps of non-commissioned officers. (Finkelstein, 2004:13-15)

[109] Please refer to Section 3.4 for more details.

[110] As Scobell (2009:10) notes, the first major reform would inevitably involve a massive downsizing of the force. Since 1985, the PLA's manpower has been reduced by approximately 1.7 million people. More recently, the "Active-Duty Officers Law" launched mandatory retirement ages for each officer grade as well as minimum service requirements prior to retirement eligibility.

However, unlike in Mao's era, where the main tactic was to lure the enemy into a certain geographical territory and then wear them down by the use of sheer numbers, Jiang's concept of People's War 'under high-tech conditions' involves strategically mobilising the people and enabling defeat of the militarily superior despite possible military inferiority on the part of China. The features of 'Local Wars under Hi-Tech Conditions' are: the geographical space of war is smaller; the pace and progress of war is faster; and due to these conditions, the transparency of information and accuracy of attack have become much more important in warfare than they used to be, thus changing the face of war. Furthermore, as a Chinese scholar (Zhang, 1999:84) states, 'hi-tech conditions' basically refer to the conditions of information warfare. The strategy of 'Winning Local Wars under Hi-Tech Conditions' guides the preparation of military operations in accordance with the features of information warfare, and focuses on the preparation of warfare to comply with the transformation from the industrial age to the information age. (Zhang, 1999:184)

In 2004, Hu Jintao took over the Chinese leadership. In 2006, he clearly specified that the PRC must accelerate informationisation and aim to 'win local wars under *information* conditions'. (Xiu and Yang, 2007:82) Meanwhile, 'active defence' has still been retained as the main tactic to achieve this strategic aim and in fact, since 2006, has become even more of a clear tactic than it originally was. As Peng (2006:228) points out, in terms of active defence, to offend is in order to defend and to retreat is in order to progress. In addition, recent research shows that modern Chinese strategy persistently focuses on tactics and techniques, such as rapid movements, surprise, deception, camouflage, and concealment, by which 'military inferiority can overcome the military superiority.' (Blasko, 2003:66) As Chinese scholar Deng (2006:219) points out, the original army of the Chinese Communist Party (CCP) used old equipment to successfully defeat an enemy using modern equipment. Having access to superior high technology, following traditional military principles and conducting regular warfare, are no longer necessarily satisfactory to overcome all of a range of potential attacks in new warfare. Deng (2006:219) asserts that the operational thought of 'an inferior military defeating superior adversaries' reflects the basic idea of 'asymmetric

warfare,'[111] which has been studied by many Chinese strategists recently. Blasko (2003:66) points out that a report of the US-China Economic and Security Review Commission concludes that the PLA is fascinated by asymmetric strategies such as cyber warfare and information warfare due to the belief that these strategies can counter the military superiority of countries such as the USA. Taiwanese scholar Li-Ming Gu (2009:79) also indicates that the implicit concept of People's War is the insistence on implementing asymmetric warfare. He additionally states that the mobilisation of people has been modified to focus on indirect mobilisation of the private sectors of society, a strategy which applies to new forms of battlefield, such as cyber space, the economy, trade, information, and psychology.

3.4 China's Revolution in Military Affairs (RMA)

Apart from Chinese strategic culture and the passing of traditional doctrine from one generation to another, the Revolution in Military Affairs (RMA)[112] is another key influence on modern Chinese strategy. The RMA creates policy for China to develop cyber warfare in the digital age in order to successfully proceed with the national strategic guideline: 'winning local war under hi-tech conditions.'[113] RMA basically implies that the tactics and operational methods of warfare must undergo a critical change.[114] Historically, as Knox and Murray (2001:13-14) explain, there have been five general forms of RMA through time:

> Military Revolution 1: the seventeenth-century creation of the modern state and of modern military institutions; Military Revolution 2 and 3: the French and Industrial Revolutions; Military Revolution 4: the First World War; Military Revolution 5: nuclear weapons and ballistic missile delivery systems.

---

[111] The 1997Quadrennial Defense Review (a study by the United States Department of Defense that analyses strategic objectives and potential military threats), reports that the doctrine of 'US Vision of Joint Operations' has been unveiled, encouraging the US to adopt the strategy of 'asymmetric warfare.' Cassidy (2003:8) interprets that asymmetric is 'acting, organising and thinking differently from opponents to maximize relative strengths, exploit opponents' weaknesses or gain greater freedom of action. It can be political-strategic, military-strategic, operational or a combination, and entail different methods, technologies, values, organisations or time perspectives.'

[112] According to *The Dynamics of Military Revolution, 1300-2050*, the term 'Revolution in Military Affairs' (RMA) was coined by Michael Roberts, a British historian, in a speech in 1955. (Knox and Murray, 2001:1) The term implies a conceptualisation of future warfare, especially associated with information and communication technology.

[113] Please refer to Section 3.2.3 for a more in-depth discussion.

[114] As explained by Toffler (1993:32), 'A military revolution, in the fullest sense, occurs only when a new civilisation arises to challenge the old, when an entire society transforms itself, forcing its armed services to change at every level simultaneously – from technology and culture to organisation, strategy, tactics, training, doctrine, and logistics.'

At every military revolution, each state will review its own military ability to set up a new goal of state strategy. In 2002, the PRC clearly proclaimed in its national defence report that China has started developing the strategy of information warfare[115] as the primary stage of China's Revolution of Military Affairs (RMA). (China's National Defence, 2002) In addition, recent research shows that the conduct of cyber warfare is one of the significant strategies forming China's response to US military transformation in the 21st century. (Mulvenon et al., 2006:5-10) As a result, according to precepts of modern Chinese strategy, the Chinese government is devoted to develop its own RMA with unique Chinese characteristics, cultivated by the thinking of modern Chinese strategy. This revolution focuses on the development of cyber warfare as an asymmetric strategy. This involves avoiding the opponent's strengths and instead attacking vulnerabilities in order to allow the militarily inferior to beat superior opponents. As such, it is believed that China's RMA may be different to the RMAs developed by Western countries. (Blasko, 2005)

As investigated by Lin Chong-Bin[116], Chinese military leaders have been promoting a vision of China's RMA since the mid-1990s, clearly stating that China must: 1) catch up to the level of informationisation of developed Western countries; 2) digitalise the functioning of the PLA's armed forces and troops; 3) establish the ability to oppose an opponent's C4ISR system in order to 'paralyse' the enemy; 4) establish the ability of pre-emptive strike; 5) establish the ability to deploy computer viruses in cyber warfare. (Lin, 1999:6) China's 2002 national defence report clearly shows that the PLA will attempt to use information technology to establish a 'multi-dimensional' battle space (including land, sea, air, space and cyberspace). As a result of this, 20,000km of optical fibre cable networks were laid in Western China in 2002. China is strengthening its military ability through the establishment of a civil information infrastructure, particularly reinforcing cyber warfare and information operations capacities. As Chinese Major General Dai Qingmin (2002) notes, according to a report of the PLA Military Science Academy to the National Chinese Military Committee, a significant indication of China's RMA, China is desperate to develop cyber warfare. Dai (2002:112-117) points out that some critical issues of China's cyber warfare in this report are: 1) reliance on opponents'

[115] Initially, the PRC used the term 'information warfare' 信息戰 [*Xinxi Zhan*], rather than using the term 'cyber warfare.' However recent focus seems to be on cyberspace rather than information systems.

[116] Professor Lin Chong-Bin is a well-known expert in China's military studies and is a former Deputy National Defence Minister in the Republic of China.

information infrastructures; 2) vulnerabilities of cyberspace; 3) indispensable technical training for cyber warfare; 4) achievement of information superiority; 5) incorporating characteristics of Chinese modern strategy. Moreover, in terms of military modernisation, the PLA believes that implementing cyber warfare will be conducive to the successful development of China's RMA as well as creating a symbolic application of advanced information technology in China's military. Developing cyber warfare can therefore be regarded as a consensus of state strategy in China.

Chapter Four:

China's Cyber Warfare/Strategy – *An analytical framework*

As discussed in Chapter Three, People's War can be defined as the strategy of mobilising the populace to achieve a strategic aim. Originally, People's War was conducted on geographic battlefields located in Mainland China. The Chinese Communist Party (CCP) employed the strategy of People's War to drive the massive populace, mainly consisting of the Chinese proletariat, into wearing down the CCP's militarily superior opponent in order to ultimately gain victory during the Chinese Civil War of the early 20th century. Subsequently, since the founding of the PRC in 1949, People's War became and has remained a key guideline for China, not only in terms of military strategy but also for national development. The concept of People's War incorporates the ideas of active defence, asymmetric warfare, protracted warfare, and guerrilla warfare[117]; thus, those with inferior military capability are able to deter and even defeat those superior to them. When the PRC's opponent, the Republic of China (ROC), governed by the Chinese Nationalist Party, retreated across the Taiwan Strait during the civil war, the CCP was forced to accept that People's War was restricted by conditions of geographical territory. Meanwhile, in the modern digital age, the inherent features[118] of cyberspace have shaped it into a potential battleground. It can be seen that some principles deriving from People's War may in fact be applicable to cyber warfare, and in turn, the features of cyberspace also lend themselves to the strategic concept of People's War, so that it may be carried out without any geographical limitation in this virtual battlefield. In addition, as Timothy Thomas (2007) notes, China's cyber warfare doctrine and theory are heavily infused with a unique concept of the 'stratagem' inherited from ancient Chinese strategy, which historically has had no direct parallel in Western military culture. Briefly, a 'stratagem' is 'a manoeuvre to deceive or outwit an enemy in war.'

As Chapter Three outlines, Chinese strategies are an integral part of the military cultural heritage of China dating back 2000 years, first conceived by ancient strategists and philosophers (primarily Sun Tzu, Confucius and Mencius). In the modern era,

[117] Please refer to Section 3.2.

[118] These features are: the permeability of cyberspace, the military, government and civil sectors sharing cyberspace, the asymmetry and vulnerability of cyberspace, and the anonymity of actors in this non-state space, as discussed in depth in Chapter Two.

however, it is arguable that the primary Chinese 'stratagem' is that of People's War. It may therefore be believed that, hypothetically, the PRC may adopt the strategy of People's War to achieve strategic aims via the medium of cyberspace. It is important to note that, in general, a state's capability in cyberspace relies on the private sector, as the military sector and civil society share the same civil information network infrastructure. Consequently, it can be concluded that People's War, if not already so, is likely to become the primary strategic guideline for Chinese cyber warfare. Meanwhile, in order to investigate Chinese cyber warfare, it is imperative to identify cyber warfare by employing a theoretical tool, namely the principles of virtual cyber-territoriality as proposed later in Section 4.1.2.

Following the examination of cyberspace and modern Chinese strategy, and before approaching the analysis of empirical findings on China's cyber warfare in Chapter Five, it is important to also consider significant recent incidents of cyber attack, some of which have even been defined as acts of war. In the following sections, the analytical framework in this research will subsequently be outlined in sections 4.1 to 4.3, which respectively reflect sections 5.3 to 5.6 in the empirical analysis of Chapter Five.

4.1 Strategic value of cyberspace

Since civil society, government and the military sectors share the same national information infrastructure, shown in Figure-4 below, this feature offers a strategic value for developing cyber warfare through construction of the civil sector and the national information infrastructure. Moreover, the asymmetry and anonymity of cyberspace also make this value even more attractive for conducting attacks or counter-attacks against adversaries. Evidence shows that China has potentially adopted this strategic value into the guideline of national defence as a way to strengthen military capability in cyberspace.

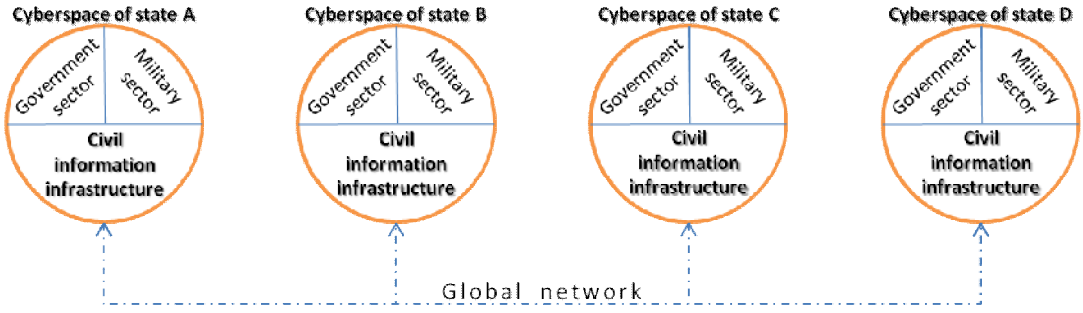

Figure-4: Inter-relations of states' cyberspace

This diagram, drawn by the author, demonstrates that the cyberspace of each state shares the same civil electronic information infrastructure between three

sectors: civil, government and military. Meanwhile, states' civil information infrastructures are connected to one another through international cable networks, namely the World Wide Web, in global cyberspace as a whole. The development of cyber warfare could reinforce the protection of cyberspace. However, in geographic battlegrounds, the direction of threat against a nation-state is from the military sector towards civil society; but, in terms of the potential battleground of cyberspace, the threat against a nation-state may change the direction, arising from civil society towards the government or military sectors, since the civil sector, which is relatively vulnerable, shares the same electronic information infrastructure with the government and military sectors. As a result, the threat caused by cyber attacks could be regarded as a collective threat for all three sectors, which can be identified to define any counter attack as collective defence. In that case, it is vital to securely construct the civil information infrastructure and establish 'fortifications' in this potential battleground in order to achieve military purposes.

4.1.1 *Transcendence of territory caused by the growth of cyberspace*

As examined in the Introduction, traditionally territorial states such as the Netherlands or Belgium were self-protective of their territory through fortification or fortresses. Due to the invention of new destructive weapons, however, the impermeability of such territorial states was decreased as the concentrated offensive power of the atomic bomb was bigger than any other offensive military power. Some states with special terrain in their geographic location could protect their territory from attack by destructive weapons through natural barriers. Such states would survive even if they are small, since the factor of territory size is no longer of crucial importance. An example from Mencius, an ancient Chinese philosopher, reflects the condition of territorial security. Mencius provided guidance for the governor of a small state about a thousand years ago by advising: 'Dig deeper your moats; build higher your walls; guard them along with your people.' But in modern times, destructive weapons have perhaps changed such territorial thinking because nuclear power shattered all previous conceptions. This argument is not only applicable to nuclear warfare in the atomic age, but also to cyber warfare in the digital age. Moreover, the destruction caused by cyber attack may be on an even larger scale, as the operation of nuclear plants and combat

systems are mostly controlled by computer network-based systems. According to the analysis provided in Section 2.1, the strategic values of cyberspace causing the transcendence of state territory can be interpreted as:

1) Indiscernibility of offence and defence

According to Clausewitz, 'One might think of a strategic attack as an entity with well-defined limits. But practice – seeing things in the light of actual events – does not bear this out. In practice the stages of the offensive as often turn into defensive action as defensive plans grow into offensive.' (Rattray, 2001:77) The boundary between offensive strategy and defensive strategy in warfare may thus be indiscernible, and this is likely to prove the same in cyberspace. In other words, as cyberspace has become a potential battleground, an important military issue is the increase in dominant capabilities in this battleground whilst reinforcing the ability of securing the civil information infrastructure contained therein.

2) Permeability and vulnerability of cyberspace

As examined in Section 2.2, the nature of cyberspace creates the features of cyberspace, offering conditions transforming cyberspace into a potential battleground. Technically, the shared information network infrastructure links together the civil society, government and military sectors, meaning the government and military sectors may be permeated via the civil sector. This condition of cyberspace makes it an attractive target for adversaries.

3) Asymmetry and anonymity of cyberspace

As examined in Section 2.3, the asymmetric features of cyberspace, such as the speed of attacks and the causal scale of damages, provide opponents with a strategic value to carry out operations for certain purposes. In other words, in the potential battleground of cyberspace, an inferior military may defeat a superior military through conducting appropriate warfare/strategy.[119] In addition, cyberspace conceptually represents an 'information society' for humans, forming a unique culture in this realm. However, due to the anonymity of cyberspace, it is possible for everyone and anyone to become a 'cyber-warrior' in this battlefield. While the USA is now placing increasing attention on the development of cyber warfare, the PRC has attached great

[119] This argument will be further elaborated empirically in Chapter Five.

importance to it since as long as a decade ago. In particular, ever since 1999 when the PRC first considered the concept of 'Unrestricted Warfare', cyber warfare has been viewed as a crucial element therein.

4.1.2 *A theoretical tool: a set of principles of cyber-territoriality*

Due to the transcendence of territory facilitated by cyberspace, it is necessary to propose a theoretical tool to identify any conflicts happening in this medium, because current international politics, based on a territorial system, lacks a theoretical basis with which to handle cyber conflicts.[120] As outlined in Section 2.3, this research proposes the term *cyber-territoriality*[121] to delineate the concept of cyberspace as a battleground. Compared with a conventional war, a war waged in cyberspace in the digital age is relatively difficult to define due to the inherent features of cyberspace. Once cyberspace has a conceptualised territoriality, it is important to produce principles of this cyber-territoriality to generate a theoretical tool to identify cyber war, as well as to possibly provide a justification for actors to deal with cyber attacks. This research posits that it is logical to borrow the discourse of principles of territoriality based on the state system to generate equivalent principles of cyber-territoriality, even though cyber territoriality is not necessary in total accord with the state system.

In terms of political territoriality based on the international state system, Hartmut Behr (2008:359-382) identifies three principles of territoriality, which are 'the concepts of sovereignty, (national) integration, and borders.' It is suggested that these three principles of territoriality are applicable to non-territorial space, but with slightly different interpretations.

1) Sovereignty/Authority

In terms of the concept of sovereignty, the owners of different ISP services, information networks, and telecommunications in cyberspace, such as states, non-state organisations, private companies, and even individuals, could claim ownership to provide authority for the legitimate control and access of their information network systems. This authority could be equivalent to sovereignty over their cyber-territorialities.

[120] As discussed in Section 5.2.1 regarding recent cyber incidents, disputes among actors remain in the scope of the current international system due to the lack of a theoretical basis to identify cyber conflicts.

[121] Please refer to Section 2.3 for more detail.

2) Integration/Cyber culture

In terms of the concept of integration[122], the similarity drawn from cyber-territoriality could be established upon cyber culture, including behaviours, customs, genres, and languages in cyberspace, according to the specifications and characteristics of the DNS and TCP/IP.

3) Borders/Functional borders

Finally, the concept of borders is a very important factor in establishing a manner of protection from external threats as well as distinguishing actors and actions inside and outside of a territory, even though threats may also come from within. In cyber-territoriality, the equivalent of functional boundaries could be drawn by several functional servers, such as Names Servers, Proxy Servers, and Firewall Servers. The operations of these functional servers are also carried out through the techniques of the DNS and TCP/IP. These servers could filter malicious activities and block unwanted information in cyberspace. In addition, servers are geographically located in a territory, though this may be different to the territory of the nationality in which the owners of these servers are registered.[123]

4) Users as the internet populace

In addition to the three principles of cyber-territoriality outlined above, it shall be argued that the internet users (individuals) who serve as the virtual inhabitants of this cyber-territoriality are extremely crucial actors, as they drive the flows of information in cyberspace and are the primary instigators of communication. In cyber-territoriality in the non-state system, individuals and social groups are more significant than in the state system, where they are simply considered as one of the sub-principles under the principle of integration. In addition, according to the conceptual investigation of cyberspace, virtual cyber-territoriality contains information flows. Lucas Walsh and Julien Barbara consider 'the image of war as spectator sport, creating a contemporary ''fog of war'' beneath which states can mobilise citizens in pursuit of traditional geo-political goals' (Walsh and Barbara, 2006:205). This demonstrates that the internet populace can be mobilised for a

[122] In Behr's research, this 'integration' refers to the integration of three domains: 'the state', 'individuals and social groups', and 'values, norms, and political practices.' (Behr, 2008:363-364)

[123] For example, Google is registered as a US company. However, some of its servers are geographically located outside of the US territory in other states' territories.

political purpose. Moreover, the security of cyberspace rests on 'active cyber citizenship' as a strong and crucial component to tackle new and challenging security issues (Harknett and Stever, 2009). It can thus be suggested an additional principle of cyber-territoriality concerns the internet populace as virtual 'citizens'.

It can be criticised that the West has undoubtedly been the dominant actor in cyberspace, since essential facilities, such as the Domain Name System, Operating System (OS) and firewalls or database software, were invented and are provided mostly by Western countries. Nevertheless, as demonstrated by the possibility of the hypothetical virtual territory outlined above, it can be concluded that states no longer dominate the cyber-territoriality issue.

In addition, it can be suggested that threats in relation to cyber-territoriality can be dealt with through the territorial assumptions[124] used to formulate strategies of national security based on traditional territory as identified by Hartmut Behr (2008:365). Firstly, in cyber-territory, the origin of a threat can be located through the Domain Name System and TCP/IP, and the 'final *causus belli*' can be devised when cyber-territory is attacked. However, due to the anonymity of cyberspace, even though relevant techniques are in development, in most cases it is still not possible to identify the actor behind the threat with certainty. In addition, in comparison to territorial assumptions, digital attacks arising from cyberspace are limited inside the computer networks in non-violent cyber-territoriality; however, the damages can traverse cyber-territory to affect real territories and transform into physical damage. For instance, an attack inside the control systems of public transportation or state power supply may cause a physical crash outside the virtual realm. In addition, fake information in the public media could lead to physical conflict or panic[125], and could also attempt to disrupt people's opinions or beliefs through use of

[124] The five territorial assumptions are: '(1) the threat arises from a territorially definable actor; (2) the threat's range is territorially limited; (3) the threat is directed at a territorially determinable area with the aim of conquering and occupying it;' and accordingly, '(4) territory and the state's claim on territory are the final *causus belli*; that is why (5) security politics can be distinguished, according to "inside-outside"-logic, into territorially specified *external* and *internal* affairs.' (Behr, 2008:365)

[125] On 14 March 2010, panic in Georgia resulted from the fake news that 'Russian tanks had invaded the capital and the country's president was dead.' Though the show opened with a disclaimer that it was not real, it featured a familiar news anchor who appeared to be unsettled by breaking news of fighting in Tblisi and it was stated that Russian bombers were headed for Georgian airspace, and troops and tanks were also on their way. (Kramer, 2010)

propaganda[126]. (Rattray, 2001:19) It can consequently be argued that the security of cyberspace is basically indistinguishable from the specified territorial 'external and internal affairs' though threats go beyond the boundaries of both real territory and virtual territoriality. Meanwhile, this cyberspace is also associated with not just states, but also with transnational actors.

It may therefore be concluded that the four principles of cyber-territoriality generated above, namely, *authority*, *cyber culture*, *functional borders*, and *people*, may form the specific characteristics of cyberspace which, if violated, allow a universal identification of warfare acknowledged by all states. In the territorial state system, a war can be defined based on whether principles of territoriality are compromised. By the same logic, if at least one of the principles of cyber-territoriality is affected, a defensive strategy could be invoked. Without a clear definition, one might argue that although a cyber attack is obviously an act of war, it cannot be defined as such unless there is a general concept achieving global consensus.

Another way to interpret cyber warfare comes through the understanding of cyberspace as an intangible battle space consisting of three layers: 'the physical layer, a syntactic layer sitting above the physical layer, and a semantic layer sitting on top.' (Libicki, 2009:12) The physical layer is composed of the servers and cables. This layer could be associated with the principle of *functional borders* of cyber-territoriality. Secondly, the syntactic layer refers to the rules and norms of the computer systems and their owners, such as the Domain Name System (DNS) and TCP/IP. This layer also forms the principle of *cyber culture*. The third semantic layer is the information stored in the computer networks and database servers. This information is contributed by internet users and information providers and could be regarded as the intellectual property of owners in cyberspace, reflecting the principle of *authority*. Consequently, once one or more of these three layers is damaged by threats or attacks, it is reasonable to assume that actors could resort to defensive strategies of cyber warfare. In addition, damage in this intangible space, whether deliberate or accidental, may also cause very serious damage in the physical world. For instance, in October 2010, the US

[126] On January 2009, Israeli military forces reportedly hacked into a Hamas-run TV station to broadcast propaganda, in order to disrupt peoples' faith. (Leyden, 2009)

military lost control of 50 nuclear warheads for 45 minutes due to a 'computer glitch', which could have been caused by a planted computer virus via the network system.[127] In other words, since the control and command systems of traditional weapons rely heavily on computer network systems in the digital age, it might be possible for an intercontinental ballistic missile to be launched through a takeover of the command and control computer system[128], potentially causing not only massive destruction but also inter-state conflict. As a result, the impact of cyber warfare can be transferred from cyberspace (intangible territory) to the physical world (tangible territory) as combat systems are established upon computer systems. That is to say, though a cyber war may not cause any casualties within cyberspace, physical damage and casualty in our tangible territory may be the fallout of cyber war. In this manner, we can see that cyber warfare is in fact related to the concept of traditional warfare.

4.2 China integrates electromagnetic environments into informationisation

According to the examination of modern Chinese strategy in Section 3.2.3, 'informationisation' has become a critical guideline for the entire nation in the digital age. This informationisation also establishes a preparatory platform for China to develop cyber warfare. In so doing, once People's War is adopted to conduct cyber warfare, the massive Chinese populace can be integrated into cyberspace via the national information network infrastructure. In addition, according to the claims of China's thoughts towards cyberspace laid out in Chapter Two, China's cyberspace channels various electromagnetic environments into an integrated platform to enlarge the potential strategic value of cyberspace. These two arguments are described in more detail in the following sections, and will also be elaborated upon empirically in Chapter Five.

---

[127] This incident saw one ninth of the entire US arsenal of intercontinental ballistic missiles knocked offline. As indicated by a missile launch officer, this was one of the most concerning mistakes to ever occur in the nuclear command and control system. (Daily Mail Reporter, 2010)

[128] There is another form and target of cyber warfare called C4ISR, which stands for Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance. This is basically a computer system controlling and commanding combat systems of different military carriers, such as aircrafts, warships, and ground missile vehicles, through communicating and sharing intelligence, in order to integrate the army, navy and air force into joint operations. The most significant warfare using C4ISR occurred in 1991 in the Persian Gulf War, also known as the Gulf War or Operation Desert Storm. This war caused states to realise that information technology can powerfully master control and command of weaponry in 21st century battlegrounds.

4.2.1 *Establishment of China's national information infrastructure*

In addition to China's Revolution in Military Affairs examined in Section 3.4, it is generally believed that the civil information infrastructure will be built up before the military sector through 'national informationisation'. Revolution in business will subsequently drive revolution in the military. As John Seely Brown and Paul Duguid (2000) point out, nation-states might be prone to fail economically by the rise of powerful private companies.[129] In other words, some transnational private companies might become more powerful than a state.[130] In terms of guidelines presented by modern Chinese strategy, China's RMA also incorporates civil resources for the further mobilisation of the massive Chinese populace and its civil society. In addition, as Sheng (2005:136-137) stresses, one of the principles of China's cyber warfare is to develop warfare based on the continued construction of the civil information infrastructure.

However, due to the one-party system, the Chinese government controls the majority of a wide range of civil resources. China's political trends may thus heavily affect the direction of the development of its civil information infrastructure. It is believed that the thinking[131] of the Chinese government and the development of China's information infrastructure are firmly associated with one another. (Kao, 2000) In terms of governmental policy, in 2006 the PRC published *2006-2020 國家信息化發展戰略 (Guojia xinxihua fazhan zhanlüe, The strategy of the development of national informationisation 2006-2020)*. This official guideline proposes strategic principles for the development of China's information infrastructure as follows: (PRC State Council, 2006)

1) conduct economic informationisation;
2) establish e-government;
3) construct a quality cyber culture;
4) promote societal informationisation;

[129] The authors also refer to the concept of the 'global city' coined by Saskia Sassen. It is believed that new world citizens are not those literally living on the earth but instead the individuals belonging to transnational enterprises. (Brown and Duguid, 2000:30)

[130] For instance, in a congressional debate, it was reported that the transnational IT company Apple Inc. has more cash than the US government according to Apple's profit report of 2011. In other words, the world's largest technology company might be more economically powerful than the world's largest sovereign government. (Rosoff, 2011) Interestingly, this is similar to the popular Chinese idiom '富可敵國' (*fu ke di guo, Wealthy enough to resist a state*) which has also influenced Chinese thinking about statehood from time to time.

[131] This thinking is based on Chinese strategic culture, investigated in Section 3.3.

5) complete a comprehensive information infrastructure;
6) enhance competitiveness of the information industry;
7) establish a national system of cyber security;
8) strengthen people's abilities in information technology, and cultivate experts of informationisation

Therefore, in order to propel national informationisation, China's Ministry of Post and Telecommunication proposed the China Information Infrastructure (CII) system to construct China's information infrastructure in practice. For example, the Golden Bridge Project, a significant project for China's information infrastructure, implements techniques such as optical fibre, microwave, program control, satellite and wireless, to build up China's cyberspace, thus integrating internet and telecommunication into a national information platform. (Wang, 2007:89-92) However, China's current information infrastructure still relies on Western technology. In other words, it is still inevitable that China needs to employ advanced core techniques from the West in order to continue the construction of its national information infrastructure.[132]

Moreover, the PRC's Ministry of Public Security (MPS) manages an official internet police force which is officially charged with preventing cyber attacks from civil society. (Damm and Thomas, 2009:73) In terms of the development of China's fundamental informationisation, the governmental department MPS operates the 'Golden Shield Project', also known as the 'Great Firewall of China', which began operations in 2003, in order to reinforce China's information infrastructure and reinforce cyber security. The project includes design of both software and hardware. (Damm and Thomas, 2009:105) This project ensures that all internet activities in China can be monitored through methods such as IP blocking, DNS filtering and re-direction, web address filtering, and connection resetting,[133] so that the PRC may ensure the domestic Chinese populace cannot access websites and retrieve information deemed inappropriate by the Chinese government. As a result, two notable points can be argued: firstly, engagement in daily, active network monitoring, control and espionage provides

[132] For instance, American, British, and Israeli technology companies are all involved in the construction of China's information infrastructure. Cisco, a well-known American company supplying computer servers, has offered massive amounts of equipment to China. Cisco was criticised by some American congressmen and media at the time. (Chen, 2006)

[133] These methods are commonly used for censoring. China's cyberspace is under enforced censorship, which may be considered to be part of China's cyber warfare.

intensive defensive practice for China's cyber warfare actors; secondly, monitoring all internet access into and out of China is significant when it comes to evaluating civilian hackers in the world. It is not far-fetched to suggest that China regards the Golden Shield Project as part of its cyber warfare. That is to say, the PRC government is likely to have the aim of technically controlling and monitoring the massive populace via the censorship of the Golden Shield Project in China's cyberspace. Moreover, this project may resolve a certain dilemma for the Chinese government: on the one hand, the PRC could take advantage of the massive populace to function as 'cyber-warriors' pursuing cyber warfare, but on the other hand, the PRC has to overcome the challenge that the Chinese people may be too numerous to control and command into disciplined cyber warriors in the intangible cyber territory.[134]

4.2.2 *Integration with electromagnetic environments*

In addition to the construction of China's national information infrastructure, and according to the definition of cyberspace as examined in Section 2.1, cyberspace may consist of the internet, computer network based systems, and telecommunication. China's cyberspace is essentially the same; however, in order to increase its strategic value, it could be argued that China constructs this cyberspace by combining various electronic environments, other than just telecommunication, into an integrated platform to order to coordinate electronic warfare in this potential battleground. This integrated platform of China's cyberspace characterises China's cyber warfare as 'Integrated Network Electronic Warfare,' according to the US military report to US Congress in 2010, as noted: (US Department of Defense, 2010:34)

> *'PRC military writings highlight the seizure of electromagnetic dominance in the early phases of a campaign as among the foremost tasks to ensure battlefield success. PLA theorists have coined the term "integrated network electronic warfare" (網電一體戰, wangdian yitizhan) to describe the use of electronic warfare, computer network operations, and kinetic strikes to disrupt battlefield information systems that support an adversary's warfighting and power projection capabilities. PLA writings on future models of joint operations identify "integrated network electronic warfare" as one of the basic forms of*

[134] This argument will be explained in the later Section 4.3.5 in this chapter.

"integrated joint operations," suggesting the centrality of seizing and dominating the electromagnetic spectrum in PLA campaign theory.'

According to this report, China's cyber warfare is likely to include electronic warfare as a whole. In other words, China's cyberspace will combine various electronic environments in the ground, air and even outer space, in order to develop an integrated warfare. The empirical evidence for this will be presented in Section 5.3.

4.3 Cyberspace as a potential battleground suited to People's War

Due to the strategic value of the potential battleground of cyberspace, it is arguably perfectly suited to People's War. This means that the tradition of People's War remains the most up-to-date strategic doctrine for China's cyber warfare in the digital age.

Compared with the ease of access to US military publications, the Chinese government's lack of transparency in the field of cyber warfare makes the analysis of involvement of its state or non-state actors somewhat challenging. According to examinations in previous chapters, China's cyber warfare is certainly guided by modern Chinese strategy, which in turn is deeply influenced by traditional Chinese strategic culture. In addition, the tenets of the significant inherited strategy of People's War remain the same, although its context has shifted from the conventional land-based battlefield to cyberspace. The massive Chinese populace is a significant advantage for China to carry out cyber warfare without the traditional limitation of boundaries. In order to fit People's War into the new context of cyberspace, the PRC has dedicated a great deal of resources within the past decade to observing the character of the transformation of the USA military and its national strategy. According to China's 2002 National Defence white paper, the PRC officially proclaimed for the first time that the Chinese revolution of military strategy would focus on the development of information warfare and information operations. (PRC State Council, 2002) Furthermore, in the same year, a US governmental report officially stated that China's military modernisation is combined with tactics of information warfare such as 'computer hacking', creating an irregular warfare in the domain of cyberspace. (US DoD, 2002:31) As Sevastopuloin and McGregor (2007) report, 'The PLA has demonstrated the ability to conduct attacks that disable our [US] system . . . and the ability in a conflict

situation to re-enter and disrupt on a very large scale.' However, China does not officially publish its endorsed doctrine in the same way as the US military. Only the writings of several Chinese military leaders and scholars can provide some basic ideas of China's cyber warfare. Aside from referring to these documental resources, China's cyber warfare can also be examined from several different perspectives such as China's RMA, the national information infrastructure, the strategic logic behind the warfare, and military capabilities, and, finally, the implementation of People's War in China's cyber warfare.

From Sun Tzu's *The Art of War* and Mao's People's War, it can be argued that the Chinese army has inherited a distinctive strategic style. In addition, the evolution of People's War triggered a Revolution in Military Affairs (RMA) in China and subtly modified the original concept of People's War.[135] The theory of People's War was raised from a tactical level to a strategic level. In the present day, the latest strategic thinking of the Chinese military strategy, 'Fight and Win Local Wars under Information Conditions'[136], has been combined with the thought of Sun Tzu and Mao to become a critical guideline for warfare in the digital age. It is clearly indicated in the defence policy of the 2008 China National Defence report that the Ministry of National Defence still insists upon and consistently carries out guidelines adopting the concept of People's War at a strategic level. (PRC Ministry of National Defence, 2008) Through examining its advantages and characteristics, it can therefore be concluded that the theory of People's War has constantly remained behind critical strategy in the modern Chinese era.

Furthermore, it is argued that the principles of People's War provide a supportive framework of strategic guidelines for asymmetric warfare, such as cyber warfare, in the digital era. As cyberspace has become a potential battlefield, the possible combat zone has expanded from the battle zone of military conflict to include societal sectors such as the banking system and the public construction

[135] In Hu Jintao's report at the CCP 17th National Congress in 2007, he announced: 'We must implement a military strategy for the new era, accelerate the revolution in military affairs, ensure military preparedness and enhance the military's capability to respond to various threats of security and accomplish diverse tasks.'

[136] As the 2004 China National Defence report states, the PLA regards this guideline as an objective. The first priority is developing weaponry and equipment, followed by building joint operational capabilities, and then making full preparations for the battlefield. Meanwhile, the PLA adheres to the concept of People's War in order to develop fitting strategies and tactics. For the requirements of integrated and joint operations, the PLA endeavours to establish a modern operational system capable of giving full play to the overall efficiency of the armed forces as well as the national war potential. (PRC Ministry of National Defence, 2004)

system. Due to this, the battlefield covers the domestic or even the international reach of a country, so that the features of People's War can be perfectly applied to this virtual battlefield. The strategy of Chinese cyber warfare is thus in close accord with the theory of People's War, combining the power of military troops and the civil masses in both visible and invisible areas. Regardless of whether the actions are offensive or defensive, it can be suggested that China's strategy of cyber warfare is People's War. In the potential battleground of cyberspace, creating a justification for war and then mobilising the people is an efficient way of defending China from any threat from other states, thereby establishing a virtual 'hard shell' for the purpose of national defence. In terms of asymmetric warfare, the mobilisation of people can also act as the active defence of cyber deterrence[137] to deter the otherwise militarily superior. This strategy of asymmetric warfare is also developed based on the principles of People's War, and its paradoxes[138] have become an integral part of modern Chinese strategy.

In terms of the tactics of People's War, in the absence of a regular army, armed struggles, revolutionary riots, and even terrorist conflicts can simply be regarded as irregular warfare akin to guerrilla warfare. As Clausewitz (2001:466) states in his work *On War*, the power of the masses in waging war is fragile and limited, so they cannot carry out a decisive campaign against the opponent's regular army. They can instead only attack the enemy's transportation and supply lines which lie outside of their fortified position. On the other hand, Clausewitz (2001:467-470) also points out that the masses who wage war are like a 'fog'; they do not assemble together in a particular area, but spread around everywhere in the battlefield. Consequently these armed masses are not a major core group which can be easily targeted by the opponent. This is therefore a good strategy for avoiding attack. Mao's People's War combines the assurance of justifying war and the feature of 'fog' with the use of regular armed forces. People's War allows for irregular warfare to be conducted in the battlefield with the support of the people, but can also make use of regular logistics. People's War efficiently provides strategic guidelines for information warfare as a type of asymmetric warfare in the digital age. Using

[137] In addition to offence and defence in a war, cyber deterrence has become another strategy in cyberspace. As Libicki points out, a capability needs to be developed in cyberspace to 'do unto others what others may want to do unto us.' (Libicki, 2009:27)

[138] Cassidy (2003:7) claims that there are six paradoxes of asymmetric conflict, which are 'strategic goals,' 'strategic means,' 'technology/armament,' 'will/domestic cohesion,' 'military culture' and 'time and space.' An asymmetric strategy can be depicted through evaluation of the six paradoxes.

asymmetric warfare through the strategy of People's War may well mean that it is possible to defend against or even defeat a relatively superior adversary by consolidating the powers of people from all sectors – not only military or governmental sectors but also societal sectors and private industries. This is consequently an effective guideline for a defensive strategy.

Briefly speaking, the strategy of China's cyber warfare combines the aspects of evolving warfare and general modern Chinese strategy to form a new kind of warfare supported by the specific traditional principle of People's War. In the digital age, as Damm and Thomas (2009:118) point out, the people are not just Mao's '*renmin*' (人民, *the masses*) any more. The 'people' of People's War does not refer only to the domestic populace, but in fact may indicate all global Chinese users of the internet all over the world. The mobilisation of this global population is accordingly not limited to Chinese geographical territory.

4.3.1 *Strategic ideas of People's War*

In terms of the features of cyberspace, some principles which derive from People's War can be applied to cyber warfare in the digital age. Vice versa, the features of cyberspace also lend themselves to the strategic concept of People's War so that it can be carried out without any geographical limit in the virtual battlefield. The principles are as follows:

1) All-out defence/offence

As 'everyone is a soldier,' the theory of People's War primarily combines the people and the military forces of the state to reinforce the state's power to defend against or defeat the enemy. It had been queried that this was no longer practical for China when the battleground changed from the domestic theatre to the international theatre, including cross-sea warfare. (Hong, 2007:25) However, the combination of people and military forces can function not only in a physical sense, but also in a virtual sense, for example by cultivating people's thoughts to make them determined to defend against the enemy. (Hong, 2007:24) In addition, unlike conventional warfare or even nuclear warfare, regardless of whether they are civilian or military, every member of the population would potentially be able to defend against or attack the enemy on behalf of the state in cyberspace, no matter where they are.

2) Defeating an enemy without fighting or massive numbers of casualties

'Subduing the enemy without fighting' is one of the most famous principles of Sun Tzu's strategic thought, and Johnston argues that this was referred to by Mao in his People's War. (Johnston, 1995:255) It is suggested that this strategic principle is applicable to cyber warfare, since despite there being no physical fighting or casualties in cyberspace, cyber warfare is still able to wear down, deter or even defeat the enemy if a war is inevitable. Furthermore, the societal sector is a significant support for a state. As the societal sector, including private systems such as the banking system, public transportation service and supply systems, relies on cyberspace so heavily in the digital age, cyber warfare can be the most efficient military approach to attack the state societal sector and thus wear down a state's power.

3) 'Know the enemy and know yourself, and in one hundred battles you will not be in danger'

This is another principle taken from the chapter 'Planning Offensives' in Sun Tzu's work, and Johnston argues that it, too, was referred to by Mao in his People's War. (Johnston, 1995:255) In the digital age, unlike conventional documentary archives, most official documents are stored in one copy of electronic format in a computer system. Due to this, it is possible that not just public governmental information, but also the official documents or even intelligence material of a state can be intentionally hacked by other states via cyberspace. Vice versa, it is also possible that a state can spread false information through cyberspace to deceive its enemies, so that they may miscalculate. Thus, even in terms of cyber strategy, Sun Tzu's (translation by Sawyer, 2007:158) maxims apply: 'Warfare is the way of deception,' and 'Although [you are] capable, display incapability to them. When [your objective] is nearby, make it appear as if distant.'

4) Guerrilla strategy with swarm effect and sting effect

Rosita Dellios (1989:205) claims that two effects appear as strategies of attrition warfare in Mao's People's War to wear and tear down the enemy. One effect is the 'swarm effect' and the other is the 'sting effect.' The former refers to taking advantage of plentiful manpower to exhaust the enemy on the battlefield; the latter is the use of mobile weaponry equipment to sneak up on the enemy. These two effects are applicable to cyber warfare, for example by

paralysing computer servers by spamming lots of junk requests and computer systems by transmitting viruses.

In sum, as Xiong Guankai (2003:41) points out, the latest Chinese strategy is to win and fight local wars under information conditions through joint operations across the five dimensions of land, sea, air, space, and electromagnetism. These joint operations are conducted on the information platform of cyberspace. Therefore, implementing the strategy of People's War by combining the people with military forces and by mobilising social resources is a feasible strategy to protect the state's security in cyberspace. The 'hard shell'[139] formed by the mobilisation of the people provides not only strong protection preventing permeability to enemy attacks in cyberspace, but also cyber deterrence to avoid the outbreak of cyber war in this potential battleground.

4.3.2 *Strategic logics of China's cyber warfare*

The PRC reaction to US military transformation is mainly based on the requirement to maintain China's national security and to therefore consider appropriate responses within China's military strategy and tactics. With regards traditional combat capability, the PLA believes that it must evaluate every step very carefully in confrontations with enemies with high-tech military capabilities. According to the PLA's *Campaign Studies*, the PLA divides armed conflict into three categories: war, campaign, and combat. A war is made up of a number of decisive campaigns and the nature of a strategy of warfare is directly associated with national politics, economics, and diplomacy. A campaign is carried out in a limited geographical area where armed actions relating to the needs of a state's politics, economy and diplomacy are necessary. Combat is a tactical operation to achieve campaign goals. (Ye, 2001:239) Since the 1990s, in particular after the American Operation Desert Storm which drew to an end in 1995, the PRC has come to realise that the next war for the PLA need not be a total war, but was more likely to be a limited war with features such as a short duration, restricted environment and reduced objectives. In addition, future conflicts would certainly

[139] According to John H. Herz's argument, in the Machiavellian system, a state was influenced by power politics, and international relations followed the higher law and higher authority. (Herz, 1962:39) At that time, states protected their own interests and territoriality by using military force or economic approaches to threaten one another. Upon the emergence of the modern state system, 'international anarchy' and 'collective security' appeared. Modern territorial states were protected by a so-called 'hard shell', which acts like a cell wall protecting a small unit within a larger body. This 'hard shell' presents a state's defensive features such as 'impenetrability' or 'territoriality'. (Herz, 1962:40)

contain intensive use of cutting-edge technology, shown to improve the capability of reconnaissance, the precision of weapon delivery, and the speed of processing masses of information, in order to perform precise strikes on the battlefield and ultimately gain locational advantages. The PLA conceptualises this type of modern war as a local war under high-tech conditions. (Ye, 2001:240) Based on this analysis, a modern war, confined to smaller and limited objectives, must consist of high mobility and rapid weapons delivery capability. As a result, the PLA may only be capable of being involved in two or three campaigns at one time. In order to achieve victory in the modern era, the PLA must make decisions within a short time to cope with the fast pace of modern wars. As pointed out by a PRC analyst: 'In a high-tech war, the pace of military action is fast, but time period is short; obviously, the speed and determination during the battles will be extremely important in a such war.' (Lu, 2001)

However, the characteristics of this future war put the PLA into a predicament, as it is difficult for the PLA to defeat an adversary whose military capability and technology is as advanced as that of the USA. The PRC has strived to accelerate the modernisation of its national defence and the construction of new weapon systems in recent years. However, it still remains uncertain that the capability of the PRC's national defence has caught up with the military ability of the United States. Chinese military experts also believe that in the foreseeable future, regardless of further enhancements to the performance of conventional weapon systems, the PLA's traditional weapons systems will still be inferior compared to those of the US military. (Peng, 2001) Peng also states, 'Using inferior weaponry to confront militarily advanced enemies is the very real situation that the PLA would face in future campaigns.' (Peng, 2001:466-467)

As a result, the PLA has no choice but to develop the strategic thinking of 'defeat military superiority by military inferiority'. This conceptual thinking may be converted into practical actions such as developing an asymmetric warfare to avoid direct engagement. The basis of the PLA's strategic vision is to formulate the strategy and tactics necessary to be able to seize the initiative in a war. In accordance with previous analysis in Section 3.2, the development of China's military ability must be under the condition of ensuring objectives of national security. This development must not affect the PRC's regime, nor can it decrease China's economic growth. There are thus some remaining possible options for the

development of China's military strategy. As recent assessment indicates, the possible options include: 1) transformation of People's War into local war under hi-tech conditions and 2) development of cyber warfare in order to carry out asymmetric and pre-emptive action[140] in a war. Therefore, cyber warfare is likely to be adopted as the main focus of China's strategic development. This cyber warfare will also consolidate China's strategic logic of warfare, also reflecting on the features of cyberspace as well as People's War, the constant principle of modern Chinese strategy, as follows:

1) Active defence

Victory of local war under hi-tech conditions depends on whether military reactions are fast enough to dominate information in the initial stage of a campaign. As a recent study points out, attaining a dominating position through pre-emptive actions in a war makes subsequent military actions more flexible; in turn, military operations will be restricted if the chance for pre-emption is missed. (Ye, 2001:150) For the militarily inferior, commencing military actions only after the militarily superior are prepared for deployment spells certain defeat.[141] The PLA conceptualises pre-emption based on the logical thinking of active defence, which is one of the principles of People's War, in line with Chinese military thought and opinions of warfare as examined in Chapter Three. In addition, according to ancient Chinese strategic thought, active attack should be the last resort to resolving conflict between nation-states. As a result, active defence is therefore considered the best pre-emptive strategy for preparing to conduct necessary counter-attacks against enemies' attacks at any given time. Recent research shows that one of the PLA's ideas of active defence is to ensure attaining domination from the first strike to enable further military actions. (Cliff, et al., 2007:49) In addition, the PLA also believes that maintaining an aggressive mentality is a necessary condition for active defence. Therefore, the PRC not only trains their soldiers in this way, but also educates the people to be ready at any time for

[140] A number of Chinese authors describe *pre-emptive attacks* as a necessary and logical strategy for a less advanced country to utilise against a more powerful adversary. If future wars will be decided largely by the outcome of the initial engagement or campaign, attempting to take the initiative after hostilities have commenced seems a risky strategy, particularly for the weaker side. (Li, 2006:46-51)

[141] For example, as Lu Linqi (2003) points out, sources in the PRC commented that during the Persian Gulf War of 1992, had Iraq waged military attacks before the allied forces were completely assembled, Iraq may have defeated the US military and its allies. (Lu, 2003)

mobilisation. In this respect, cyber warfare perfectly matches aspects of strategic thinking for the attainment of active defence.

2) Defence by deterrence

In addition to the strategic logic of active defence, the concept of the pre-emptive strike is similar to the concept of deterrence in Western strategic thinking. As Gene Sharp (1990:3) notes, 'The aim of deterrence is to convince potential attackers not to attack because the consequences could be unacceptably costly to them, including the failure to gain their objectives.' Traditionally, the purpose of military strategy is to pursue operational victory in the battleground, so that a state's security and its national interests can be maintained. However, this concept was drastically altered when the nuclear weapon was invented in the 1950s, as threats to a state shifted from conventional violence to an imagined fear prompted by possible massive destruction by atomic bombs. As Liddell Hart (1960:60) points out, the development of the nuclear weapon makes traditional strategy, wherein the purpose is to win victory on a traditional battleground, largely pointless. Deterrence therefore became a contemporary focus in International Security Studies.[142] (Jervis, 1979) Furthermore, as Patric Morgan (2003) asserts, the existence of nuclear weapons is not necessarily the only concern of deterrence for states. In the digital age, cyber warfare also has the capability to be adopted as a strategy of deterrence, particularly as massive destructive weapons are run by control and command computer systems. (Libicki, 2009:27) As long as potential attackers resign their intent to attack as the result of any form of deterrence, the goals of defence are achieved. It is possible to employ cyber warfare to pose a significant threat to deter adversaries. Linking with the concept of 'active defence' explained above, China realises that this active defence could indeed be defence by deterrence. (Chen, 2009:32) The strategic logic of defence by deterrence may be performed through practical tactics such as anti-access and area-denial.

[142] However, in the post-Cold War era, critics argued that Strategic Studies had been focusing on false issues and the topic of deterrence, particularly nuclear deterrence, was to blame for its lack of testability. Under such circumstances, many scholars switched their research from Strategic Studies to Security Studies, adhering to the statement that the occurrence of major wars in international society was highly improbable. This has rendered both 'deterrence' and 'defence' studies peripheral fields under the umbrella of International Security Studies.

3) Anti-access tactics

The 2010 US DoD report to Congress, further to annual reports of previous years, declares that China is likely to use the strategy of 'anti-access' and 'area-denial' to prevent other military powers accessing the areas of strategic importance for China's military forces, which may include the Western Pacific region. (US DoD, 2010:29-30) As Cliff and other authors (2007:81-83) outline, anti-access is a strategic logic that the PLA has harnessed in order to wear down the advance or hamper the operational tempo of an opposing force in a theatre of military operations during wartime. In fact, 'anti-access' is not a formal Chinese military strategy. Rather, it is a way of summing up Chinese doctrine that addresses the problem of asymmetrically defeating a superior adversary. For example, in the case of the USA, that means recognising the US reliance on cyberspace, including information networks, as a significant vulnerability that, if exploited, could cause the USA to be bogged down in chaos and delay or even impel the suspension of any impending military attack. Cyber warfare is therefore one of the best strategies for the PRC. Targets could be computer systems built either inside or outside of an opponent state's territory, as long as the computer systems in charge of command and control nodes, satellite intelligence, surveillance, reconnaissance and communications can be blocked or even damaged to achieve the purpose of anti-access and area-denial.

4.3.3 *Military capability of China's cyber warfare*

Alexander Neil, the head of the Asian Programme at the Royal United Services Institute (RUSI), predicts that countries will wage both offensive and defensive wars in cyberspace in the near future to crush the enemy before a conventional battle can occur. (DMJ, 2009) According to the strategic value of cyberspace and information technology (IT) examined in Section 4.1, China's cyber warfare is facilitated by the dual-use nature of IT and the growth of its civilian information infrastructure. The increasing defensive ability of cyber warfare will also likely enhance the comprehension of offensive approaches, and offensive abilities will almost inevitably be developed. The process of developing offensive abilities may include hacking governmental computer systems around the world in exercises of cyber warfare.

According to the analysis of cyber incidents investigated in section 5.6 of this chapter, no matter how low the threat level, all threats hailing from China are treated as a cause for concern. Recently, the US government has pointed out that the threat of China's cyber warfare has been systematically underestimated. For example, Richard Lawless, the former Deputy Assistant Secretary of Defence for Asian and Pacific Affairs, believes that the PLA has already developed a mature warfare capability which would be able to cripple US network systems to achieve their purposes. He goes on to claim that the focus of China's cyber warfare is to penetrate American computer networks in order to steal wanted information and develop conditions in which China is able to paralyse critical US infrastructure, such as power grids, financial systems and transportation services, if necessary. (Bruno, 2007)

China's cyber warfare doctrine is essentially a military dialogue that reveals the PLA's primary position in cyber operations. Delving beyond that very generic assertion, however, reveals how little of the PLA's actual cyber organisation and manpower capacity is actually actively employed. As recent research reveals, some military units in charge of cyber warfare have been established in the active-duty PLA sector; however, it is very possible that regional aligned reserve or militia units are also capable of conducting cyber operations.[143] As Xia Yibing (1999) notes, the PLA has established cyber warfare departments within its headquarters.[144] Jane's Sentinel Security Assessment of China's military capabilities points out that every military region of the PLA includes a 'special Technical Reconnaissance Unit' to wage both defensive and offensive cyber action. The mission of these specialised units is to conduct network defence, network exploitation/reconnaissance, data theft, and cyber counter-measures. (Jane's Information Group, 2007:1-3) As part of the modernisation process, the PLA prioritises developing cyber warfare training, in keeping with the key importance that information warfare holds in the current

[143] As Liao Wenzhong points out, for example, there is a Centre for Modelling & Simulation in Jinan Theatre and a Centre for Information Operations in Beijing Theatre. Liao also indicates that a civilian 'cyber army' is organised into local militia categorised as the 'Reserve Information Division', which includes the Electronic Warfare Group, Cyber Warfare Group, and Hacker Group. (Liao, 2007:266-268)

[144] Xia also describes these units as 'prepared to fight foreign attacks as well as to tamper with information in terms of order, time, flow, content, and form; deleting information in parts, in order to create a fragmented information; and inserting information to include irrelevant information in order to confuse and mislead.' (Xia, 1999:64-67)

military establishment. As Thomas (2000:9) claims, PLA senior strategists believe that 'Warfare is now about intelligence and resourcefulness, new temporal-spatial concepts, resolute decisiveness, and "soft science"[145] technology located in new weapons.' Different levels of PLA officers must be trained in these new concepts and their application. Thomas (2000) also indicates that some cyber training centres in China employ civil computer experts and professors to teach relevant theories and techniques of cyber warfare. The PLA leadership also recognises the need to restructure the officer corps training, including strategy, tactics, network technology, and use of information systems for command and control.

Though China does not publish any doctrine of cyber warfare as the USA does, Shen (2005) has established that the PLA has incorporated cyber warfare into military training exercises since as far back as 1997. Shen (2005:167-198) cites the example of an exercise of simulated attack in 1997 in which a Shenyang Group Army sustained a computer attack that paralysed its systems. The Group Army countered with virus-destroying software, and the press described the exercise as an episode of 'invasion and counter-invasion'. In 1999, the PLA conducted another simulation of cyber warfare that involved two Army Groups in the Beijing Military Region simulating a 'confrontation campaign' against computer networks. Network reconnaissance, network interference, network defence, air strikes and subsequent counter-measures were employed in this training exercise. (Thomas, 2004:129) In the 2003 US DoD report, it is noted that the PLA conducted a staggering forty-three cyber warfare training exercises in that year alone.[146] Furthermore, the PLA formation of cyber reserves (militia) and forces is even more significant. As the 2006 US DoD report states, 'Militia/reserve personnel would make civilian computer expertise and equipment available to support PLA military training and operations… by conducting "hacker attacks" and network intrusions, or other forms of cyber warfare, on an adversary's military and commercial computer systems, while helping to defend Chinese networks.' (US DoD, 2006:35) In terms of the mobilisation of the civil sector for

[145] According to Chinese academia, 'soft science' does not belong to the fields of the natural, physical sciences or computing sciences often described as 'hard science', but instead the social sciences and similar fields such as information science and behavioural science.

[146] This report also indicates that the PRC is 'using academic exchange as a medium to train scientists and to develop ties between scientists.' Several PLA units recruit members from college and universities, as well as from the information technology industries. That is to say, China develops cyber warfare through building up an informal science and technology network within civil sectors.

China's cyber warfare, it is believed that the 'PLA has created a reserve telecom forces structure with a reserve telecom regiment as the backbone, with an information industrial department as the base.' (Thomas, 2001) Another capable approach of the PLA's cyber warfare is to mobilise hackers to penetrate targeted computer systems, so that network servers can be controlled in order to conduct further actions once necessary. As Chinese Major General Dai Qingmin (2002) stresses in his book[147], PLA cyber warfare units should seek and infiltrate target networks during peacetime. In addition, as Thomas (2004:59) describes, the PLA produces a document for the formation of a cyber arm of the military service in order to develop capabilities, refine tactics and techniques, and even execute cyber missions at a strategic level for the sake of China's national interests. As a result, it could be said that China may be prepared and capable of conducting cyber warfare to achieve the ambition of 'winning local war under hi-tech conditions.'

4.3.4 *Implementation of People's War in China's cyber strategy*

As Wen Jiabao, the current Chinese Premier, points out, 'In China, there are about 400 million internet users and 800 million mobile phone subscribers', who are basically able to access the internet. (Wen, 2010) Significantly, this number is, for example, nearly seven times more than the total UK population of 61.8 million in 2009. However, the Chinese internet user population is still only about 32% of China's total population. With the present growth rate in internet access, it is believed that China will become the most networked nation. (Damm and Thomas, 2009) With a population base of 1.3 billion and rising, China has tremendous advantages in implementing a cyber campaign. In a very primitive operation, China could utilise citizens' computers to host a botnet and conduct a simple Distributed Denial of Service (DDoS)[148] attack. In addition, DDoS is a typical example of attack in cyberspace, where the ideas of People's War could be carried out perfectly.

As incidents of hacking are rapidly increasing, China has often been criticised for having a large, active civilian hacker community. A comprehensive interpretation of People's War in China's cyber warfare may therefore involve

[147] In Dai's book, *Direct Information Warfare*, he points out that there are two ways to influence the adversary's information functions: indirectly and directly. Indirect information warfare affects information by creating information, which the adversary will perceive, interpret, and act upon. Military deception and physical attacks have traditionally achieved their ends indirectly.

[148] Please refer to the Glossary.

both civilian hackers and the integration of the state's information technology industry, cyber security police, and reserve forces in order to strengthen the capability of PLA – the regular armed forces – when conducting sophisticated cyber warfare. As such, this integration implements the strategy of People's War in the Chinese military tradition.

In addition, the concept of People's War also draws on concepts of the ancient Chinese *Thirty-Six Stratagems*.[149] Certain stratagems could be seen as examples of China's cyber warfare, as follows:

1) Fool the emperor to cross the sea (瞞天過海, *man tian guo hai*): this alludes to lowering the enemy's guard while masking one's own intentions. A cyber scenario could be luring computer manufacturers into the Chinese market and thereby building back doors into the systems. Another cyber application could be using normal email traffic to insert viruses.
2) Kill with a borrowed sword (借刀殺人, *jie dao sha ren*): this implies using surrogates to attack an adversary. A cyber example would be to use botnets[150] of zombie computers, hosted around the globe, to conduct a network attack. Another application could be to use malware planted in opponents' computers as sentinels to send back critical data or even disable the network without the operator's knowledge.
3) Await the exhausted enemy at your ease (以逸待勞, *yi yi dai lao*): this refers to choosing the time and place of battle and encouraging the enemy to expend energy in fruitless endeavours. A cyber scenario may be to increase the number of hacking attempts by masses of Chinese civilian hackers to fully engage computer network defence teams and exhaust them while holding the most sophisticated virus/attack in reserve. This is also similar to the idea of 'lure the enemy in'[151] from People's War.
4) Borrow a corpse to resurrect the soul (借屍還魂, *jie shi huan hun*): this suggests taking an institution, a technology, a method or even an ideology that has been forgotten or discarded and appropriate it for your own purpose.

[149] The *Thirty-Six Stratagems [三十六計, Sanshiliu Ji]* are divided into a preface, six chapters containing six stratagems each, and an afterword that was incomplete with missing text.
[150] Please refer to the Glossary.
[151] 'Lure the enemy in' is a tactic of 'strategic retreat' from Mao's military thought. Facing invasion from outside imperialists, it would have been unlikely to successfully prevent the enemy from encroaching on territory, and so it would in fact be better to let the enemy enter further into the territory where the CCP would be more likely to win struggles. (Wang, 1999:94)

Possible cyber applications include planting individuals or malware in unnoticed units or computers of the opponent, which alters them from within to facilitate outside control.

4.3.5 *The methods of discipline for 'cyber warriors'*

According to the propositions generated above, China's cyber warfare is a strategic warfare that adopts the principle of People's War. In so doing, internet control and censorship are also likely to be an element of China's cyber warfare, in order to prevent the masses from accessing politically sensitive information and to control and command civilians into disciplined cyber warriors for military purposes. However, once the massive Chinese populace is indoctrinated by the Chinese government into patriotism or even nationalism, political events could possibly be interpreted and discussed very aggressively in cyberspace by online users, whose opinions may not be merely anti-Western imperialism but also in opposition to the government itself. As Shen (2007:196) suggests, 'Online platforms can be easily used to mount populist pressure in real life.'[152] In other words, the combination of the indoctrinated nationalism of masses of people and the ease and speed of circulating political information due to the strategic value of cyberspace may allow a new formation of nationalism in the case of certain political triggers, which can be set off not only by the Chinese government but also by the people themselves. In addition, as James Leibold (2010:539) argues, online nationalism might particularly reflect 'Han supremacism' over the Chinese internet, reflecting 'a complicated mix of emotions among Chinese youth' in the modern era. (Leibold, 2010:541)

As a result, in order that China's cyber warfare, adopting principles of People's War, can be performed securely, aside from technical measures to conduct internet control and censorship such as the Golden Shield Project, the factors[153] outlined below may reveal how China disciplines 'cyber warriors'.

Military significance

Whilst China carries out cyber warfare by adopting the strategy of People's War, the management and control of cyber attacks conducted by civilians may become

[152] As noted, 'A significantly large critical mass of upset chat-room postings makes something an issue for everybody to take seriously.' (Shen, 2007:196)
[153] Further empirical elaboration will follow in Section 5.6.

an issue. The military significance of this warfare must therefore be justified for the massive Chinese populace.

Factors indoctrinating the Chinese people

The justification of China's cyber warfare above may be constituted by several causal factors, which are able to drive the Chinese massive populace into conducting warfare. These factors, such as the tenets of ideological education, concept of the century of humiliation, and all-out defence, are likely to be the fundamental measures of discipline for China's cyber warfare. Empirical evidence of these factors will be collected and analysed in Section 5.5 in Chapter Five.

Chapter Five:

China's cyber warfare – *Empirical findings*

Chapters Two, Three and Four of this research engage with relevant literature in order to develop an analytical framework to now investigate empirically how China conducts cyber warfare. This chapter will present the empirical findings ascertained by following the research methodology laid out below, in order to articulate the theoretical propositions generated in the framework and work towards conclusions.

The features of cyberspace[154] have been theoretically interpreted in this research, demonstrating that cyberspace may be apt to become a potential battleground for both state and non-state actors. The concept of cyberspace has been carefully defined to facilitate identification of warfare conducted in this battle space. Furthermore, the four principles of cyber-territoriality[155] have been discussed in order to possibly delineate the extent of cyber warfare; in the event that one of the four principles is compromised, it may be possible to justify defensive actions in cyberspace. In addition, these conceptual ideas may also be applied to China's cyber warfare, which adopts the principles of People's War as its strategic guideline. According to the analytical framework, certain theoretical propositions are:

4. The strategic values of cyberspace make it an intangible arena in which states contend for predominance over one another.

5. China's cyberspace is constructed based on an integrated platform consisting of computer networks, telecommunications, and electromagnetic environments in order to enlarge the strategic value of cyberspace.

[154] The features are: the permeability of cyberspace; the military, government and civil society sectors sharing cyberspace; the asymmetry and vulnerability of cyberspace; and the anonymity of actors in this non-state space. These aspects are discussed in detail in Chapter Two.

[155] The first three principles are *autonomy*, *cyber culture*, and *functional borders*, which are respectively equivalent to *sovereignty*, *[national] integration*, and *borders* in the state territorial system. In addition to these three principles, the fourth principle of *people* refers to the population in cyberspace. Due to the features of the battleground, it is relatively difficult to define a war waged in cyberspace in the digital age. Thus, once cyberspace has a conceptualised territoriality, the four principles of cyber-territoriality can make up a theoretical tool to identify a cyber war in order to legitimately conduct defensive solutions. The concept of territoriality was originally established upon the state territorial system, but the principles of territoriality may be applied to a territory no matter whether it is tangible or intangible. Thus, the principles of territoriality based on the state system can be borrowed to generate equivalent principles of cyber-territoriality, even though cyber territoriality is not in absolute accord with the state system.

6. Cyberspace as a potential battle space is particularly suited to the tradition of People's War. This means that this strategic tradition remains an up-to-date doctrine in modern Chinese strategy.

7. China's cyber warfare is a strategic warfare that adopts the principle of People's War. In so doing, internet control and monitoring are also likely to be an element of China's cyber warfare in order to control and command civilians into disciplined cyber warriors for military purposes.

5.1 Methodology

As stated in the Introduction, this work falls into the category of Strategic Studies, which attempts to analyse how best to promote state security by preventing and managing conflict. However, this raises a methodological problem for Strategic Studies: unlike scientific research, for instance, one cannot create an actual war in a laboratory. Researchers do not have experimental cases in which to test their hypotheses and put their recommendations into practice. Thus, in terms of selecting cases, this situation may impede high quality research on war. As Most and Starr (1982:854) point out, case selection is crucial for war studies since research on wars is of a 'non-experimental design'.

Primarily, the aim of this research is to investigate the relation between the growth of cyberspace as a potential battleground and the doctrine of modern Chinese strategy. I therefore employed a qualitative methodology, which is appropriate to reach this aim. In this research I developed an analytical framework to produce the propositions contained in Chapters Two, Three, and Four. In order to further delineate these propositions in light of the evidence, I also carried out a case study to present an empirical indication of how China develops cyber warfare. However, valid and reliable empirical data on China's warfare is near impossible to collect inside China due to the sensitivity of studies on the PRC's military. In Bryman's view (2008:150-152), researchers need to be sensitive to whether respondents are reluctant to give socially unacceptable answers for fear of being judged, which can break down the validity of data collection. In the same way, conducting interviews inside China, particularly in this military-oriented research, may fail data validity, since respondents within the Chinese military could be extremely reluctant to be interviewed, let alone to give politically unacceptable answers, for fear of putting themselves at risk. Thus, on the one hand, China Studies

are thriving due to the attention garnered by China's dramatic rise, but on the other hand, work on the Chinese military or Chinese warfare still remain largely sealed to the world's public. As a result, conducting interviews from within China raised numerous problems for this research, including the possibility of a 'looseness' of data collection.[156] Therefore, I felt that conducting fieldwork and interviews in Taiwan instead was an effective alternative measure to formulate empirical indications as to how China implements strategies in cyberspace.

This is not only because China and Taiwan have inherited the same ancient Chinese culture and share the same language, but also because abundant resources of China Studies are located in Taiwan.[157] In addition, following the conclusion of the Chinese Civil War in 1949, the PRC regime of Mainland China and the ROC government situated in Taiwan have been constant potential opponents, and so the ROC military continues to closely scrutinise the PRC military. In addition, many incidents show that Taiwan has been the likely primary target of mainland Chinese cyber warfare. The ROC military therefore has obtained plentiful experience of exercises against China's cyber warfare.

In addition, this research is premised on the evidential indication that China conducts cyber warfare as shown in Section 5.7. The case study of this research is therefore a means to collect data in order to comprehensively investigate the propositions generated through the analytical framework in Chapter Four. Interviews in Taiwan were also conducted based on the presupposition that China conducts cyber warfare. For this reason, rather than proving whether China conducts cyber warfare, the interviews were solely focused on the investigation of modern Chinese strategy and the methods of China's cyber warfare; thus, the political confrontation between the two sides was not necessarily a causal factor to cause bias of conducting Taiwanese interviews for this research.

---

[156] According to John Gerring (2004:350), 'For the looseness of case study research is a boon to new conceptualisations just as it is a bane to falsification.'

[157] The advantage of this similarity is particularly large in this research, since, as examined in Chapter Three, Chinese ancient culture is a key factor guiding Chinese strategic culture as well as the strategy of cyber warfare. As Yang Kai-Huang (2000:71) investigates, China Studies resources in Taiwanare adequate as 'China and Taiwan share the same culture, traditions and language,' which is 'a strength of Taiwanese academia.' In addition, unlike the relations between North Korea and South Korea, the tense situation between China and Taiwan has been easing since the 1990s as martial law was lifted in Taiwan in 1987. Furthermore, the research methods employed in China Studies are becoming more mature in order to sidestep politically judgmental biases. (Yang, 2007:84-85) For this reason, any bias caused by the historical confrontation between the PRC and ROC may now be considerably reduced.

Moreover, as Alvesson and Sköldberg (2008:7-8) point out, qualitative research can be seen as 'a fundamentally interpretive activity,' and thus '[theoretical] assumptions and other elements of pre-understanding' [such as the analytical framework of this research] can offer a 'qualified methodological view' to resolve the causal bias in a reflexive case study [such as the Taiwan-based interviews of this research]. As a result, the analytical framework developed from Chapter Two to Four offers a methodological view to help answer this potential bias. Furthermore, in terms of the Chinese strategic culture referred to in this research, according to Pierre Bourdieu, it is likely that the similarities[158] between Mainland China and Taiwan could establish a condition of 'homology'[159] as a methodological tool. This allows for conducting interviews in Taiwan as way of understanding how Chinese strategic culture guides China's modern strategy and the development of cyber warfare.

However, despite contextualising these research rationales for methodological justification, I acknowledge that certain qualitative biases of this research could still exist.[160] One might still argue that, even though conducting interviews for case study in Taiwan is a sensible approach to facilitate empirical elaboration in this research,[161] it is still inevitable that the data collected from Taiwan may contain some blind-spots or even bias due to the military confrontation between Mainland China and Taiwan. For this reason, when designing my fieldwork in Taiwan, I was

[158] Despite the military confrontation, in terms of the research issues in this study, such as Chinese strategy and strategic culture, there is a certain level of similarity between the PRC and ROC military, which allows the generation of a methodological homology in order to complement the lack of information available on the PLA, as Mainland China and Taiwan historically share the same culture and language.

[159] Bourdieu's central contention in his study of France's cultural taste in the late 1960s is that tastes – for art, literature, fashion, film, sport, food and drink – can be divided into 'zones of taste,' each of which corresponds to particular social classes (Bourdieu, 1984: 16). This is what he calls 'homologies of social space' by which (relatively) homogeneous conditions of existence are translated in a particular lifestyle. This may be extended to the case of China and Taiwan due to the similarity of their 'tastes,' which also refers to their way of thinking. For instance, the notion of 'worry mentality (憂患意識 *youhuan yishi*)' often emerges from many Chinese policies designed to prevent further dangers. (Harvard, 2009:15) This notion is a common mentality of both the Chinese and Taiwanese people. Therefore, in accordance with the concept of homology, strategic thinking, comprising various cultural factors, may be the same though the regimes of China and Taiwan are different.

[160] As Karl Maton (2003:62) indicates, the way to avoid bias is 'by seeing bias everywhere.' For this reason, in this research I did not try to eliminate research biases completely. Instead, by understanding that these biases may inevitably occur, I tried to employ some research methods in order to lessen biases as much as possible in the stage of data collection. This is shown in the following Sections 5.1.1 to 5.1.4.

[161] As Peter Burnham *et al*. (2008:89) point out, 'methodological trade-offs' are unavoidable when drawing up a research design. Choosing Taiwanese interviews in this research could be a methodological trade-off in order to collect sufficient interview data and produce valuable analyses.

aware of this inevitable situation, and thus balance the causal bias against the advantages of collecting data from Taiwan, in order to reduce potential bias as much as possible. In addition, with regards the validation of the interview data, according to Burnham et al (2008:333), 'Triangulation can overcome the problems associated with single data [such as Taiwanese interviews]…'[162] Therefore, though the interviews form the primary resource for data collection in the case study, I also consulted the collections of government documents and military doctrine from the PRC and the USA, as well as related media reports from various countries, using these as 'different aspects of empirical reality' to corroborate each other by 'data triangulation.' (Denzin and Lincoln, 1994:454-455) In so doing, I have been able to ameliorate the situation caused by possible bias in order to ensure that the data is valid and reliable. Meanwhile, it may well be believed that every piece of research contains pros and cons. On the one hand, the fieldwork in Taiwan might have inevitable bias against Mainland China; on the other hand, the opposing position of the Taiwanese military may make their judgments conceptually critical once the judgments can be reflected through resources of the third party (i.e. the researcher in question).

In addition, the purpose of this case study is to collect empirical evidence to comprehensively answer the research questions. However, the common contentious issue of a case study is to what extent it can be generalised. In Buzan's (2010:14) view, the study of military strategy can be complementary to the concept of security. Furthermore, as Lawrence Freeman (1992:280) stresses, 'For many the only reason to study war was in order to design an international order in which disputes would be settled without resort to arms.' That is to say, even though the case study on China's cyber warfare is a specific case, the arguments produced by this research could contribute to International Security Studies in order to prevent conflicts whilst the research into China's cyber warfare can be seen as part of Military and Strategic Studies. More potential contributions of the study for the national security of states will be discussed in the Conclusion.

This empirical chapter will be developed through a thematic analysis under the umbrella of each theoretical proposition outlined in the introduction to this chapter. The themes, emerging from data collection, will be analytically allocated

[162] Besides, in a case study, combining several methods, such as 'interviews,' 'observations,' and 'collecting documents,' can form this 'methodological triangulation.' (Silverman, 2005:121)

into each proposition, with the fourth serving as a summary of this empirical chapter towards the conclusion which follows. This will link the analytical framework with empirical evidence. A diagram of the inter-relationship of these sections is shown below.

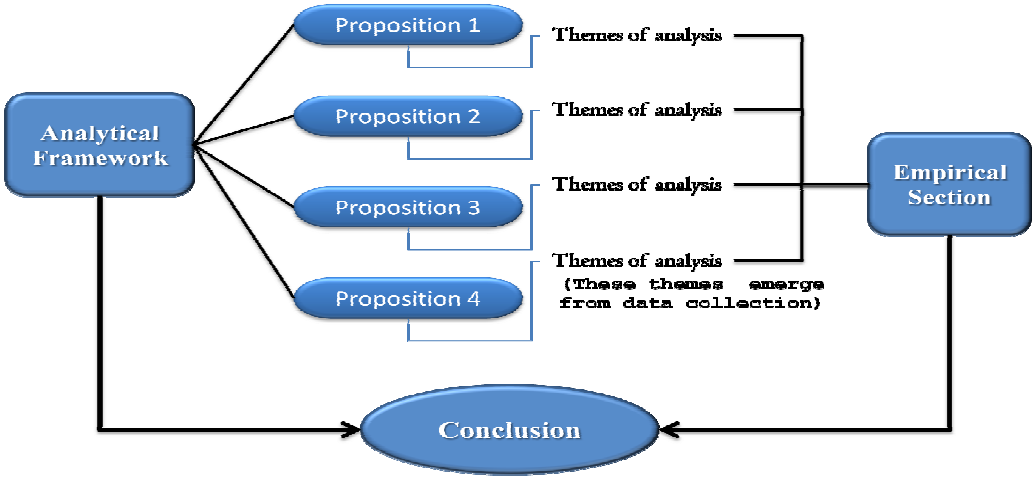

Figure-5: Inter-relationship of the analytical framework and the empirical section

5.1.1 *Data Collection*

In addition to the literature reviews, documentary analysis, and archival analysis, which form the analytical framework, this empirical section relies on the use of three distinct types of evidence: interviews, analysis of recent cyber incidents, and documentary resources, which also can form a methodological validity of triangulation. These data collection are are described as follows:

1. Interviews with Taiwanese military, government and civilian sectors presenting their perception on China's cyber warfare. These interviews are analysed as shown as Section 5.2 to Section 5.5.

   According to the organisational feature of the armed forces in the ROC, under the General Staff Headquarters, defence strategy and approaches are deployed by three different services: the army, navy and air force. (ROC National Defence Report of Taiwan, 2008) Therefore, in order to collect complete data, the research includes eighteen interviews conducted with active or retired senior military officers in different ranks and from all three different services, as well as interviewees from the civil and government sectors, listed in the table below:

Interview sectors / Interviewee	Government Sector	Military Sector	Civil Sector	Total
Respondents	8	18	4	30

Table-1: Statistical table of interview respondents

The 18 active senior military officers were based across the ROC National Defense University, War College, Army, Navy, and Air Force Command & Staff College, and other military units associated with the affairs of cyber warfare. Since I have worked in the military sector in Taiwan before, I was able to secure interviews with these active military officers who are suited to this research topic as a result of their decades of experience. Some details are briefly listed here as follows:

- Seven active Army Colonels who were in relevant military positions and involved in cyber warfare-related projects at the time of interview. Some of these respondents also hold PhD degrees.
- Four active Army Lieutenant Colonels who were in relevant military positions and involved in cyber warfare-related projects at the time of interview. Some of these also hold PhD or MA degrees.
- Two active Navy Captains holding PhD degrees, who were in relevant military positions and involved in cyber warfare-related projects at the time of interview.
- Three Air Force Colonels and one Air Force Lieutenant Colonel who were in relevant military positions and involved in cyber warfare-related projects at the time of interview.
- One retired Navy Rear Admiral holding a PhD degree, who formerly supervised a Lab of Cyber Warfare Exercise at the Ministry of National Defense (MND) in the ROC.
- One retired Army Lt. General who was formerly Chief of Staff in the ROC Army Command Headquarters, and one retired Major General who was formerly the Chief of Division of Communications, Electronics and Information at MND. Both now work for the Society for Strategic Studies, which is made up of retired Generals and sponsored by the ROC government.
- Six respondents from the government sector who work for the Institute of PLA Studies or the Institute of Information Studies sponsored by the ROC government.
- Four respondents who work for civil research institutions or private companies in the civil sector.

2. Recent cyber incidents which suggest actual implementation of PRC cyber warfare strategy. This date collection is presented in Section 5.6.

3. Documentary evidence of China's cyber warfare from the PRC, which also includes existing doctrines of military strategy associated with China's cyber warfare.

5.1.2 *The process of conducting interviews*

I conducted in-depth semi-structured interviews (Burnham, 2008). This was directed by questions and topics provided by the researcher, and accordingly articulated the theoretical propositions generated in the analytical framework. In addition to the primary research question, the interview questions designed in the case study were also based on the secondary research questions as addressed in the Introduction. Meanwhile, a range of document-based resources were comprehensively analysed, so that interview questions were able to be generated more precisely.

As mentioned previously, this chapter draws on interviews with subjects from the military, government and civil sectors in Taiwan, as well as document-based evidence, such as the PRC's military doctrines and government documents. Regarding collection of interview data, the model of interview in this research can be regarded as the model of 'interactionism' as defined by Silverman (1994:98), since the interview data are authentic experiences collected from the interviewees and the interviews were conducted[163] via open-ended interaction. As Denzin and Lincoln (2005:696) point out, 'Interviewing is not merely the neutral exchange of asking questions and getting answers,' and accordingly 'conscious and unconscious motives, desires and feelings' are unavoidable. I was therefore aware of the need to avoid any possible interview biases when interviewing.[164]

In addition, the interview questions are divided into three categories: cyberspace/Information Technology, Chinese strategy/warfare, and cyber warfare, which were put forward based on the respective areas of expertise of the interviewees. In the interview process, I asked a range of interview questions, some of which were follow-up questions to interviewees' responses. There were a total of 16 planned interview questions. The categories of all the questions and the

[163] These interview questions are designed by the author of this research, who was also the interviewer and created the interview context; the respondents either complied with or resisted the definition of this context, according to Silverman's qualitative research method. (Silverman, 1994:94)

[164] I was aware of interviewer bias whilst conducting interviews, since the interviewer may subconsciously give subtle clues with body language, or tone of voice, that subtly influence the subject into giving answers skewed towards the interviewer's own opinions, prejudices and values.

sectors that a group of questions were posed to are displayed in the table below, so that it can easily be identified which sector was asked which category of questions.

Sectors / Question Category	Government Sector	Military Sector	Civil Sector
Cyberspace/IT	Q1-2, Q9-12,	Q2-3, Q9-13	Q1, Q9-13,
Chinese strategy/warfare	Q1-2, Q4, Q7-8, Q14 -15	Q2-8, Q14-15	Q1, Q4, Q7-8, Q14
Cyber warfare	Q1-2, Q4, Q7-12, Q14-15	Q1-16	Q1, Q4, Q7-14

Table-2: Categories of interview questions[165]

5.1.3 *The validity of data collection*

As mentioned earlier, bias in qualitative research is inevitable. However, as Mats Alvesson and Kaj Sköldberg (2009:111) point out, 'A certain established bias – for instance, an ideological one – can, on the other hand, contain very valuable information from the perspective of ideology research: what message is being conveyed?' Since the ideological doctrines of the PRC and the ROC usually run counter to one another politically, any inevitable bias of the interview data is therefore likely to be an ideological one. However, though data is collected from the opposition it can still contain very valuable information for this research, especially due to implementation of data triangulation as mentioned previously.

Moreover, as Carolyn Baker discusses, the relation between the interview and the interviewee has to be understood. (Silverman, 1994:90) In line with Baker, I regarded the interviewees as experienced subjects who actively construct their in-depth observations. Even though the interviews were structured loosely on a framework of themes for exploration, following the semi-structured interview method, in order to generate data which gives an authentic insight into the interviewees' experiences, the interactions of the interviews were open-ended. The interviews were also conducted in an interactive-relational manner. That is to say, I understood what my position in this research is and clarified the purpose of the interviews with the respondents. Meanwhile, I brought the attributes and values produced in the analytical framework to the interviews, and thus did my best to avoid masking personal views.

[165] Apart from this table, the list of interview questions can also be found in Appendix 1.

Moreover, according to Burnham's view, the interviews in this research can be understood to be 'elite interviewing,' also known as interviewing the 'target group,' since it is appropriate to consider the interviewees as experts in this research topic. For example, many of the interviewees have earned PhD degrees in related fields. In addition, as Burnham points out, the semi-structured interview type adopted by this study is the best instrument for conducting 'elite interviewing.' (Burnham, 2008:231) For methodological reasons, I did not create any incentive for interviewees to be favourable to the arguments presented. However, I mentioned some arguments made in the analytical framework, such as the definition of cyberspace and principles of cyber-territoriality. This was not intended to encourage interviewees to demonstrate support for these arguments, but instead to reflect upon some answers given by respondents, as well as to hear further opinions to potentially elaborate upon the arguments and propositions. With the permission of the interviewees, interviews were conducted and recorded in Mandarin Chinese. On average each interview lasted 60 minutes, with the shortest interview running for 40 minutes and the longest for 90 minutes. A Chinese language summary was made of the interview content, which was then translated into English for the purpose of reference and quotation in this research. In addition, rather than citing the full names of the respondents, only their last names and ranks (where applicable) will be referred to in this study, as agreed with the interviewees at the time of interview.

In order to help illustrate the validity and reliability of data collection, this research relies on Hammersley's 'subtle form of realism', which consists of three epistemological elements, as follows: (Silverman, 1994:155)

1. Validity is identified with confidence in our knowledge but not certainty.
2. Reality is assumed to be independent of the claims that researchers make about it.
3. Reality is always viewed through particular perspectives; hence though our accounts represent reality they do not reproduce it.

In other words, according to the methodological judgment above, I argue that we can only know reality from our own perspective of it. Thus, the validity of the interviews in this research is established, in part, through the experiences and self reporting of the interviewees' social world.

5.1.4 *Data analysis*

The purpose of analysing the interviews and document-based evidence was to make critical judgements in light of the four theoretical propositions generated in the analytical framework. Analysis of the interviews was in part guided by the questions raised in the existing literature, but was also inductive, in that new findings generated in the early interviews were used to challenge and develop understandings of these issues in the later interviews. The analysis of the interview data was therefore designed to seek themes emerging from the respondents' content. Through critical and reflexive reading of the rich description gathered in the interviews, commonly occurring points of view emerged as strong themes. These often concerned the material and non-material values of the development of China's cyber warfare.

However, as mentioned previously, this research is necessarily limited by the general characteristics of Military and Warfare Studies since a war cannot be artificially created in order to test conclusions. The background of the interview samples mentioned earlier may also cause a possible limitation of this research. As a result, through a series of methodological steps above, a balanced integration of theoretical propositions, data collection, and data analysis can be ensured for this research to aim to uncover new findings.

Ultimately, no matter whether or not the emerging themes[166] of interviews are supportive of theoretical propositions, the interviews are valuable for the analysis of each proposition, as they are real and practical in accordance with the experiences of interviewees. Under the frame of each analytical proposition, a set of themes emerge from both the interviews and the PRC government documents, which will be laid out in full in each section through critical interpretations and primary source quotations.

5.2 The strategic value of cyberspace for China

This section will reflect Section 4.1 of the analytical framework through analysing themes emerging from the data collection to reveal empirically how China employs the strategic value of cyberspace. As examined in Section 2.2, the features of cyberspace form a strategic value, which may shape this space into a potential

[166] These emerging themes can be found in the subtitles of each of the following sections in this chapter.

battlefield.[167] In addition, these features may cause perceived insecurity as a result of people's heavy reliance on cyberspace in the present day, caused by concern that the daily functions of cyberspace will not operate securely as normal. Thus, due to the fact that states' critical infrastructures rely heavily upon cyberspace, as shown in Section 2.2, it is imperative to provide protection for this space to ensure perceived security and retain normal functionality in national politics, the economy, social public services, and even the military sector.

In China, as stated previously, the national infrastructure includes the internet, communication satellites, and nationwide cable infrastructure. China is striving hard to develop this national information infrastructure yet further. As a result, the population of China's 'netizens'[168], virtual 'habitants' of cyberspace, has also increased exponentially.

As Joseph Nye (2011:3) states in *Cyberspace Wars*, 'Unlike atoms, human adversaries are purposeful and intelligent. Mountains and oceans are hard to move, but portions of cyberspace can be turned on and off at the click of a mouse. It is cheaper and quicker to move electrons across the globe than to move large ships long distances through the friction of salt water. The costs of developing multiple carrier taskforces and submarine fleets create enormous barriers to entry and make it possible to speak of US naval dominance. In contrast, the barriers to entry in the cyber-domain are so low that non-state actors and small states can play significant roles at low levels of cost.' (Nye, 2011) This statement by Nye succinctly demonstrates that cyberspace presents a strategic value for states contending for predominance over one another. The more advantages cyberspace offers, the more vulnerable states' security will become. On the one hand, the strategic value of cyberspace can be harnessed by any state, but on the other hand, states must consider the vulnerabilities of cyberspace caused by the advantages of the same strategic value to others. As shown in Section 2.2, the key features of cyberspace potentially simultaneously cause the vulnerability of this space as well as the reasons behind its strategic value for actors in cyberspace, including both states and non-states. For example, the shared cyberspace links together civil society, government and even, possibly, the military sectors. Though this enables states to

[167] Please refer to Section 2.2 for more detail on the features of cyberspace.
[168] According to the PRC's '27th Annual Report China Internet Network Information' (2011) concerning China's internet status, the population of China's netizens is 457 million, and additionally 303 million people connect to the internet via mobile phones.

rely on cyberspace, this strategic value also makes it an attractive target for adversaries. Meanwhile, cyberspace's feature of asymmetry also offers actors a tempting strategic opportunity to carry out attacks in order to accomplish certain political purposes. In addition, due to the anonymity of cyberspace, adversaries conducting cyber attacks are unlikely to be identified in this intangible space. However, according to the investigation presented in Section 2.3, cyber-territoriality could potentially be recognised through mapping between the Domain Name System and TCP/IP in cyberspace. The characteristics of cyber-territoriality must therefore be typified in order to trace back the origin of hostile attacks.

The conceptual analysis of this research suggests the theoretical proposition that the strategic value of cyberspace shapes it into an intangible arena in which China is likely to contend for predominance over other states. The following sections will elaborate this theoretical proposition empirically through data collected in the case study.

5.2.1 *The strategic value*

This section will explain exactly how China realises the strategic value of cyberspace. When asked in interview how China regards the protection of cyberspace as part of its cyber warfare, ROC Navy Captain Chang (2011) responded:

> *'[According to Chinese ideology] I think whatever space human beings can reach will inevitably turn into space for human struggle. Consider the following formula: human beings engage in a space's activities thus creating a space's interests. As the space's interests cannot satisfy all parties involved in such activities, the space's struggles naturally appear in human society. We, the human being, may subsequently develop intellectual concepts of the space's control or the space's security in order to secure its freedom of choice as a policy formulation, and freedom of action in policy implementation: in other words, secure total dominance of the space. This is the general rule of human nature, no more, no less.'* [In Captain Chang's view, this can also be applied to other domains such as sea, the electromagnetic spectrum, air, and outer-space, though the PLA defines cyberspace as including the electromagnetic spectrum.]

In Captain C. (2011) view, China may value cyberspace as a potential battleground similar to the traditional battlefields for 'human struggle.'[169] In so doing, the value of this cyberspace for China is beyond the various functions of banking, transportation, and public services used by civil society, but instead is suited for military purposes. As a result, China's cyber warfare may be deployed via embedding military actions into the civil sector.

However, one might argue whether China is capable of dominating the strategic value of cyberspace. In the view of ROC Air Force Colonel Liu (2010), 'Fairly speaking, I think that the USA might be the state which is able to dominate the field of cyber warfare on a global scale rather than China. This is because the major hardware, software, and databases, such as Intel CPU (Central Processing Unit), OS (Operating System), Windows, Linux OS, and Oracle database, were originally invented and produced in the USA. These techniques are the fundamental facilities used to control computer systems in cyberspace and are indispensible for developing cyber warfare.' In other words, other states may have to follow in the wake of the US military due to US technological dominance. The related argument that China learns warfare from the USA will be thoroughly considered in Section 5.3.2.

5.2.2 *The national information infrastructure*

Professor Ding (2011), an expert on the Chinese military, evaluates the aforementioned Chinese National Defence report in his interview:

> *'In terms of interpretation of the Chinese National Defence report 2010, I do believe that the PRC constantly espouses the strategy of cyber warfare in order to fulfil its strategic thinking, which is the defeat of the militarily superior by the militarily inferior, through the feature of asymmetry of cyberspace [as you argue in your research]. In addition, the development of China's cyber warfare not only involves securing China's own cyberspace but also contending dominance in cyberspace. China therefore will never give up developing cyber warfare, and this is stated without any evasion in the PRC official report, despite the fact that this report is published in order to earn the trust of other states. Moreover, this military*

[169] See Chapter Two for a further examination of this idea.

development is built on the civil information infrastructure, as the report notes.'

According to interviewee ROC Army Lieutenant Colonel Xiu (2010): *'Taiwan has been the target of China's cyber warfare exercises for many years, so I have had many experiences with tackling China's cyber attacks. In cyberspace, unlike on the traditional battlefield, there are no limitations such as time or weather conditions to prepare defensive measures [like traditional military fortifications], or to counter-attack your enemies in this battlespace, so actions can be carried out 7 days a week and 24 hours a day on a massive scale. China has also realised this potential strategic value, and there is some documental evidence of this, so it is not necessary to evade the fact of China's cyber warfare development.'*

This discourse reflects the argument that warfare in cyberspace may contain strategic value, as the boundary between offensive strategy and defensive strategy in cyberspace is also indiscernible. As identified in Section 2.2.2, one of the features of cyberspace is that a state's military and government sectors share the same electronic information infrastructure, namely cyberspace, with its civil society. In other words, as cyberspace has become a potential battleground, a pertinent issue is whether a state's military capability in this battleground could be enhanced in order to increase its ability to secure the civil information infrastructure contained therein. As a result, cyber warfare, an issue of the military sector, can be established through the information infrastructure, part of the civil sector. Therefore, based on this strategic value, it is very likely that China's cyber warfare will be developed through reinforcement of the civil information infrastructure, not necessarily through the military sector.[170]

According to interviews, it can be argued that China harnesses the strategic value of cyberspace via its national information infrastructure, particularly that of the civil sector, in order to develop cyber warfare. Meanwhile,

[170] This concept may also apply to other weapon technology development of. Technology has long influenced the development of military warfare, particularly since the industrial revolution. However, as examined in earlier chapters, the scope of information technology is on a relatively large scale, meaning its strategic value is consequently more influential than other technologies.

as PLA's Major General Wang Baocun (2010) asserts[171], 'Propelling the military via civil industry [以商促軍, *yi shang cu jun*]' is the key purpose behind reinforcing China's civil information infrastructure, thus strengthening the PLA's capacity for cyber warfare. Chinese Major General Wang states:

> *'The concept of "propelling the military via civil industry" is based on the idea of societal or national informationisation promoting military informationisation. There are three main reasons: firstly, the Chinese national information infrastructure was constructed earlier than that of the armed forces, and therefore the former can provide a point of reference for the latter; secondly, the extent of informationisation of local businesses is generally* higher *than that of the Chinese military, and therefore the former can have an 'infiltrative' function for the latter; thirdly, the development of civil information technology is more rapid than military information technology, which sets the technical conditions of "civilians driving the military". The PLA's informationisation should be guided by the strategy of national informationisation as well as relying on the foundation of the national information infrastructure, in order to achieve the goals of "combining peace with wartime; combining the military with civil society; military use of civil technologies, and embedding the military in civil society".'*

Furthermore, practical evidence further validates this viewpoint. On 31st March 2011, the PRC officially published the 2010 China National Defence Report.[172] This report clearly proclaims that China's civil information infrastructure is a vital construction of the national defence. This government report primarily addresses the strategic guideline of 'speeding up the construction

[171] Major General Wang made this assertion in an article entitled *View of PLA's Informationisation Construction (我軍信息化建設管窺, wo jun xinxihua jianshe guankui)* which can be found in the Chinese monograph *China's Information Warfare*, acknowledged as a critical guideline of China's cyber warfare doctrine. The hard copy was located in the archival collection of the ROC National War College in Taiwan. (PLA, 2010:116-137)

[172] In general, the motivation behind the publication of this white paper is to provide information on China's national defence in order to remove any concern about China's threat to other states. However, this report stresses that the development of information/cyber warfare remains a key element in China's national defence, implying that China may be expending great effort in developing cyber warfare.

of [China's] informationisation', in order to connect the civil information infrastructure and China's cyber warfare in the military sector.

> *'People's Liberation Army (PLA) troops must closely embrace the construction of an informationised military to achieve the strategic aim of winning information war [cyber war][…] constructing a civil information infrastructure to realise aims of rapid, striding development. The total length of optical fibre available for communication is much more than a decade ago, creating a new generation information transmission network based mainly on optical fibre communication, and supplemented with satellite and shortwave communication. This rapid developmental route is principally led by informationisation, driving modernisation through preparation for military struggle in order to reinforce defensive capabilities under the conditions of information warfare. ….] To confront the new developments and changes in national security requirements, the PLA has to strengthen the construction of new operational ability [cyber warfare] in order to meet the requirements of "winning local under information conditions"*[173]*.'*

5.2.3 *The military task of reinforcing the civil information infrastructure*

In addition to the benefit to the military produced by the civil sector, in turn, the development of China's cyber warfare not only seeks strategic warfare in the military sector but also facilitates the protection of China's civil information infrastructure. As the features of cyberspace create the condition that any actors may possibly pose a threat in this civil information infrastructure, China regards protection of cyberspace to ensure its strategic value as a military task. The purpose of cyber security is to prevent the threat caused by the inherent features of cyberspace. Normally, these threats need not be dealt with by the military alone. However, in China, any issues relating to cyberspace, regardless of whether they occur in the military or civil spheres, fall under the umbrella of cyber warfare.

Further to this, according to ROC retired Lieutenant General Deng (2010), 'Though China is a country that has been developing rapidly in terms of "informationisation," the extent of this development is unbalanced [between the

[173] This is the latest military strategic guideline, in place since 1992. Please refer to Section 2.2.3 in Chapter Two for more information.

military and civil sectors]. Therefore, the rule of developing the national information infrastructure may be different to that of other developed countries.' In Deng's view, China's informationisation targets the development of cyber warfare in the *military* sector rather than cyber security in the *civil* sector. In addition, this guideline may be based on the evaluation of the strategic value of developing warfare in cyberspace, meaning that the deployment of military actions in the civil sector could be justified as 'protection' of the military. Moreover, in terms of China's cyber security ideology, as Adam Segal (2011), a member of the Council on Foreign Relations (CFR), points out, 'I think the way that the United States, the United Kingdom, and most other Western countries use it [cyber security] is for defence of computers and communications networks [in the civil society]. The Chinese, like the Russians, also use the term "information security," which includes content. They are not only concerned about attacks on [civil] networks, but which information is being carried on them – which could affect national security.' In other words, for China all matters associated with cyber security are not only regarded as an issue of national security, but also specifically as an issue of military strategy, demonstrating that China's cyber warfare may even include the deployment of military actions in civil society.

5.2.4 *Gaining strategic value through non-military approaches*

Aside from embedding strategic value in China's national infrastructure, interviewees suggest that there is another approach, known as Military Operations Other Than War[174], in which China pursues strategic value for military purposes via non-military operations.

Since the 1980s, the PRC has proclaimed that China's rise is peaceful, and that China would not carry out any military operations unless necessary. However, after the idea of Military Operations Other Than War (MOOTW), involving aspects such as humanitarian aid, disaster relief, and rescue of societal emergencies, was introduced to the world, it can be believed that the Chinese military 'put out feelers' to test the possibilities of employing the non-traditional

[174] The term MOOTW was introduced in the US Joint Doctrine JP-3-07. It focuses on deterring war, resolving conflict, promoting peace, and supporting civil authorities in response to domestic crises. MOOTW may involve elements of both combat and noncombat operations in peacetime, conflict, and war situations. MOOTW involving combat, such as peace enforcement, may have many of the same characteristics of war, including active combat operations and employment of most combat capabilities. (US Joint Doctrine, 1995)

military circumstances of MOOTW to achieve certain military goals for the PLA, such as the exercise of logistics and long-distance troop deployment. This may be homologous to China developing cyber warfare through non-traditional military actions. Some existing Chinese MOOTW actions could be explained in terms of the strategic thinking of using non-traditional military actions to reinforce military capabilities, demonstrating that the PRC intends to adopt the strategy of Military Operations Other Than War to exercise and shape its military capabilities.

ROC military officer Army Colonel Lien (2010) provides his empirical experience in military logistics to state:

> *'Based on the PRC's Constitutional Law amended in 2004 and the PRC's Regulation of Measures for Contingency amended in 2007, it can be seen that the idea of "Military Operations Other Than War" has been noted in these laws, so that the Chinese armed forces can get involved in many non-military actions, such as rescue from natural disasters or societal accidents and international humanitarian aid in order to exercise military abilities and cooperate with private sectors. For example, the Chinese navy sent three battleships to join the anti-pirate activities in Somalia in December 2009 to practice the military logistics of long sailing, and also carried out some domestic joint exercises between the military and civil sectors in many local regions by reason of homeland security in order to reinforce the cooperative relations between the two sectors for later occasions.'*

In Lien's view (2010), the PLA has used the term 'diversified military tasks [多樣化軍事任務, *duoyanghua junshi renwu*]' appearing in China's National Defence reports since 2006, to represent the same tasks and goals as MOOTW. Further evidence corroborates China's intention of conducting MOOTW. Since 2010, the PRC has created new opportunities for cooperation with other states, including peacekeeping efforts, humanitarian and disaster relief, and counter-piracy operations, in order to carry out military practice, such as logistics, and reinforce China's military modernisation. For example, in March 2011, many nation-states sent emergency rescue teams to help Japan recover from a massively destructive earthquake and tsunami. China attempted to take this opportunity to send supplies to the damaged area, but as the supplies would be

carried not by a civil ship but instead by a Chinese Navy ship, the offer was therefore declined by the Japanese government.[175]

An additional strategic thought behind China's adoption of the strategy of cyber warfare may be that similarities between civil technology and military technology are very extensive. Thus, both military defence and offence can rely on the civil sector to stealthily develop China's cyber warfare without drawing the attention of other states, particularly in areas such as research and development and expenditure. In terms of this strategic pattern, the interviewee ROC Air Force Colonel Huang (2011) states:

> *'From reliable sources in my military experiences, I have accessed evidence showing that China has merged a few military academies into the PLA Institute of Technology, where a Research Centre for Cyber-Technology was established in 1998. More than 400 civil IT experts have been recruited to develop the critical techniques of cyber warfare, and some technical cooperation between military and civilian universities has also been carried out.*

In Colonel Huang's view, both the professionals and the advanced techniques of the civil sector are incorporated into the military sector via the PLA Institute. Thus, the research and development of China's cyber warfare is not necessarily carried out by the military sector alone, but also involves cooperation with the civil sector. In addition, due to the similarity of IT in cyberspace in the two sectors, any outcomes of research and development in the civil sector can be easily transferred to the military sector.

5.2.5 *The principles of cyber territoriality*

It is necessary to create principles for actors to deal with the strategic value of cyberspace. However, due to the inherent anonymity of cyberspace, it is hard to define a cyber war and identify attackers to confer responsibility for any damage caused by cyber attacks. As a result, the four principles of cyber-territoriality generated in Section 2.3 of the analytical framework may offer cyber-actors, both state and non-state, the justification needed to seek possible solutions to deal with cyber attacks.

[175] Japan also ruled out China's emergency rescue team. According to Japanese officials, this was because the Japanese airport open to landing for foreign rescue teams was the US military base during the Korean War. (China News, 2011)

In an interview with Feng, based on his experience involving cooperative investigations, Feng (2010) points to empirical evidence showing that cyber warfare was often applied by China as a method of espionage:

> *'On 7th March 2011, François Baroin, the French Minister of Budget, indicated that the computer system of the French Financial Administration Department was extensively hacked into, by hackers whose IP addresses were situated in Mainland China, and that this hacking caused roughly ten thousand computers to be shut down. Patrick Pailloux, the Chief of the French National Agency for Information Technology Security, claims that these large-scale attacks, the likes of which France had never seen before, were intended to retrieve documents related to G20 as France was the host state at the time. In addition, Xin Heyoung, a congressman and member of the National Defence Committee in the Congress of South Korea, indicated that Chinese hackers invaded the computer system of the Ministry of National Defence of South Korea in order to access some information relating to a weapon acquisition of the USA Global Hawk UAV* [Unmanned Aerial Vehicle].'

Further to this, the interviewee ISP General Manager Yan Fang-Bin in Taiwan evaluated, from his experiences of dealing with China's information industry, that:

> *'Firstly, normally it would not be an important point that Chinese civilians hacked the email accounts of Chinese rights activists, unless they were encouraged by the government. Secondly, this attack was on a large scale and highly complicated. Some IT experts used the technique of "Reverse Engineering" to deconstruct the computer programme of the attacks, and then discovered that the primary codes contain a unique algorithm which has been introduced only in Chinese technical reports.' […] 'In addition to the dispute, the USA government reports might be trustworthy, since 13 of the most advanced machines of the Domain Name System server in the world are supervised by the USA so that they are able to trace attacks through logs on these servers.'*

However, some offer differing points of view. One of the interviewees, ROC Navy Captain Chang (2011), argues:

> *'Even though the Taiwanese military has had many empirical conflicts with Mainland China, I have to state fairly that distinguishing boundaries in cyberspace remains uncertain, since all states are linked together creating a certain level of dispute over benefits. Besides this, though Domain Names and IP addresses can be linked to states, this still cannot represent the boundary of states' territories, and lacks the meaning of sovereignty. Like traditional wars which are based ex soli, offensive and defensive military actions can be identified according to the boundary of territories. Therefore, it is necessary to offer the equivalent concept in cyberspace in order to further recognise the purpose of cyber attacks.'*

This infers that whether China conducted the cyber attacks on Google or not still remains contentious. Navy Captain Chang's (2011) critiques that 'It is impractical to view that cyberspace possesses the essence of territoriality as a real territory does [since cyberspace is not physical].' As Captain Chang further conjectures, many transnational cyber-attacks take advantage of the difference between the network Domain Name and their true physical location.[176] As stated by Captain Chang, a state's sovereignty is closely associated with 'judicial jurisdiction'. Most of the time, this jurisdiction is limited to the physical territory of the state itself. However, though there is a difference between the Domain Name of a website and its real geographic location, it is still possible to trace an attack to a geographical location via its digital TCP/IP address, rather than its Domain Name or the website address. In an interview, ROC Army Lieutenant Colonel Chang (2010) corroborates: 'According to my experience of dealing with cyberspace, I have to say that the Domain Name System and TCP/IP addresses give this cyberspace the feature of regionality since the distribution of IP addresses is based on the regionalisation of cyberspace. Thus any computer in cyberspace can be traced back to a geographical location.[177] China's cyberspace is

[176] For example, some website's domain names end with co.uk, but the servers are not necessarily physically located in UK territory.

[177] Lt. Colonel Chang also demonstrated how to trace IP addresses via a real web-based system: http://www.ipaddresslocation.org/. If you input an IP address, the system will show its geographical attributions, such as country, city, latitude, longitude, local time, and the IP's Host and organisation.

no exception as well.' In other words, based on the technique of the DNS and TCP/IP mapping system, every computer in cyberspace represents an IP address which links up to a geographical location; this may delineate an intangible space possessing the metaphorical concept of territoriality if one of the potential four principles – the functional borders of cyberspace – can be recognised.

In addition, as the incidents of cyber attacks examined in Section 5.6 later, it illustrates that the IP addresses of some cyber attacks have been traced to geographic locations within China's territory. Nevertheless, one might argue this cannot prove whether these attacks were supported by the Chinese government or the military sector, or were simply from civilian hackers. In addition to this, the cyber attack on Google in 2010, apparently carried out by actors inside China, may be regarded as the most significant case[178] of cyber attack, as despite the huge costs, the Google company even considered pulling out of China and giving up the huge Chinese market in response. Moreover, in unprecedented circumstances, the US government also became involved, urging China to respond to Google's investigations of a sophisticated hacking attack into the Gmail accounts of Chinese rights activists.

However, whilst the PRC continued to rebuff the claims that some of the cyber attacks could be traced back to geographic locations in China's territory[179] due to the controversy, in late 2010, an apparent state secret was surprisingly revealed by WikiLeaks[180] in its publication of a classified diplomatic cable. According to the released cable, the Google attack was very possibly an approved operation by Chinese government officials. The cable summaries that:

---

[178] The seriousness of the issue could be seen by Google's response to the hacking and their threat to pull out of China altogether, and also from the US State Department's involvement in the issue. The fact that the State Department and even someone as high up as Hillary Clinton got involved in the issue shows how important this single hacking event was (not just because Google is the current market leader).

[179] For example, in terms of the US government urging Beijing to investigate Google's complaints that cyber attacks had originated in China, the PRC's Foreign Ministry spokesman Ma Zhaoxu said the US should 'respect the facts and stop making groundless accusations against China.' The rough timeline of events is below: (BBC News, 2010)

- 12 January 2010: Google's Chief Legal Officer, David Drummond, announces Google may leave China after cyber attacks and calls for an end to censorship of its search results.
- 22 January 2010: China rejects US criticism as 'groundless.'
- 22 March 2010: Google announces it will redirect its Mainland China customers to an uncensored Hong Kong-based site.
- 29 June 2010: Google says users inside Mainland China now have to actively click on a link before accessing unfiltered search results.

[180] WikiLeaks is a non-profit media organisation dedicated to bringing important news and information to the public.

> *'A well-placed contact claims that the Chinese government coordinated the recent intrusions of Google systems. According to our contact, the closely held operations were directed at the Politburo Standing Committee level'*[181] *[…] 'Another contact claimed a top PRC leader was actively working with Google competitor Baidu against Google.'* [The Chinese private sector would be willing to cooperate with the Chinese government in certain cases since their relations are very close.]

This well-known incident of cyber attack has more relevance to this research than just this. Without the leaked cable information, it may be impossible to assign responsibility for the Google attack. In Section 5.5 of this chapter, further investigation relating to the Google case will be analysed to provide arguments for other propositions.

Furthermore, on 16th July 2011, China Central Television 7 (CCTV-7), China's official channel for military and agriculture issues, broadcast a 20 minute programme called '網絡風暴來了 (*Wanglu fengbao lai le, Cyber Storm Is Coming*),' in which it was inadvertently revealed that a PLA institute was developing cyber attacks targeting certain websites situated inside US territory.[182] It is highly possible that this is the first visual material released from a unit in the Chinese government sector that significantly presents China's cyber warfare. As a report further evaluates, this incident is likely to lead to international tension. (Erickson and Collins, 2011) As a result of incidents such as these, it is now imperative to generate certain rules to identify which kinds of act constitute an act of war and which do not.

However, as yet, there is no international legal framework or rules to build up a solid set of evidence for assigning responsibility. As Christopher Hughes

[181] The cable of 18th May 2009, entitled 'Google China Paying Price for Resisting Censorship,' goes on to quote a well-placed source clearly indicating that two members of China's toping ruling body, the Politburo Standing Committee, Li Changchun (李长春) and Zhou Yongkang (周永康), issued approvals of the hacking of Google. This cable is likely to provide a patchwork of detail about cyber attacks originated in China. (WikiLeaks, 2010)

[182] In the programme, a web-based system of cyber attack was demonstrated in order to explain to audiences how cyber warfare works. This web-based system showed a list of attack targets users could select, inadvertently demonstrating the attack source and the system designed by the PLA Electronic Engineering Institute with the system title showing on-screen. As soon as the mistake was reported, the programme was pulled from the CCTV-7 website on 24th August 2011. Nevertheless, the programme can still be found via a web blog (http://xlolix.com/bujieshi.html#comments), and was also reported on by *China SignPost*. (Erickson and Collins, 2011)

(2010:22) points out, 'It has still been impossible to identify specific computers without cooperation from Chinese authorities.' As a result, due to the anonymity of cyberspace, it is theoretically difficult to identify attackers. According to Lene Hansen (2009), it is therefore highly necessary that networks and cyber actors be identifiable or linked to a nation-state or a regime, so that responsibility for a cyber attack can be assigned once an actor is attacked in cyberspace. This links with the four principles of cyber-territoriality (*autonomy*, *cyber culture*, *functional borders*, and *people*) proposed in Section 4.2.[183] To resolve the difficulty of defining a cyber war, if cyberspace had a conceptualised territoriality, the four principles could combine into a theoretical tool to identify cyber war to allow for the legitimate conduct of defensive solutions. Even though the concept of territoriality was originally established upon the state territorial system, the principles of territoriality can be applied to a domain regardless of whether it is tangible or intangible. The principles of territoriality based on the state system can be borrowed to generate equivalent principles of cyber-territoriality even though cyber territoriality is not in absolute accord with the state system.

If physical locations of cyber attacks can be linked to state's sovereignty, as proposed by Hansen (2009), the principles of cyber-territoriality may grant either state or non-state actors in cyberspace the justification necessary to arbitrate or deal with disputes in the event that the principles were compromised. For example, the infamous Google incident could represent an ideal case for a private company to assert its own cyber-territoriality, in line with the four conceptual principles. Firstly, the principle of 'autonomy' can apply to the company's authority over access to its servers and data. Secondly, the principle of 'cyber culture' reflects the norms, behaviours, and communications carried out via Google's websites, which form a global community. Thirdly, the principle of 'functional borders' can imply functional servers, such as filters, firewalls and proxy servers, used to scrutinise and countercheck any malicious intrusions in much the same way as a territorial state's borders. Fourthly, the principle of 'people' would refer to the users of Google; Google has the obligation to protect its 'people' from misuse or theft of their accounts or information. As such, if these principles became accepted rules recognised in the international framework, Google would be able to resort to

[183] This proposition is also based on the metaphorical territoriality of cyberspace examined in Section 2.3.

justifiable measures if any one of the principles is violated. Finally, if every state or regime were responsible for the IP addresses located geographically inside its territory, rules of engagement of cyber warfare could be introduced to function similarly to those of traditional warfare in international politics.

5.3 How China establishes its cyberspace as an integrated platform

This section empirically reflects Section 4.2 of the analytical framework through analysing the themes emerging from data collection. As defined conceptually in Section 2.1, the development of China's cyberspace is particularly based on an integrated platform consisting of computer networks, telecommunications, and electromagnetic infrastructure.

According to the interviews in this section, the tactics of China's cyber warfare include a combination of operational methods of electronic warfare, which may demonstrate integration with the electromagnetic environment. In this way, the extent of China's cyber warfare is relatively wider than the warfare of other countries, as it is not merely limited to the internet and computer-based network systems. Analysis in this section is carried out via the themes emerging from interviews and related government documents.

5.3.1 *The PRC's one-party government and China's informationisation*

China's cyber warfare is developed on an integrated platform which has been constructed efficiently by the PRC government as a result of China's one-party political system. As ROC Army Colonel Zhou (2010) points out, it is very important for any state to have a reliable and trustworthy private Information Service Provider (ISP) to build up its national information infrastructure. This is true not solely for the military sector, but also for cyber security in general, since all sectors in a state – civil society, government, and the military – rely on a cable system normally provided by private industries. According to Zhou (2010), 'There is no doubt that this issue would be the same for the construction of China's cyberspace in order to develop cyber warfare.'

However, since China is ruled by the CCP government in a one-party regime, it is possible that the development of this integrated platform, consisting of computer networks, telecommunication, and electromagnetic infrastructure, may be easily accelerated. As Army Colonel Lien (2010) argues in interview, 'Because of the one-party dictatorship in China, budget planning, equipment

procurement, and policy-making have enabled a faster development of network communication infrastructure than that of other countries. The most evidential example is that of the construction of the National Cable Infrastructure by following the model "Eight Railway Lines from South to North and Eight Railway Lines from East to West"[184] in China.' In fact, according to a PRC government report, this construction of the National Cable Infrastructure, starting from 1998 and finished within only five years, is named 'The Communication Network of Eight North-to-South and Eight East-to-West Optical Fibre Routes' (八縱八橫光纖通信網, *ba zong ba heng guangxian tongxin wang*). Currently, optical fibre makes up more than 90% of the long-distance transmission network, which covers more than 85% of all Chinese counties and cities. The total length of the 23 main fibre cables is about 37,000 kilometres.[185]

In other words, this massive cable construction makes it possible for people everywhere in China to connect to cyberspace and act as a cyber warrior if necessary. However, despite the fact that China's national cable infrastructure is huge and covers very wide areas geographically, the ports connecting to the global WWW (World Wide Web) are relatively few within China's territory. It is thus easier for the Chinese government to set up censorship mechanisms on these ports to control and monitor the extensive cyberspace.

In terms of mobilising civil professionals to develop this integrated platform, ROC Army Colonel Zhou (2010) stresses that in addition to deploying a state's military troops, every state should have its own laws regarding mobilisation of civil resources to allow the government to assemble functional units engaging in rescue activities in war or natural disasters if necessary: 'I therefore believe that China is no exception in doing so. In addition, China is able to accelerate this mobilisation on a large scale because of its one-party

[184] The idea of 'Eight Railway Lines from South to North and Eight Railway Lines from East to West' refers to the main railway lines into which increased effort of construction and upgrading was put during the Tenth Five-Year Plan period (2001-2005). The 'Eight Railway Lines from South to North' are the railway lines between Beijing and Harbin; Beijing and Shanghai; Beijing and Jiulong; Beijing and Guangzhou; Datong and Zhanjiang; Baotou and Liuzhou; Lanzhou and Kunming; and the east coast railways lines. The 'Eight Railway Lines from East to West' are the railway lines between Beijing and Lanzhou; the Northern Channel for Transporting Coal; the Southern Channel for Transporting Coal; railway lines between Longhai and Lanxin; railway lines between Nanjing and Xi'an; railway passage along the Yangtze River; railway lines between Shanghai and Kunming; and railway passage to the sea in the Southwest.

[185] The key points of the report are noted in Appendix 2: China's National Telecommunication Network: Eight North-to-South and Eight East-to-West Optical Fibre Routes.

dictatorship.'[186] Moreover, Colonel Zhou (2010) states that 'A reliable source indicates a few of China's private IT companies engage in certain tasks assigned by the Chinese government and military to indirectly strengthen the capability of China's cyber warfare during peacetime.'

In general, using search engines to look for key words that the Chinese government regards as sensitive may ultimately turn up no results. For example, in May 2011, Baidu, the biggest internet search engine company in China, was accused of compromising internet freedom in cooperation with the Chinese government, which was the first case in which an internet search engine was sued. (*The Economist*, 2011) However, this cooperation is likely inevitable due to laws made by the one-party authority. This may thus explain how the Chinese government is able to efficiently control and monitor cyberspace activities inside Mainland China.

5.3.2 *China's 'Integrated Network Electronic Warfare'*

Following the discussion of the construction of China's national information infrastructure, it can be believed that electromagnetic environments are integrated into China's cyberspace. This section explains that China also characterises its cyber warfare as *Integrated Network Electronic Warfare* (INEW).

In ROC Army Colonel Lu's (2010) view, it is likely that China's cyber warfare will draw from the US military's idea of 'Network-Centric Warfare', which fits well with China's integrated cyberspace. According to Colonel Lu (2010), Network-Centric Warfare refers to warfare applied in 'the electromagnetic environment.' This warfare enables the employment of a variety of resources in the environment, the flexibility of carrying out a variety of tasks, the command and control of resources in electronic warfare, 'control of the electromagnetic spectrum' and a gain in advantage in 'combat space.'

From a technical perspective, as interviewee Zhang (2010) indicates, 'Seven Layers'[187] is currently the global standard for network transmission architecture. The first and second layers are used for communication; the third layer and above are used for networks. 'Based on this bedrock, network and

[186] Colonel Zhou also mentions the opinion of a US senior military officer that the US military would recognise China's authority to mobilise its people if they needed to do so.

[187] This is a standard of the Open System Interconnection Reference Mode published by the International Organisation for Standardization (ISO). For the concept of 'Seven Layers,' please refer to Section 2.1.1.

communication should be regarded as an integrated platform, where telecommunication bears any packages transmitted.'

In addition, as ROC Air Force Lt. Colonel Hao (2010) notes from his working experience with military intelligence, 'Regarding the collection of electronic information, the principle of sending and receiving information is the same for wireless networks and electromagnetic waves, and both require the use of coding and encoding.' He also believes that cyberspace is characterised by the feature of networks and electromagnetics. Lt. Colonel Hao stresses that the basic military tactics of 'countermeasure' and 'anti-countermeasure' are therefore made possible by the long-distance transmission of low-frequency electromagnetic waves in the air and analysed through the combined application of the cable network and wireless network on the ground. That is to say, in modern, technology-based warfare, wireless networks and electronic waves are auxiliary to one other.

Apart from that, as ROC Air Force Colonel Huang (2011) reveals from his experience of China's cyber warfare against Taiwan, 'China's cyber troop includes an air/space unit, an information warfare unit, an electronic warfare unit, and a psychological warfare unit, all of which together form the basis of China's cyber warfare.' China's cyber warfare is thus carried out in cyberspace and electromagnetic environments. Colonel Huang's view also echoes the concept of an integrated platform consisting of computer networks, telecommunication, and electromagnetic infrastructure. In fact, in January 2002, the PRC issued the 7th edition of '*The Guideline of Military Training and Evaluation*'. This document notes that China has established research and testing troops to meet the strategic need of 'Local War under Hi-Tech Conditions'[188] in the 21st century. This guideline concludes that INEW, containing various forms of tactics, is the focus of cyber warfare.

Furthermore, as ROC Air Force Colonel Yao (2010) corroborates, the PLA has possibly already put Integrated Network Electronic Warfare into action, even though this term has not yet been published in any official government documents. In Yao's view, this warfare can be regarded as a 'Chinese version' of USA cyber warfare, which means that, as the field of electromagnetic operations

[188] Please refer to section 3.3.3 in Chapter Three on Modern Chinese Strategy.

is additional to US cyber warfare, the same goes for China's cyber warfare.[189] In one review, as PLA Major General Dai Qingmin (2008) states, the PRC considers it necessary to launch a '人民网路战 *ren min wang lu zhan* [People's Cyber Warfare],' which divides cyber warfare into six categories (operational security, military deception, psychological warfare, electronic warfare, computer network warfare and destroying entities), in which the ideas of People's War can be effectively implemented. According to Dai, '"Integrated Network Electronic Warfare" refers to the action of disturbing the enemy's battlefield system and protecting one's own battlefield system through a series of electronic warfare and computer network warfare so as to gain an advantage in information.' (Dai, 2008) In Dai's (2008) view, the core of this warfare is to 'seize and defend the control of cyberspace in order to disturb the enemy's information handling at different levels.' To enhance efficiency, electronic warfare has become the major method for use in the cyberspace information system and information weapons system. Dai (2008) also argues that as the information system is the centre of the warfare, in the information warfare battlefield, 'Integrated Network Electronic Warfare' is an indispensible weapon. Any disturbance to the system would lead to enforced separation of warfare participants and weapons. Accordingly, 'Integrated Network Electronic Warfare' especially emphasises incorporating Command, Control, Communication, Computer, Intelligence and Surveillance (C4IS), and integrating the phases of combat vehicle and combat system, which all help achieve certain tasks. The effectiveness of the combat vehicle and combat system phases is proportionate to the degree of integration. In other fields, the effectiveness of integration is greater than the sum total of the individual systems' effectiveness. This can also explain why China's cyber warfare is developed based on an integrated platform.

In terms of Chinese documentary evidence, an interior PLA document[190] of 2009 shows that the PLA carries out the concept of 'Network-Centric Electronic Warfare,' similar to the Network-Centric Warfare cited above, as a directive of military operations. As this document notes, 'Network-Centric

[189] This argument reflects Chinese thinking represented by the idiom: 以子之矛攻子之盾 (yǐ zǐ zhī máo, gōng zǐ zhī dùn, attack [an adversary] with what one has learnt from them.)

[190] This interior PLA document, produced by the PLA's General Staff Headquarter s 53rd Institute, is entitled '*Transformation of Electronic Warfare*,' and was not officially published. It was investigated by a researcher from the PLA Archive Room at the ROC National Defence University in Taiwan.

Electronic Warfare makes use of the powerful information network and electronic warfare data link to assemble a number of interconnected electronic warfare equipments into an adaptive network.' Various electronic warfare equipments with different spectrums, functions, and locations can access the electronic information network via special terminals and nodes. Internet-based electronic warfare is used to carry out tasks, receive supervision, and benefit from internet resources and services. It integrates the electronic reconnaissance system, command and control centre, interference system and fire system into a whole on the internet in order to achieve the sharing of information, optimisation of resources and an effective use and control of the electromagnetic spectrum. Equipment from different platforms can thus work together on the same integrated platform. This network can adapt to the constantly changing environment, and further enhance responsive abilities and threat situation awareness. In addition, as this document states, Network-Centric Electronic Warfare encompasses precise situation awareness and the capability of target acquisition. Both can operate simultaneously, providing 'a platform for coordinated electronic warfare on the land, at sea, in the air and in space.' To make the enemy's command and control ineffective, electronic methods are used to intercept, attack and countermeasure enemy spies, and for target acquisition and tracking. Additionally, the advanced navigation and information network known as 'Worldwide Military Communication System' (or 'Public Communication System for Military Purposes') can be called into use. Furthermore, the supporting function of electronic warfare, its combat identification, precision engagement and close coordination make it possible to carry out various operational proposals, such as supporting the information-based weapons attacking an enemy's anti-aircraft guided missile sites, command posts, electromagnetic radiant points or other military targets.

5.3.3 *The integration of outer space*

In addition to the network system on the ground and electromagnetic transmission in the sea and air, which together form the integrated platform, this section moots that integration additionally includes the dimension of outer space.

ROC Air Force Colonel Liu (2010) argues, 'I believe that China's integrated platform, a potential battlefield, also includes the dimension of *outer*

space. This is carried out by integration of this platform, cyberspace, via satellite communication.' According to PLA Army Major General He Lei[191], the combat capability of a three-dimensional battlefield mainly consists of the power of that space to comprise a fourth dimension, in order to securely carry out information transmission and protection for campaigns. Power in space is thus an indispensible capability in modern Joint Operations. Major General He further indicates that, 'So far, in the PLA's Joint Operations, this power is a critical element with the aim of providing different services with accurate information support and protection.' As a result, the harnessing of space as a battlefield could assist other battlefields in terms of investigation, surveillance, communication, location, navigation, warning, command and control, allowing for the deployment of the combat system of 'controlling the land from the air,' which could include attacking an enemy's large and important targets in the air, on land and at sea. 'Though the integrated network-electronic battlefield is neither visible nor tangible, it does exist,' states PLA Major General He (2010). There is no definite boundary in this battlefield, and there is no division between the front and the rear line, or military and public use. Wherever network or electromagnetic equipment exists, there may be an integrated network electronic battlefield. In this battlefield, warfare takes place without the use of traditional weapons, but it can be extremely fierce, and the result of the warfare in an integrated network electronic battlefield has a decisive influence on other battlefields. Thus, apart from the network systems of the land, sea and air, China's cyber warfare is developed based on a four-dimensional battlefield, with outer space constituting the fourth dimension.

5.4 How cyberspace as a potential battleground is suited for People's War

According to the proposition of Section 4.3, the potential battleground of cyberspace is particularly suited for China's tradition of People's War. As a result, China develops its cyber warfare in the digital age through the adoption of this tradition. In addition, the concept of People's War can arguably be considered an inherent

[191] His view can be found in the interview 'Beyond armed forces services: who controls the digital battleground in the future?' given on 9th September 2010 via China Military Online, sponsored by the PLA Daily of the Chinese People's Liberation Army. (China Military, 2010)

'Chinese characteristic' due to its extensive reach in China's strategic culture. The following sections will empirically analyse this proposition in accordance with evidence given in interviews.

5.4.1 *People's War and the potential battleground of cyberspace*

As investigated in Section 3.3, the two primary aspects of People's War are: mobilisation of the masses to achieve a political goal and the defeat of superior adversaries by the militarily inferior. According to the interviews carried out in this study, cyber warfare is not only suited for the first aspect; is also very likely that cyber warfare represents the best chance for China to achieve the second aspect in the digital age.

1) Cyberspace facilitates the mobilisation of the masses

What's more, the role of people remains paramount in high-tech warfare. As ROC government researcher Chen (2010) indicates, in terms of weapons, not only should a 'trump weapon' be developed, but methods to employ modern equipment to defeat the enemy through asymmetric warfare should also be considered. Meanwhile, as any weapon would still be operated by humans, the leading role of people in modern warfare will not be changed by the application of high-tech weapons. People are still the creators of warfare resources. Since combat ability relating to the information system of command and control has become a fundamental element of war, the expertise of the people involved has become an extremely important factor; high-tech weapons can only be made full use of by high-tech experts.

One might thus argue that mobilisation need not be mass mobilisation, but instead 'targeted mobilisation.' In interview, Shen (2010) pointed out that, according to Mao's strategic thought 'you fight in your way and we fight in ours,' under the circumstances of informationisation, the core concept of asymmetric warfare involves making best use of advantages and bypassing disadvantages. Specifically speaking, one must fight the enemy at a favourable time, in a favourable place and with a favourable method. Therefore, influenced by the rapid development of modern technology, the CCP's concept of People's War has been modified from merely mass mobilisation and a 'human wave attack' (swarm effect) strategy to a 'targeted mobilisation', whereby more attention is paid to trained high-tech experts and intellectuals.

However, it can be argued that China's online nationalism discussed previously in Section 4.3.5 is likely to be manifested in two types: internal and external. The Deng Yujiao incident[192] of 10th May 2009 is an example of internal online nationalism. Discussion of this incident spread nationwide via cyberspace, and masses of cyber users decried the government, some even setting up websites to support Deng. Incidents such as these make the Chinese government truly aware of the concentrated power of virtual netizens.

An example of the external type of online nationalism is the response to an attack on a Chinese ship in the Mekong River in Southeast Asia on 5th October 2011, which resulted in the murder of 12 Chinese crew members.[193] This incident set in motion a wave of online nationalism as the news spread rapidly in cyberspace. Chinese netizens strongly urged the government to get involved in the international investigation of the incident. In addition, one online comment stated 'This incident may represent contempt and derision of China due to her weakness for a long time.' (BBC Chinese News, 2011) This shows that Chinese nationalism may have shifted to the medium of cyberspace, creating the phenomenon of online nationalism.

2) The defeat of superior adversaries by an inferior military:

ROC retired Rear Admiral Liu (2011) senses that the concern of the superior side in modern warfare is that: 'Information technology has produced a contradiction where the openness of information is a disadvantage whilst rapid information communication is an advantage.' This contradiction means that democratic countries might have a higher possibility of being attacked by cyber warfare. In fact, their reliance on information technology, as well as the existence of many IT weapons, is an existing dilemma that worries those world powers possessing the most advanced technology. Any state that overlooks such a predicament will very likely make itself defenceless in the initial stage of a battle no matter how powerful its military may be.

[192] This incident occurred on 10th May 2009 at a hotel located in Badong County, Hubei Province, China. Deng Yujiao, a 21-year-old female pedicure worker, tried to rebuff the advances of a local official, who had come to the hotel seeking sexual services. She allegedly stabbed her assailant several times trying to fight him off, resulting in his death. Badong County police subsequently arrested Deng Yujiao and charged her with homicide, refusing to grant bail.

[193] This incident has been discussed extensively by Chinese 'virtual netizens.' According to online discussions, even though this Chinese ship was suspected of smuggling illegal drugs, some commenters still strongly urged that the Chinese government use its growing power to forcibly intervene in the case. (BBC Chinese News, 2011)

Professor Lin echoes this point of view. In Lin's (2011) opinion, the increased openness of information systems offers invaders a better chance for success, which in turn threatens the security of confidential information, information transmission and information assurance. That is to say, since states have begun to focus on the possibility of 'controlling a war,' information systems, in particular those based on the internet, have revealed the vulnerability of cyberspace. Besides, even if measures in a war are adopted only by the military, the security of information transmission would still be very important in civil society for economic reasons. Any weapon or armed force has both strong and weak points. Asymmetric warfare focuses on making use of this dialectic, exploiting one's own advantages and targeting enemy troops' weak points through active attacks, potentially cyber attacks. In other words, cyberspace indeed offers asymmetric features facilitating the 'defeat of the superior by an inferior military'. This is due to the fact that in information warfare, the reliance of advanced countries on high-tech information weapons leads to deficiencies, which is advantageous to the inferior side as it can launch a fatal attack on the superior side. Under such circumstances, the superior side's weakness brings benefit to the inferior side.

Furthermore, China's cyber warfare is unique in its emphasis on 'soft kill' (non-physical destruction), which is characterised by the idea of an inferior military defeating a superior adversary through attacks on the enemy's information systems and computer systems in asymmetric warfare. According to ROC Lt. Colonel Chang (2010), this strategy is suitable for a military fighting a more powerful enemy. In fact, the concept of the militarily inferior defeating superior adversaries is often associated with 'computer-based weapons' (cruise missiles, ballistic missiles, information and communication systems, and advanced satellite operations). Though 'soft kill' sounds non-lethal, in reality, it also includes 'hard kill' (physical destruction) through the control of destructive weapons, such as cruise missiles, ballistic missiles, and nuclear weapons.

Interviewee ROC Army Colonel Liang (2010) questioned how deeply China's cyber army has penetrated into the military logistics system of the USA. Though probably no one knows the precise answer at the present time, the Economic and Security Review Commission of the USA Congress is

concerned that 'Globalised economics and the low price of Chinese computer products make it possible that more and more US military weapons would be made of raw materials or products from China.' In addition to the fear of a heavy reliance on Chinese products, the US military is concerned about the possibility of spy products. The Lenovo Incident in 2006, in which the USA suspected that computers from Lenovo, a significantly sized Chinese computer product company, might have been implanted with a Trojan horse virus which could be executed remotely without notice. The incident caused a heated debate between the USA and China. In Liang's view, this incident revealed the possibility that the tactical deployment of China's cyber warfare could potentially occur through the dissemination of computer products with viruses embedded into the hardware.

5.4.2 *Asymmetry: a corresponding feature of both cyberspace and People's War*

In the view of Army Colonel Yu (2010), one key feature of People's War is that resistance is everywhere. He points out that, though potentially on a small scale, resistance repeatedly takes place, making enemies feel that it is elusive and difficult to handle. People's War is naturally an idea of irregular warfare, which can be echoed through the methods of 'swarm effect' and 'sting effect' as examined in Section 3.2.1. This means People's War contains the feature of asymmetry. Colonel Yu (2010) takes the Chinese Civil War in the 1940s as an example: 'In many areas, the proximity between homes was far. Such circumstances are good for carrying out the idea of People's War because hiding, and using guerrilla tactics are easier.' According to the military principle 'concentration and dispersion of forces,' the regular army represents *concentration*, while the armed masses take on the form of *dispersion*. Complete destruction of the latter is consequently not an easy task. Initially in People's War, the area and scale of the armed masses was quite restricted. However, when faced with the potential excessive dispersion of forces, one might argue that the opposing army will not concentrate its own forces further to cope with the armed masses. In the case that the regular army disperses into small-scale, scattered forces as a response, the armed masses may have a chance of victory by making use of numerical superiority. Through such small triumphs, the morale may be

greatly boosted and this, in turn, may determine the final result of the war. Another respondent, Colonel Lu (2010), also of the ROC Army College, argues:

> *'People's War is a kind of irregular warfare but it is not all-powerful as there are limitations to its application. First of all, the militia and the armed masses cannot compete with the regular army in terms of organisation and equipment. Therefore, they cannot fight with the enemy's main force or a large force. They can only be used to destroy the enemy through damaging the transportation and the supply line in the periphery. But in cyberspace, this limitation does not exist.'*

In summary, People's War was originally suited for the battlefield in certain circumstances, but still remains ideal for the potential battlefield of cyberspace in the digital age.

Furthermore, in the Persian Gulf War of 1991, the US army not only controlled battlefield information and deployed its troops with ease by means of high-tech electronic equipment, but also prevented Iraqi forces from using electronic equipment. The Persian Gulf War was a high-tech war in which the US army gained absolute control and victory. The American army successfully won a big victory at a small cost in this war, and it later also used high-tech electronic equipment in the Kosovo War, the Afghan War and the 2003 Iraq War. However, according to observations by ROC retired Major General Chai (2010): 'Informationised weapons are not omnipotent, and sometimes, more high-tech weapons may be more vulnerable and more easily damaged.' This suggests that the more heavily an army relies on high-tech weapons, the easier it would be for the enemy to mount a countermeasure. As Major General Chai (2010) believes, this advantage of cyberspace has been grasped by the PRC to achieve 'the asymmetric strategy' of People's War through cyber warfare.

Meanwhile, ROC retired Navy Rear Admiral Liu (2011) points out that China covers a large geographical area, has a large population, rich information resources, and many IT talents, and also that the popularisation and development of the internet are continuing at a rapid pace. However, 'The military's reliance on the internet is very low, which is an advantage for the PRC military.' Networking in society, the government, and the army remains at a low technological level. Rear Admiral Liu explains 'Some core techniques in the information industry are

still at a low level. In particular, the updating of new concepts is very slow, which is a disadvantage.' The former advantage demonstrates that there is great room for potential in China's cyber warfare, whereas the disadvantage determines that cyber attacks and defences may not yet be very efficient, and could easily be controlled by opponents in the initial stage of a battle.

In addition, one might consider that, for many developing countries, cyber attack could also constitute an asymmetrical approach to a 'profitable' military action. As ROC Army Lt. Colonel Yang (2010) notes: 'In fact, cyber attack does not necessarily mean to cause network paralysis; it can also involve stealing or falsifying information through backdoor or Trojan-horse viruses. If information mistakes occur on several occasions, a user's trust in the whole information system would significantly decrease. Once any packages of important intelligence are intercepted, this would bring immense harm to a campaign.' To put it another way, as ROC Army Colonel Lu (2010) points out, 'Just as every coin has two sides, the US army's heavy reliance on high-tech weapons has both advantages and disadvantages. On the one hand, the information technology of cyberspace exerts a great and unprecedented effect on weapon systems; but on the other hand, any deficiencies of the IT would attract much attention and these might be the points where the enemy would attack.' In their development of cyber warfare, the PLA's strategists are thus focused on these pros and cons so as to maximise the potential effects of asymmetric strategy.

According to Huang (2010), the Chief of the ROC Computer Emergency Response Team (CERT), 'Nowadays, advanced countries are developing towards digitalisation, cyberisation, and informationisation. Once a war breaks out, cyber warfare would be different from traditional warfare in both form and connotation.' Huang indicates that in this hypothetical war, both sides would spare no efforts to attack the other side's information system, and this strategy, the purpose of which is to 'protect one's information superiority,' would play a leading role in future warfare. The USA's high reliance on information technology leads to serious deficiencies, and China's cyber warfare aims at making use of those deficiencies. In such warfare, electronic devices and computer equipment would be the main targets for China's cyber warfare.

Regarding the units engaged in this asymmetric warfare, according to investigations by ROC Army Colonel Liang (2010), the PRC's cyber army is

possibly distributed across the government, military and civil sectors. The cyber army's main tasks, assigned by the Ministry of Information Industry and the Ministry of Public Security[194], are focused on the security and defence of China's cyberspace. The PLA and the Chinese State Security Bureau are, however, ultimately responsible for conducting cyber attacks. This takes the form of the 'hidden and distributed way', which implies that attackers hide themselves secretly inside various organisations and departments without official unit titles. In addition, achieving the goal of the 'human wave attack'[195] strategy on the internet is a core value behind the establishment of China's cyber army, emphasising the launch of a new form of 'asymmetric warfare.'

Just as the computer and the internet were invented, so was the by-product of the computer virus. In ROC Army Lt. Colonel Wu's (2010) view, 'In cyber warfare, the participants fight with each other furiously in cyberspace, and often the computer virus would be a powerful weapon to attack the enemy.' Sending mêlée computer viruses into the opponent's 'cyberspace' could cause the enemy to lose control of information and undergo a failure in this potential battlefield. For example, the strategic plan and military actions of the USA's Network Centric Warfare, mentioned in Section 5.4.2, have enabled the US army to enhance the effectiveness of warfare and to reduce the time needed for information transmission. According to US military doctrine, under such circumstances, traditional weapons could also be used with more efficiency in urgent crises and in the nearest battlefield. However, such a system, in which every part is closely interconnected, has a higher possibility of suffering virus and cyber attack. In fact, because of such military deficiencies, even the USA, the world's superpower, considers hacking attacks arising from all over the globe to be highly problematic; there can be no total insurance against such attacks. As a result, the potentially

[194] As Colonel Liang (2010) also observes, in March 2003, the Information Regiment of the PLA General Staff Department stated that an Information Mobilisation Office should be set up under the National Defence Mobilisation Committee. Its main job would be information mobilisation, which would play a role in the protection of national security in the digital era. This demonstrates that the PRC is actively building up a cyber army. In addition, to ensure the combat effectives of the cyber army, the National Security Mobilisation Committee is involved in synchronising manpower and material resources, liaising between the military and the government, and coordinating between warfare and the economy. To date, the PRC possesses a substantial militia which could carry out cyber warfare as investigated in section 4.3.3.

[195] This term refers to an offensive infantry tactic, in which an attacker conducts an unprotected frontal assault with densely concentrated infantry formations against the enemy line, intended to overrun the defenders by engaging in mêlée combat. There must be a massive amount of soldiers or people to make up this 'wave.'

fatal vulnerability caused by advanced countries' heavy reliance on information technology lays the theoretical basis for the PRC to develop cyber warfare, allowing an inferior military to defeat superior adversaries, in accordance with the asymmetric concept featured in People's War.

5.4.3 *Mass mobilisation to convert China's cyber warfare into total warfare*

China's cyber warfare could arguably be converted into a total warfare once the People's War strategy of mobilising the massive populace is applied.

In ROC Air Force Colonel Yao's (2010) view, local wars under modern high-tech conditions cover various fields, just like a 'total war', even though the war is 'local' in name. Colonel Yao believes that China's cyber warfare has never been restricted to competition in just the military field. Instead, the competition is actually spread amongst the fields of politics, the economy, culture, and diplomacy, consituting a form of total warfare. The content of the warfare thus extends with the development of society. In addition, the information age can be regarded as an age of total warfare; Colonel Yao claims that 'In such total warfare, there is no difference between peacetime and wartime'. Thus, cyber warfare can be total warfare, which may be developed and conducted in both peacetime and wartime. Cyber warfare means far more than just armed struggle.

As Feng (2010) also argues, cyber warfare could threaten the infrastructure of a state, society or even an international region. Thus, the strategic planning of the warfare has to include 'not only preparation for waging the warfare, but also for ending the warfare and reconstructing the peace.'

China's cyber warfare would inevitably become total warfare with the application of People's War. According to ROC retired Major General Chai (2010), not only does warfare pose a threat to a country's territorial land, sea and air, but in addition, other forms of warfare, such as psychological warfare, information warfare, and electronic warfare, could also be carried out in cyberspace. Cyber warfare is therefore likely to change the traditional concept of the 'front line' and 'rear line' and would indeed become a total warfare once the idea of People's War is applied. Total warfare would involve Joint Operations amongst different armed services; China's cyber warfare certainly involves cooperation between all kinds of armed forces and even non-armed forces, potentially creating a form of total warfare in cyberspace.

5.4.4 *The tactics of China's cyber warfare*

This section will illustrate that tactics of Chinese cyber warfare, in which civilian hackers and computer viruses are deployed, may be presented through a set of existing patterns.

According to ROC Air Force Colonel Huang (2011), in order to Win Local Wars under High-tech Conditions, which is the latest guideline of China's national defence in the modern era, the PRC is enthusiastically developing the military doctrine of cyber warfare, which may also be associated with the concept of Integrated Network Electronic Warfare. Colonel Huang also points out that 'The University of National Defence Technology in Beijing is playing a leading role in the research on military theory and practice of China's cyber warfare.' (Huang, 2011)

Air Force Lt. Colonel Hao's (2010) experience of working in the field of operational command reveals that any military action would be based on an operational 'directive/instruction' and 'This directive/instruction would form the basis of military manoeuvres and would become the code of conduct in future warfare.' Therefore, it is likely that 'Even if official instructions for the PRC's cyber warfare do not exist, there must be a handbook or some materials.' However, 'We do not know whether the PRC would disclose such information as the US army has done. Even the doctrines of the ROC's armed forces are classified as restricted reading.'

However, Colonel Liu (2010) states: 'I do not think the development of China's cyber warfare is "sophisticated" enough to have a set of directives or instructions, but I believe that it has a "set of patterns" instead.' He also stresses that 'We can learn from China's doctrine of Joint Operations, modelled on the US army's doctrine of Joint Operations, that the five core capabilities in China's Joint Operations are electronic warfare, cyber warfare, psychological warfare, operational security, and military deception.' According to Colonel Liu, the CCP regards cyber warfare and electronic warfare as the main forms of warfare to achieve the latter three core capabilities.

Though the official instructions of China's cyber warfare remain uncertain, in this study's interview, ROC Air Force Colonel Huang (2011) further illustrated that research into China's cyber warfare carried out by the University of National Defence Technology in Beijing contains three major tactical elements which

could constitute a 'set of patterns': 'cyber attack', 'prevention and control of hackers', and 'virus attack.' The approaches for each element are laid out as follows:

1) Cyber attack:

When it comes to cyber attack, the main goal of the PRC is to paralyse the enemy's C4IS system through the methods of network overload, release of viruses, and stopping the nodes. The PRC's research reveals 'Five Ways to Defeat the Enemy in Cyberspace' (power failure, precise attacks, network overload, release of viruses and hackers' penetration) and 'Methods for Cyberspace Confrontation' (cyber snooping, stopping the nodes, cyber interception[196], cyber attack and paralysing the internet). This demonstrates that the PRC has a clear plan regarding methods to use in the case of cyber warfare.

2) Prevention and control of hackers:

In terms of anti-hacker methods, isolation of entities[197], safety protection and deceiving the enemy are central. In addition, having examined hackers' methods of attack in other countries, the PRC has come up with an anti-hacker doctrine, the main seven methods of which are transformation and isolation; distinguishing between the real and the fake; flexible organisation; information leakage prevention; ambush and circumvention; deceiving the enemy; and disturbing and destroying.

3) Virus attack:

The doctrine of the PRC's virus attack puts an emphasis on pre-planting the enemy's computer system with viruses and manipulating the time of initiating the viruses. This is mainly achieved through paralysing the network system with destructive viruses that can be replicated and distributed. The main four methods include 'feed-forward latency', 'indirect attack', 'planting the viruses through the interface', and 'sniffing attacks'.

[196] The action of intercepting information on the internet.

[197] This refers to the action of isolating hardware, including cutting off power supply, disconnecting the internet, and removing the connection between computers.

Thus, in terms of combining attack and defence, cyber offence mainly takes the form of electronic warfare, cyber warfare, psychological warfare, military deception and destroying entities. These forms can stop, disturb, weaken, make use of, deceive and destroy the enemy's critical information system; vice versa, cyber defence refers to a variety of actions to protect one's own critical information infrastructure from damage.

In addition, as ROC Army Colonel Hsieh (2010) points out in his interview, 'The doctrine of China's cyber warfare combines 'specific professionals' and 'common professionals' into an integrated force.' The former refers to PLA soldiers working in the units of cyber warfare and military weapons, including electronic warfare troops and weapons with high precision, such as laser, nuclear power, or magnetic pulsation. The latter refers to professionals of the civil sector who could pose a threat to important systems of the enemy.

According to ROC researcher Chen (2010), the patterns of China's cyber warfare include 'cyber attack, cyber defence, and cyber spying.' Regardless of whether the PRC holds any specific instructions regarding cyber warfare, the PLA has considered it the key to gaining the war initiative and ensuring 'electromagnetic dominance' in the initial stages of a war. It is also seen as an effective weapon in the destruction of entities and the fight against the enemy's C4IS to damage information systems on the battlefield. The PLA has therefore raised the importance of cyber warfare in military manoeuvres. Early training was centred on improving the army's defence capabilities, but now recent military manoeuvres have introduced offensive operations, expected to be the major method of attacking an enemy's network.

In addition, the PRC believes that the optimum time to take advantage of the enemy's (especially the US army's) weakness in war is during its operational deployment. The US relies heavily on computer and communication systems, in both the military and non-military fields. Its logistical network is the weakest, and most vulnerable to attack. Although penetrating the command post and information links may achieve a larger-scale outcome, penetrating the logistical network seems to have a better chance of success. The primary task of the PRC's cyber warfare seems to be preventing the US army's operational deployment as soon as possible and then cutting the connection link between the decision makers and the combat vehicle and combat system phases. This method perfectly reflects

the PRC's traditional emphasis on staying clear of the enemy's main force and attacking vulnerable spots. As ROC retired Major General Chai (2010) sums up in three points, the main reasons for China to develop cyber warfare are therefore:

1. Cyber warfare has become the most effective way to win even if one's side is weaker and outnumbered.
2. Cyber warfare could be used to deter the enemy.
3. Cyber warfare has a longer attack range than other warfare where the army possesses long-range control and precise, strong and long-range attack capability.

5.4.5 *Summary*

In summary, the concept of People's War was originally considered a military thought suited to the traditional battlefields of Mainland China, involving mobilisation of the massive populace in order for the inferior CCP forces to defeat a superior adversary. However, in the past few decades, this tradition of People's War has not merely been useful for developing military strategy, but has also been applicable to many other national developments, such as economics, social modernisation, and government and public affairs, as a vital 'behind-the-scenes' guideline to garner a certain consensus from the Chinese people in order to carry out the policies that the Chinese government wishes to accomplish. In particular, this tradition can be perfectly applied to China's cyber warfare in the digital age, as the strategic value of cyberspace has removed the restriction of traditional geographic barriers and borders between states. Thus the potential masses of Chinese 'cyber warriors' can carry out attacks geographically unhindered in cyberspace.

In addition, regarding whether such warfare can successfully accomplish its political purpose, the quality of soldiers, for example in terms of professionalism and loyalty, is a vital element to consider. Due to a lack of regular discipline, civilians are unlikely to follow commands and orders as the regular armed forces would, even if they are very professional. A potential concern for the Chinese government is thus whether or not the masses of civilians might in fact carry out cyber warfare against the government whilst simultaneously conducting attacks against the state's external adversaries. In general, it is an inevitable, though rare, possibility that states' own military may choose to conduct revolution

against their government. In comparison, the masses of cyber warriors adopted by the application of the strategy of People's War to China's cyber warfare could prove even more problematic. The details of this issue will be further examined via analysis of the relevant interviews and document-based evidence in the following section 5.6.

5.5 How China disciplines 'cyber warriors' whilst adopting People's War

According to the propositions of Section 4.3, China's cyber warfare is a strategic warfare that adopts the principle of People's War. In so doing, internet control and monitoring are also likely to become a crucial element of China's cyber warfare in order to control and command civilians into disciplined cyber warriors for military purposes.

As set out in the analytical framework, the concept of People's War can primarily be defined as the strategy of mobilising the populace to achieve a strategic aim, whilst also allowing an inferior military to defeat a superior opponent. Furthermore, as examined in Section 3.2, China is in fact still likely to insist on the legitimate heritage of People's War. Historically, People's War, a term coined by Mao Zedong (Mao Tze-Tung) in 1927, would be conducted on geographic battlefields located in Mainland China. The Chinese Communist Party (CCP) employed the strategy of People's War to drive the massive populace, mainly comprising the Chinese proletariat, into wearing down the CCP's militarily superior opponent, to ultimately gain victory during the Chinese Civil War in the first half of the 20th century. Subsequently, since the founding of the PRC in 1949, People's War became and has remained a key guideline for China, not only in terms of military strategy but also for national development. The concept of People's War incorporates the ideas of active defence, asymmetric warfare, protracted warfare, and guerrilla warfare[198]; thus, those with inferior military capability are able to deter and even defeat those superior to them. When the PRC's opponent, the Republic of China (ROC), governed by the Chinese Nationalist Party, retreated across the Taiwan Strait during the civil war, the CCP was forced to accept that People's War was actually restricted by conditions of geographical territory.

[198] Please refer to Section 3.2.1

The three stages[199] of Chinese strategic guidelines in recent decades were identified in Sections 4.3.1 and 4.3.2 the most recent of which is guiding the development of China's cyber warfare in the digital age. People's War has remained a constant core principle of modern Chinese strategy throughout these three stages. This section will touch upon this empirically through evidential points of view emerging from interviews concerning ideas of civilian-based defence, the Chinese militia, and Chinese ideological education.

Therefore, this section will firstly summarise how China's cyber warfare effectively channels the principle of People's War into a strategic level warfare. Secondly, it will be argue that China's internet control and monitoring are actually an element of China's cyber warfare. This will be approached through an examination of China's censorship of Google, which is not solely to prevent politically sensitive information from reaching the Chinese internet populace, but also to gather critical information in a tactical approach of cyber warfare. Thirdly, the investigation of certain ideas, such as China's nationalism, ideological/patriotic education, and all-out defence, will illustrate how China can manage to discipline masses of internet users to facilitate 'control and command' of civilian 'cyber warriors' as military sentinels in the virtual world of cyberspace.

5.5.1 *Military significance: supporting China's cyber warfare*

ROC Navy Captain Chang (2011) explains that 'The idea of a chain of military-political relevance is a critical guideline for waging wars.' In his view, each war or warfare must have 'military significance' in order to achieve political influence. In other words, coherence amongst warfare, military significance and political influence must exist in order to measure and control the scale of damage caused by a war. This coherence can help keep a war organised and may provide political purposes for legitimate violence. Otherwise, warfare may be overused, creating unnecessary damage or even causing conflicts between states in world politics.[200] In Captain Chang's (2011) view, this concept is highly relevant for China's cyber warfare. As examined in Section 4.3.5, China's cyber warfare strategically aims to

[199] The three stages are:
1927-1977: People's War
1978-1991: People's War under Modern Conditions
1992-present: Local Wars under Hi-Tech Conditions
Further details can be found in Section 3.2

[200] For example, the use of bio-weapons in warfare may spiral out of control, ultimately causing unexpected damage which may far exceed its original political purpose.

mobilise a massive amount of people which may easily give rise to situations outside of the authorities' control. Thus, a hypothetical question to China's cyber warfare is how precisely to discipline cyber warriors in order to prevent this warfare from being overused as Chang explains. In other words, the tactics of China's cyber warfare may include internet control and monitoring in order to securely measure the extent of its military significance.

Further to this, there is another aspect which may justify the military significance of China's cyber warfare. From the view of ROC retired Lieutenant General Deng (2011), in a traditional sense the CCP would still believe that the 'justice of a war' is a determinant of modern warfare. Therefore, the concept of justice in People's War and the inclination for a just war still remain a necessary prerequisite for China's cyber warfare, further facilitating the mobilisation of the people. The victory of People's War may rely on converting political advantage into military advantage, and vice versa, which can be leveraged against enemies to gain pre-emptive control in a war and earn the final victory.

However, aside from the military significance of justifying China's cyber warfare, one might ask what the PRC's motivation of controlling its domestic internet could actually be. As ROC Major General Chai (2010) indicates, in China, the concept of 'national defence' can be 'elastic.' This means that many varied issues can be classified under the umbrella of national defence to provide the Chinese government with necessary military significance and subsequent justification of any actions to the Chinese populace. For example, in late 2010 WikiLeaks revealed correspondence of the American embassy in China, which, if true, demonstrates that one of the tasks of China's national defence is to seize global data in cyberspace. WikiLeaks, though the only source in this case, claims that it was officially informed that the order for Chinese hackers to attack the Google search engine was authorised by the Chinese political leadership. In addition, it may be that China has surpassed the USA by now possessing the world's fastest computer; Chinese super computers are extremely powerful and able to decode and process any data collected. (Chai, 2010) According to Major General Chai's experiences, reliable evidence shows that a large amount of very sensitive information was directed from American computer servers to servers in China's territory. She reports that on 8th April 2010, it was revealed that the state-owned company China Telecom re-routed the emails of the website of the US

Senate, the Department of Defense (DoD), and other government units to Chinese filter servers for 18 minutes. That is more than enough time for a super computer to filter incredible amounts of data. This illustrates that a potential approach of China cyber warfare is the seizure of valuable information by hacking database servers and global websites such as the Google search engine.

5.5.2 *Ideological education: driving those conducting China's cyber warfare*

ROC retired Major General Chai (2010) states, 'Whether it is seen as negative or positive, China's nationalism is the most impressive in the world due to China's huge populace and the ideological/patriotic education delivered through various systems.' As ROC Colonel Yu (2010) suggests, two questions should be raised when exploring the factors driving People's War in the modern Chinese era. The first is how the PRC can mobilise the Chinese people to develop China's cyber warfare in order to defeat or oppose external enemies. The second is how, in the meantime, the government can discipline the huge amount of internal internet users into becoming 'cyber warriors', in order to guarantee that cyber warfare adopting People's War is under control and consistent with its initial political purpose. Colonel Yu (2010) argues that in determining a common answer to these two questions, certain measures employed by the PRC, such as 'patriotic education,' 'ideological cultivation,' 'internet control and monitoring' should be taken into account.

Moreover, as Navy Captain Lin (2010), a senior instructor in the ROC Navy College, argues, 'in the process of Chinese economic reform, on the one hand, China is enjoying the fruits of Western capitalism; but on the other hand, China is unable to eliminate the nationalism caused by humiliation from Western imperialists in the past century, which still viciously resists anything Western.' As a result, as one of the fundamental ideas of People's War is to mobilise the populace to resist Western imperialism, it is possible to harness this nationalism to drive the people to support not only the government revolution of the Chinese Civil War but also a resistance of the entire Chinese nation; to turn from a solely geographical campaign to an all-out battle, including not only military aspects, but also political, economic, and cultural struggles.

In addition, according to Air Force Colonel Liu's (2010) view, People's War could be also driven by the 'Chinese national character,'[201] which can be regarded as one of the major reasons behind the long persistence of the concept of People's War. As Liu (2010) states, 'the century of humiliation' and 'a long period of poverty and weakness' oppressed the Chinese in the past, and this oppression became a feature of the national character. Therefore, despite the fact that the PRC claims to be rising peacefully, the Chinese national character determines that China will inevitably compete tooth and nail with the USA's hegemony, in order to symbolically wipe out past humiliations. Meanwhile, the feeling of oppression displayed in the Chinese national character makes it easier to incite the Chinese to a large-scale attack in boundless cyberspace.

According to this study's interviews, three points of view can be summarised:

1. Firstly, as the century of humiliation has become an unforgettable part of history for the Chinese people, this collective memory is one of the best tools to cement nationalism. The mobilisation on which the PRC's People's War places emphasis is driven by enthusiasm for this nationalism. It can therefore be argued that the century of humiliation is one of the motivations behind the launch and development of People's War.
2. Secondly, based on the theory of People's War, the anti-government movements during the late Qing Dynasty and the ten revolutions led by Dr Sun Yat-sen, the founding father of the Republic of China, are categorised into armed uprisings in the early stages of People's War. At the time, the armed masses fought alone without cooperating with the regular army, and it was this lack of armed forces that led to their failure. This proves that an essential element of People's War is the combination of both the regular army and the mobilisation of the people.

[201] The concept of the Chinese national character (中國民族性, *zhongguo minzu xing*) consists of various aspects. (Zheng, 2009) However, it basically refers to the general characteristics of the various Chinese peoples, significantly influenced by Confucianism and Taoism. In Colonel Liu's (2010) view, according to a definition by China's national father Sun Yat-Sen, the Chinese national character contains a particular mental tension, which is that, on the one hand, the character of the Chinese people tends to be negative and lacks the spirit of positive resistance to overcome Western invasion, but on the other hand, it contains a deep-rooted ideology of empire and ancient civilisation. This means that the Chinese want to surpass other countries, not least in making up for the century of humiliation.

3. Thirdly, the CCP's establishment of political power started from zero. The CCP has a ninety-year history, stretching from 1921 to today (2011).[202] During the CCP's growth, People's War has always been the most fundamental guiding principle for the PRC in terms of military affairs and the form of warfare. In Lin's view (2010), the formation of People's War was not based on the theories that already existed at the time, but instead was formed gradually alongside the development of warfare.

In fact, evidence suggests that in 2010, the Chinese State Council officially proclaimed the guideline of patriotic education, which should be assimilated into university curricula in order to progressively 'educate' the students' ideology. This 'patriotic education,' also known in China as ideological education (*思想教育 sixiang jiaoyu*), is a compulsory element in China's education system used to formulate a unique political ideology. It is distinct from general citizenship education, and is not merely for military soldiers, but also for civilians, in accordance with the tenet of People's War. The structure of the Central Committee of the CCP and the State Council's 2010 guidelines on further strengthening and improving students' ideological education can be summarised as follows: (People's Daily, 2010)

1. *An important and urgent strategic task is strengthening and improving students' ideological education.*
2. *Outline of guiding thoughts and basic principles for strengthening and improving students' ideological education.*
3. *Explanation of the mission of strengthening and improving students' ideological education.*
4. *Maximise the guidance effect of lecture-style teaching in students' ideological education.*
5. *Develop effective new methods of ideological education for university students.*
6. *Expand the important role of party groups and organisations in ideological education.*
7. *Build up teaching staff teams for ideological education of university students.*
8. *Create a beneficial social environment for the ideological education of university students.*
9. *Strengthen the guidance of ideological education and its teaching practices.*

[202] 1st July 2011 marks the Chinese Communist Party's 90th Anniversary. The CCP is aiming to consolidating its rule by celebrating Mao's legacy.

The following key notes of the government announcement may further elaborate the context of the guideline of patriotic education: (Chinese State Council, 2010)

> *'Ardently love the Party, the motherland and socialism; resolutely advocate the Party's policies; strongly recognise Deng Xiaoping Theory and the "Three Represents"; fully trust the Party Central Committee with Comrade Hu Jintao as Secretary General; have full confidence in resolutely following the path of socialism with Chinese characteristics and achieving the grand ambition of comprehensively building a prosperous society.'*
>
> *'Persist in using Marxism-Leninism, Mao Zedong Thought, Deng Xiaoping Theory and the "Three Represents" as guidance; thoroughly implement the Party spirit of the 16th National Congress of the Communist Party of China [16th NCCPC] and comprehensively put the Party's education policy into effect… with patriotic education as the main focus.'*
>
> *'Persistently use Marxism-Leninism, Mao Zedong Thought, Deng Xiaoping Theory and the "Three Represents" to equip the minds of students; thoroughly develop education of the Party's basic theory, basic line, basic programme and basic experience; develop historical education of the Chinese revolution, construction and the "opening up and reform" policy... Establish the path of socialism with Chinese characteristics led by the Communist Party of China and achieve the common ideal and firm convictions of the rejuvenation of the Chinese nation.'*

In other words, this guideline also focuses on the reflection of the latest achievements of contemporary Marxism. The document demonstrates the aims of comprehensively strengthening the development of the disciplines of the ideological course, its curriculum, teaching materials and teachers and further incorporating Deng Xiaoping Theory and the 'Three Represents' into teaching materials and lectures, and therefore students' minds. The document also suggests integrating the ideas of Deng's 'opening up' policy reform and the realities of socialist modernisation into students' thinking; assimilating knowledge transfer

into ideological education; combining systematic teaching practice with thematic teaching practice; and closely combining theoretical knowledge transfer with teaching practices. Based on all of these measures, it can be argued that the ideology of Chinese people undergoes political cultivation through such measures of patriotic education, which may indoctrinate students into unequivocally supporting the government. The Chinese government can therefore implement People's War strategy of mobilising the populace to achieve a political purpose, in particular concerning national issues opposing Western imperialism.This also applies to China's cyber warfare.

5.5.3 *All-out defence: an ideal tenet for the 'active defence' of People's War*

In addition to ideological education, in order to encourage the huge Chinese populace to espouse the necessity of mobilisation for a certain purpose, 'all-out defence' is likely to be an ideal tenet to indoctrinate the people.

As Ding (2010), an interviewee in the civil sector, points out, 'If we explore the origin of People's War, we can see that it actually originated from the concept of "all-out defence"[203], a concept introduced into China thousands of years ago.' According to his investigations, in ancient China, kings would make use of the slack season in farming to train farmers in battlefield skills. For example, the 'well-field system'[204] of the Zhou Dynasty was invented based on the concept of ensuring a military reserve among the peasants; in the Spring and Autumn and the Warring States Periods, Guan Zhong invented the 'Shi Wu System'[205]; in the Song Dynasty, Wang Anshi created the 'Baojia System'[206] which is the predecessor of the militia system; the Ming Dynasty and the following dynasties all spent a huge amount of money on mobilising the masses to build the Great Wall to resist foreign aggression; also in the Ming Dynasty, Wang

[203] In fact, there is a similar concept in Western thinking. The American sociologist Gene Sharp advocated the concept of 'Civilian-based Defence' in the 1990s, which concentrates on deterring the enemy and protecting oneself. In the current Revolution of Military Affairs, the US army has come up with the concept of 'Shock and Awe: Achieving Rapid Dominance' which aims at destroying the enemy's morale and giving the enemy no choice but to act according to one's own strategy.

[204] This was a system in which a square area of land was divided into nine identically-sized sections; the eight outer sections were privately cultivated by serfs and the centre section was communally cultivated on behalf of the landowning aristocrat. In this system, the peasants also practised some defence skills and would be organised based on this land system if war broke out.

[205] This was a system that prevented the flow of people.

[206] This was a community-based system of law enforcement and civil control.

Yangming suppressed the Revolt of Zhu Chenhao[207]; the 'Tun Bing System'[208] was practiced in the Kingdom of Tungning; and in the Qing Dynasty, the Xiang Army and the Huai Army were made up of village militia forces. All of these ancient Chinese examples laid a historical foundation for the development of the concept of a military reserve among the masses of peasants in China.

Consequently, the PRC believes that the best way to achieve the goal of 'all-out defence' is through giving all citizens an education in national defence, which is a special educational activity aimed at resisting foreign invasion, preventing armed subversion, and protecting the country's sovereignty, unity, territorial integrity and security. The PRC emphasises that national defence is indispensible for the survival and the development of China, since the century of humiliation must be washed away. In other words, this 'all-out defence' is a military action to prevent foreign invasion and subversion. Furthermore, the national defence aims to protect the sovereignty, territorial integrity, national security, unity and development of China through military or military-related actions in the field of politics, the economy, science, culture, education and diplomacy.

In addition, according to China's 'Outline of All-Out Defence Education,' in order to carry out this education thoroughly, the PRC asks organisations at all levels to meet the following requirements. Firstly, they must organise extensive study and publicity to raise awareness of the importance of all-out defence in civil society; secondly, they must work out a plan to improve all-out defence education in practice; thirdly, they must take any measures possible to achieve the success of all-out defence education. The dogma of this all-out defence education is:

> *'Firstly, all-out defence education is an effective way to protect the country's safety; secondly, all-out defence education satisfies the needs of perceived security and defence; thirdly, people should pay attention to the PRC's action of legalising all-out defence education; fourthly, this education deepens the influence of freedom, democracy and human rights; and fifthly, carrying out the "Outline of All-out Defence Education" instils an imperceptible influence in citizens.'*

[207] Zhu Chenhao was a warlord leading a local revolt against the Ming dynasty. Wang Yangming, a Neo-Confucian philosophical strategist, deployed very few regular troops but also mobilised local peasants to suppress the revolt. This was one of Wang's historical significant achievements.

[208] This was a system in which soldiers served both in the army and in agriculture.

In other words, the concept of 'all-out defence' is likely to be a form of total mobilisation. Once a supportive consensus is achieved between the Chinese government and the masses, it would be easier to mobilise them into devotion to China's cyber warfare with a certain degree of discipline. This mobilisation may also include political, economic and ideological mobilisation as a form of 'total mobilisation' in direct accordance with the idea of 'all-out defence.' This also echoes Mao Zedong's thinking: 'What is political mobilisation? First of all, you should tell the political purpose of warfare to soldiers and people. Then, you should elaborate on how to achieve that political purpose. In other words, you should tell them the procedures and the policies that would be adopted. After that, one mobilisation is not enough; political mobilisation should be frequently launched because it determines the victory of warfare.'

5.5.4 *Chinese militia: implementing the concept 'everyone is a solider'*

Apart from this all-out defence education, there is another practical application of People's War: the Chinese militia. According to ROC retired Major General Chai's (2010) observations, there are three major forces in China: the People's Liberation Army, which is the regular armed forces, the People's Armed Police,[209] and the Chinese militia, the scale of which is larger than the two former forces. Major General Chai also indicates the number of militia involved in Chinese cyber warfare as about '300 to 400 thousand, making up the main force developing China's cyber warfare.'

In the view of ROC Army Colonel Chen (2010):

> *The Chinese militia was first set up during the First Chinese Revolutionary Civil War. During that period, it was believed that the militia made a great contribution to liberating the nation, driving off the Japanese invaders and establishing the People's Republic of China. The militia is therefore the country's military reserves.*

According to the Chinese government document 'Rules and Regulations of the Militia,' the task of militia work is to 'Organise the militia for war, supply the front, resist invasion and protect the country.' The emergency detachment is already on the track to normalisation, achieving 'weapons modernisation' and

[209] The People's Armed Police (PAP) is officially called Chinese People's Armed Police Force (PAPF), which is different to the public security People's Police.

'communications modernisation,' becoming a 'well-qualified,' 'quickly-mobilised' and 'strong force.' Meanwhile, the construction of the technical detachment has taken off. Currently, there are around 'ten thousand militia units' in China. They play an active role in production, construction, disaster relief work and military activities.

Interviewee ROC Navy Captain Lin (2010) describes from his experiences of the Chinese militia how it works in practice:

> *'In principle, the training for militia cadres and primary militia is organised by the county's (or the city's, or the district's) Department of People's Armed Forces. According to the training programme, training time for cadres is 30 days, which is normally finished within the space of one year; training time for primary militiamen is 15 days, which should all be finished in one go. Through training, the cadres acquire certain military skills and the skills of organising and commanding. They should also improve the capability of carrying out their own work. The primary militiamen are expected to know how to use military weapons, grasp basic military skills and be able to fulfil some general combat missions. Militia cadres mainly receive training on instructional methods and commanding at their own level, while the primary militia mainly receives technical and basic tactical training.'* [210]

For example, on December 25th 2010, Xu Qiliang, the PLA Chief of the Air Force, and political commissar Deng Changyou, issued an order to publish 'The Rules and Regulations for the Air Force Militia,' which has since been enforced from January 1st 2011 onwards. (People's Daily, 2010) The publication of this document indicates that the building of the air force militia has entered a stage of systemisation and standardisation. In order to respond to new conditions and new tasks, and to improve the Air Force militia detachments' capability of

[210] The period of training for professional technical militiamen is based on actual needs. Many county-level militia military training bases have been established, where militiamen can receive intensive training. Based on necessity, myriad professional technical training centres have also been set up. These bases and centres can provide trainees with catering, accommodation and training venues. In terms of the training methods, electrical audio-visual instruction and simulation training are being actively promoted. As this kind of training is vivid and visual, the quality of the training has been dramatically improved. In sum, the training for militia cadres, emergency detachments and technical detachments has been improved.

rapid mobilisation and execution of tasks, the Air Force drew up the 'The Rules and Regulations for the Air Force Militia' in accordance with relevant laws and regulations and the realities of the Air Force militia.

'The Rules and Regulations for the Air Force Militia' [211] clearly outlines the Air Force militia's role, guidelines and basic tasks. It also systematically defines the mission of different governing units, improves the Air Force militia system, and stipulates the categories of Air Force militia detachments, organisational system of the militia and resource allocation for different armed groups. Additionally, it also states the content, procedure and requirements for army building during peacetime and mobilisation during wartime. Hence, the regulations are one of the military documents standardising and providing guidelines for the building of the air force militia, serving as the basis for authorities and army units at all levels to carry out militia work.

In fact, a recent interview[212] reveals that the Chinese military mobilises civilians into cyber militiamen. As Bai (2011) points out, since 2005 his company Nanhao Group has been home to a cyber militia unit organised by the PLA. He further claims that 'All staff under the age of 30 belong to the unit.' According to the interview, the tasks of the unit are mainly cyber attack and cyber defence. This could mean that even some of China's best-known technology companies could embed cyber militia as part of a cyber warfare unit.

Aside from the militia, the ROC government researcher Gu (2010) reinforces that two of the most important points in the argument of People's War are 'mobilising the masses' and 'an inferior military defeating a superior enemy.' He indicates that, with regards the former, Lin Biao, the former intended successor of Mao Zedong, once said, 'There is no special secret strategy, but most important of all is to mobilise the masses, depend on the masses, bring the entire nation to arms and launch People's War.' In Gu's (2010) view, this practice of People's War originates from peasants' armed uprisings in the history of China. He explains Mao cultivated his military thought to form the concept of People's

[211] 'The Rules and Regulations for the Air Force Militia' consists of 10 chapters with 101 items, which include general rules, responsibilities, regulations, political work, organisation construction, military training, logistical service, armament-related work, mobilisation and supplementary articles. It covers every aspect of the militia work, offers a clear-cut job responsibility, enables the procedure of work to be detailed, and clearly defines the time requirement. (China Org, 2011)

[212] Bai Guoliang, the vice president of the ordinary civilian technology company Nanhao Group, was interviewed by Kathrin Hille, a reporter for the *Financial Times*. Mr Bai confirmed that the cyber militia unit was led by the local PLA command and has 'regular exchanges.' (Bai, 2011)

War through reading many historical collections[213] outlining such ancient incidents. This interview reinforces the historical origins of both the Chinese militia and of People's War, mirroring the importance of historical factors outlined throughout Chapter Three.

5.5.5 *Internet control and monitoring: China's censorship of Google*

Aside from the interview analysis carried out in this research, the dispute between China and the USA caused by China's censorship of Google, a significant recent case, can be seen as empirical evidence of how China carries out cyber warfare in practice. The internet giant Google announced on 22nd March 2010 that it had transferred the information retrieval service of its search engine servers from Mainland China to Hong Kong, and would begin re-routing search queries to its Hong Kong-based site.[214] The crisis began on 12th January in the same year when Google claimed that its users were frequently attacked by Chinese hackers, and Google asked the Chinese government to stop the censorship of search results. After that, the Chinese government, Google and the US government carried out negotiations and by 22nd March, the situation seemed to be considerably more stable. However, on 19th April 2010, the *New York Times* reported that in January 2009 hackers located in Mainland China had stolen information from Google's servers, and that the losses included one of 'Google's crown jewels', a password system controlling access to millions of internet users worldwide. However, Google refused to comment on the news at that time and instead simply reiterated that hackers did not succeed in stealing any Gmail accounts. Following Google's claims of 12th January, on 21st January Secretary of State Hillary Clinton urged China to conduct a 'transparent' inquiry into the attack. She also called for an uncensored and free flow of information, saying that American companies consider internet use to be a very important aspect of business. This suggested that the censorship was influencing American companies' interests in China. Clinton

[213] Mao's favourite history books included '*Er Shi Si Shi*' [*二十四史*], '*Zi Zhi Tong Jian*' [*資治通鑑*], and '*Gang Jian Yi Zhi Lu*' [*剛鑑易知錄*], which elaborate on various revolutions and dynasties in ancient Chinese periods. He also showed great interest in unofficial histories, such as '*Zhong Guo Li Dai Tong Su Yan Yi*' [*中國歷代通俗演義*], '*Dong Zhou Lie Guo Zhi*' [*東周列國誌*], '*San Guo Yan Yi*' [*三國演義*], and '*Shui Hu Zhuan*' [*水滸傳*]. These books are ancient Chinese folk novels which discuss how some historical heroes led the masses of oppressed peasants to oppose the empires in different Chinese dynasties.

[214] For the details of this Google incident, please refer to the news reports examined in Section 5.6.5.

also appealed to other networking companies in China for a rejection of any censorship.

From another perspective, however, Google may simply be seeking dominance of cyberspace. Through investigation of technology marketing news, it can be seen that Google's dominance may also be noted in the telecommunication systems of mobile phones and the Operating Systems (OS) of personal computers. In 2008, Google released Android, a mobile application, and announced that it would open Android's platform. For other telecommunication companies, this posed a threat to their own markets. In 2010, Google released Chrome OS which broke Microsoft's monopoly of OS. For customers and computer producers, this simply means one more option to choose from, but for Google, this presents the possibility of becoming more powerful than Microsoft and even becoming the world's biggest Internet Service Provider, monopolising both the internet and OS.

Fairly speaking, every country might have hackers inside of its territory. In addition, there may be many categories of hackers in the world, such as civil individual hackers, hackers from non-government groups, government-employed hackers and even military-employed hackers; however, China is the only state officially proclaiming a national strategy of People's War, a theory which involves the indoctrination of the people in preparation for mobilisation. Though it is difficult to exactly clarify the sources of cyber attacks due to the feature of anonymity in cyberspace investigated in Section 2.2.4, it is clear that large database systems could be considered attractive targets for attack in order to achieve political or military goals. China's censorship of Google can therefore be seen as one aspect of China's fight with the USA for information control, facilitating China's cyber warfare deployment in the future. In China's view, such censorship is also indispensible for any future warfare.

Meanwhile, one might argue that the attack on Google was part of the PRC's new wave of blocking sensitive information for political purposes. Ever since Chinese net citizens' strong response to the Deng Yujiao incident[215] and condemnation of the Green Dam Censorware System, the latest censorship software introduced by the Chinese government, the PRC has been keeping a tighter control over the internet. According to ROC civil sector interviewee Yan

[215] Please refer to Section 5.4.1.

(2010), by the beginning of December 2009, around 7,000 internet cafes in China had been shut down by the government. However, this was not enough to satisfy the CCP. In the middle of December, another wave of blockades of certain websites was launched, which in essence turned the worldwide internet into a Local Access Net (LAN) to facilitate the maintenance of control. The PRC also monitors QQ, the most popular web-based communication application, bans private BT download websites[216], prohibits any application for personal websites, has stopped providing registration services of '.cn' Domain Names and uses 'blacklist' and 'whitelist', which refers to the policy of first blanket blocking all websites and then lifting the blockade on the approved ones. With regards any request to connect to a computer server, as soon as a problematic request is suspected, the server will be completely shut down. In other words, the Chinese government applies the Chinese strategic concept of 'rather kill a thousand innocent people than let off one guilty one' as a measure of internet control. In the case of Google, the PRC also took its usual measure of recoursing to both rules and threats in order to maintain control. Through the blockade of sensitive websites, China aims to make not only Google accept its rules, but also other domestic Internet Service Providers like Baidu.

A further example of China's internet control was laid out in *The Epoch Times* (2011). It is believed that the PRC plans to conduct 'physical disconnection' on some selected network cables in order to reconstruct a restricted Chinese internet network, in which only a very few network ports can connect to the World Wide Web.[217] As *The Epoch Times* (2011) notes, it has been argued that there are two reasons for the Chinese government to do so: 'One is that the recent 'Jasmine Revolution' triggered via the internet; and the second is that the US government has claimed to have invested 25 million dollars to support research into opposing the Chinese blockade of the internet.'

Furthermore, attacking Google can also be seen as a PRC military manoeuvre to conduct asymmetric warfare and unrestricted warfare. The Chinese military put forward the ideas of both asymmetric warfare and unrestricted

[216] This is a new Point-to-Point technique of file transmission. The more users that join the download, the faster the download will be.

[217] As the report points out, since 21st February 2011, some big cities in China, such as Shanghai, Beijing, and Chongqing, have occasionally encountered internet disconnection on a large scale, caused by the loss of DNS service due to 'physical disconnection.'

warfare many years ago. As the PRC cannot catch up with the USA in the field of high technology within a short time period, the Chinese army prefers to develop asymmetrical measures to offset US military advantages, and as this research has shown, cyber warfare is the most significant amongst these measures. As a result, it is very possible that the PRC chose to assess the effectiveness of its asymmetric strategy in cyber warfare, as well as its diplomatic response through attacking Google.

Yet another reason for attacking Google might be to facilitate Baidu's dominance of information services in China. The field of information services controlled by the PRC has two conflicting aspects. Firstly, the commercial action of searching for the truth directly clashes with the CCP Propaganda Department's concealing of the truth; however, China still needs to learn from Google's operation and technology, and may wish to take advantage of the just image of this Western company.

In sum, it can be concluded from the Google case that censorship is a critical approach in China's cyber warfare that attempts to gain dominance on the internet and control freedom of speech in order to discipline the masses of Chinese netizens. Whilst this warfare targets the governments of other states and foreign private companies in China, it also controls the domestic Chinese populace. This implies that it is not necessary to distinguish between carrying out 'cyber suppression' – internal internet control and monitoring – and external cyber attacks. The Chinese government can entrust civil actors with the tasks of censorship and internet control. A challenge for the Chinese authorities is grasping the perfect balance between censorship and the Chinese people's needs of being involved in the global internet community. Meanwhile, China as a whole is also seeking a balanced status between international cooperation and cyber attacks. For example, whilst the Chinese authorities and its hackers target global cyberspace, on 12th November 2010, Hu Qiheng, the chairman of the Internet Society of China, praised the Internet Engineering Task Force (IETF) for its 'candid culture' on behalf of the host organisation at the 79th conference of the IETF in Beijing. (*The Epoch Times*, 2010)

It is likely, then, that China's censorship of Google's search engine was an approach of cyber warfare, enabling the seizure of important information. In other words, it may be argued that censorship does not merely prevent the public from

accessing politically sensitive information, but is also a tactic of China's cyber warfare, which includes ideologically controlling and commanding civilians into disciplined cyber warriors. As a result, the strategy of People's War can be carried out securely without loss of control in the potential battlefield of cyberspace. The dictatorship of the Chinese one-party government offers a further unique advantage in this respect.

5.6 A review of recent cyber incidents

An increasing number of cases of cyber attack or even war have been revealed in public in the past few years. In order to present a common pattern of cyber attack for subsequent empirical analysis, a review of recent cyber attacks will be examined in this section. As recent reliable evidence demonstrates, states have begun to contend with one another in cyberspace, and a strategy of cyber warfare has been adopted not only by China, but also by other countries within the last decade. In a report to the US congress in 2009, it is noted that 'President Obama labelled cyber attacks one of the most serious economic and national security challenges.' (USCC Report, 2009:167) An article appearing in *The New York Times* further states that the US plans to develop strategies of cyberspace warfare, not just for *defence* but also for *offence*, by enlarging the government budget to establish cyber units.[218] Aside from official US reports, China's official media responded to accusations that China conducted cyber warfare as part of national strategy by unveiling claims that the US military also puts a great deal of effort into the development of cyber warfare.[219] It is thus apparent that there may be another wave of arms race between states, this time waged in cyberspace.

5.6.1 *Recent incidents of cyber attack*

[218] The Pentagon will develop a new strategy of cyber warfare in order to fully comprehend and defend against potential attacks in which the adversary may 'shut down the country's power stations, telecommunications and aviation systems, or freeze the financial markets'. (Sanger, Markoff and Shanker, 2009) In addition, on 23rd June 2009, US Defence Secretary Robert Gates declared cyberspace to be 'the "fifth domain" of military operations, alongside land, sea, air and space. It is the first man-made military domain, requiring an entirely new Pentagon command'; he set up the United States Cyber Command to respond to this. (Glenny, 2010) The United States Cyber Command was officially activated on 21st May 2010 and achieved full operational capability from 31st October 2010. This Command is at a level equal to Air Force Operation Command and Space Command, and is headed by a four-starred General. (McMichael, 2010)

[219] As China's Xinhua News reports, it is believed that the US military has 3,000 to 5,000 cyber experts, and 50,000 to 70,000 soldiers engaged in cyber warfare as 'cyber warriors'. (Xinhua News, 2010) in addition, it is officially claimed that the US military will spend 17 billion dollars on the development of cyber warfare in a five year project starting from 2008. (Sanger, Markoff and Shanker, 2009) Thus it is clear that, if necessary, the US is able to carry out cyber warfare.

In April 2007, according to news reports, whilst Estonia relocated the Bronze Soldier of Tallinn dedicated to soldiers of the former Soviet Union who died in battle, the country was subjected to a three-week barrage of cyber-attacks, which disabled the websites of government ministries, political parties, newspapers, banks, and companies. (BBC, 2007) The cyber attacks inundated Estonia's websites with 'Denial-of-Service' (DoS)[220] attacks, overwhelming servers and forcing them to shut down for a few hours or even longer. The internet linked to the outside of Estonia was closed for a week. In addition, as Steven Lee Myers (2007) reports, the Estonian Defence Ministry pointed out the most crucial issue: 'If you have a missile attack against, let's say, an airport, it is an act of war…If the same result is caused by computers, then how else do you describe that kind of attack?'

In June 2007, the *Financial Times* of London broke the story that Chinese hackers had penetrated the Pentagon's unclassified computer network, which also served the office of Defence Secretary Robert Gates. It was labelled 'the most successful cyber attack against the Department of Defence.' (Sevastopuloin and McGregor, 2007) According to the report, this incident prompted Pentagon security experts to shut down unclassified email communication systems for a week. Although details remain classified, an unnamed source revealed that the hackers spent months exploring the network before finally penetrating it and then transmitting data and files to an outside IP address located in China.[221] Though by all accounts the cyber attacks did not corrupt or destroy data, the actions did show the capability to penetrate the computer networks and deposit malware, and demonstrated the capacity to launch future actions. Not long after the Pentagon attack, in August 2007, the German magazine *Der Spiegel* reported that German security agencies discovered computers in Chancellor Merkel's office, as well as other German ministries, infected with spying software traceable back to China. A top German internal official did not hesitate to point the blame at the Chinese government: 'In our view, state Chinese interests stand behind these digital

[220] A 'Denial of Service' (DoS), also known as 'Distributed Denial of Service' (DDoS), attack is characterised by an explicit attempt by attackers to prevent legitimate users of a service from using it. Attacks can be directed at any network device, including attacks on routing devices and web, electronic mail, or Domain Name System (DNS) servers. (Carr, 2009:27)

[221] According to this report, 'Current and former officials have told the *Financial Times* that an internal investigation has revealed that the incursion came from the People's Liberation Army [PLA].' (Sevastopuloin and McGregor, 2007)

attacks.' (Tkacik, 2007) December 2007 brought another round of Chinese-related cyber news: the Director of Britain's MI5, Jonathan Evans, made an unprecedented public warning that China was spying on British corporate computer networks. Evans sent letters to over 300 British corporate chiefs and security officers warning that they were under attack 'from Chinese state organisations.' The recipients included banks, accountants, and legal firms: all part of Britain's critical economic infrastructure. According to *The Times*, the MI5 document warns that British companies conducting business in China were being targeted via the internet with the purpose of stealing privileged business information.[222] These accusations do not directly point to the Chinese government or PLA. However, a list of IP addresses attacking the sites can be linked to locations in China. (Markoff, 2007) In 2009, Robert Gates, the US Defence Secretary, pointed out that the computer system at the US Department of Defence controlling military equipment and the air traffic control system had been under cyber attack, and the evidence showed the attack was traceable to China. (CBS News, 2009) Moreover, as the Director of the UK Government Communications Headquarters (GCHQ), Iain Lobban, states, the UK's infrastructure, including such aspects as power grids and emergency services, has to face a 'real and credible' threat in cyberspace. He further stresses that the UK government network has previously been seriously attacked, and evidence shows that China is involved. (Shipman, 2010)[223]

In fact, these cyber attacks are all strikingly similar in methods and tactics, even though the targets are different. A study shows that the attacker exploits a complex network of websites that 'bypass traditional information security technology.'[224] (Finjan, 2008) Trojans are embedded in the target computer, infecting other computers in the network and covertly directing the target computer browser to malicious websites. These attacks can be traced back to

[222] This can be found in the article 'MI5 alert on China's cyberspace spy threat.' (Blakely, Richards, Rossiter and Beeston, 2007)

[223] The GCHQ governmental report indicates, 'There are over 20,000 malicious emails on government networks each month, 1,000 of which are deliberately targeting them.' (GCHQ report, 2010) In addition, as Tim Shipman indicates, 'Chinese intelligence is engaged in a systematic attempt to steal UK industrial and military secrets, often with cyber attacks on defence firms.' (Shipman, 2010)

[224] All of the attacks employed a Trojan virus, which is a small program embedded in seemingly legitimate emails, hacked trusted websites, links from spam email, copycat domain names, or infected content injected into websites.

locations situated inside China's territory.[225] Though the Chinese government always officially denies any accusations, these incidents still demonstrate that China would be easily capable of conducting cyber attacks in cyber warfare in the future if Chinese civilian hackers are systemically mobilised for a specific political purpose, regardless of their precise location within China.

5.6.2 *Cases of cyber warfare conducted during military conflicts*

In addition to incidents of cyber attack, some states have already conducted cyber warfare during military conflicts. According to Dunn Cavelty (2007), NATO's intervention against Yugoslavia in 1999 during the Kosovo War, known as Operation Allied Force, is recognised as the first war fought in cyberspace. In this war, the Federal Republic of Yugoslavia effectively employed methods of cyber warfare against NATO forces. The Yugoslav military implemented the military strategy of mobilising hackers[226] to conduct cyber attacks and deploy a range of computer viruses. Some websites of the NATO military were blocked by spam information and some computer network systems were even paralysed as a result. NATO subsequently strengthened their network systems through protective measures against cyber attack. They also deployed their own cyber counter-attacks, in which they penetrated the Yugoslav Army's computer networks and communication systems in order to plant a large number of viruses and deceptive information. The computer systems they destroyed dealt with command, control, and communications of the Yugoslav military troops and the combat systems of traditional weapons. Certain critical infrastructures, such as public services and power grids, were also paralysed. (Chen and Wang, 2009) In addition to the impact on military operations in the Kosovo War, the conflict also raised an important general issue: 'the use of the internet in conflicts by a wide variety of actors,' which may not necessarily be states. (Cavelty, 2007:75)

In August 2008, during the Russo-Georgian War, Russian hackers successfully intruded into Georgia's network systems, taking over many important

[225] Finjan, a global provider of internet security solutions, 'investigated a very sophisticated attack that used zero-day exploits (malware for which there is no security patch) as well as other new hacking techniques and discovered a centralised group of activity based from China […]one of the websites in the group belongs to a Chinese governmental office.' (Finjan, 2008)

[226] According to John Arquilla, 'Perhaps the most fascinating aspect of cyber warfare in Kosovo came after the armistice and the Serbian withdrawal from Kosovo. A group of hackers known as the Black Hand did not have to withdraw, because they weren't in Kosovo. They began to wage a campaign, a cyber war, to try to prevent the reconstitution of [civil] society.' (Arquilla, 2003)

web servers and thus paralysing certain parts of Georgia's national information infrastructure. In so doing, Russia was regarding as having created a radical case of cyber war in the international system. In order to deploy military operational intrusion into Georgia, before the launch of armed actions, Russia first took control of Georgia's network systems to cripple transportations, communications, media and financial network systems, as well as government websites.[227] However, though Russia's cyber warfare capability is indeed impressive, the core techniques still lie in US hands. (Chen and Wang, 2009)

The Israel-Hamas conflict in Gaza has also suffered cases of cyber attacks. In December 2008, cyber warfare occurred between Israeli and Arabic hackers during the Gaza strip conflict known as Operation Cast Lead. As Carr (2009:19) states, in this conflict nearly 10,000 websites were attacked within the space of only two weeks. As the websites of a few larger corporations were also targeted, the attacks had a financial impact too. (Carr, 2009) It is believed that some critical state infrastructures were damaged. An important concept of cyber warfare raised during this conflict is the idea of using multiple zombie systems, or building zombie nets[228], to achieve political gain or support propaganda claims. Viruses are employed as a weapon which can affect the digital state system in many different dimensions.

5.6.3 *Summary*

Regardless of whether a case can be categorised as a cyber attack or a cyber war, one might argue that, according to existing norms of international politics such as those proposed by NATO, it is unlikely that cyber attacks will be classified as a war which requires resorting to mediation from other states. For example, further to Libicki's (2009) explanation of what constitutes an act of war, examined in Section 2.4, he also states that, though they did provide Estonia with some

[227] The website of Georgian President Saakashvili was simultaneously attacked from 500 IP addresses. In addition, the websites of the Georgian parliament, government, and foreign ministry also suffered malicious attacks. (Carr, 2009:16-17) One Georgian network provider counted a total of 128 attacks, including 36 on the websites of the government and parliament, 35 on the Georgian police and another 35 on the finance ministry. Georgia's financial institutions cancelled all online banking and transactions for 10 days. (Goetz, Rosenbach, and Szandar, 2009)

[228] A zombie net, also known as a botnet, is a group of computers infected with a malicious kind of robot software, known as bots, which present a security threat to the computer owner. Once the robot software (malicious software or malware) has been successfully installed in a computer, this computer becomes a zombie or a drone, unable to resist the commands of the bot commander. It is estimated that 'One botnet of one million hosts could conservatively generate enough traffic to take most [targeted] 500 companies collectively offline.' (Carr, 2009:13)

technical help, NATO declared that the cyber attack on Estonia was not worth invocation of the treaty's collective-defence clauses. Nevertheless, NATO has since actively advocated the development of an international treaty on cyber warfare. If it were established that a state actor was behind the cyber attacks, it would be a case of one state targeting another via cyber warfare. In fact, a cyber war involving sides with equal military capability has not yet occurred in the international system. Previous cyber attacks and cyber wars have thus far always been 'one-sided' asymmetrical attacks. In the present day, with continued advances in information technology, offensive and defensive activities in cyberspace will become all the more common. Previously, main concerns were merely hackings and virus planting, but as capabilities develop, a current key issue is how the different sectors, such as private information providers, civil society, and military forces, can be integrated into cyber warfare capacity at a state level.

In addition, one might argue that incidents of cyber attacks should be treated merely as crimes, and that only some of them constitute military action justifying retaliatory attacks. As Brenner (2009:118) points out, in terms of the United Nations Charter, only an 'armed attack' allows a country to legitimately defend itself. It could be argued that any self-defence argument is irrelevant in many cases of cyber attack since they do not always constitute 'nation-state on nation-state' conflict. Regardless of the various debates involved in the issue of cyber warfare, one thing is clear: cyber warfare is an alarming issue at a state level of concern, because cyber warfare can cause a scale of physical destruction equivalent to that of a conventional war. In addition, cyber warfare can also boost states in enhancing their military operational capability. In terms of maintaining state military superiority, controlling cyberspace has become as critically important as dominating land, sea, air, and space. Moreover, in the digital age, both military and civil infrastructures, such as finance, transportation, supply services and telecommunication systems, have been bundled and embedded into cyberspace. Cyberspace is thus a vital factor for normal operation of a state.[229] In other words, once vulnerabilities occur in cyberspace, many important state infrastructures may be paralysed, thus jeopardising national security. The very real

[229] For example, as Mikhail Tammet, the head of IT security in Estonia's defence ministry, reveals, 'Estonia depends largely on the internet. We have e-government, government is so-called paperless... all the bank services are on the internet. We even elect our parliament via the internet.' (BBC, 2007)

potential of the threat of cyber attacks and cyber wars reveals that states are, as yet, unsecured against them, which may in turn affect the international system. This has triggered states to begin shifting their attention to developing their own cyber capabilities in order to tackle the issue of cyber security or even potentially contest the global power of other states via cyberspace in the future.[230] In so doing, militarisation of cyberspace has gradually advanced towards the stage of cyber warfare; cyber warfare can be conducted in cyberspace to achieve essentially the same results that states pursue through the adoption of conventional warfare, such as achieving advantages over a competing state or preventing a competing state from achieving advantages over them. In order to build up a collective defence strategy to prevent states from contending with one another, on 15th May 2008, eight nation states (Estonia, Latvia, Lithuania, Germany, Italy, Spain, Slovakia, and the USA) as well as the Supreme Allied Commander of Transformation (SACT)[231] signed an agreement to establish a jointly funded 'Cooperative Cyber Defence Centre of Excellence' (CCDCOE), which aimed to enhance NATO's cyber defence capability against cyber attacks, and seek a comprehensive defence strategy in cyberspace.[232]

5.7 Documentary evidence of China's cyber warfare

As stated in Section 5.1, due to the lack of availability of official Chinese military doctrine, it is hard to definitively state how China conducts cyber warfare. However, some related materials may offer an indication of China's cyber warfare, manifested in the integration of China cyberspace, even though official directives still remain uncertain.

As ROC retired Navy Rear Admiral Liu (2011) points out, an indication of how China carries out cyber warfare on an integrated platform can still be drawn from Chinese military news and some interior PLA documents. According to the *People's Daily* on 28th June 2011, Chinese Colonel Geng Yansheng, the Chief of

[230] For instance, in addition to China and the USA as already mentioned, a recent report notes, 'Germany's military, the Bundeswehr, trains its own hackers and it's not the only official effort to defend a nation from cyber attack, but also prepare for the future of war.' (Goetz, Rosenbach, and Szandar, 2009)

[231] SACT is in charge of NATO's highest military authority, the Military Committee, for promoting and overseeing the continuing transformation of Alliance forces and capabilities.

[232] This research centre, located in Estonia, is in charge of research and training on cyber warfare and develops NATO standards and capabilities for cyber defence. In addition, it provides expert advice on a regular basis as well as in emergencies. It reached full operational capability in the second half of 2008 with a staff of 30, half of them from the founding countries and half from other NATO member countries. (Socor, 2008)

the Public Affairs Bureau at the PRC's Ministry of National Defence, disclosed that China's PLA had established a 'cyber blue team' in order to conduct 'cyber exercises' to strengthen the 'cyber security of the Chinese military.' Geng also stated that China's Guangzhou Theatre organised one of these 'cyber exercises' in April 2011, in which there was a cyber confrontation between an offensive blue team and a defensive red team. (People's Daily, 2011) In addition, according to Deputy Commanding Officer of the Theatre Li's view (2011), preparing exercises for cyber warfare takes the PLA's cyber blue team less than ten days, and is relatively low cost. Cyber exercises are likely to contain three aims, which are 'controlling,' 'paralysing opponents' network system,' and 'data filching.' In terms of strategic considerations, controlling would be the optimum goal to achieve if possible. Paralysing would only be employed when controlling cannot or does not work. (China Economy, 2011)

Moreover, according to a classified interior PLA document[233], there are five methods of constructing China's complex electromagnetic environment to formulate an integrated platform on which to develop and exercise China's cyber warfare. These five methods are as follows:

1. 'Strong Electromagnetic Interference Environment'

   The communication countermeasure ability and radar countermeasure ability of the simulated blue team are used for interference in the military manoeuvre field. The purpose of this is to blind the radar of the drilling troops and cause failure of communication and malfunction.

2. 'Strong Electromagnetic Pulse Attack Environment'

   The simulated blue team and engineer troops reduce the effect of the electronic equipment of the drilling troops through the instantaneous radiation of high-power interference equipment and high-power electromagnetic pulse attack of microwave transmission equipment. To induce the drilling troops to carry out protective actions, flares, smoke, crackers and other forms of simulated nuclear explosion and electro-optical countermeasure environment are also employed.

3. 'Multi-faceted Network-based Attack Environment'

[233] This interior PLA document, produced by the PLA's General Staff Headquarter s 54th Institute, is entitled '*Operational Training under Complex Electromagnetic Environments*,' and was not officially published. It was investigated by a researcher from the PLA Archive Room at the ROC National Defence University in Taiwan.

The Network-Based Attack Unit of the blue team makes use of all kinds of network access equipment and deception to secretly access the internet, mainly through connecting wires and wireless nodes. They can access the drilling troops' wired and wireless LAN. Through multi-faceted and all-time internet attack and penetration, the enemy's internet resources would be damaged and stolen, and the computer system would be paralysed, leading to the creation of an environment where cyber attack is everywhere and is impossible to prevent, and where it is difficult to distinguish between the fake and the real.

4. 'Natural Disturbance Environment'

   There are three ways to set up such an environment. Firstly, through distributed written commands, the source and strength of interference are provided; secondly, organising the troops for drill in the places of mountains or mines where there is natural clutter, or during thunderstorms; thirdly, inducing the drilling troops to choose an appropriate location for their weapons and effective counter measures through the use of photoelectric equipment to simulate the effect of natural lightning's interference.

5. 'Public Equipment Interference Environment'

   Interfering with wireless communication by simulating local radio stations in the method of playing recorded tapes through short-wave radio set; simulating public electronic appliances' clutter through high-power electric generators, automotive engines and other equipment with clutter radiation; inducing the drilling troops to take measures to protect the electronic equipment by making use of the strong electromagnetic field of the high-power jammer during the period of starting up the equipment.

This complex electromagnetic environment may also be interfered with by computer viruses whilst regular electromagnetic systems are operated via computer systems. These regular electromagnetic systems include radar, transducers, the command and control system, communication and electronic combat systems and other electronic equipment. The communication system provides accurate connections and links between battalions and the highest commanding unit through the exchange of sound and data. The electronic combat system provides warning and supervision of the electronic spectrum, and interferes with the enemy's interference system through use of the electromagnetic medium. Almost all of these

systems make use of complex software, and therefore computer viruses could rapidly damage an enemy's computer systems through attacking the computer systems and network software, potentially 'paralysing' the enemy's whole network. The electric systems for military use rely heavily on computer software, which increases the vulnerability to virus attack. For example, a new form of electronic warfare is to 'plant' the microcode of the computer virus into a computer system.

Consequently, this section presents a clear indication that China does conduct cyber warfare. The empirical analyses in the earlier sections in this chapter are premised on this indication. In addition, the tactical methods deployed to exercise China's military also indirectly give an indication of how China constructs this integrated platform as a potential battleground for developing cyber warfare. The tactics of China's cyber warfare are combined with practical methods of electromagnetic warfare for implementation on this integrated platform as shown in Section 5.3 by evidence from interviews.

Chapter Six: Conclusion

Information technology (IT) plays a crucial role in determining the result of a modern war. The aim of a superior military is to concentrate its superior force to gain a pre-emptive advantage through the application of science and technology. In terms of combat capability, a technology-intensive military holds an advantageous position in local wars involving high technology. Under such circumstances, a mere reliance on numerical superiority cannot win against a technology-intensive military. The fundamental prerequisite for People's War is the justice of conducting a war. Only a feeling of justice for conducting a war can arouse people's enthusiasm for battle and invoke confidence in its warfare. As examined in this research, the traditional concept of People's War involves mobilising the masses to the greatest extent to create a ubiquitous resistance against the encroaching enemy. However, the basic form of modern warfare is long-range operations; it is rare that the enemy would deploy its armed forces for invasion. In the future, it is most likely that combatants will use tactics of long-range precise strikes. In the initial stage, large-scale electronic suppression techniques, constant air raids and blockades of coastal areas through attacking anti-radiation missiles and cruise missiles can be expected. In the following stage, the Navy and Air Force would cooperate, and aircraft carrier formation would be employed to achieve the goal of air and sea blockade if possible. Surprisingly, sometimes warfare would only take place in the sea and air. In this form of warfare, traditional People's War would produce little effect. The issue of improving the efficacy of People's War against a technology-intensive superior adversary needs urgently to be solved. A new military strategy, which both maintains the traditional classic military strategy but which can also effectively beat the enemy under new conditions, is necessary in the modern era. As a result, under the conditions of high-tech warfare in the digital age, it is likely that China will opt for cyber warfare adopting the strategy of People's War.

As discussed in this research, the characteristics of People's War involve a great number of participants on a large scale, but there are no main forces. People's War draws on one's advantages whilst avoiding any disadvantages, utilises one's strong points to attack the enemy via its weak points, harnesses a variety of flexible tactics, and presents a ubiquitous resistance against the enemy. When the enemy fails to identify a main force and key objectives, it would not be able to defend and attack effectively,

eventually leading to losses in battle. In order to utility the leverage of the huge Chinese populace, cyberspace can provide a new platform for battles through the launch of cyber warfare. In addition, as investigated, China's cyber warfare could include hostile operations aimed at attacking the enemy's telecommunication network and information systems in order to influence or even change decision makers' plans. In terms of military significance, China's cyber warfare means that both sides in any warfare will attempt to control information as a way to gain the pre-emptive advantage in a war and weaken the other side.

According to the procedure and effect of People's War in cyberspace, it can be concluded that China's cyber warfare could have five key characteristics, as follows. Firstly, China's cyber warfare aims to deal a fatal strike to superior opponents, since the world's economy, society, military and all other fields heavily rely on cyberspace. For example, the USA has set up as many as 20 large military networks. Once the command and control network is compromised, weaponry, no matter how powerful, cannot exert its influence and the whole military system may be paralysed. Secondly, China's cyber warfare could achieve the goal of 'subduing the enemy without physical fighting'. Cyber warfare does not begin with the appearance of missiles or other traditional weapons on the battlefield, but instead with antagonism in cyberspace. Once one side scores a key victory, the outcome of the war may be determined. Thirdly, the boundary between the battlefront and the rear does not exist in China's cyber warfare. Wherever cyberspace is involved, cyber warfare may take place. Fourthly, in terms of defence acquisition, the cost of cyber warfare is respectively low as it does not require much equipment, as the cases of cyber attack investigated in Section 5.2 demonstrate.

However, the fifth, most notable, characteristic involves the similarities and differences between cyber warfare and nuclear warfare. Just like nuclear warfare, cyber warfare also has a destructive force. Once it takes place, the side which is attacked or defeated may face the danger of a total collapse of the national economy. The potential of nuclear warfare has a huge effect on mentality, and likewise, cyber warfare could also shake the enemy's morale. The moment a nuclear weapon is launched, the outcome of warfare may be out of human control; this also applies to cyber warfare. When computer viruses are spread in the global network of cyberspace, the consequences may become out of control, which might cause a 'double sword' effect. However, the key difference between cyber warfare and nuclear warfare is that for the former, victory is

not achieved at the cost of numerous lives and there may not be much physical damage. Therefore, execution of cyber warfare might be more easily justified.

As a result, taking China's human resources and computer technology into account, it is possible to argue that the strategy of People's War is perfectly suited to be carried out in cyberspace if properly organised and precisely directed.

This research relies on an extensive review of China's military studies in order to reveal the significant addition Chinese cyber warfare has made to China's military affairs in the digital age. China's rise based on its own 'Chinese model' is tremendously impressive in terms of world politics, causing any potential military threats posed by China to be both widely influential and controversial. However, other than some limited government reports, there has been very little literature published to assist Western scholars in the formation of a body of related academic knowledge. (Zheng, 2011) Due to these resource constraints, this research cannot be so presumptuous as to attempt to resolve all the issues touched upon in this thesis. The goal is rather to explain why these issues must be discussed and to offer some modest suggestions regarding the direction and efforts of future research.

This may not seem particularly enterprising, but in fact, as explained in the methodological self-identification in the Introduction, this research can be regarded as making a contribution to the field of International Security Studies (ISS) and its encompassing areas of Strategic Studies and War Studies. The primary research question in this study focuses on the relationship between the growth of cyberspace as a potential battleground and existing doctrines of modern Chinese strategy. The research aim is to address this question through an empirical case study of China's cyber warfare. As the issue of cyber warfare is a relatively new agenda for Security Studies and Strategic Studies, this research must first establish a conceptual framework with which to approach the issue. This framework is developed throughout Chapter Two, Three and Four, and the propositions formed in these chapters inform the empirical case study analysis presented in Chapter Five. According to the analysis of these chapters, this research concludes that China's cyber warfare is a particular warfare with Chinese characteristics that adopts the doctrine of People's War. Each chapter raises some individual valuable conclusions for this research, which can be summarised in the following five points, representing the primary research outcomes of this study:

1. Chapter Two examines the nature of cyberspace through both physical and conceptual aspects. These features include permeability, a shared network platform,

asymmetry, and anonymity, allowing civil affairs and military action to regularly overlap and intertwine. Civil matters, such as IT research and development, are carried out in order to secure cyberspace for states; advanced information technology further reinforces a state's military capacity in cyberspace. Thus, the features of cyberspace present a certain strategic value for both state and non-state cyber actors, leading to struggles for domination. This in turn has raised the potential of cyberspace as a battle space, in which the shared information network infrastructure links civil, government, and military sectors. Moreover, the boundary between defensive and offensive strategy in cyberspace is also largely indiscernible. The key issue for states is to extend their dominant capabilities in this battle space whilst simultaneously reinforcing their defensive ability to secure the civil information infrastructure contained therein. These features and developments have led to an inevitable and urgent need for investigation into relevant strategy; this research looks in particular into strategies of modern Chinese cyber warfare.

2. According to the examination of modern Chinese strategy in Chapter Three, the strategic doctrine of People's War is a constant and crucial guiding principle of Chinese strategy in the modern era. People's War mainly consists of two conceptual components. The first is the mobilisation of not only the massive Chinese populace but also all civil resources in order to achieve a planned political goal. The second is the defeat of a superior adversary by an inferior power. This doctrine is likely to contain the concept of asymmetry, which has remained an important principle within the doctrine since it was raised in 1978 from a tactical level concerning just the physical battlefield to a strategic level.[234] Without the geographical limits of traditional battlefields, cyberspace offers the strategic doctrine of People's War a potential battle space perfectly suited to asymmetrical actions. The principles of Chinese strategy best suited for cyberspace can be briefly listed as follows:

   2.1 Achievement of all-out defence, and even offence, espoused by the doctrine of People's War, due to the potential for every citizen to act as a warrior in cyberspace.

   2.2 Defeat of the enemy without fighting or massive numbers of casualties in accordance with Sun Tzu's strategic maxim: 'subdue the enemy without

[234] For further information on the three transformations of People's War, please refer to Section 2 in Chapter Three.

fighting.' Most states' facilities rely on computer network systems, and combat in cyberspace can target these facilities in a relatively virtual manner without physical fighting. This principle may also be applied as a measure of deterrence, allowing paralysis of the opponent's critical information network infrastructure in order to discourage the adversary from taking any action during a potential conflict.

2.3 Knowing the enemy and knowing yourself so that you will not be in danger – another of Sun Tzu's guidelines. Dominating information in cyberspace is now vital for command and control of forces in any campaign. The Chinese PLA recognises that this ancient principle could thus be accomplished through cyber warfare.

2.4 Mobilisation of the massive number of Chinese internet users in order to carry out guerrilla strategy through the tactics of swarm and sting effect: cyber attacks can be fast and numerous, crippling the opponent's computer networks, including both civil facilities and combat systems. The manner of this mobilisation is investigated in Chapter Five.

3. Chapter Four presents a conceptual examination of the incorporation of the doctrine of People's War into China's cyber warfare. Concisely speaking, the strategy of China's cyber warfare combines the aspects of evolving warfare and general Chinese modern strategy to form a new kind of warfare supported by the traditional principle of People's War. Moreover, strategic principles of China's cyber warfare may adopt aspects contained within the strategy of People's War, such as 'active defence,' 'defence by deterrence,' and 'anti-access.' Theoretically, it can be claimed that the strategic value of cyberspace offers the strategy of People's War a perfect battle space. The doctrine of People's War also, in turn, ideally fits China's cyber warfare due to its history as a guiding strategic culture with Chinese characteristics. Interestingly, in the digital age, China, particularly the Chinese military, is able to harness technical skills arising in the West, such as information technology, to potentially eliminate foreign interference into China's affairs.[235]

4. The propositions of the previous analytical chapters are reflected through the analysis of the case study in Chapter Five. In this chapter, it is argued that China's cyber warfare, which incorporates the doctrine of People's War, aims not merely to

[235] This point of view also reflects a Chinese strategic thought from 1842: 師夷長技以制夷 (*shi yi chang ìì yi zhi yi*), which means 'To counter the West by learning from the West.' (Liu, 2010)

achieve military purposes, but also to discipline the huge number of Chinese netizens via internet control and monitoring. China's internet censorship is a fundamental measure of China's cyber warfare, both gathering important information and also preventing the public from uncovering politically sensitive material. In addition, factors such as patriotic education and ideological doctrine drive the military significance and justification of China's cyber warfare, further explaining how the Chinese government is able to mobilise the massive populace in line with People's War. Based on all of the measures of patriotic education examined, it is possible to argue that the ideology of the Chinese people is politically cultivated, as these measures are able to indoctrinate people into supporting nationalism. The Chinese government can thus carry out People's War strategy of mobilising the populace to achieve a political purpose, in particular concerning national issues in resistance to Western imperialism. This would also apply to online nationalism as part of China's cyber warfare.

5. In order to seek a possible general solution for actors to cope with cyber conflicts and to make a contribution to the field of International Security Studies, this research suggests a set of principles of 'cyber territoriality,' namely: *authority*, *cyber culture*, *functional borders*, and *people*. As cyberspace contains features of a virtual territory, the idea of cyber territoriality metaphorically territorialises cyberspace in parallel with the three principles[236] of the territorial state system. In so doing, possible rules of engagement in cyberspace as well as justification for the actions of cyber actors can be developed based upon these principles. Incidents such as the Google affair illustrate the potential useful application of the four principles of cyber territoriality. For example, once some Google email accounts were 'stolen,' the autonomy of its servers and the privacy of its users were compromised, effectively meaning the functional borders of the actor Google were intruded upon. If the principles of cyber territoriality could be converted into an accepted modus operandi for solving cyber conflict in world politics, actors such as Google may have a justification to carry out defensive measures.

[236] Sovereignty, integration, and borders.

Appendix 1:

Interviews in Taiwan
Aim: to provide empirical indications of how the PRC carries out cyber warfare/strategy

Opening greeting:
(Briefly introduce myself and the research topic, and offer my thanks for the interview)

Request interviewees to briefly introduce themselves and state how their background is associated with cyberspace/information technology, China's cyber warfare, or Chinese strategy.

Prepared interview questions:

Relevant areas			Interview Questions
CI	CS	CW	
✓	✓	✓	據報導，中共被 Google 指控對 Google 用戶進行攻擊 (是利用台灣當做跳板主機)，您的看法如何？ Q1: According to some news sources, the PRC was recently accused of conducting attacks on the accounts of Google users (by using Taiwanese computers as a bridge). What do you make of this claim?
✓	✓	✓	中國如何實施網路戰法與戰略？ Q2: How does the PRC carry out cyber warfare/strategy?
✓	✓	✓	當網路空間成爲一個戰場時，對現有的軍事準則和戰略影響如何？ Q3: How does cyberspace as a potential battleground challenge existing military doctrine and strategy?
	✓	✓	全民國防的概念如何可以應用於網路戰爭的防衛策略？ Q4: How does the idea of civilian-based defence apply to the defensive strategy of cyber warfare?
	✓	✓	網路戰與中國軍事事務革新之關係如何？ Q5: How is cyber warfare related to the PRC's Revolution of Military Affairs?
	✓	✓	中共非對稱戰略及人民戰爭，與網路戰關係如何？ Q6: What relation do the PRC's asymmetric warfare and People's War have with cyber warfare?
	✓	✓	您認爲台灣是中共網路戰的主要攻擊目標嗎？ Q7: In your opinion, does the PRC regard Taiwan as its primary target in terms of cyber warfare?
	✓	✓	接續前題，台灣目前的防衛措施如何應付中共網路攻擊？ Q8: Further to the previous question, what are Taiwan's existing defensive measures/doctrines to cope with the PRC's cyber warfare?
✓		✓	中共資訊戰的發展是否受到民間資訊基礎建設的影響？爲了達到‘打贏資訊化的局部戰爭’，中共的資訊化建設如何軍民一體？ Q9: How does the PRC's civil information infrastructure affect the development of PRC cyber warfare? How does the PRC's infrastructure combine the military and civilian sectors to pursue the aim of 'winning local wars under informationisation'?

✓		✓	對網路攻擊事件防衛或反擊措施的正當性如何重要？ Q10: How important is it to establish legitimacy in law and policy for carrying out defensive measures against cyber attack, or even counter attacks?
✓		✓	在很多實際案例中，如何可以證明中共使用資訊戰攻擊手段？ Q11: How can previous related incidents demonstrate that the PRC already employs cyber warfare as an offensive approach?
✓		✓	您認爲 DNS 對網路空間的安全性措施有何影響？ Q12: How do you think the DNS affects security in cyberspace?
✓		✓	台灣軍事網路與民間網路實體隔離的措施成效如何？ Q13: The Taiwanese military has a policy of physically separating the military net and the civil net. How effective do you consider this approach to be?
	✓	✓	中共控制網路的動機何在？是否擔心人民發動網路的人民戰爭對抗中共政權？ Q14: What could be the PRC's motive for controlling its domestic internet? In your opinion, is it possible that the motive lies in a fear of the populace carrying out 'People's War' against the PRC's own regime via use of the internet?
	✓	✓	中共爲何要發展網路戰爭當成是一種軍事戰略？ Q15: Why and how does the PRC develop cyber warfare as a state military strategy?
		✓	網路戰和所謂的指管通情軍事系統關聯如何？ Q16: How is cyber warfare associated with the C4ISR military system?

Key:
CI: Cyberspace/information technology
CS: Chinese strategy/China Studies
CW: China's cyber warfare/strategy

(These questions were not necessarily carried out one by one, but it was ensured that all the questions recorded responses.)

Appendix 2:

China's National Telecommunication Network:
Eight North-to-South and Eight East-to-West Optical Fibre Routes

In China, researches on optic fibre started from the mid 1980s. With thirty years of development, China's optical fibre and optical cables industry is leading the world. In China, the six major telecommunication operators own 4,322,000 kilometres of optical cable, using 80,720,000 kilometres of optical fibre. Including radio and television, electricity, petroleum, and other industries, the whole country has a 5,772,000 kilometres of optical cable, which uses 107,810,000 kilometres of optical fibre. In the 1990s, the fast development of the communication industry spurred a rapid growth in the optical fibre communication market. Currently, optical fibre makes up more than 90% of the long-distance transmission network in China. China has constructed the Communication Network of Eight East-to-West and Eight North-to-South Optical Fibre Routes, which covers more than 85% of all the counties and cities.

China now owns the world's widest information super highway. The WDM system, the information transmission capacity of which is terabit (namely 1×1012 bit), has self-owned intellectual property rights. The first-class information route between Shanghai and Hangzhou (80×40Gb/s) can enable 40,000,000 people to make phone calls at the same time. The 2007 construction project of the state's first-class information route, the 1.6TDWDM high-end optical network equipment built by FiberHome Telecommunication, brought benefits to Shanghai, Jiangsu, Guangzhou, Hubei, Jiangxi, Anhui and other provinces.

Infonetics Research recently reported in 'Optical Network Hardware in Asia Pacific: China, Japan, India, and the Republic of Korea' that in 2007 China had the largest single-country optical spending in the Asia Pacific, which was more than double Japan's and surpassed the total spending of other countries in the Asia Pacific. China represented 43% of the $3.4 billion spent on optical hardware in 2007 by Asia Pacific countries.

The Communication Network of Eight North-to-South and Eight East-to-West Optical Fibre Routes

The Eight North-to-South Optical Fibre Routes are:

1. Harbin—Shenyang—Dalian—Shanghai—Guangzhou

2. Qiqiha’er—Beijing—Zhengzhou—Guangzhou—Haikou—Sanya
3. Beijing—Shanghai
4. Beijing—Guangzhou
5. Hohhot—Beihai, Guangxi
6. Hohhot—Kunming
7. Xining—Lhasa
8. Chengdu—Nanning

The Eight East-to-West Optical Fibre Routes are:

1. Beijing—Lanzhou
2. Qingdao—Yinchuan
3. Shanghai—Xi’an
4. Lianyungang—Yining, Xinjiang
5. Shanghai—Chongqing
6. Hangzhou—Chengdu
7. Guangzhou—Nanning—Kunming
8. Guangzhou—Beihai—Kunming

References

Adie, W. A. C. (1972) *Chinese strategic thinking under Mao Tse-tung*. Canberra: Australian National University Press.

Alvesson, Mats and Sköldberg, Kaj (2008) *Reflexive methodology: new vistas for qualitative research*. London: SAGE Publications Ltd.

Arquilla, John and Ronfeldt, David. (2001) *Networks and Netwars: The future of Terror, Crime, and Militancy*. Washington, D.C. RAND Press.

Arquilla, John (2003) 'Cyber War.' [interviewed by Frontline] *Public Broadcasting Service*. 4 March 2003. Available from <http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/arquilla.html> [8 November 2010]

Babulak, E. (2009) *Computational Intelligence, Modelling and Simulation, 2009. CSSim '09. International Conference on.*

Bai Guoliang (2011) *Chinese Military Mobilises Cyber-militias* [interview by Kathrin Hille] Beijing, [online] 12th October. *Financila Times* Available from: <http://www.ft.com/cms/s/0/33dc83e4-c800-11e0-9501-00144feabdc0.html#axzz1b5RMrcE7>

Baylis, J. Booth K. Garnett J. and Williams P. (1987) *Contemporary Strategy II*. Surry Hills: Holmes & Meier Publishers.

Baylis, J. and Smith, S. (2005) *The globalization of world politics: an introduction to international relations.*3rd Oxford ; New York: Oxford University Press.

Baylis, J., Wirtz, J. J., Gray, C. S. and Cohen, E. (2007) *Strategy in the contemporary world: an introduction to strategic studies.*2nd ed. Oxford: Oxford University Press.

Bayne, Jay S. (2008) 'Cyberspatial Mechanics', *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on*, 38, (3), pp. 629-644.

Baylis, J., Wirtz, J. J., and Gray, C. S. (2010) *Strategy in the contemporary world: an introduction to strategic studies.*3nd ed. Oxford: Oxford University Press.

BBC News (2007) 'Estonia Hit by "Moscow Cyber War".' *BBC News* [online] 17th May. available from < http://news.bbc.co.uk/1/hi/world/europe/6665145.stm> [30th October 2010]

BBC News (2010) 'Timeline: China and Net Censorship.' [online] 23rd March. Available from: <http://news.bbc.co.uk/1/hi/world/asia-pacific/8460129.stm> [accessed 23rd March 2010]

BBC Chinese News (2011) '中國網民關注湄公河慘案[Chinese Netcitizens Concern the Incident of Mekong River]' [online] 13rd October. Available from: <http://www.bbc.co.uk/zhongwen/trad/chinese_news/2011/10/111013_china_mekong_netviews.shtml> [accessed 13rd October 2011]

Benedikt, M. (1991) *Cyberspace : first steps.* Cambridge, Mass.: MIT Press.

Beebe, S.A., Beebe, S.J., and Redmond, M.V. (2008) *Interpersonal Communication: 5th Edition.* Boston: Pearson Education.

Behr, Harmut (2008) 'Deterialization and the Transformation of Statehood: The Paradox of Globalisation', *Geopolitics*, 13, pp. 359-382.

Blasko, Dennis J. (2003) 'PLA Ground Forces Lessons Learned: Experience and Theory.' *The Lessons of History: The Chinese People's Liberation Army at 75.* Pennsylvania: Army War College Press.

Blasko, Denis J. (2005) 'Chinese Army Modernization: An Overview.' *Military Review.* September-October 2005. Fort Leavenworth: United States Army Combined Arms Center.

Blasko, Dennis J. (2006) *The Chinese Army Today: Tradition and Transformation for the 21st century*. New York: Routledge.

Blakely, R. Richards, J. Rossiter, J. and Beeston, R. (2007) 'MI5 alert on China's cyberspace spy threat.' *The Times* [online] 1st December. available from < http://business.timesonline.co.uk/tol/business/industry_sectors/technology/article2980250.ece> [25th October 2010]

Booth, Kenneth (1990) 'The Concept of Strategic Culture Affirmed'. in *Strategic Power. USA/USSR.* ed. by Jacobsen, Carl G. London: Macmilla.

Booth, Kenneth (1997) 'Security and Self: Reflections of a Fallen Realist'. In Keith Krause and Michael Williams (eds), *Critical Security Studies: Concepts and Cases*. London: UCL Press.

Bradner, S. (1996) 'The Internet Standards Process: Revision 3', *The Internet Engineering Task Force (IETF).* Available from <http://tools.ietf.org/html/rfc2026#section-1.1> [accessed March 23, 2010].

Brooks, E. Bruce and Confucius (1998) *The Original Analects: Sayings of Confucius and His Successors.* trans. by Brooks, E. Bruce. New York: Columbia University Press.

Brenner, S. W. (2009) *Cyber Threats: the Emerging Fault Lines of the Nation State.* New York: Oxford University Press.

Brown, John Seely and Duguid, Paul (2000) *The Social Life of Information.* Boston: Harvard Business School Press.

Bruno, Greg (2008) 'The Evolution of Cyber Warfare.' [online] 27th February. *Council on Foreign Relations.* Available from < http://www.cfr.org/publication/15577/evolution_of_cyber_warfare.html> [12th November 2010]

Buchanan, Ian and Parr, Adrian (2006) *Deleuze and the Contemporary World.* Edinburgh: Edinburgh University Press.

Burles, Mark and Shulsky, Abram (2000) *Patterns in China's Use of Force: Evidence from History and Doctrinal Writing.* Santa Monica: RAND Corporation.

Burnham, Peter (2008) *Research methods in politics*.2nd ed. Basingstoke: Palgrave Macmillan.

Buzan, Barry (1991) *People, State, and Fear: An Agenda for International Security Studies in the Post-Cold Era*, pp. 116-134

Buzan, Barry and Hansen, Lene (2010) *The Evolution of International Security Studies.* 2nd ed. Cambridge: Cambridge University Press.

Carr, J. and Shepherd, L. (2010) *Inside Cyber Warfare.* Sebastopol, CA: O'Reilly Media Inc.

Castells, M. (2000) The rise of the network society.2nd Malden, MA: Blackwell Publishers.

Cassidy, Robert M. (2003) *Russian in Afghanistan and Chechnya: Military Strategic Culture and the Paradoxes OF Asymmetric Conflict.* Pennsylvania: Army War College Press.

Cavelty, Myriam Dunn (2007) *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. Hoboken: Taylor & Francis.

Cavelty, Myriam Dunn, Mauer, Victor, and Krishna-Hensel, Sai Felicia (2008) *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace*. Farnham: Ashgate Publishing Ltd.

CBS News (2009) 'Gates: Cyber Attacks A Constant Threat.' *CBS News* [online] 21st April. available from < http://www.cbsnews.com/stories/2009/04/21/tech/main4959079.shtml> [25th October 2010]

CCDCOE official website (2010) Introduction of Cooperative Cyber Defense Center of Excellence. [online] available from < http://www.ccdcoe.org> [9th November 2010]

Chai (2010) *How China's Cyber Warfare Develops and Conducts* [interview by author] Taipei, August 2010

Chang (2010) *How China's Cyber Warfare Develops and Conducts* [interview by author] Taipei, August 2010

Chang-1 (2010) *How China's Cyber Warfare Develops and Conducts* [interview by author] Taipei, August 2010

Chang (2011) *How China's Cyber Warfare Develops and Conducts* [interview by author via phone] Kaoshiung, May 2011

Charter of United Nations. (1945) Chapter I: Article 2. Retrieved 28 January 2009 from: <http://www.un.org/aboutun/charter/pdf/uncharter.pdf>

Cheng, W. H. (2003) *軍事研究方法 [Theory of Research Methods in Military Studies]*. Taoyuan: NDU Press. July 2003.

Chen, JunCun (2006) '美國公司助中共高科技化[American Companies Help the PRC with Advanced Technology]' *Epoch Times* [online] 18th September. available from <http://www.epochtimes.com/b5/6/9/18/n1458209.htm> [10th November 2010]

Chen, A. and Wang, J. (2009) *資訊戰視野中的典型戰例研究 [War Case Studies in the Scope of Information Warfare]* Shanghai: Xiu Lin Publisher.

Chen, Wei-Hwa (2009) 'Concepts of Deterrence and Defense: Similarity and Difference.' Defence Journal. No.2 Vol. 5 Taoyuan: ROC National Defense Univeristy.

Chen (2010) *How China's Cyber Warfare Develops and Conducts* [interview by author] Taoyuan, August 2010

Chen-1 (2010) *How China's Cyber Warfare Develops and Conducts* [interview by author] Taoyuan, August 2010

China Internet Network Information Center (2011) *27th Annual Report of China Internet Network Information* [white paper] 19th January. Beijing: CINIC Office.

China Military (2010) '超越軍種：未來信息化戰場主宰[Beyond Military Services: Cyber Warfare Dominates the Future Battlefield]' China Military Daily. 9th September. [collected 10th September 2010]

China News (2011) '日本婉拒中国海军医疗船地震救援[Japan declined Chinese navy ships supplies for the damages caused by earthquake]' China.Com [online] 13rd March. Available from: <http://www.epochtimes.com/b5/11/3/13/n3195925.htm> [accessed 10th May 2011]

China Org (2011) '中國空軍民兵條例細則 [China's The Rules and Regulations for the Air Force Militia].' [online] 13rd January. Available from: <http://big5.china.org.cn/military/txt/2011-01/13/content_21730945.htm> [accessed 28th January 2011]

China Economy (2011) '中國解放軍建立"網路藍軍" [PLA Establishes "Cyber Blue Team"].' [online] 31st May. Available from: <http://big5.ce.cn/xwzx/gnsz/gdxw/201105/31/t20110531_22451766.shtml> [accessed 10th June 2011]

Chou (2010) *How China's Cyber Warfare Develops and Conducts* [interview by author] Taipei, August 2010

Clausewitz, C. v. (1976) *Vom Kriege [On war]*. trans. by Howard and Paret. Princeton: Princeton University Press.

Clausewitz, C. v. (2001) *Vom Kriege [戰爭論(The theory of war)]*. trans. by Yang, Fang-Nian Taipei: Cite Publisher.

Cliff, Roger, Burles, Mark, Chase, Michael S., Eaton, Derek and Pollpeter, Kevin L. (2007) *Entering the dragon's lair: Chinese antiaccess strategies and their implications for the United States.* Santa Monica: RAND Corporation.

Confucius (1998) *論語[The Analects of Confucius: A Philosophical Translation]*. trans. by Ames, Roger T. and Rosemont Jr, Henry New York: The Random House Publishing Group.

Congressional Report (2003) *The Military power of the People's Republic of China.*

Collins, Alan (2010) *Contemporary Security Studies.*2nd ed. Oxford: Oxford University Press.

Creveld, Martin Van (1991) *Technology and War.* New York: Maxwell Inc.

Dai, Qingmin (2002) '論整合型網路電子戰 [The Integration of Cyber Warfare and Electronic Warfare]' *中國軍事科學[China's Military Science]* Beijing: The Academy of Military Science Press.

Dai, Qingmin (2002) *直面信息戰 [Direct Information Warfare]* Beijing: The PRC National Defense University Press.

Dai, Qingmin (2008) '論整合型網路電子戰[Study of Electric Warfare: A Form of Integrated Network].' *Chinese Military Science*. Beijing: Military Science Press.

Daily Mail Reporter (2010) 'Mr. Present we've lost control of FIFTY nuclear warheads: Obama told how his arsenal was hit by 45 minutes computer glitch.' *Daily Mail* [online] 27th October. available from <http://www.dailymail.co.uk/news/article-1324190/Obama-told-nuclear-arsenal-hit-45-minute-glitch.html> [27th October 2010]

Damm, Jens and Thomas, Simona (2009) *Chinese Cyberspaces: Technological Changes and Political Effects.* London: Routledge.

Defence Management Journal (DMJ) (2009) 'The Next Battlefield.' *Defence Management Journal*. 12 June 2009. Available from < http://www.defencemanagement.com/feature_story.asp?id=12170> [8 October 2010]

Deleuze, Gilles and Guattari, Felix (1994) *What Is Philosophy?* London: Verso.

Dellios, Rosita. (1997) '"How May the World Be at Peace?": Idealism as Realism in Chinese Strategic Culture' in *Culture and Foreign Policy*. ed. By Hudson, Valerie M. Colorado: Lynne Rienner. Available from <http://works.bepress.com/rosita_dellios/9> [12 November 2009]

Deng-1, Xiaoping (1994) *Deng Xiaoping Wen Xuan II(鄧小平文選 II)* [*Selected Work of Deng Xiaoping II]*. Beijing: People Press.

Deng-2, Xiaoping (1993) *Deng Xiaoping Wen Xuan III(鄧小平文選 III)* [*Selected Work of Deng Xiaoping III]*. Beijing: People Press.

Deng, Feng (2006) *轉型中的軍事理論[The Transforming Military Theory]*. Beijing: National Defense University Press.

Deng (2010) *How China's Cyber Warfare Develops and Conducts* [interview by author] Taipei, August 2010

Department of Defense (2007) *Global Information Architectural Vision: Vision for a Net-Centric, Service-Oriented DoD Enterprise*. Washington D.C.: Chief Information Office. Available from <http://www.msco.mil/files/MSCO%20Online%20Library/GIG%20Architectural%20Vision%20-%20200706%20v1.0.pdf> [accessed 31 March 2010].

Denzin, N. K. & Lincoln, Y. S. (2005) *Handbook of qualitative research*. CA: Sage Publications, Inc.

Ding, Author Shuh-Fan. (1996) *中共軍事思想的發展[PRC's Changing Military Theory 1979-1991]*. Taipei: Tan-Shan Publishing House.

Ding (2010) *How China's Cyber Warfare Develops and Conducts* [interview by author] Taipei, August 2010

Doctrine of Information Operations. (2006) *Joint Doctrine.* Joint Education and Doctrine Division at Department of Defense in USA. Retrieved 12 February 2009 from: http://www.dtic.mil/doctrine/doctrine.htm

Doctrine of Information Operations. (2006) *Joint Doctrine.* Joint Education and Doctrine Division at Department of Defense in USA. Retrieved 12 February 2009 from: http://www.dtic.mil/doctrine/doctrine.htm

Doctrine of Electronic Warfare. (2007) *Joint Doctrine.* Joint Education and Doctrine Division at Department of Defense in USA. Retrieved 12 February 2009 from: http://www.dtic.mil/doctrine/doctrine.htm

Doctrine of Electronic Warfare. (2007) *Joint Doctrine.* Joint Education and Doctrine Division at Department of Defense in USA. Retrieved 12 February 2009 from: http://www.dtic.mil/doctrine/doctrine.htm

Dong, Tzfeng (2006) *信息化戰爭型態論 [The Theory of Informationisation Warfare]* Beijing: The PLA Press.

Edwards, James (2009) *Networking Self-Teaching Guide: OSI, TCP/IP, LAN's, MAN's, WAN's, Implementation, Management, and Maintenance*. Hoboken: John Wiley & Sons, Inc.

Erickson, Andrew and Collins, Gabe. (2011) 'A Smoking Cursor? New Window Opens on China's Potential Cyberwarfare Development: CCTV 7 program raises new questions about Beijing's support for hacking.' 24th August. *China SignPost™ (洞察中国)*, No. 46.

Eriksson, J. and Giacomello, G. (2006) 'The information revolution, security, and international relations: (IR)relevant theory?' *International Political Science Review*, 27, (3), pp. 221-244.

Eriksson, J. and Giacomello, G. (2006) 'The information revolution, security, and international relations: (IR)relevant theory?' *International Political Science Review*, 27, (3), pp. 221-244.

Fahrenkrug, D. (2008) *3rd International Conference on Information Warfare and Security, Proceedings.* Omaha, APR 24-25, 2008.Academic Conferences Ltd.

Feng (2010) *How China's Cyber Warfare Develops and Conducts* [interview by author] Taipei, August 2010

Finjan, Inc. (2008) 'Finjan reveals new Trojan activity involves Chinese Government website.' [online] 21st January. *IT Reseller Magazine*. Available from < http://www.itrportal.com/absolutenm/templates/article-logistics.aspx?articleid=4678&zoneid=68 > [12th September 2010]

Finkelstein, M. (1999) 'China's National Military Strategy.' *People's Liberation Army in the Information Age.* Santa Monica: RAND Corporation.

Finkelstein, M. (2004) ' The Chinese People's Liberation Army In 2020.' *The Changing Nature of Warfare — Global Trends 2020.* Conference. 26th May 2004.

Freeman, Lawrence (2010) 'Does Strategic Studies Have Future?' [Baylis, J., Wirtz, J. J., and Gray, C. S. Ed.] *Strategy in the contemporary world: an introduction to strategic studies.*3nd ed. Oxford: Oxford University Press.

Green, Philip (1966) *Deadly logic: the Theory of Nuclear Deterrence.* Columbus: Ohio State University Press.

Gao, Z. H. (2003) 'The integrated Military Theory with Confucianism.' *Journal of Chinese Military*. Vol. 16. p.p. 122-129

Gerring, John (2004) 'What Is a Case Study and What Is It Good for?', *American Political Science Review*, 98, (02), pp. 341-354.

Gerring, John (2008) *Case Study Research: Principles and Practices.* Cambridge: Cambridge University Press.

Gill, Bates. and Henley, Lonnie (1996) *China and Revolutionary in Military Affairs.* Pennsylvania: Army War College Press.

Glenny, Misha (2010) 'Who Controls the Internet?' *Financial Times* [online] 8th October. available from <http://www.ft.com/cms/s/2/3e52897c-d0ee-11df-a426-00144feabdc0.html#axzz14xnI1sEe> [5th November 2010]

Godwin, P. H. B. (1987) 'Changing Concepts of Doctrine, Strategy and Operations in the Chinese People's Liberation Army 1978-87', *The China Quarterly* 112, pp. 572-590.

Godwin, P. H. B. (1992) 'Chinese Military Strategy Revised: Local and Limited War', *Annals of the American Academy of Political and Social Science,* 519 pp. 191-201.

Goetz, J., Rosenbach, M., and Szandar, A. (2009) 'War of Future: National Defense in Cyberspace.' *Spiegel* [online] 11th February. available from < http://www.spiegel.de/international/germany/0,1518,606987,00.html> [2nd October 2009]

Gong, Yuzhen (2002) *中國戰略文化解析[Analysis of Chinese Strategic Culture]*. Beijing: Military Science Press.

Gorge, M. (2007) 'Cyberterrorism: hype or reality?' *Computer Fraud and Security*, 2007, (2), pp. 9-12.

Gu, Li-Min (2009) 'Analysis on the thought of People's War.' *國防雜誌[Defense Journal]*. No.5, Vol.24 p.p. 64-79

Gu (2010) *How China's Cyber Warfare Develops and Conducts* [interview by author] Taoyuan, August 2010

Hakken, David (2003) *The knowledge landscapes of cyberspace.* New York, London: Routledge.

Hansen, Andrew, Williams, Paul, Mills, Robert, and Kanko, Mark (2008) 'Cyber Flag: A Realistic Training Environment for the Future', *Air & Space Power Journal*, Fall 2008.

Hansen, Lene (2009) 'Digital Disaster, Cyber Security, and the Copenhagen School', *International Studies Quarterly*, 53, pp. 1155-1175.

Hao (2010) *How China's Cyber Warfare Develops and Conducts* [interview by author] Taipei, August 2010

Hart, Liddell B. H. (1960) *Deterrence and Defence.* London: Stevens Publisher.

Hart, Liddell B. H. (1991) *Strategy.* New York: Meridian Book.

Harknett, Richard and Stever, James (2009) 'The Cybersecurity Triad: Government, Private Sector Panters, and the Engaged Cybersecurity Citizen', *Journal of Homeland Security and Emergency Management,* 6, (1): Art. No. 79.

Herz, John H. (1962) *International politics in the atomic age*. New York,: Columbia University Press.

Hildreth, Steven (2001) Congressional Research Service (CRS) Report for Congress. *Cyber warfare*. available from <http://www.loc.gov/crsinfo/aboutcrs.html#report> [accessed 26 November, 2008]

Holloway, E. M., Lamont, G. B. and Peterson, G. L. (2009) 'CyberSociety: computer-mediated communication and community', *Computational Intelligence in Cyber Security, 2009. CICS '09. IEEE Symposium on.*

Housworth, Gordon (2008) 'Operational Analysis of Chinese "Cyber Army" Penetration and Recovery Techniques.' [online] 1st August. *ICG Intellectual Capital Group*. Available from <

http://spaces.icgpartners.com/index2.asp?NGuid=CC1A1D4812474F5B809C542F3CDF163A> [17th September 2010]

Howard, M., B. H. S. and E.Liddell Hart (1965) *The Theory and Practice of War.* Essays presented to Captain B. H. Liddell Hart. Editor: Michael Howard. [By various authors.] Cassell: London.

Hsieh (2010) *How China's Cyber Warfare Develops and Conducts* [interview by author] Taoyuan, August 2010

Huang (2010) *How China's Cyber Warfare Develops and Conducts* [interview by author] Taipei, August 2010

Huang (2011) *How China's Cyber Warfare Develops and Conducts* [interview by author via phone] Taoyuan, April 2011

Hughes, Christopher R. (2010) 'Google and the Great Firewall', Survival, 52:2, pp. 19-26

Hundley, H. O. and Anderson, R. H. (1995) 'Emerging challenge: security and safety in cyberspace', *Technology and Society Magazine, IEEE,* 14, (4), pp. 19-28.

Independent News (2010) 'Obama Would Sack BP Boss Hayward.' *Independent News* [online] 8th June. available from <http://www.independent.co.uk/news/world/americas/obama-would-sack-bp-boss-hayward-1994370.html> [25th October 2010]

Jane's Information Group (2007) 'China and North East Asia' *Jane's Sentinel Security Assessment.* 17th October 2007. Coulsdon: Jane's Information Group.

Jervis, Robert (1979) 'Deterrence Theory Revisited'. *World Politics* 31 (2), 289-324

Jiang Zhemin (2001) *論三個代表[On the Three Represents]*. Beijing: Central Archive Press.

Jiang, Zemin (2002) *中國共產黨第16屆人民代表大會報告[Proceedings of the 16th Chinese Communist Party Congress]*. [online] 8-14 November. available from <http://big5.xinhuanet.com/gate/big5/news.xinhuanet.com/newscenter/2002-11/17/content_632239.htm> [10 December 2009]

Joffe, E. (1987) '"People's War under Modern Conditions": A Doctrine for Modern War', *The China Quarterly* 112, pp. 555-571.

Jones, S. (1995) *CyberSociety : computer-mediated communication and community.* Thousand Oaks, Calif.: Sage Publications.

Johnston-1, Alastair Iain (1995) *Cultural Realism: Strategic Culture and Grand Strategy in Chinese History*. Princeton N.J.: Princeton University Press.

Johnston-2, A. I. (1995) 'Thinking about Strategic Culture', *International Security,* 19 (4), pp. 32-64.

Johnston-3, A. I. (1996) 'Cultural Realism and Strategy in Maoist China.' *The Culture of National Security: Norms and Identity in World Politics.* Edited by Katzenstein, Peter J. New York: Columbia University Press.

Jordan, T. (1999) *Cyberpower : the culture and politics of cyberspace and the Internet.* London: Routledge.

Jordan, D., Kiras, J. D., Lonsdale, D. J., Speller, I., Tuck, C. and Walton, C. D. (2008) *Understanding modern warfare.* Cambridge: Cambridge University Press.

Kao, Sean (2000) *中國大陸資通產業政策 [The Industry Policy of China's Information and Telecommunication]* Taipei: Ministry of Economics ROC.

Karatzogianni, A. and Ebooks Corporation. (2008) *Cyber-Conflict and Global Politics.* Hoboken: Taylor & Francis.

Kelly, D., Raines, R., Baldwin, R., Mullins, B. and Grimaila, M. (2008) 'A framework for classifying anonymous networks in cyberspace', *3rd International Conference on Information Warfare and Security, Proceedings.* Omaha, APR 24-25, 2008.Academic Conferences Ltd.

Klein, Yitzhak (1991) 'A theory of strategic culture', *Comparative Strategy*, 10, (1), pp. 3 - 23.Millett, A. R. (1997) 'A Reader's Guide to the Korean War', *The Journal of Military History*, 61, (3), pp. 583-597.

Klein, Bradley S. (1994) *Strategic Studies and World Order.* Cambridge: Cambridge University Press.

Kleinwächter, Wolfgang. (2000) 'Icann as the "United Nations" of the Global Information Society: The Long Road Towards Self-Regulation of the Internet', *International Communication Gazette*, 62, pp. 451-476

Knox, MacGregor and Murray, Williamson (2001) *The Dynamics of Military Revolution, 1300-2050.* Cambridge: Cambridge University Press.

Kramer, Andrew E. (2010) 'Panic in Georgia After a Mock News Broadcast'. The New York Times [online] 14 March. available from < http://www.nytimes.com/2010/03/15/world/europe/15georgia.html > [accessed 14 March 2010]

Kruger, Lennard G. (2005) 'Internet Domain Names: Background and Policy Issues', *Congressional Research Service.* D.C.: Library of Congress.

Lantis, Jeffrey and Howlett, Darryl (2010) 'Strategic Culture' [Baylis, J., Wirtz, J. J., and Gray, C. S. Ed.] *Strategy in the contemporary world: an introduction to strategic studies.*3nd ed. Oxford: Oxford University Press.

Leibold, James (2010) 'More Than a Category: Han Supremacism on the Chinese Internet', *The China Quarterly*, 203, pp. 539-559.

Leonard, Mark (2008) *What Does China Think?* e-book, accessed 21 September 2011, <http://NCL.eblib.com/patron/FullRecord.aspx?p=679935>.

Lessig, Lawrence (1996) 'Reading the Constitution in Cyberspace', *Emory Law Journal*, 45, pp. 869-910.

Lewis, J. A. (2003) *Cyber security: turning national solutions into international cooperation.* Washington, D.C.: CSIS Press, Center for Strategic and International Studies.

Leyden, John (2009) 'Cyberspace becomes battleground in Gaza conflict.' 6 January 2009. *Enterprise Security.* available from <http://www.theregister.co.uk/2009/01/06/idf_al_aqsa_hack/> [accessed 15 January, 2009]

Libicki, Martin C., Frelinger, David R., and Gompert, David C. (1995) *Byting Back-Regaining Information Superiority Against 21st-Century Insurgents.* Santa Monica: RAND Corporation.

Lin, Chong-Bin (1999) *核霸-透視跨世紀中共戰略武力 [Scope of the PRC's strategic Forces]* Taipei: Student Book Co. Ltd.

Liu, Jixiang and Wang, Yimin (2000) *鄧小平軍事理論教程 [The Instruction of Deng's Military Theory]*. Beijing: Military Science Press

Li, J. J. (1998) *Jun Shi Zhan Lue Si We (軍事戰略思維) [Military Strategic Thinking]*. Beijing: Military Science Press.

Li, Hailong (2006) *作戰的非對稱機理研究 [A Study on Operational Asymmetry]* Beijing: National Defense University Press.

Liu, Cricket and Albitz, Paul (2006) *DNS and BIND,* 5th edition. New York: O'Reilly Inc.

Liang (2010) *How China's Cyber Warfare Develops and Conducts* [interview by author] Taoyuan, August 2010

Liao, Wen-Zhong (2007) '中共組建國家網軍進行全球資訊戰 [The PRC Establishes its National Cyber Army to Conduct Global Cyber Warfare]' *解放軍論壇彙編 [The PLA Symposium]* Taoyuan: ROC National Defense University Press.

Libicki, M. C. (2007) *Conquest in cyberspace: national security and information warfare*. Cambridge: Cambridge University Press.

Libicki, Martin C. (2009) *Cyberdeterrence and cyberwar*. Santa Monica: RAND Corporation.

Li, S. and Wang, Y. (2010) 'Report on the Comprehensive National Power Assessment', *Annual Report On International Politics and Security*. [yellow paper] Beijing: Social Science Academic Press. pp. 257-276.

Lien (2010) *How China's Cyber Warfare Develops and Conducts* [interview by author] Taipei, August 2010

Lin (2010) *How China's Cyber Warfare Develops and Conducts* [interview by author] Taoyuan, August 2010

Lin, C. (2010) *How China's Cyber Warfare Develops and Conducts* [interview by author] Taipei, August 2010

Lin, T. (2010) *How China's Cyber Warfare Develops and Conducts* [interview by author] Taipei, August 2010

Liu, Yen (2010) '论魏源"师夷长技以制夷"思想[Study on Wei's Thought of "To Counter Western by What Learning from Western"]' *Journal of Hua Zhang.* Vol. 25. available from < http://mall.cnki.net/magazine/article/HJTS201025012.htm> [accessed 1 November, 2011]

Liu (2010) *How China's Cyber Warfare Develops and Conducts* [interview by author] Taipei, August 2010

Liu (2011) *How China's Cyber Warfare Develops and Conducts* [interview by author] Newcastle upon Tyne, June 2011

Lou, Chin-Bo (2005) *中共「人民戰爭」之解析[The Analysis of the PRC's People's War]*. Unpublished thesis. Hua-Lian: National Dong Hwa University.

Lu (2010) *How China's Cyber Warfare Develops and Conducts* [interview by author] Taoyuan, August 2010

Luke, T. W. (1995) 'Simulated Sovereignty, Telematic Territoriality: The Political Economy of Cyberspace', The Second Theory, Culture & Society Conference. 10th-14th August 1995, USA.

Luke, T. W. (1997) 'Running Flat Out on the Road Ahead: Nationality, Sovereignty and Territoriality in the World of the Informational Superhighway', Annual meeting of the midwest Political Science Association. 10th-13rd April 1997, USA.

Mao, T. D. (1950) *中國革命戰爭的戰略問題[Strategic Problems of Chinese Revolution War]*. Taipei: Revolution Practice Institute.

Mao, T.-t. (1954) *Selected works of Mao Tse-Tung.* Trans. by Lawrence. London: Lawrence & Wishart Ltd.

Mao, T. D. (1991) *毛澤東選集[Selected Work of Mao Ze Dong]*. Beijing: People Press.

Mao I, T. D. (1993) *毛澤東軍事文選[Selected Military Work of Mao Ze Dong II]*. Beijing: Military Science Press.

Mao II, T. D. (1993) *毛澤東軍事文選[Selected Military Work of Mao Ze Dong V]*. Beijing: Military Science Press.

Mao III, T. D. (1993) *毛澤東軍事文選[Selected Military Work of Mao Ze Dong VI]*. Beijing: Military Science Press.

Map of World Official Website. (2008) The Map of Internet Hosts 2008. available from <http://www.mapsofworld.com/thematic-maps/world-internet-hosts-map.html> [accessed 5 March, 2010]

Markoff, John (2007) 'China Link Suspected in Lab Hacking.' *The New York Times* [online] 9th December. available from < http://www.nytimes.com/2007/12/09/us/nationalspecial3/09hack.html> [25th April 2010]

McMichael, William H. (2010) 'DoD Cyber Command Is Officially Online.' *Army Times* [online] 22nd May. available from <http://www.armytimes.com/news/2010/05/military_cyber_command_052110/> [10th November 2010]

Mencius (1970) *The works of Mencius*. trans. by Legge, James. New York: Dover Publications, Inc.

Mi, Zhenyu (2004) *戰爭與戰略理論探研 [Study on Theory of Chinese Wars and Strategy]*. Beijing: People Liberation Army Press.

Miller, H. G. and Murphy, R. H. (2009) 'Secure Cyberspace: Answering the Call for Intelligent Action', *IT Professional,* 11, (3), pp. 60-63.

Miller, Jody, and Barry Glassner (2004) 'The "Inside" and the "Outside": Finding Realities in Interviews.' *Qualitative Research: Theory, Method and Practice.* Ed. David Silverman. London: Sage Publications. p.p. 125-139.

Millett, A. R. (1997) 'A Reader's Guide to the Korean War', *The Journal of Military History,* 61, (3), pp. 583-597.

Mockapetris, Paul (1983) 'Domain Names: Implementation specification', *The Internet Engineering Task Force (IETF).* Available from <ftp://ftp.rfc-editor.org/in-notes/rfc883.txt> [accessed March 23, 2010].

Morgan, Patric (2003) *Deterrence Now.* Cambridge: Cambridge University Press.

Moran, Daniel (2010) 'Geography and Strategy' [Baylis, J., Wirtz, J. J., and Gray, C. S. Ed.] *Strategy in the contemporary world: an introduction to strategic studies.*3nd ed. Oxford: Oxford University Press.

Most, B. A. and Starr, H. (1982) 'Case Selection, Conceptualizations and Basic Logic in the Study of War', *American Journal of Political Science,* 26, (4), pp. 834-856.

Mueller, M., Mathiason, J. and Klein, H. (2007) 'The Internet and Global Governance: Principles and Norms for a New Regime', *Global Governance,* 13, (2), pp. 237-254.

Mulevenon, J.C. and Yang, N.D. (2001) *Seeking Truth from Facts: A Retrospective on Chinese Military Studies in the Post-Mao Era*. Santa Monica: RAND Corporation.

Mulvenon, James C., Tanner, Murray S., Chase, Michael S., Frelinger, David R., Gompert, David C., Libicki, Martin C., and Pollpeter, Kevin L. (2006) *Chinese Responses to U.S. Military Transformation and Implication for the Department of Defense.* Santa Monica: RAND Corporation.

Myers, Steven Lee (2007) 'Cyberattack on Estonia Stirs Fear of "Virtual War."' *The New York Times* [online] 18th May. available from < http://www.nytimes.com/2007/05/18/world/europe/18iht-estonia.4.5774234.html> [20th April 2010]

Niu, Xian-Zhong (1997) *Li Shi yu Zhan Lue(歷史與戰略) [History and Strategy]*. Taipei: Mai-Tien Publisher.

Niu, X. Z. (2003) *西方戰略思想史[History of Western Strategic thought]*. Guangxi: Guangxi Normal University Press.

Niu, X. Z. (2003) *中國戰略思想史[History of Chinese Strategic thought]*. Guangxi: Guangxi Normal University Press.

Nykodym, N. and Taylor, R. (2004) 'The world's current legislative efforts against cyber crime', *Computer Law and Security Report,* 20, (5), pp. 390-395.

Nye, Joseph (2011) 'Cyberspace Wars.' New York: EastWest Institute. [online] 28th February. Available from: <http://www.ewi.info/cyberspace-wars> [accessed 28th February 2011]

O'Dowd, Edward C. (2007) *Chinese Strategy in the Third Indochina War: The Last Maoist War.* New York: Routledge.

OPTE Project Official Website. (2005) The Map of the Internet. available from: <http://www.opte.org/maps/> [accessed 10 March, 2010]

O'Tuathail, G. (1999) 'Borderless worlds? Problematising discourses of deterritorialisation', *Geopolitics,* 4, (2), pp. 139-154.

Pan, Shiying (1992) 'Study on the Theoretical issues of Mao's Military Thought.' *當代中國思想精要*[*Modern Chinese Military Thought]*. Beijing: People Liberation Army Press.

Pan, Zhaohuan (2002) *毛澤東思想研究的歷史進程*[*Study on the historical Progress of Mao's Thought]*. Beijing: People University Press.

Paret, P., Craig, G. A. and Gilbert, F. (1986) *Makers of modern strategy : from Machiavelli to the nuclear age.* Princeton, N.J.: Princeton University Press.

Peng, Guangqian (2000) *鄧小平戰略思想教程[The Instruction of Deng's Strategic Thought]*. Beijing: Military Science Press.

Peng, Guangqian (2001) *戰役學 [Campaign Studies]* Beijing: Military Science Press.

Peng, Guangqian (2006) *中國軍事戰略問題研究[Study on the Problem of Chinese Military Strategy]*. Beijing: People Liberation Army Press.

Peng, Guichuan (2008) 'The Strategic Inspiration from Mao's Military theory.' *毛澤東思想研究 [Maozedong Thought Study]*. No. 4 Vol 25. p.p. 31-34.

People's Liberation Army, PLA (2009) *Operational Training under Complex Electromagnetic Environment.* Beijing: PLA General Staff Department.

People's Liberation Army, PLA (2009) *Transformation of Electronic Warfare.* Beijing: PLA General Staff Department.

People's Daily (2010) '中國空軍民兵條例細則頒布施行 [China's "The Rules and Regulations for the Air Force Militia" Is Enforced].' [online] 30th December. Available from: <http://military.people.com.cn/BIG5/13625379.html> [accessed 28th June 2011]

People's Daily (2010) '大學生思想政治教育 [China's Guideline of "Ideology and Politics Education upon Undergraduate Students"].' [online] 30th January. Available from: <http://edu.people.com.cn/GB/8216/39572/index.html> [accessed 28th August 2010]

People's Liberation Army, PLA (2010) *China's Information [Cyber] Warfare*. Beijing: Xinhua Press.

People's Daily (2011) 'Why China Established "Online Blue Army".' [online] 28th June. Available from: <http://english.peopledaily.com.cn/90001/90780/7423270.html#> [accessed 28th June 2011]

People.Com (2011) '略谈孔子塑像[Confucian Statue]' *People.Com News* [online] 31st January. available from <http://theory.people.com.cn/GB/13856702.html> [3rd November 2011]

Pillsbury, Michael (2008) 'China's Military Space Strategy: An Exchange Response', *Survival Global Politics and Strategy*. 50 (1), p 181.

Ploug, T. and Ebooks Corporation. (2009) *Ethics in Cyberspace.* Dordrecht: Springer.

Polyaenus, Krentz, P. and Wheeler, E. L. (1994) *Stratagems of war.* Trans. by Krentz, Peter and Wheeler, Everett L. Chicago: Ares Publishers INC.

Postel, J. and Reynolds, J. (1984) 'Domain Requirements', *The Internet Engineering Task Force (IETF)*. Available from <http://www.ietf.org/rfc/rfc920.txt> [accessed March 23, 2010].

PRC Ministry of National Defense (2008) *A Report on China's National Defense in 2008*. [online] available from <http://www.mod.gov.cn/big5/gwgb/2009-01/21/content_3055010.htm> [10 December 2009]

PRC State Council (2002) *China's National Defense 2002*. [white paper] Beijing: The State Council Office. Available from <http://www.gov.cn/zwgk/2005-05/26/content_1384.htm> [15 October 2010]

PRC Ministry of National Defense (2004) *A Report on China's National Defense in 2004*. [online] available from <http://www.mod.gov.cn/big5/gwgb/2004-12/27/content_3054940.htm> [5 December 2009]

PRC State Council (2006) *The Strategy of the Development of National Informationalization 2006-2020*. [white paper] Beijing: The State Council Office. Available from <http://news.xinhuanet.com/newscenter/2006-05/08/content_4522878.htm> [15 November 2010]

PRC State Council (2011) *China's National Defense 2010*. [white paper] 31st March. Beijing: The State Council Office. Available from <http://www.gov.cn/jrzg/2011-03/31/content_1835289.htm> [accessed 1st April 2011]

PRC State Council (2011) *China's Peaceful Development*. [white paper] 6th September. Beijing: The State Council Office. Available from <http://big5.gov.cn/gate/big5/www.gov.cn/zwgk/2011-09/06/content_1941258.htm> [accessed 21st September 2011]

Qiao, Liang and Wang, Xiangsui (1999) *超限戰 [Unrestricted Warfare]*. Beijing: The PLA Press.

Rattray, Gregory J. (2001) *Strategic Warfare in Cyberspace*. Cambridge: The MIT Press.

Rawnsley, Gary D. (2005) *Political Communication and Democracy*, e-book, accessed 29 September 2011, <http://NCL.eblib.com/patron/FullRecord.aspx?p=285608>.

Repperger, D. W., Haas, M. W., McDonald, J. T. and Ewing, R. L. (2008) 'Cyberspace and Networked System – Paradigms for Security and Dynamic Attacks', *Aerospace and Electronics Conference, 2008. NAECON 2008. IEEE National.*

ROC Ministry of National Defense (2010) *ROC's [Taiwan] National Defense 2009*. [white paper] Taipei: ROC Ministry of National Defense. available from <http://www.mnd.gov.tw/Default.aspx> [accessed 1st April 2011]

Ross, Robert S. (2009) *Chinese Security Policy: Structure, Power and Politics*. London: Routledge.

Rosoff, Matt (2011) 'Apple Now Has More Cash Than The U.S. Government.' *Business Insider*. [online] 28th July. available from <http://www.businessinsider.com/apple-has-more-cash-on-hand-than-the-us-government-2011-7> [25th September 2011]

Rowe, N. C., Duong, B. T. and Custy, E. J. (2006) *Information Assurance Workshop, 2006 IEEE*.

Sanger, D., Markoff, J. and Shanker, T. (2009) 'U.S. Steps Up Effort on Digital Defenses.' *The New York Times* [online] 27th April. available from <http://www.nytimes.com/2009/04/28/us/28cyber.html> [25th September 2010]

Sawyer, R. D. and Sawyer, M. -c. n. (2007) *Wu Jing Chi Shu [The Seven Military Classics of Ancient China]*. trans. by Sawyer, R. D. and Sawyer, M. -c. n. New York: Perseus Books Group.

Schmitt, C. (1996) The concept of the political. Chicago, Ill. ; London: University of Chicago Press.

Schwartz, John. (2001) 'A Nation Challenged: The Computer Networks; Cyberspace Seen as Potential Battleground.' 23 November 2001. *The New York Times.* available from <http://query.nytimes.com/gst/fullpage.html?res=9F00E3DD153AF930A15752C1> [accessed 14 January, 2010]

Schiff, Rebecca L. (2008) *The Military and Domestic Politics: A Concordance Theory of Civil-Military Relations*. e-book, available from: <http://NCL.eblib.com/patron/FullRecord.aspx?p=355877> [accessed 05 August 2011]

Scobell, Andrew (2002) *China and Strategic Culture.* Pennsylvania: Army War College Press.

Scobell, Andrew. Kamphaysen, R. and Tanner T. (2008) *The 'People' in PLA: Recruitment, Traning, and Education in China's Military.* Pennsylvania: Army War College Press.

Segal, Adam (2011) *The Chinese Way of Hacking* [interview by Neal Ungerleider], New York. 13th July 2011. Available from:<http://www.cfr.org/experts/india-china-economics/adam-segal/b8863> [accessed 4th August 2011]

Sevastopuloin, Demetri and McGregor, Richard (2007) 'China "Hacked" into Pentagon Defence System.' *Financial Times* [online] 4th September. available from <http://www.ft.com/cms/s/0/4f25940e-5a7e-11dc-9bcd-0000779fd2ac.html> [25th October 2010]

Shambaugh, David L. (1996) 'China's Military in Transition: Politics, Professionalism, Procurement and Power Projection', *The China Quarterly* 146, p 274.

Shambaugh, David (1999) 'The People's Liberation Army and the People's Republic at 50: Reform at Last', *The China Quaeterly* 159, p 663

Shambaugh, David L. (2004) *Modernizing China's Military: Progress, Problems and Prospects*. LA: University of California Press.

Shambaugh, David L. (2008) 'Training China's Political Elite: The Party School System', *The China Quarterly* 196, p.p. 827-844.

Shambaugh, David (2009) 'The Road to Prosperity', [28 September 2009] *Time International*. Available from <http://www.time.com/time/printout/0,8816,1924366,00.html/> [accessed November 15, 2009].

Sharp, Gene (1990) *Civilian-Based Defense* Princeton: Princeton University Press.

Shen, Weiguang (1990) *新戰爭論 [Theory of New Warfare]* Hangzhou: Zhejiang University Press.

Shen, Weiguang (2005) *中國信息戰 [Chinese Information Warfare]* Beijing: Xin Hua Publisher.

Sheng, Jie and Wan, Tong (2006) *Sun Zi Bing Fa(孫子兵法) [Study on The Art of War]*. Taipei: Han Yu International Press.

Shen, S. (2007) *Redefining Nationalism in Modern China: Sino-American Relations and the Emergence of Chinese Public Opinion in the 21st Century*. e-book, accessed 11 October 2011, <http://NCL.eblib.com/patron/FullRecord.aspx?p=367926>.

Shen (2010) *How China's Cyber Warfare Develops and Conducts* [interview by author] Taoyuan, August 2010

Shambaugh, David L. (2009) *China's Communist Party*. LA: University of California Press.

Silverman, David. (1994) *Interpreting Qualitative Data: Methods for Analysing Talk, Text, and Interaction.* 2nd ed. London: SAGE Publications Ltd.

Singer, J. D. a. S. and Small, M. (1972) The wages of war, *1816-1965: a statistical handbook*. New York, London: Wiley.

Snyder, Jack L. (1977) *The Soviet Strategic Culture: Implications for Limited Nuclear Operations.* Santa Monica: RAND Corporation.

Slouka, M. (1996) *War of the Worlds: Cyberspace and the High-tech Assault on Reality*. Basic Books.

Steinert, Heinz (2003) 'The Indispensable Metaphor of War: On Populist Politics and the Contradictions of the State's Monopoly of Force', *Theoretical Criminology*, 7, (3) pp. 265-291.

Strate, Lance (1999) 'The varieties of cyberspace: Problems in definition and delimitation', *Western Journal of Communication*, 63, (3), pp. 382-412.

Sun, Tzu (1971) *Sun Zi Bing Fa(孫子兵法) [The Art of War]*. trans. by Griffith, S. B. Oxford: Oxford University Press.

Swane, Michael D. and Tellis, Ashley J. (2000) *Interpreting China's Grand Strategy.* Santa Monica: RAND Corporation.

Tkacik, John Jr. (2007) *Trojan Dragons: China's International Cyber Warriors.* [online] 12th December. Washington D.C.: The Heritage Foundation. available from <http://www.heritage.org/research/reports/2007/12/trojan-dragons-chinas-international-cyber-warriors> [20th October 2010]

Toffler, Alvin and Heidi (1993) *War and Anti-War: Survival at the Dawn of the 21st Century.* Boston: Little, Brown and Company.

Tai, Z. and Ebooks Corporation. (2006) *The Internet in China: Cyberspace and Civil Society*. Hoboken: Routledge.

The Office for National Statistics. The Statistics of Internet Access in UK. available from <http://www.statistics.gov.uk/cci/nugget.asp?id=8> [accessed 16 March, 2010]

The U.S. White House (2009) *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*. Washington D.C.: White House.

The U.S. Congress Research Service. (2009) *Cyberspace Policy Review.* Washington D.C.: Library of Congress

The Epoch Times (2010) '北京的網路戰爭[Beijing's Cyber Warfare]' [online] 4th December. Available from: <http://tw.aboluowang.com/comment/data/2010/1204/article_17984.html> [accessed 4th December 2010]

The White House (2011) *International Strategy for Cyberspace*. [white paper] The White House: Washington, D.C.

The Epoch Times (2011) '北京高層徹底斷絕網絡[Beijing Authority Determines Disconnecting Internet Network]' [online] 13rd March. Available from: <http://www.epochtimes.com/b5/11/3/13/n3195925.htm> [accessed 14th March 2011]

The Economist (2011) 'Internet Freedom: Tort and Technology.' [online] 21st July. Available from: <http://www.economist.com/node/18986482?story_id=18986482&fsrc=rss> [accessed 3rd August 2011]

Thomas, Timothy L. (2000) 'Like Adding Wings to the Tiger: Chinese Information War Theory and Practice.' *Military Review.* Fort Leavenworth: USA Foreign Military Studies Office. available from < http://www.iwar.org.uk/iwar/resources/china/iw/chinaiw.htm> [25th October 2010]

Thomas, Timothy L. (2001) 'China's Electronic Strategies.' *Military Review.* Fort Leavenworth: USA Foreign Military Studies Office. available from < http://fmso.leavenworth.army.mil/documents/china_electric/china_electric.htm> [20th October 2010]

Thomas, Timothy L. (2004) 'Dragon Bytes: Chinese Information War Theory and Practice.' *Military Review.* Fort Leavenworth: USA Foreign Military Studies Office.

U.S. Doctrine (1995) *Joint Doctrine for Military Operations Other Than War.* Joint Education and Doctrine at Department of Defense in USA. Available from: <http://www.globalsecurity.org/military/library/policy/army/fm/100-7/f1007_13.htm> [accessed 4th April 2011]

U.S. Department of Defense (DoD) (2002) *Annual Report to Congress: Military Power of the People's Republic of China.* [white paper] Washington D.C.: The Office of the Secretary of Defense. Available from < http://www.globalsecurity.org/military/library/report/2002/d20020712china.pdf > [10 October 2010]

U.S. Department of Defense (DoD) (2006) *Annual Report to Congress: Military Power of the People's Republic of China.* [white paper] Washington D.C.: The Office of the Secretary of Defense. Available from < http://www.globalsecurity.org/military/library/report/2006/2006-prc-military-power.htm> [10 November 2010]

USCC Report (2009) 'China's Cyber Activities that Target the United States, and Resulting Impacts on U.S. National Secuirty.'*2009 Report to Congress of the US-China Economic and Security Review Commission.* [white paper] Washington D.C.: the US-China Economic and Security Review Commission. Available from <http://www.uscc.gov/annual_report/2009/09report_chapters.php> [29 October 2010]

U.S. Department of Defense (DoD) (2010) *Annual Report to Congress: Military and Security developments Involving the People's Republic of China 2010.* [white paper] 31st March. Washington D.C.: Office of the Secretary of Defense. Available from <http://www.globalsecurity.org/military/library/report/2010/2010-prc-military-power.htm> [accessed 1st April 2011]

U.S. Department of Homeland Security (DHS) (2010) *Cyber Storm: Securing Cyber Space*. [white paper] Washington D.C.: The Department of Homeland Security. Available from <http://www.dhs.gov/files/training/gc_1204738275985.shtm > [12 November 2010]

U.S. Air Force (2010) *Cyberspace Operations.* [doctrine document] Washington D.C.: The Office of the Secretary of Air Force. 15th July. Available from <http://www.fas.org/irp/doddir/usaf/afdd3-12.pdf> [20 November 2010]

U.S. Department of Defense (2011) *Annual Report to Congress: Military and Security developments Involving the People's Republic of China 2011*. [white paper] 24th August. Washington D.C.: Office of the Secretary of Defense. Available from <http://www.defense.gov/pubs/pdfs/2011_CMPR_Final.pdf> [accessed 24th August 2011]

U.S. Department of Defense (2011) *Strategy For Operating in Cyberspace.* [white paper] 14th July. Washington D.C.: Office of the Secretary of Defense. Available from < www.defense.gov/news/d20110714cyber.pdf> [accessed 21st July 2011]

Virilio, Paul (2000) *The Kosovo War Took Place In Orbital Space* [interviewed by John Armitage] Paris, 18 October 2000. Available from <http://www.ctheory.net/articles.aspx?id=132#bio > [accessed March 20, 2010]

Walsh, Lucas and Barbara, Julien (2006). 'Speed, international security, and "new war" coverage in cyberspace', *Journal of Computer-Mediated Communication*, *12*(1), pp. 189-208.

Wallis, Gavin (2006) Office for National Statistics. Internet Spending: Measurement and Recent Trends. available from <http://www.statistics.gov.uk/articles/economic_trends/ET628InternetSpending.pdf> [accessed 16 March, 2010]

Wang, P. (1998) *Modern Military Theory*. Beijing: Xin hua Press, China. p2.

Wang, PuFeng (1999) *毛澤東軍事戰略教程 [The Instruction of Mao's military Strategy]*. Beijing: Military Science Press.

Wang, Hongxu (2011) '中国共产党领导人的外交理念及其文化渊源[The cultural origins of CCP's Leadership].' *當代世界 The Contemporary World.* 24th August. Available from: < http://www.bjqx.org.cn/qxweb/n33004c7.aspx> [accessed 31th October 2011]

Wang, Jiang-Nan (2007) *論中共資訊權力 [The PRC's Information Power]*. Unpublished thesis. Taipei: Tamkang University.

Weller, Toni (2011) *Information History in the Modern World: Histories of the Modern Age.* Basingstoke: Palgrave Macmillan.

Wen, Jiabao (2010) *The New Challenge from China.* [interviewed by Fareed Zakaria] New York, 3 October 2010. Available from *Time October 18 2010.*

West, Ian J. (2010) *The Forces Awakening to the Need for Cyber Security* [interviewed by Defence Forum] London, 9 March 2010. Available from <http://www.defenceiq.com/video.cfm?id=622&mac=DFIQ_OI_Featured_2010&utm_source=defenceiq.com&utm_medium=email&utm_campaign=DefOptIn&utm_content=3/11/10> [accessed March 12, 2010]

WikiLeaks (2010) 'Google China Paying Price for Resisting Censorship.' *USA Diplomatic Cable* on 18th May 2009. Available from: <http://www.wikileaks.ch/wiki/Main_Page> [accessed 4th April 2011]

Wong, Ming-Xien (2007) *Theory of New Chinese Strategy*. Taipei: Wu-Nian Publisher.

Wong, Zaibong (2011) '和平发展白皮书体现中国的思想和传统[The White Paper of China's Peaceful Development Reflects Chinese Traditions]' *China's Daily* [online] 14th September. available from <http://www.chinadaily.com.cn/zgrbjx/2011-09/14/content_13679776.htm> [3rd November 2011]

Wu (2010) *How China's Cyber Warfare Develops and Conducts* [interview by author] Taipei, August 2010

Xia, YiBing (1999) '中國的太空之路 [The Chinese Road Towards Space]' *廣角鏡月刊 Guang Jiao Jing Jurnal.*

Xiao, ZhiLin and Hu JianGan (2004) *江澤民軍事創新思想研究[Study on Jiang's Creative Military Thought]*. Beijing: Military Science Press.

Xin Hua News (2010) '美軍網戰兵力 [The US military Capability of Cyber Warfare]' *Xin Hua News* [online] 25th August. available from <http://news.xinhuanet.com/observation/2010-08/25/c_12483327.htm> [10th November 2010]

Xin Hua News-1 (2010) '胡锦涛:在全党深入学习实践科学发展观活动总结大会上的讲话 [Hu Jintao's Speech]' *Xin Hua News* [online] 6th April. available from <http://news.xinhuanet.com/politics/2010-04/06/c_1219752.htm> [31th October 2011]

Xin Hua News (2011) 'Chinese State Councilor Dai Bingguo: China will unswervingly follow path of peaceful development' *Xin Hua News* [online] 25th September. available from <http://news.xinhuanet.com/english2010/china/2011-09/25/c_131159052.htm> [25th September 2011]

Xiong, GuanKai (2003) *國際戰略與新軍事變革 [International Strategy and New Military Reforms]* Beijing: Qing Hua University Press.

Xiu, Mingshan and Fang, Yonggang (2007) *新世紀新階段中國國防和軍隊建設 [China's National Defense and Army Construction in the New Era]*. Beijing: People Press.

Xu, Keqian (2009) '儒家思想与中国传统文化的价值优先观[Comparative value of Confucian Thought and Chinese Traditional Culture]' *Confucian Studies*. Vol.2. available from < http://www.confucius2000.com/admin/list.asp?id=4547> [31th October 2011]

Xu (2010) *How China's Cyber Warfare Develops and Conducts* [interview by author] Taoyuan, August 2010

Yang, Kai-Huang (2000) '台灣「大陸研究」回顧 [Review on Taiwanese China Studies]', *Soochow Journal of Political Science* vol 11, p.p. 71-105.

Yang (2010) *How China's Cyber Warfare Develops and Conducts* [interview by author] Taoyuan, August 2010

Yan, Fang-Bin (2010) *How China's Cyber Warfare Develops and Conducts* [interview by author] Taipei, August 2010

Yan, Xuetong (2011) '中国行为根源[The Source of Chinese Conduct]' *Xin Hua News* [online] 31st March. available from < http://www.chinanews.com/hb/2011/03-31/2943520.shtml> [3rd November 2011]

Yan, Xuetong, Bell, Daniel A., Zhe, Sun, and Ryden, Edmund (2011) *Ancient Chinese Thought, Modern Chinese Power.* e-book, accessed 03 November 2011, <http://NCL.eblib.com/patron/FullRecord.aspx?p=664619>.

Yang, Jiemian (2011) '中國共產黨和中國外交理論新發展[New Development of CCP and China's Foreign Theory]' *People.Com News* [online] 4th July. available from <http://theory.people.com.cn/BIG5/15066912.html> [3rd November 2011]

Yao (2010) *How China's Cyber Warfare Develops and Conducts* [interview by author] Taipei, August 2010

Ye, Zheng (2001) *陸軍戰役學教程 [Instruction of Army Campaign Studies]* Beijing: The Academy of Military Science.

Yu, Xiaohwa and Zhou, Bison (2001) *電子空間：網路信息戰 [Electronic Space: Cyber & Information Warfare]* Beijing: The PLA Press.

Yu (2010) *How China's Cyber Warfare Develops and Conducts* [interview by author] Taoyuan, August 2010

Yuan, Dejin (2000) *毛澤東軍事思想教程[The Instruction of Mao's military Strategy]*. Beijing: Military Science Press.

Zhang, Jayu. (1997) *人民戰爭[People's War]*. Beijing: Military Science Press.

Zhang, Zhen (1997) *軍事科學[Chinese Military Science]*. Beijing: Military Science Press.

Zheng, Da-Cheng (2001) Analysis for the Military Theory of Jiang Zhemin. *陸軍學術月刊[The Army Academic Journal]*. Taoyuan: ROC[Taiwan] Army Command Headquarters.

Zheng, Da-Cheng (2008) '中共網軍發展與評估 [The Development and Evaluation of the PRC's Cyber Army]', *空軍學術月刊[The ROC Air Force Academic Journal]* 606, p.p. 3-15. Taipei: ROC Air Force Command Headquarters.

Zheng, Yongnian (2009) *全球化與中國國家轉型[Globalisation and State Transformation in China]* Hangzhou: Zhejiang People's Press.

Zheng, Yongnian (2011) *中國模式：經驗與困局[*Chinese Model: Experiences and Difficulties*]* Hangzhou: Zhejiang People's Press.