China's Emergence as a Cyber Power

Munish Sharma*

Cyberspace is increasingly becoming an area of contestation among nation states. Similar to the physical domains of land, sea, air and space, superiority in the cyber domain enables a nation state to exert its cyber power. In recent years, China has invested colossal amounts in building the requisite infrastructure and capabilities of its armed forces as well as governance practices to advance towards 'informationalisation'. This article seeks to discern the motives, threats, objectives, strategy and intent that drive China to amass cyber power.

> We should attach great importance to maritime, space and Cyberspace security. We should make active planning for the use of military forces in peacetime, expand and intensify military preparedness, and enhance the capability to accomplish a wide range of military tasks, the most important of which is to win local war in an information age.
>
> – Hu Jintao[1]

The world today is intertwined in the cyber realm, exchanging information and ideas in real time. The last decade-and-a half has witnessed an exponential rise in the use of cyberspace, including services in the form of e-mail, social networking, instant messaging, search engines, banking, e-governance, e-commerce and so on. The benefits of cyberspace are harnessed by individuals, business enterprises and governmental bodies. On the other hand, arduous competition among the growing as well as developed economies is compelling nation states to exercise their power

* Munish Sharma is an Associate Fellow with IDSA.

ISSN 0976-1004 print

Journal of Defence Studies, Vol. 10, No. 1, January–March 2016, pp. 43–68

in the cyberspace to secure their interests. The intellectual property, secure communication channels, data pertaining to national security, and research in strategic areas or technology are at persistent risk from a plethora of threats. The threats and challenges increase manifold when the military dimension is added to cyberspace.

Cyberspace has become an intrinsic part of the national power constituents, namely, military, economy, diplomacy and technology. This phenomenon has made cyberspace an area of contest where nation states are willing to gain superiority in order to establish themselves as a cyber power. In February 2014, Chinese President Xi Jinping called for collective efforts to build China as a cyber power. The statement holds salience as China is steadily picking up pace in the development of its science and technology base, and its intention to dominate cyberspace is evident from the support of the country's political leadership. The concept of cyber power needs analysis with reference to China's aspirations to be a cyber power, which is quite relevant amidst the investments in infrastructure and capabilities under the auspices of its armed forces.

Nation states have documented their cyber strategies and executed them in the form of cyber commands. This opens up a war front in cyberspace, where nation states try to exert their power to gain control or to maintain their access to cyberspace. Hence, the concept of cyber power has emerged, in accordance with the likes of airpower or maritime power. It takes ample time to develop capability and exhibit the intent to exert power in a given domain of warfare.

Wars have historically been fought in two domains—the land and the sea. In the beginning of the twentieth century, the domains of warfare extended to air and later on, by the middle of the century, Space emerged as the fourth domain. The beginning of the twenty-first century witnessed evolution of cyber as the fifth domain of warfare. The military operations are increasingly becoming network centric, with the integration of platforms and efficient exploitation of the electromagnetic spectrum. The dominance has percolated into the information sphere where a nation state or a non-state actor has the ability to manipulate, deny, steal, and even destroy information which is critical to decision-making. In order to defend national interests and attain national power, nation states tend to develop military capabilities, such as, navy for sea power projection, army for land power and air force for airpower.[2] These powers are instrumental for nation states to establish control and wield influence across the domains as means to realise their objectives.

Over the years, China has demonstrated its intent, while bridging the immense gaps in its capability. An assessment of China's cyber power is requisite against the background of the 2013 edition of *The Science of Military Strategy*, a document published by the People's Liberation Army (PLA), but translated recently. Generally, cyber strategy documents provide a peek into the present and future of warfare in the cyberspace, and provide information to analysts for assessments. This document, published 'once a generation', is authored by top-ranking generals of the PLA, who are members of the Academy of Military Sciences—the premiere research institute of the PLA—having very close ties with the Central Military Commission.[3] According to *The Diplomat*, this is the first time this document has included an entire chapter on cyber war, elaborating various military operations feasible in the cyberspace: network reconnaissance, network defence, network attack and network deterrence.[4]

The Essentials of a Cyber Power

American naval strategist, Alfred T. Mahan, propounded the concept of sea power, elaborating the imperatives of naval supremacy.[5] Somehow, a clear definition of the term 'sea power' was never put across. Similarly, Giulio Douhet never defined 'airpower', although the work built scenarios to demonstrate the impact of airpower on the warfare of future.[6] But all these concepts converge on the point that power in the respective domains was primarily the ability to use and exploit the physical environments, the sea or the air, to extend the sphere of influence on the land or high seas. Correspondingly, cyber power can be defined as: 'the ability to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of power.'[7] According to Joseph Nye, in behavioural terms, cyber power is 'the ability to obtain preferred outcomes through use of the electronically interconnected information resources of the cyber domain.'[8]

Drawing correlation from the concept of national power, which 'involves the capacity to use force or threat of the use of force over other nations',[9] as nation states become more dependent upon their information infrastructure, cyber power can capacitate a nation to use cyber offence or threat of the use of cyber offence over other nations to attain political, economic or military objectives. Although cyberspace is in the virtual realm, physical entities are dependent on it, and hence it

can be an instrument to influence the decision-making of others without the use of physical force.

Li Zhang, Director of the Institute of Information and Social Development Studies at the China Institutes of Contemporary International Relations, defines cyber power as 'a country's capability to both take action and exert influence in cyberspace.'[10] In a 2012 article,[11] Li has listed down seven essential factors that make cyber power. These are:

1. *Internet and information technology (IT) capabilities*: The capability of a nation state to conduct research and development in IT, and promote innovation and application of research into industry, so that these technologies can transform the industrial and business processes.
2. *IT industry capabilities*: The existence of global IT industry leaders in a nation state is a definite parameter of cyber power. The United States (US) is home to a majority of IT industry leaders, across every segment of hardware, software or networking equipments, having global footprint under the names of IBM, Microsoft, Intel, Google, Cisco and Apple. These global IT giants are way ahead of their next competitors, having monopolistic hold on their respective segment of products, applications or services.
3. *Internet market capabilities*: The size and scale of the domestic Internet infrastructure is a major push factor. It consists of the number of Internet users, the number of computers owned, how well is the Internet infrastructure integrated, use of Internet in governance and so on.
4. *The influence of Internet culture*: The reach and penetration of the Internet has triggered behavioural changes in the populace. The Internet is being used for diverse uses in communication, networking, learning and so on. The degree of influence on behaviour, exerted by the Internet culture, provides a glimpse of how well the society is integrated with it.
5. *Internet diplomacy/foreign policy capabilities*: This is the bargaining power of a nation state and its ability to influence the modern multilateral or multi-stakeholder platforms for Internet governance, such as, the Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet Governance Forum and International Telecommunication Union (ITU). This factor regards the extent to which a nation state can play a leading role in Internet governance, security and its future.

6. *Cyber military strength*: It consists of the ability to defend critical national and military IT infrastructure from attacks, deterrent capability, the ability to conduct offensive operations in cyberspace and the ability to prevent own networks from espionage.
7. *National interest in taking part in a cyberspace strategy*: In order to be a cyber power, it is not sufficient for a nation state to merely possess part or all of the capabilities. It depends upon the motive or willingness to use the possessed power. The cyberspace strategy for a nation state must lay down the theoretical guidance, behavioural norms/criteria for action and a strategic plan.

Although a nation state might possess the resources and capabilities, but the intention to leverage the capability in order to support its political goals establishes it as a cyber power. A capable cyber power should be able to use cyberspace for 'exploitation' of targets bearing economic and political imperatives; 'disruption' of services through distributed denial of service (DDoS) attacks or malware; or in extreme case, 'destruction' of the physical or cyber infrastructure in the case of an eventuality. Power is an outcome of multiple factors and is shaped by the interplay of these factors. Organisational factors play a prominent role because the organisations reflect purposes, objectives and perspectives of power. In the case of cyber power, perspective of a nation state on its creation would be shaped by the organisational mission, be it military, economic or political. China's presence in cyberspace has generated strategic and academic discourse, but its emergence as cyber power remains to be analysed. There is a need for thorough assessment of whether the Chinese perspective of cyber power is shaped by military, economic or political imperatives, and to what extent.

China as a Cyber Power

Deng Xiaoping once said, 'to be rich is glorious'. The statement is an accurate explanation of Chinese behaviour. He sanctioned illicit technology acquisition; later on, Jiang Zemin sanctioned cyber espionage, making it a commercial activity supporting the growth of its business houses and in turn, its economy. The emergence of China in both global and regional contexts has triggered intense competition in economic sphere for market expansion and control over depleting resources, culminating into economic warfare.[12]

The use of economic warfare 'involves a deliberate strategy on the part of the state to restrict or manipulate trade, financial markets and access to technology to harm an opponent.'[13] China's foreign policy practices are propelled by its intense need to secure energy, metals[14] and strategic minerals in order to support the rising living standards of its immense population. China has continuously been accused of espionage to acquire the latest technology to catch up with and surpass the technologically advanced countries of the West, both economically and militarily. Recently, attempts of espionage have been made in the cyberspace as well.

The roots of China's present-day 'informatisation' can be traced back to 1982, when the State Council, the Cabinet, founded a leading group to steer the development of computers and large-scale integrated circuits, under the leadership of the then vice premier.[15] Over the last three decades, China has emerged as the world's largest population of Internet users, demanding infrastructure and services supporting the vast demand of the user base. In terms of its contribution to the global IT market, China has cultivated IT companies with global footprint, such as Tencent and Alibaba. But given the extent and volume of domestic market, the sector needs structural changes and further improvement. It is supported by the fact that the ITU ranks China 86th in the world on ICT Development Index for 2014.[16] Nevertheless, the government has swung into action to bridge the gap; a high-level Internet Security and Informatization Leading Group is anticipated to be a giant leap in this direction.

The radical changes in the military doctrine and strategy of the PLA were brought in after the Gulf War of 1991. The leadership, both political and military, realised the shortcomings of the armed forces in terms of its size and warfighting techniques.[17] The Chinese military leadership studied American warfighting meticulously. The Gulf War, the subsequent Kosovo War and the invasion of Afghanistan and Iraq, all gave the PLA enormous opportunities to analyse the successes and failures of the US armed forces. The then Chairman, Jiang Zemin, brought in revolution in military affairs (RMA) under the ambit of the official National Military Strategy in 1993, with the objective of building the PLA into a force capable of winning 'local wars under high-tech conditions or the conditions of informationization'.[18] Military analysts in the US deemed this to be a Chinese effort to achieve strategic parity with the West, focusing heavily on acquiring advanced

military technology. One such analysis suggested that there are two characteristics of China's military modernisation efforts:[19] (a) the PLA, primarily a ground force and more adept at executing war operations in the Chinese interior, is being transformed to defend China's interests in its geographical proximity or periphery; and (b) the force is becoming adroit at superior military hardware in all the wings of army, navy and air force, with access to precision strike weapons and command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) for improved situational awareness. Both the above-mentioned factors are driven by emphatic investments in the science and technology infrastructure, revamped defence manufacturing industry and procurement of advanced weaponry from abroad.

'Informatisation' in the PLA: China's National Defence Policy

China's Internet Security and Informatization Leading Group is charged with bringing out a cyber strategy for China. Premier Li Keqiang and Liu Yunshang, First-ranked Secretary of the Central Secretariat, both serve as the deputy heads of the Internet group. The fact that the group includes the top leadership demonstrates China's deep interest in cyberspace activities at both domestic and international fronts, with commitment to develop infrastructure and human resources.[20]

On 27 February 2014, Chinese President Xi Jinping took over as the head of Central Internet Security and Informatization Leading Group. The political leadership of China has demonstrated its aspirations to pursue 'informatisation' as high priority and has laid great emphasis on 'informatisation' of public services and economy. Stating that 'Efforts should be made to build our country into a Cyber Power',[21] Xi has stressed upon cyber power to be a national priority for China to reach its economic, societal and military potential. He has called on the army to create a new strategy for 'information warfare', which would require the army 'to establish a new military doctrine, institutions, equipment systems, strategies and tactics and management modes for information warfare.'[22]

The leadership has addressed to the need to move China from a 'big' network country to a 'strong' cyber power, listing down six indicators of cyber power: [23]

1. Infrastructure, including network size and broadband penetration.

2. A clear international strategy that lays out priorities and defends China's right to have a voice on cyber issues.
3. Independent technological capabilities, especially in the areas of operating systems and central processing units.
4. The ability to defend networks, be it for national security, economic security, user privacy, or social stability and harmony.
5. Competitiveness in the development of software applications, e-commerce, and online markets.
6. Occupying the 'commanding heights' of Cyberspace.

The white papers of the Chinese government on National Defence Policy suggest that the military leadership aspires to build the PLA into 'a lean and strong military force the Chinese way'.[24] The white papers published in 2000, 2002, 2004, 2006, 2008 and 2010 explain their motivation to enhance the quality and strengthen the armed forces by relying on science and technology, and transform to a qualitatively superior technology-intensive armed force.[25]

The logistical work of the Chinese armed forces is also undergoing transformation and it is being integrated and evolved into combined logistics for all the services and arms, under the high-tech conditions. The white paper issued in the year 2000 stated: 'The Chinese armed forces will, in the course of modernizing their weaponry, devote themselves to transforming semi-mechanized and mechanized weapon systems to automatized and informationized systems as soon as possible.'[26]

It is evident from the papers that China is conscientious about the application of advanced technologies led by IT, which has 'stretched the battlefield into multidimensional space, which includes the land, sea, air, outer Space and electron'.[27] The warfare is increasingly becoming information oriented and all major military powers across the globe have rolled out modernisation plans as well as amended their military strategies in accordance with the new technologies and operational challenges.[28]

The 2004 white paper on National Defence Policy makes a mention about worldwide RMA, which is leading to a change in forms of war, from mechanisation to informatisation. The white paper has emphasised on the readjustments in the security and military strategies of major countries across the globe, compelled by the changes in their military doctrines. The paper has pressed on the need for speeding up informatisation, and making it the orientation and strategic focus of the modernisation drive of the PLA, and takes stock of progress in the process of informatisation at the operational level, which focuses on command automation.

On similar lines, the white paper of 2008 on National Defence Policy has laid down the strategic plans for national defence: setting up a target for informatisation by 2020; and modernisation of national defence and armed forces by the mid-twenty-first century.[29] The paper has stated that the priority is being given to command information systems, and the focus was to 'increase the capability of the main battle weapon systems in the areas of rapid detection, target location, friend-or-foe identification and precision strikes.'[30]

China's armed forces firmly base their military preparedness on winning local wars under the conditions of informatisation.[31] The armed forces, functioning under the auspices of the governing principles, aim to promote their preparedness through coordination in all strategic directions, intensifying the joint employment of different services and arms, and enhancing warfighting capabilities based on information systems.[32] The last 15 years of white papers on National Defence Policy bring up the underpinnings of the Chinese behaviour in cyberspace in general, and its aspirations to be a cyber power in particular. The endeavour is spearheaded by the military leadership, while resources in the form of technology development and human resources are pooled in from public and private sectors.

The geopolitical developments in the surrounding areas and the changes brought in by IT at the levels of military strategy and doctrine have shaped the modernisation efforts of the PLA. The PLA envisions a lean and agile armed force, well-connected command and troops on the ground, robust information infrastructure and automatised and informatised main battle weapon systems, supporting integrated joint operations. It is gearing up to engage in localised wars, probably in its geographical vicinity, under high-tech conditions or conditions of informatisation. It would be feasible when China has substantial expertise in development of digitised weapon systems and information infrastructure for communication, a pertinent indicator of a cyber power.

Cyber Exploitation and Cyber Espionage

The first instance of a hacker war between China and Taiwan erupted in 1999, as a backlash to the suggestion made by the President of Taiwan for state-to-state relations between mainland China and the island. The Chinese hackers retorted in form of defacements of websites belonging to the Government of Taiwan.[33] Again, in 2003, Chinese hackers were

able to penetrate the computer networks of the governmental agencies of Taiwan, notably the Ministry of Defence, Election Commission and the National Police Administration. A year later, similar intrusions surfaced in the computer networks of Taiwanese Ministry of Finance and Kuomintang Party.[34]

There have been numerous instances of cyber espionage where economic imperatives are clearly evident. A massive cyber espionage ring surfaced in 2004 in the US, where hackers were able to intrude into the networks of organisations affiliated to the defence industry, such as Lockheed Martin, Sandia National Laboratories, Redstone Arsenal and National Aeronautics and Space Administration (NASA). This series of carefully coordinated attacks on the computer networks and defence systems, which probably lasted for three years, was designated by the government as Titan Rain Attacks.[35]

In 2008, some of the US and European energy companies, including British Petroleum, Royal Dutch Shell, Exxon Mobil and ConocoPhillips, faced cyber attacks, compromising information regarding oil and gas field bids.[36] In 2009, the US reported a hack into the servers of defence contractor Lockheed Martin, which were housing information related to the Joint Strike Fighter Aircraft F-35. The investigators suspected China to be behind the attacks.[37] The gathered information pertaining to bids or weapon system designs could be leveraged in the interests of the state while competing for oil fields or development of indigenous technology.

There are numerous cases of insiders, primarily employees of private companies, found carrying or in possession of proprietary information, allegedly for the purpose of transferring to China.[38] The report by the cyber security firm, Mandiant, in 2013, stated that the Chinese PLA[39] is responsible for an array of cyberattacks through a specialised Shanghai-based unit known as Unit Number 61398.[40] The growing capabilities of China and the intention to use cyber espionage have raised alarm bells among policymakers across the globe. The US firmly believes that China has infiltrated the networks of its Department of Defense, private sector defence contractors and some of the private enterprises. It can be deducted that information related to defence projects is of utmost interest to China followed by information pertaining to the energy sector, specifically petroleum exploration. Besides that, there are certain geopolitical developments which shape China's threat perception and push it to to adopt asymmetric means.

Geopolitical Reasons for China to Become a Cyber Power

China's geographical location is politically fragile. China is already entangled in various maritime disputes, both in the East and South China Seas, namely, the Diaoyu/Senkaku and Spratley Islands.[41] The modernisation of PLA is driven by an amalgamation of economic, political and security factors. The increased impetus to modernisation efforts was a resultant of series of events in the decade of the 1990s. The US had deployed two aircraft carrier battle groups off the coast of Taiwan during the 1996 Taiwan Strait Crisis. This influenced China to develop its military assets and capability with the objective of denying the US forces any access to the Western Pacific in the case of a military conflict with Taiwan.[42] The Kosovo War in 1999, with aerial support from North Atlantic Treaty Organization (NATO) and active US-led intervention, substantiated China's assumption that the US can violate another country's sovereignty.[43]

The National Defence Policy white papers of China discuss the emerging geopolitical scenario and Asia-Pacific security situation, which tend to be of primary concern to its political and military leadership. The white papers of the last one decade have mentioned that the major powers are increasing their strategic investment in the Asia-Pacific region, pointing towards the reinforcement of regional military alliances and increased involvement in regional security affairs by the US. China finds this to be a major geopolitical concern[44] and, according to it, this is triggering a military competition between China and the US.

Furthermore, one of the white papers states: 'China confronts diverse and complex security challenges due to its vast territories and territorial seas and therefore, it faces heavy demands in safeguarding national security.'[45] The Chinese government has always held the stance that it promotes policies for advancing peaceful development of cross-strait relations. But Taiwan's independence and adherence to the 1992 Consensus remains an impediment and, according to China, the issue must be resolved for the peaceful development of cross-strait relations. China insists that the continued supply of weapons and arms to Taiwan by the US[46] is severely affecting Sino-US relations and hampering the process of peaceful development of cross-strait relations.[47] Under such circumstances, China has to preserve its territorial integrity and maritime rights and interests. Nevertheless, non-traditional security concerns, such

as terrorism, energy, finance, information and natural disasters, add to its woes. In order to gain strategic advantage, China has adopted the means of asymmetric warfare.

China's Approach: PLA's Asymmetric Warfare

The enormous investments made by China in developing submarine capabilities and anti-ship ballistic missile (ASBM) (DF-21D) corresponds with the strategy of maritime area denial, which Robert D. Kaplan describes as 'developing asymmetric niche capabilities designed to block the U.S. Navy from entering the East China Sea and other Chinese coastal waters.'[48] In an interview to the German magazine, *Spiegel*, in 2008, Chinese military strategist Chen Zhou made it abundantly clear that the Chinese concern is to prevent an intervention by the US during a crisis in the Taiwan Strait.[49] To achieve that, according to Seth Cropsey, a former Deputy Undersecretary of the US Navy, 'the Chinese navy plans to use over-the-horizon radars, satellites, seabed sonar networks, and cyber warfare in the service of anti ship ballistic missiles equipped with manoeuvrable re-entry vehicles.'[50] China does not want any kind of external intervention to resolve the Taiwan issue, whether it is done peacefully or militarily.[51] China needs to be militarily prepared and its modernisation effort largely aims to deny freedom of action for any external force in the Western Pacific, especially in the periphery of Taiwan. China understands that in the case of a conflict, although local, it might engage militarily with a technologically advanced nation. Informatisation would facilitate its armed forces in conducting joint operations, while cyber warfare, submarine warfare, DF-21D, etc., would give it the much-desired 'asymmetric' advantage.

The top leadership of military and government perceives the use of computers to be a real game changer in the future battlefield which facilitates real-time access to information and intelligence. Lieutenant General Qi Jianguo of PLA stated: 'In the information era, seizing and maintaining superiority in Cyberspace is more important than seizing command of sea and command of the air were in World War II.'[52] Hence, by modernising its forces, China wants to be in a commanding position to address any situation with Taiwan militarily, if the need arises. Additionally, it wants to maintain its assertive posture with respect to its territorial claims in the South China Sea and East China Sea, and thereby regulate military and economic activities in its maritime exclusive economic zone (EEZ).

China's Cyber Power: PLA as a Factor

The willingness of China to use its capabilities as a power against political, governmental, industrial and military targets clearly establishes its aspirations for cyberspace dominance. The offensive capabilities of China are concentrated in its military establishment. In a report by computer security firm, Mandiant[53], the military cyber warfare Unit 61398 was identified to be the 2nd Bureau of 3rd Department of PLA's General Staff Headquarter. The unit is building expertise in covert communications, network security, operating systems design and development, English language and digital signal processing. As per the report, Unit 61398 is based in Shanghai and it has led numerous cyber-based attacks to gain important information for China's military programmes and civilian enterprises by targeting the networks of the US government and private organisations.

China's military has been denouncing Mandiant's analysis and accusations, and maintains the stance that the country's armed forces have never backed any hacking activities.[54] Chinese Defence Ministry spokesman, Geng Yansheng, had expressed Chinese concerns pertaining to the US Cyber Security Strategy of 2013, which states that 'the Defense Department should be able to use cyber operations to disrupt an adversary's command and control networks, military-related critical infrastructure and weapons capabilities.'[55] Therefore, for China, PLA is tasked with enhancing the country's ability to safeguard cyber security and it is dissociated from any intent of conducting cyberattacks.[56]

As the role of military grows in national cyber security policies, nation states are laying down more emphasis on attaining dominant position in the cyberspace, in order to guard their economic and political interests. Despite various multilateral efforts at regional and international levels, pertaining to information and cyber security, the role of nation states in developing offensive capabilities cannot be denied.

Information and Communications Technology (ICT) in Economy and Society: Civilian Factor in China's Cyber Power

China's national power is mainly a result of its rapid economic growth over the past few decades, as the country continues to convert its vast resources into growing influence.[57] In order to continue this growth trajectory, in terms of both economic and national power, the strategic plan is to build China into a cyber power by building network infrastructure, enhancing independent innovation and developing a comprehensive information

economy.[58] The Chinese perspective of ICT has two primary facets: first, it is a cutting-edge industry for China to make a transition from a manufacturing-oriented economy to a knowledge-based economy; and second, it is paramount to elevate the living standards of the society.[59] The Chinese government discerns that the Internet is going to play a pivotal role in the national economic and societal development. A white paper, 'The Internet in China', notes that 'the development of the Internet is an important booster of nationwide application of IT, sound development of the economy and society, enhancement of scientific and technological innovation, and livelihood improvement'.[60] The first step in this direction was taken in 1993 when the State Economic Informationization Joint Meeting was initiated to build a national network of public economic information. Thereafter, the Ninth Five Year Plan for State Informationization in 1997 and, in 2002, the Specialized Plan for Informationization in the Tenth Five Year Plan for National Economic and Social Development were promulgated. In November 2005, the State Informatization Development Strategy (2006–20)[61] was formulated, which further substantiated that Internet development is one of the topmost priorities to promote national economic informatisation. Thereon, the Internet propelled the economic and social development of China and, coupled with IT, it made a significant contribution to the rapid growth of the Chinese economy.[62]

The Communist Party of China's Central Committee and State Council started off with 'Golden Technology' application projects. The Golden Projects refer to the Chinese government's systematic acceleration of IT infrastructure deployment in state agencies, schools and hospitals to enhance government administration and management. Originally, the goals of e-government were slated to be fulfilled in three stages: the first stage was 'Office Automation in Agencies'; the second stage was 'Twelve Golden Projects'; and the third stage was known as 'Government Online'.[63]

The National Information Development Strategy recognises the significance of IT application in various fields of national economy and traditional industries, such as energy, transportation, metallurgy, machinery and chemicals. It calls for further development of modern industries of financial services and e-business, in addition to science and technology, education, culture, health, social security and environmental protection. It emphasises that e-government transforms government functions, improves administrative efficiency and promotes effective

means of openness in government affairs.[64] A study on correlation between China's informatisation level and its national 'well-being' found that the provinces and autonomous regions of China are demonstrating a trend of a close-to-one positive correlation between the informatisation index and the well-being index, which means that the process of informatisation improves the level of national well-being correspondingly. Therefore, promoting the adoption of IT in governance and societal services improves the living standards of the populace[65] and if the degree of informatisation improves, there is corresponding improvement in the national well-being.

The strategy led by the highest echelons of decision-making has embarked China on an elevated growth rate of its technological development. Consequently, China has emerged as the computer production base for the world. It is also the world's biggest personal computer (PC) market.[66] The growth in domestic and global demand for computers has driven the development of the computer manufacturing industry in China.[67] Chinese PC manufacturer, Lenovo, is the world's biggest seller of PCs, ahead of Hewlett-Packard (HP).[68] At present, China is the largest consumer of semiconductors, primarily fuelled by mobile handset and computer manufacturing industry. In 2013, China's semiconductor consumption was highest at 55.6 per cent of the global market.[69]

The investments in futuristic technologies have begun reaping fruits for China. Encryption systems are the backbone of secure communication, used in government, military and commercial communications. There have been significant developments in this field, and the present-day encryption systems are by and large secure for the given computing power available. China is among the few countries involved in advance research on quantum cryptography and computing, which, according to experts, is slated to disrupt the technology used for computerised security.[70] The National University of Defense Technology[71] and University of Science and Technology of China (USTC)[72] in Hefei are known to house the research laboratories. China has made several breakthroughs in its endeavour.[73] China has been able to distinguish itself in supercomputing technology as well. China's National University of Defense Technology has developed a supercomputer, Tianhe-2, whose performance of 33.86 petaflop/s (quadrillions of calculations per second) on the Linpack benchmark makes it the world's most powerful supercomputer.[74] It is pursuing research on cloud computing,[75] Internet

of things, supercomputing, quantum computing and other disciplines of computer science which are slated to shape the future of global economy and society.[76] Perhaps, the more dependency that China develops on cyberspace to deliver its societal functions and conduct economic activity, the more vulnerable it will become to the threats and attacks. The reports from its governmental sources substantiate that China is not insulated or immune from attacks and exploitation in cyberspace.

A Giant Leap Towards Cyber Power

China has definitely understood the wide gaps in its technological sphere and the government is trying hard to bridge the gaps in the form of policy directives. It is vying to be independent in operating systems and computing hardware domains, which have been China's shortcoming. It is certain that the effort has been broken down in such a way that each indicator of cyber power is addressed individually, while keeping an eye on offensive capabilities. China is striving to place itself at 'commanding heights' of cyberspace, denoting its vested interests in developing offensive capabilities to engage its adversary in the cyberspace if the situation so demands.

The establishment of a high-level office is generally the first step towards consolidating cyber security efforts, which in turn enhances cyber power of a nation state. Looking at the history, the US administration created the position of a 'cyber czar' and established a cyber command in 2009, while Israel established the cyber committee tasked with uniting the cyber security community and protecting key infrastructure, also termed as 'Critical Infrastructure', in May 2012.[77] Very recently, in March 2015, India appointed a National Cyber Security Coordinator in the Prime Minister's Office to step up the effort to put up a coordinated response to the various challenges in cyberspace.[78] In the case of China, the Joint Meeting of Economic Information, headed by the vice premier, was established in 1993. Later on, it was upgraded into an Information Work Leading Group of the State Council in 1996, chaired by the premier, and subsequently, in 2001, the National Information Leading Group was established. China also established the Ministry of Information Industry (MII) in 1998 and, on this very foundation, the MIIT was established in 2008.[79]

Subsequently, China elevated its diplomatic efforts and pitched at the international level for securing cyberspace. China called upon the international community to 'work together towards a peaceful, secure

and equitable information and cyber space', stating that cyber security 'represents a major non-traditional security challenge' confronting the world at large.[80] China, Russia and several other countries submitted a draft 'international code of conduct on information security' to the United Nations in 2011.[81] The Chinese government put forth some basic principles, namely:[82] the principle of full respect for the rights and freedoms in cyberspace; the principle of balance between freedom and control, rights and obligations and security and development of a nation state; the principle of the peaceful use of cyberspace; and the principle of equitable development to address the digital divide.

Conclusion

Over the years, cyberspace has influenced every walk of life. It has become an intricate part of governance, military operations, communications and statecraft. All the constituents of national power, such as military, economy, diplomacy and technology, are heavily dependent on cyberspace. Realising its strategic imperatives, nation states have developed robust infrastructure to facilitate access and penetration of the Internet, guided by the state policies and strategy for development of cyberspace. China embarked on informatisation in 1982, primarily for delivery of governance and social services, the Golden Projects being the classical example. Gradually, China has built its expertise in manufacturing PCs, networking devices and telecommunication equipment, emerging as a global player in all the segments. It has nurtured global technology brands such as Lenovo, Huawei, ZTE and Alibaba. The State Informatization Development Strategy (2006–20) envisions placing China's knowledge economy quite high in the global market, in addition to its manufacturing industry. China has invested in research facilities to conduct high-end research on advanced technologies, such as supercomputing, quantum computing and cryptography, cloud computing and big data. It has made numerous breakthroughs as well in the emerging fields of computer science. However, there remain many voids, such as dependency on imports for semiconductor chips and processors and inability to roll out an operating system or manufacture high-end servers.

China's efforts fall quite well within the six indicators of cyber power. It is building vast infrastructure to support network and increase broadband penetration. China is accelerating diplomatic efforts in the international arena to defend its right to have a voice on cyber issues. China's state policies are providing a thrust to the development of

independent technological capabilities; recently, the focus has been laid upon operating systems and software development and semiconductor fabrication. The PLA is developing offensive capabilities, in line with its asymmetric warfare practices, spearheading China's aim of 'Occupying the "commanding heights" of Cyberspace'.

China's armed forces have firmly based their military preparedness on winning local wars under the conditions of informatisation. The paradigm shift at doctrinal level is transforming its semi-mechanised and mechanised weapon systems to automatised and informatised systems. The evidences from National Defence Policy papers, from 2000 to 2010, suggest that China's perception of geopolitics in its regional setting is shaping its strategy, which includes the cross-strait relationship with Taiwan, as well as its territorial and maritime disputes with Japan, South Korea and countries in the South China Sea. It has expressed deep concerns over the growing military engagement of the US in the Asia-Pacific, particularly with Taiwan and Japan for arms assistance or theatre missile defence (TMD) deployment. The Snowden revelations of espionage operations by the National Security Agency (NSA) have perturbed China, making it extremely cautious with deployment of foreign technology in its critical government functions.

There remain many issues pertaining to China's illicit technology acquisition and economic espionage practices. If the accusations on China of executing hacking attempts—such as Titan Rain and NetTraveller—are true, then China has certainly demonstrated its intent to exert cyber power. At the strategic level, organisations play a prominent role; they reflect purposes, objectives and perspectives of power. In the case of China, its cyber power objectives and perspectives are ostensibly shaped and driven by military and economic interests.

Notes

1. Full text of Hu Jintao's report at 18th Party Congress, *Xinhua* (Beijing), 17 November 2012, available at http://news.xinhuanet.com/english/special/18cpcnc/2012-11/17/c_131981259_10.htm, accessed on 19 November 2015.
2. Available at http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-072.pdf, accessed on 18 May 2015
3. Franz-Defan Gady, 'Why the PLA Revealed its Secret Plans for Cyber War', *The Diplomat*, 24 March 2015, available at http://thediplomat.

com/2015/03/why-the-pla-revealed-its-secret-plans-for-cyber-war/, accessed on 18 May 2015.

4. Ibid.
5. Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz, "Cyberpower and National Security", *National Defense University Press* (Washington DC, 2009), pp. 259-260.
6. Ibid.
7. Daniel T. Kuehl, *From Cyberspace to Cyberpower: Defining the Problem, Cyberpower and National Security*, Washington, DC: National Defense University Press, 2009, p. 12, available at http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-02.pdf, accessed on 20 May 2015.
8. Joseph Nye, 'Cyber Power', Belfer Center for Science and International Affairs, May 2010, pp. 3–4, available at http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf, accessed on 20 May 2015.
9. 'National Power: Its Elements', p. 3, available at http://103.1.174.97/newcms/attachments/article/259/NATIONAL%20POWER.pdf, accessed on 22 May 2015.
10. Li Zhang, 'A Chinese Perspective on Cyber War', *International Review of the Red Cross*, Vol. 94, No. 886, Summer 2012, pp. 802–03, available at https://www.icrc.org/eng/assets/files/review/2012/irrc-886-zhang.pdf accessed on 20 May 2015.
11. Ibid.
12. George Shambaugh defines economic warfare as 'seeking to weaken an adversary's economy by denying the adversary access to necessary physical, financial and technological resources or by otherwise inhibiting its ability to benefit from trade, financial and technological exchanges with other countries', available at http://www.britannica.com/topic/economic-warfare, accessed on 15 June 2015.
13. James A. Lewis and Simon Hansen, 'China's Cyberpower: International and Domestic Priorities', Australian Strategic Policy Institute, November 2014, p. 2, available at https://www.aspi.org.au/publications/chinas-cyberpower-international-and-domestic-priorities/SR74_China_cyberpower.pdf, accessed on 10 June 2015.
14. 'China is world's leading consumer of aluminum, copper, lead, nickel, zinc, tin, and iron ore; China's share of the world's metal consumption has jumped from ten percent to 25 percent since the late 1990s'; see Robert D. Kaplan, 'The Geography of Chinese Power', *Foreign Affairs*, May–June 2010, available at https://www.foreignaffairs.com/articles/china/2010-05-01/geography-chinese-power, accessed on 19 June 2015.
15. 'China Eyes Internet Power', *Xinhua* (Beijing), 8 March 2014, available

at http://news.xinhuanet.com/english/special/2014-03/08/c_133171308.htm, accessed on 22 May 2015.

16. ITU, *Measuring the Information Society Report*, Geneva: International Telecommunication Union, 2014, p. 42, available at https://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2014/MIS2014_without_Annex_4.pdf, accessed on 10 June 2015.
17. Siegesmund von Ilsemann and Andreas Lorenz, 'Spiegel Interview with Top Chinese Military Strategist', *Der Spiegel*, 19 March 2008, available at http://www.spiegel.de/international/world/0,1518,542506,00.html, accessed on 22 May 2015.
18. Government of People's Republic of China, *China's National Defense in 2004*, Beijing: Information Office of the State Council, 27 December 2004, available at http://www.china.org.cn/e-white/20041227/index.htm, accessed on 24 May 2015.
19. Dallas Boyd, Jeffrey G. Lewis and Joshua H. Pollack, 'Advanced Technology Acquisition Strategies of the People's Republic of China', Defense Threat Reduction Agency, September 2010, p. 1, available at http://fas.org/irp/agency/dod/dtra/strategies.pdf, accessed on 10 June 2015.
20. Ankit Panda, 'Xi Jinping: China should Become a Cyber Power', *The Diplomat*, 4 March 2014, available at http://thediplomat.com/2014/03/xi-jinping-china-should-become-a-cyber-power/, accessed on 24 May 2015.
21. 'Xi Heads Internet Security Group', *Xinhua*, 27 February 2014, available at http://news.xinhuanet.com/english/china/2014-02/27/c_133148418.htm, accessed on 24 May 2015.
22. 'Army Needs "Information Warfare" Plan, Declares Xi', *China Daily*, 1 September 2014, available at http://www.chinadaily.com.cn/china/2014-09/01/content_18520930.htm, accessed on 10 June 2015.
23. 'How China Becomes a Cyber Power', *Forbes*, 2 July 2014, available at http://www.forbes.com/sites/adamsegal/2014/07/02/how-china-becomes-a-cyber-power/, accessed on 10 June 2015
24. Government of People's Republic of China, 'National Defense Policy', in *China's National Defense in 2000*, Beijing: Information Office of the State Council, December 2000, available at http://www.china.org.cn/e-white/2000/20-3.htm, accessed on 10 June 2015.
25. Ibid.
26. Government of People's Republic of China ,'Armed Forces Building', in *National Defense Policy–2000*, Beijing: Information Office of the State Council, December 2000, available at http://www.china.org.cn/e-white/2000/20-5.htm#a, accessed on 11 June 2015.
27. Government of People's Republic of China 'The Security Situation', in

National Defense Policy–2002, Beijing: Information Office of the State Council, December 2000, available at http://www.china.org.cn/e-white/20021209/I.htm, accessed on 12 August 2015.

28. Ibid.
29. Government of People's Republic of China, 'National Defense Policy—2008', January 2009, Beijing: Information Office of the State Council, December 2000, available at http://www.china.org.cn/government/whitepaper/2009-01/21/content_17162883.htm, accessed on 12 June 2015.
30. 'Reform and Development of the PLA', in *National Defense Policy—2008*, available at http://www.china.org.cn/government/whitepaper/2009-01/21/content_17162870.htm, accessed on 15 June 2015.
31. Information Office of the State Council, 'The Diversified Employment of China's Armed Forces', Beijing, April 2013, available at http://news.xinhuanet.com/english/china/2013-04/16/c_132312681.htm, accessed on 12 August 2015.
32. 'White Paper Introduces Policies, Principles of China's Armed Forces' Diversified Employment', *Xinhua*, 16 April 2013, available at http://news.xinhuanet.com/english/china/2013-04/16/c_132312555.htm, accessed on 17 June 2015.
33. Bryan Krekel, 'Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation', *The US–China Economic and Security Review Commission Report*, Virginia: Northrop Gruman, October 2009, pp. 67–70.
34. Ibid.
35. Nathan Thornburgh, 'Inside the Chinese Hack Attack', *Time*, 25 August 2005, available at http://content.time.com/time/nation/article/0,8599,1098371,00.html, accessed on 15 June 2015.
36. Mark Clayton, 'US Oil Industry Hit by Cyberattacks: Was China Involved?', *Christian Science Monitor.com*, 25 January 2010, available at http://www.csmonitor.com/USA/2010/0125/US-oil-industry-hit-by-cyberattacks-WasChina-involved accessed on 18 June 2015; and Michael Riley, 'Exxon, Shell, BP Said to have been Hacked through Chinese Internet Servers', *Bloomberg*, 24 February 2001, available at http://www.bloomberg.com/news/2011-02-24/exxon-shell-bpsaid-to-have-been-hacked-through-chinese-internet-servers.html, accessed on 17 June 2015.
37. 'Five Serious Cases of Cyberespionage', *Foxnews.com*, 22 April 2009, available at http://www.foxnews.com/story/2009/04/22/five-serious-casescyberespionage/, accessed on 17 June 2015.
38. Wendell Minnick, 'Chinese Cyber-espionage Growing', *DefenseNews.*

com, 6 November 2011, available at http://www.defensenews.com/article/20111106/DEFSECT04/111060302/Chinese-Cyber-Espionage-GrowingU-S-Report, accessed on 17 June 2015.

39. China's 2nd Bureau of the People's Liberation Army (PLA) General Staff Department's (GSD) 3rd Department (Military Cover Designator 61398).
40. 'US–China Cyber Espionage Comes under Increased Scrutiny', *RT.com*, 7 November 2013, available at http://rt.com/op-edge/us-china-cyberespionage-371/, accessed on 18 June 2015.; and Dan Mcwhorter, 'Mandiant Exposes APT 1', *Mandiant.com*, 18 February 2013, available at https://www.mandiant.com/ blog/mandiant-exposes-apt1-chinas-cyber-espionage-units-releases-3000- indicators/, accessed on 18 June 2015.
41. Kaplan, 'The Geography of Chinese Power', n. 14.
42. Boyd et al., 'Advanced Technology Acquisition Strategies of the People's Republic of China', n. 19.
43. Ibid.
44. Government of People's Republic of China 'The Security Situation', in *National Defense Policy–2010*, Beijing: Information Office of the State Council, December 2000, available at http://www.china.org.cn/government/whitepaper/2011-03/31/content_22263403.htm, accessed on 19 June 2015.
45. Ibid.
46. Jim Wolf and Paul Eckert, 'Obama Proposes his First Arms Sales to Taiwan', *Reuters*, 29 January 2010, available at http://www.reuters.com/article/2010/01/30/us-taiwan-arms-usa-idUSTRE60S4X420100130, accessed on 13 June 2015.
47. Government of People's Republic of China 'The Security Situation', in *National Defense Policy–2010*, Beijing: Information Office of the State Council, December 2000, available at http://www.china.org.cn/government/whitepaper/2011-03/31/content_22263403.htm, accessed on 13 June 2015.
48. Kaplan, 'The Geography of Chinese Power', n. 14.
49. SPIEGEL Interview with Top Chinese Military Strategist, March 19, 2008, http://www.spiegel.de/international/world/spiegel-interview-with-top-chinese-military-strategist-we-will-defend-our-sovereignty-with-all-means-a-542506.html, accessed 14 December 2015.
50. Seth Cropsey, 'The U.S. Navy in Distress', *Strategic Analysis*, Vol. 34, No. 1, January 2010, p. 39, available at http://www.hudson.org/content/researchattachments/attachment/766/cropsey_us_navy_in_distress.pdf, accessed on 18 June 2015.
51. 'SPIEGEL Interview with Top Chinese Military Strategist', *Spiegel Online*,

19 March 2008, available at http://www.spiegel.de/international/world/spiegel-interview-with-top-chinese-military-strategist-we-will-defend-our-sovereignty-with-all-means-a-542506.html, accessed on 19 June 2015.

52. James A. Bellacqua and Daniel M. Hartnett, 'Article by LTG Qi Jianguo on International Security Affairs', *CNA China Studies* (Virginia, 2013), p. 9, available at https://www.cna.org/CNA_files/PDF/DQR-2013-U-004445-Final.pdf, accessed 14 December 2015.
53. Mandiant Intelligence Center Report, 'APT1: Exposing One of China's Cyber Espionage Units', *Mandiant Consulting* (Virginia, 2013), available at http://intelreport.mandiant.com/, accessed 14 December 2015.
54. 'China Defense Ministry Refutes Cyber Attack Allegations', *Xinhua*, 20 February 2013, available at http://news.xinhuanet.com/english/china/2013-02/20/c_132180777.htm, accessed on 19 June 2015.
55. 'China Opposes U.S. Cybersecurity Strategy's Accusations against Beijing', *Xinhua*, 30 April 2015, available at http://english.chinamil.com.cn/news-channels/china-military-news/2015-04/30/content_6469493.htm, accessed on 19 June 2015.
56. China's Ministry of National Defense spokesman, 'China has No Cyber Warfare Troops', *Xinhua*, 28 February 2013, available at http://news.xinhuanet.com/english/china/2013-02/28/c_132199193.htm, accessed on 19 June 2015.
57. James A. Lewis and Simon Hansen, 'China's Cyberpower: International and Domestic Priorities', Australian Strategic Policy Institute, November 2014, p. 16, available at https://www.aspi.org.au/publications/chinas-cyberpower-international-and-domestic-priorities/SR74_China_cyberpower.pdf, accessed on 20 June 2015.
58. 'Xi Jinping: The Construction of the Network from the Country to become a Network Power', *Xinhua*, 27 February 2014, available at http://news.xinhuanet.com/politics/2014-02/27/c_119538788.htm, accessed on 22 June 2015.
59. Robert D. Atkinson, 'ICT Innovation Policy in China: A Review', The Information Technology and Innovation Foundation, July 2014, p. 1, available at http://www2.itif.org/2014-china-ict.pdf, accessed on 20 June 2015.
60. 'Endeavors to Spur the Development and Application of the Internet', in *The Internet in China*, 8 June 2010, available at http://www.gov.cn/english/2010-06/08/content_1622956_3.htm, accessed on 22 June 2015.
61. Published by the General Office of the Communist Party of China Central Committee and General Office of the State Council, available at http://www.china-embassy.org/eng/xw/t251756.htm accessed 22 June 2016.

62. 'Endeavors to Spur the Development and Application of the Internet', in *The Internet in China*, n. 60.
63. Guo Liang, 'Under the "Golden Shine": China's Efforts to Bridge Government and Citizens', United Nations Centre for Regional Development, 28 January 2006, p. 2, available at http://unpan1.un.org/intradoc/groups/public/documents/un-dpadm/unpan042815.pdf, accessed on 22 June 2015.
64. '2006–2020 National Information Development Strategy', *China Network*, 8 May 2006, available at http://www.china.com.cn/chinese/PI-c/1203246.htm, accessed on 22 June 2015.
65. Bin Zhang, Da Gu and Wen Ma, 'A Study of the Correlation between China's Informatization Level and its National Well-being', *Networked Planet*, Pacific Telecommunications Council, 2015, p. 8, available at https://www.ptc.org/assets/uploads/papers/ptc15/Paper_Ma_Wen.pdf accessed on 22 June 2015.
66. Owen Fletcher, 'China Passes U.S. as World's Biggest PC Market', *The Wall Street Journal*, 24 August 2011, available at http://www.wsj.com/articles/SB10001424053111903461304576525852486131230, accessed on 22 June 2015.
67. 'Computer Manufacturing in China: Market Research Report', *IBIS World*, August 2014, available at http://www.ibisworld.com/industry/china/computer-manufacturing.html, accessed on 22 June 2015.
68. 'From Guard Shack to Global Giant', *The Economist*, 12 January 2013, available at http://www.economist.com/news/business/21569398-how-did-lenovo-become-worlds-biggest-computer-company-guard-shack-global-giant, accessed on 22 June 2015.
69. 'A Decade of Unprecedented Growth: China's Impact on the Semiconductor Industry', PriceWaterhouseCoopers, August 2014, p. 2, available at http://www.pwc.com/en_GX/gx/technology/chinas-impact-on-semiconductor-industry/assets/2014-update.pdf, accessed on 28 June 2015.
70. Cindy Hurst, 'JFQ 77 | The Quantum Leap into Computing and Communication: A Chinese Perspective', National Defense University Press, 1 April 2015, available at http://ndupress.ndu.edu/Media/News/NewsArticleView/tabid/7849/Article/581868/jfq-77-the-quantum-leap-into-computing-and-communication-a-chinese-perspective.aspx, accessed on 30 June 2015.
71. National University of Defense Technology, 'Specific Research Areas', available at http://www.nudt.edu.cn/ArticleShow_eng.asp?ID=75, accessed on 30 June 2015.
72. University of Science and Technology of China, 'Key Laboratory of Quantum Information', School of Physical Sciences, available at www.

en.physics.ustc.edu.cn/research_9/Quantum/201107/t20110728_116550.html, accessed on 30 June 2015.

73. 'China Makes Breakthrough on Quantum Computer', *People's Daily*, 7 February 2013, available at http://english.peopledaily.com.cn/202936/8126200.html; accessed on 30 June 2015, see also, 'Chinese scientists claimed to be the first in the world to have succeeded in the physical teleportation of the electronic properties of remote particles, one of the important foundations for quantum computing', in Greg Austin, 'How China Plans to Become a World Class Cyber Power', *The Diplomat*, 30 April 2015, available at http://thediplomat.com/2015/05/how-china-plans-to-become-a-world-class-cyber-power/, accessed on 30 June 2015.
74. 'November 2014 Top 500 List', available at http://www.top500.org/lists/2014/11/, accessed on 22 June 2015.
75. The Chinese government has been highly supportive of the cloud computing industry under the aegis of National Development and Reform Commission (NDRC), the Ministry of Industry and Information Technology (MIIT) and the Ministry of Finance (MoF); see 'China's Cloud Computing Strategy', *HongKong Trader*, 5 June 2013, available at http://www.hktdc.com/info/mi/a/hkthk/en/1X09TCME/1/Hong-Kong-Trader-Hong-Kong-Edition/China-S-Cloud-Computing-Strategy.htm, accessed on 22 June 2015.
76. Leigh Ann Ragland, Joseph McReynolds, Matthew Southerland and James Mulvenon, 'Red Cloud Rising: Cloud Computing in China', Research Report Prepared on Behalf of the US–China Economic and Security Review Commission, Center for Intelligence Research and Analysis, 5 September 2013, available at http://www.uscc.gov/sites/default/files/Research/DGI_Red%20Cloud%20Rising_2014.pdf., accessed on 15 June 2015.
77. 'China's First Step towards Becoming a Cyber Power', *China Focus*, 13 March 2014, available at http://www.chinausfocus.com/peace-security/chinas-first-step-towards-becoming-a-cyber-power/#sthash.ZRJ2rRAq.dpuf, accessed on 15 June 2015.
78. 'Gulshan Rai Becomes First Chief of Cyber Security; Post Created to tackle Growing e-Threats', *The Economic Times*, 4 March 2015, available at http://economictimes.indiatimes.com/news/politics-and-nation/gulshan-rai-becomes-first-chief-of-cyber-security-post-created-to-tackle-growing-e-threats/articleshow/46449780.cms, accessed on 24 June 2015.
79. 'China's First Step towards Becoming a Cyber Power', n. 77.
80. 'China Calls for Joint Efforts for Peaceful, Secure, Equitable Cyber Space', *Xinhua*, 20 October 2011, available at http://news.xinhuanet.com/

english2010/china/2011-10/21/c_131203292.htm, accessed on 24 June 2015.

81. 'China Calls for Unified Rules to Counter Cyber Crime', *Xinhua*, 29 May 2012, available at http://news.xinhuanet.com/english/video/2012-05/29/c_131617550.htm, accessed on 24 June 2015.
82. Li Zhang, 'A Chinese Perspective on Cyber War', n. 10, pp. 806–07.