Red Cloud Rising: Cloud Computing in China

by

Leigh Ann Ragland, Joseph McReynolds, Matthew Southerland,
and James Mulvenon

Research Report Prepared on Behalf of the U.S.-China Economic and Security Review Commission
September 5, 2013

Revised March 22, 2014
After the publication of this report on September 5, 2013, Microsoft brought to the authors' attention new information about its partnership with Chinese company 21Vianet. The original version of the report inaccurately characterized certain aspects of the Microsoft-21Vianet partnership. A revised discussion of this partnership is provided on pages 32-34. The authors would like to thank Microsoft for their assistance in clarifying the details of 21Vianet's Windows Azure service.

Defense Group Inc.

Center for Intelligence Research and Analysis
Advancing U.S. Intelligence Through Innovative Research, Analysis, and Public Outreach

Disclaimer:

This research report was prepared at the request of the Commission to support its deliberations. Posting of the Report to the Commission's website is intended to promote greater public understanding of the issues addressed by the Commission in its ongoing assessment of U.S.-China economic relations and their implications for U.S. security, as mandated by Public Law 106-398 and Public Law 108-7. However, it does not necessarily imply an endorsement by the Commission or any individual Commissioner of the views or conclusions expressed in this commissioned research report.

About Defense Group Incorporated

Defense Group Inc. (DGI) performs work in the national interest, advancing public safety and national security through innovative research, analysis and applied technology. The DGI enterprise conducts research and analysis in defense and intelligence problem areas, provides high-level systems engineering services to selected national and homeland security organizations, and produces hardware and software products for government and commercial consumers.

About CIRA

This project was conducted within DGI's Center for Intelligence Research and Analysis (CIRA), the premier open source and cultural intelligence exploitation cell for the US intelligence community. Staffed by an experienced team of cleared analysts with advanced language skills, CIRA's mission is to provide cutting-edge, open source and cultural intelligence support to the collection, analytical, and operational activities of the US intelligence community, with the goal of achieving national strategic objectives. CIRA accomplishes its mission through the conduct of objective, independent, and relevant research and analysis, under strict quality guidelines.

Comments may be sent to the Vice President of the Intelligence Division, Dr. James Mulvenon.

Dr. James Mulvenon
Vice President, Intelligence Division
Director, Center for Intelligence Research and Analysis (CIRA)
Defense Group, Incorporated
2650 Park Tower Drive, Suite 400
Vienna, VA 22180
TEL: 571-421-8359
Email: James.Mulvenon@defensegp.com

Acronyms

Acronym	Full Name
ACSI	Advisory Committee for State Informatization
API	Application Programming Interface
C2SC	China Standard Software Co. Ltd.
CCIC	China Cloud Innovation Center
CCP	Chinese Communist Party
CCSA	Chinese Communications Standards Association
CEO	Chief Executive Officer
CESI	China Electronics Technology Standardization Institute
CETC	China Electronic Technology Group Corporation
CIE	China Institute of Electronics
CIRA	Center for Intelligence Research and Analysis
CSA	Cloud Security Alliance
CSIA	China Software Industry Association
DDoS	Distributed Denial of Service
DGI	Defense Group Inc.
DMTF	Distributed Management Task Force
DOD	Department of Defense
EC2	Amazon Elastic Computer Cloud
FDI	Foreign Direct Investment
FYP	Five Year Plan
HP	Hewlett Packard
HPC	High-Performance Computing
HTTP	Hypertext Transfer Protocol
IaaS	Infrastructure as a Service
ICP	Internet Content Provider
ICP	Integrated Command Platforms
ICT	Information and Communications Technology
IP	Internet Protocol
IT	Information Technology
ITSS	Information Technology Services Standard
ITU	International Telecom Union
MIIT	Ministry of Industry and Information Technology
MLP	Medium and Long-Term Plan
MLPS	Multi-Level Protection Scheme
MOST	Ministry of Science and Technology
MSS	Ministry of State Security
NDRC	National Development and Reform Commission
NGO	non-governmental organization

NIST	National Institute of Standards and Technology
NITSTC	National Information Technology Standards Technical Committee
NTCISS	National Technical Committee for Information Security Standardization
OECD	Organisation for Economic Co-operation and Development
PaaS	Platform as a Service
PC	Personal Computer
PLA	People's Liberation Army
PoP	Point of Presence
PUE	Power Unit Effectiveness
R&D	Research and Development
RI	Research Institute
RMB	*Renminbi*
SSD	Solid State Hard Drive
S&T	Science and Technology
SaaS	Software as a Service
SEI	Strategic Emerging Industry
SME	Small-to-Medium Enterprises
SNIA	Storage Networking Industry Association
SOA	Service Oriented Architecture
US	United States
USD	United States Dollars
USITC	United States International Trade Commission
USITO	United States Information Technology Office
VM	Virtual Machine
WOFE	Wholly-owned Foreign Entities

Table of Contents

Executive Summary

In recent years the Chinese government has prioritized the development of cloud computing technology with the twin goals of expanding Chinese military and civilian access to cloud computing information technology (IT) resources and creating an internationally competitive Chinese cloud computing service industry. As part of a larger development strategy for advancing Chinese software and information technology services, the Chinese government plans to make more than one billion dollars (USD) available over the next few years to drive cloud computing development.

China's plans in this area have the potential to materially impact US economic and security interests. The emergence of China-based cloud computing services and solutions may raise significant concerns for US consumers, particularly if their data is being stored or processed using infrastructure located within Mainland China. Chinese progress in cloud computing is also important due to the Chinese military's demonstrated interest in developing and procuring advanced cloud computing technologies.

In order to support the needs of analysts and policy makers, this report characterizes the nature, extent, and future prospects of Chinese cloud computing development from both private-sector and governmental perspectives. In the course of making these assessments, this report describes in detail the complex ecosystem of government bodies, research institutes, private-sector companies, state-owned enterprises, and military organizations that together comprise the Chinese cloud computing industry and the Chinese market for cloud technologies. Particular attention is paid to the security challenges these trends pose for US corporations, consumers, and the US government, as well as how social, legal, and regulatory developments in China may affect foreign users and providers of Chinese cloud services.

The key findings of this report are as follows:

Security Issues:

- Any future growth in US consumer use of China-based cloud computing infrastructure would likely raise significant security concerns. Regulations requiring foreign firms to enter into joint cooperative arrangements with Chinese companies in order to offer cloud computing services may jeopardize the foreign firms' information security arrangements. Furthermore, Chinese-language news sources indicate that China's primary foreign intelligence collection organization, the Ministry of State Security, has taken an oversight role in projects aimed at bringing foreign cloud computing investment to China.

- Chinese cloud computing infrastructure could be used for offensive cyber operations, but the same is true of public cloud computing platforms globally. If Chinese public cloud infrastructure were ever to become unusually popular for these purposes, it would likely be due to a relative lack of oversight and lax enforcement of rules governing users' conduct by Chinese service providers, not due to Chinese cloud infrastructure being more 'weaponized' than equivalent services in other countries.

- The security vulnerabilities of Chinese cloud infrastructure are not inherently different from those of other cloud infrastructure around the globe. To the extent Chinese cloud infrastructure might on the whole be less secure, it would likely result from increased use of Chinese hardware and software (which, generally speaking, tend to have more security holes than their American counterparts), not from the fundamental design of that infrastructure.

Development of China's Cloud Computing Industry

- Chinese industry analysis projects that China's cloud computing industry will continue to grow, with the overall value chain reaching between 750 billion and 1 trillion *renminbi* (RMB) ($122 to $163 billion USD) by 2015. However, China's cloud computing industry is beset by shortcomings such as low reliability and energy efficiency in domestic data centers, lack of innovation in core chip development, and inadequate virtualization support, resulting in a lack of domestic demand.

- Although the United States has published and shared technical requirements for its government cloud computing systems, Chinese state guiding documents show no indication that technical requirements for Chinese government cloud computing requirements will ever be shared publicly.

Innovation in China's Cloud Computing Industry

- China and the United States show differing attitudes toward the process of developing technological standards for cloud computing. While US policies aim to promote homogeneous global cloud computing standards, Chinese policies appear to seek to create additional "indigenous innovation" requirements for domestic sales of cloud computing technology in order to protect Chinese enterprises from foreign competition.

- Some Chinese companies have shown an ability to innovate in this market. Baidu, for example, has designed data centers that claim to be far more energy efficient than others in China. Questions remain, however, as to whether or not Chinese innovation in this sector is driven by intellectual property theft from foreign corporations. Although Chinese company Alibaba Cloud Computing claims that its cloud-based operating system for mobile devices is the first of its kind, Google argues that key portions of Alibaba's operating system have been copied from its Android platform.

Access to Chinese Cloud Computing for US Customers and Businesses

- China's limits and restrictions on foreign investment in value-added telecommunications services mean that US companies must enter into joint ventures with Chinese companies in order to provide cloud computing services to Chinese consumers from data centers in China. Despite challenges to foreign participation in China's cloud computing market, leading US firms are actively pursuing partnerships and opportunities there. However, questions remain as to whether or not US companies will benefit in the short- and long-term from these limited forms of market participation.

- The Chinese Ministry of Public Security's sophisticated Internet content-filtering and censorship program, commonly referred to as the "Great Firewall," continues to exacerbate current barriers to integration between the Chinese and US cloud markets. Recent efforts by investment-seeking provincial Chinese governments to carve out exceptions to the Firewall for foreign corporations appear to have been blocked by the central government.

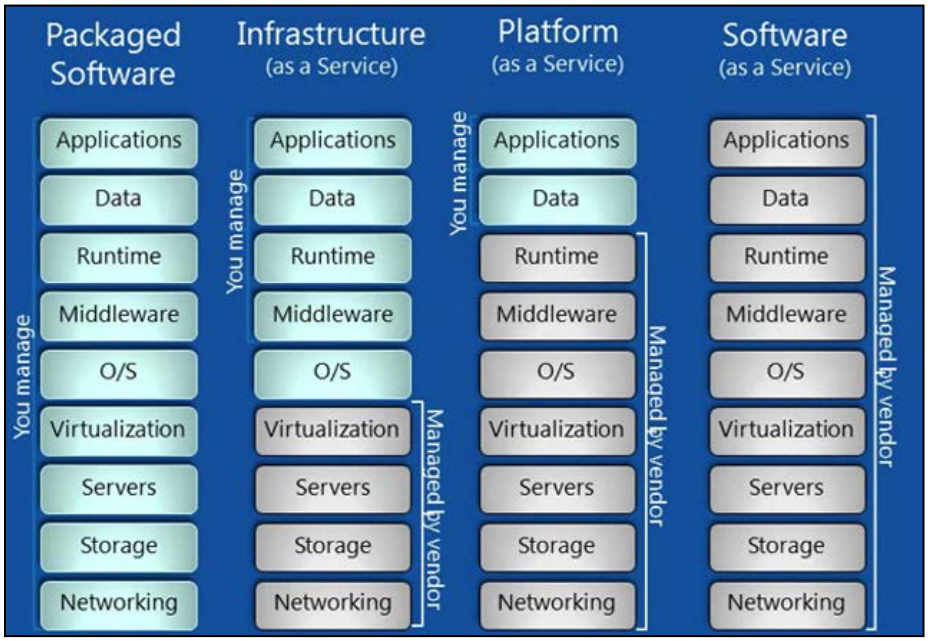
- It is unclear how competitive US cloud computing firms will be in China's government procurement market. The percentage of foreign software and hardware procured for the central government's e-government services is high but appears to be decreasing. Government policy directs agencies to buy domestic if Chinese products can meet agencies' demands.

Introduction

The term 'cloud computing' refers to the delivery of scalable IT resources over the Internet, such as data storage and computer processing capacity, providing an efficient alternative to the local hosting and operation of IT resources. Cloud computing enables end users to "rent" and remotely access IT resources from cloud providers on a pay-per-use basis, resulting in both improved system scalability and cost savings over traditional IT infrastructure. This transition to the cloud may be self-reinforcing; as businesses discover cost benefits in moving some or their entire IT infrastructure to cloud platforms, economies of scale should allow computing prices to decline further still, which in turn will attract new providers and cloud-based solutions into the market. Beyond the financial incentive to use cloud services to address current IT needs, the availability of low-cost distributed High Performance Computing (HPC) may open up new avenues of business, enabling companies that would not be able to afford traditional physical supercomputing infrastructure to tap into those services whenever necessary.

Additional cost gains tied to cloud computing can result not only from the reduced cost of computing resources under a cloud infrastructure, but also as indirect savings due to the relative ease with which cloud services and infrastructure can be deployed, managed, and maintained by an outside service provider (See Figure 1 Below). By shifting as many system management and maintenance responsibilities onto cloud services providers as possible, corporations (and other entities) may achieve significant cost savings through reductions in in-house resources for IT maintenance and personnel.

Figure 1: A Comparison of Management Responsibilities between Traditional IT Infrastructure (Left) and Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) Cloud Computing



Because businesses, governments, and individual users may store sensitive information within a cloud, cloud computing infrastructure is an attractive target for hackers and information security researchers. Vulnerabilities in either the infrastructure of a cloud provider or the programs and systems used to access the cloud may raise the risk of security intrusions. Beyond these generalized concerns, Chinese cloud computing poses additional risks for any US persons or organizations purchasing cloud services there, ranging from Internet service interruptions to government surveillance and control. With the growing popularity of commercial cloud computing in China, the implications of such vulnerabilities are wide-ranging and will only increase in importance in the years to come.

At present, Chinese firms have already benefitted from technology transferred from US and other foreign cloud computing companies. At the same time, foreign firms are effectively barred from directly competing in the domestic Chinese consumer market by strict Chinese government controls and regulations on the Internet and IT service industry, requiring US cloud computing firms such as IBM, Microsoft, and Eucalyptus to enter into joint partnerships with Chinese firms. This transfer of knowledge to Chinese firms, combined with government support for domestic 'national champion' corporations in the form of subsidies, research and development (R&D) funding, economic performance incentives for regional cloud clusters, and preferential tax policies, has helped enable the Chinese cloud computing industry to grow rapidly in recent years.

This report is organized into five chapters, which reflect the five discrete research tasks selected by the Commission. The first chapter examines how the United States and China's respective governments and industry groups conceptualize cloud computing, with an extended discussion of conceptual differences and each country's differing expectations regarding cloud computing uses and prospects. The second chapter provides a detailed history of the development of cloud computing in China, as well as an assessment of China's technical capacity and technology penetration relative to that of the United States. The third chapter examines the extent to which US citizens and corporations are linked to cloud computing infrastructure that is developed, owned, or operated within China, with particular attention paid to whether or not these linkages are transparent to the US entities involved. The fourth chapter looks at the potential security issues and risks for US consumers associated with the use of Chinese cloud infrastructure, examines the ways in which various types of Chinese entities may utilize cloud computing technology, and offers a broad assessment of the current state of Chinese cloud system security. The fifth and final chapter examines the future prospects for the private-sector cloud computing industry in China, based on an assessment of technology adoption, market potential, the innovation strategies of Chinese firms, and government support for the domestic cloud computing industry.

Chapter One: Cloud Computing Concepts in the United States and China

The Chinese government currently lags behind the United States in reaching an official definition of what 'cloud computing' entails, and a unified definition for the purposes of procurement and regulation has not yet been produced or published. Despite this ambiguity, examinations of both unofficial definitions drafted by leading government authorities and relevant government policies give a sense of what the current Chinese conception of cloud computing entails. It appears that the most widely used Chinese definition of cloud computing is heavily influenced by the US definition issued in 2011 by the US National Institute of Standards and Technology (NIST), though the presence of competing definitions within the Chinese government leaves open the possibility of a future redefinition that puts greater emphasis on China-specific standards and norms.

Chinese policymaking in this area suggests that China plans to develop unique "indigenous innovation" requirements for domestic cloud computing standards, akin to the indigenous innovation standards that have been established in the past for other emerging information technologies. The creation of separate standards and definitions outside of international norms may complement other protectionist measures to hamper foreign participation in China's cloud computing market.

The key findings of this chapter are as follows:

- The development of a Chinese technical definition and standards for cloud computing appears to be slowed by differences of opinion between the relevant organizations involved and inadequate participation from leading cloud computing firms.

- The Telecommunications Research Institute under China's Ministry of Industry and Information Technology (MIIT) appears to reject a widely accepted characteristic of cloud computing: "on-demand self-service."[1] If future Chinese standards for cloud computing were to exclude this characteristic, it would add extra technical requirements for businesses and reduce the competitiveness of foreign firms in the Chinese market due to the need to adapt products to China-specific standards.

- "Indigenous innovation" requirements to create separate standards and definitions outside of international norms may complement other protectionist measures to hamper foreign participation in China's cloud computing market.

How the United States and China Define Cloud Computing

Cloud computing is a concept that encompasses a number of systems and technologies. Although more than twenty competing definitions of cloud computing exist in the United States, the NIST,

[1] In cloud computing, 'on-demand self-service' refers to the user's ability to access a large pool of IT resources directly. Thus, a user can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

a non-regulatory agency, provides the most widely accepted definition. In short, the NIST defines cloud computing as:

"A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models."[2]

According to the NIST, cloud computing has five essential characteristics, and cloud computing services are divided into three types of service models (software, platform, and infrastructure) and four types of deployment models (private, community, public, and hybrid clouds).

The five essential characteristics of cloud computing are:[3]

- *On-demand self-service.* A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
- *Broad network access.* Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).
- *Resource pooling.* The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.
- *Rapid elasticity.* Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
- *Measured service.* Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

Although the NIST definition of cloud computing was drafted for use by US federal government agencies, many non-government organizations appear to have also accepted it voluntarily. One of the leading American cloud computing service providers, Rackspace, refers to the NIST definition as being the "generally accepted definition" of cloud computing.[4] Nevertheless, others

[2] Peter Mell and Timothy Grance, "The NIST Definition of Cloud Computing," *NIST Computer Security Division Computer Security Resource Center*, modified September, 2011, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[3] Characteristics are directly quoted from source. Peter Mell and Timothy Grance, "The NIST Definition of Cloud Computing," *NIST Computer Security Division Computer Security Resource Center*, modified September, 2011, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[4] "Understanding the Cloud Computing Stack: SaaS, PaaS, IaaS," *Rackspace*, modified September 12, 2012, http://www.rackspace.com/knowledge_center/whitepaper/understanding-the-cloud-computing-stack-saas-paas-iaas.

in the cloud computing industry maintain that no standard definition exists, and some have even openly criticized the NIST definition.[5]

As mentioned above, the Chinese government largely hews to the NIST definition of cloud computing, but there are a number of exceptions to this general rule. In addition to the NIST standards document, Chinese organizations have utilized other definitions of cloud computing technologies, including definitions developed outside the United States. The Chinese Communications Standards Association (CCSA; 中国通信标准化协会), for example, acknowledges that the NIST definition is generally accepted, but also references a number of industry-led standards in its conception of cloud computing.[6] In particular, CCSA has employed technical reference materials for virtualization, cloud computing security, and cloud storage that were developed by US-based groups, such as the Distributed Management Task Force (DMTF),[7] the Storage Networking Industry Association (SNIA),[8] and the Cloud Security Alliance (CSA).[9] For technical reference material on cloud computing and telecommunications networks, the CCSA has also referenced work developed through the International Telecom Union (ITU, based in Switzerland).[10]

Differing Views on Cloud Computing Definition in the Chinese Government

Even Chinese definitions of cloud computing that use the NIST definition as a shared basis may differ in other important respects. The MIIT's Telecommunications Research Institute (工业和信息化部, 电信研究院) defined cloud computing in its 2012 Cloud Computing White Paper (云计算白皮书) as follows:[11]

"Cloud computing is a method for achieving large-scale computing information processing, which unifies, organizes, and flexibly draws upon various Information and Communication Technology (ICT) information resources through the Internet. Cloud computing utilizes distributed computing and virtual resource management technologies, among others. Using the Internet, it takes spread-out ICT resources (including computing,

[5] Michael Daconta, "Why NIST's definition of cloud computing misses the boat – GCN," *GCN*, modified March 22, 2012, http://gcn.com/Articles/2012/04/02/Reality-Check-NIST-flawed-cloud-framework.aspx?Page=2.
[6] Caiyong Shun, Rao Shaoyang, and Feng Ming, "Urgent Need For Global Standards For Cloud Computing Standardization Research," (云计算亟需标准化 全球标准研究尚起步), *China Communication Standards Association* (云计算亟需标准化 全球标准研究尚起步), modified February 22, 2013, http://www.cwts.org/article_new/show_article.php?categories_id=912a0cdc-aacb-0a21-6620-5125850dd098&article_id=cyzx_51d40d97-dee9-cb98-6166-5125baafbb0f.
[7] "Open Virtualization Format (OVF)," *Distributed Management Task Force Incorporated*, modified June 22, 2013, http://www.dmtf.org/standards/ovf.
[8] "SNIA Storage Cloud," *SNIA*, accessed July 31, 2013, http://www.snia.org/cloud.
[9] "Cloud Security Alliance," *Cloud Security Alliance*, accessed July 31, 2013, https://cloudsecurityalliance.org/about/.
[10] "ITU-T in Brief," *ITU*, accessed July 31, 2013, http://www.itu.int/en/ITU-T/about/Pages/default.aspx.
[11] "The Ministry of Industry and Information Technology's Guidance Concerning Promoting the Informatization of Logistics Work," (工业和信息化部关于推进物流信息化工作的指导意见) *Ministry of Industry and Information Technology* (工业和信息化部), modified January 9, 2013, http://www.miit.gov.cn/n11293472/n11295327/n11297127/15121041.html.

storage, application platforms, and software, among others) and brings them together to form a shared resource pool. Furthermore, it uses dynamic, on-demand, and scalable methods to provide services to users. Users can use various types of terminals (such as personal computers (PCs), tablet computers, smart phones, even smart televisions, among others) to access ICT resource services through the Internet."

Although this definition appears largely in agreement with NIST's, it excludes several of the NIST definition's key concepts. Most notably, it defines cloud computing as having only four – rather than five – essential characteristics, appearing not to embrace the idea that providing "on-demand self-service" exists as a core characteristic of cloud computing. The NIST definition describes on-demand self-service as being the first of the five essential characteristics, stating that "a consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider." The removal of this characteristic leaves open the possibility of adding an additional layer of management and control to Chinese cloud computing systems. If acted upon, this would add extra technical requirements for businesses and likely reduce the competitiveness of foreign firms in the Chinese market due to the need to adapt internationally developed products to Chinese standards.

China's Telecommunications Research Institute's concept of cloud computing also differs from the NIST definition, in that it portrays only three deployment models, rather than four.[12] Only public, private, and hybrid clouds are introduced, with hybrid clouds representing a mixture of both public and private clouds. The white paper does not discuss the concept of a "community cloud" that would be shared by multiple organizations with shared missions, even though distributed computing resources along these lines are employed in some parts of the Chinese scientific research community.

It is important to recognize that the MIIT Telecommunications Research Institute's modified definition does not necessarily represent the views of cloud computing experts in other organizations within the Chinese government. In the absence of official cloud computing standards documents, key government experts appear to have adopted the general NIST definition. For example, Li Guojie (李国杰), an expert for the Advisory Committee for State Informatization (ACSI; 国家信息化专家咨询委员会), offered a definition of cloud computing in a November 2011 presentation that was a direct translation of the NIST definition:[13]
"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

[12] Ibid.
[13] ACSI is a think-tank that provides expert research and policy recommendations to the Chinese State Council on 'informatization' policy and global technological developments. For more information, see Joe McReynolds and James Mulvenon, "The Informatization of the PLA Under Hu Jintao," Strategic Studies Institute/US Army War College and US Pacific Command/National Bureau of Asian Research 23rd Annual People's Liberation Army Conference, October 2012, Carlisle, PA.

Li's presentation also accepted NIST's depiction of the five essential characteristics of cloud computing, including the first essential characteristic of "on-demand self-service" that was excluded from MIIT's 2012 Cloud Computing White Paper. The differences between MIIT, NIST and other definitions within the Chinese bureaucracy may be resolved through the formulation of a single authoritative standard at some point in the future, but such unification has not yet occurred.

China's Process for Defining Cloud Computing Highlights Internal Tensions

Various organizations within the Chinese government have been in the process of defining cloud computing for a number of years. In August 2011, the National Information Technology Standardization Technical Committee Service Oriented Architecture (SOA) Working Group initiated research aimed at developing standards for Chinese cloud computing, since no concrete definition had yet been offered by the national standards organizations. According to the working group, two dozen competing definitions existed in industry at the time, and a comparison of these definitions illustrated disagreement on key concepts between industry, academia, standards bodies, and associations.[14] Major organizations involved in standards development during this period included a number of Chinese government entities: the National Information Technology Standardization Technical Committee (NITSTC; 国信息技术标准化技术委员会) SOA Working Group, MIIT's Information Technology Services Standard Group (工业和信息化部信息技术服务标准工作组, often referred to as the 'ITSS working group' or 'ITSS 工作组'), and MIIT's China Electronics Technology Standardization Institute (CESI; 中国电子技术标准化研究所). The process also included the National Technical Committee for Information Security Standardization (NTCISS;全国信息安全标准化技术委员会) and the National E-government Standardization General Working Group (国家电子政务标准化总体组), which focused on cloud computing standards for government operations.[15]

Reports by these organizations often contradict one another when discussing which organizations have been given primary responsibility for undertaking cloud computing standards development work, which may reflect tensions between the various interest groups involved. For instance, materials published in February 2013 on the website of the Chinese Communications Standards Association (CCSA; 中国通信标准化协会), a non-governmental organization (NGO) offering membership exclusively to corporate bodies, emphasized the role of communications and electronics trade groups in the formation of cloud computing standards, claiming that this work was being managed by CCSA, the Cloud Computing Expert Committee (云计算专委会) under the China Institute of Electronics (CIE; 中国电子学会), an academic and professional body, Cloud Computing Expert Committee, and government working groups on IT services (IT 服务工

[14] Further research to identify other competing definitions suggested that the two dozen competing definitions referenced refer to foreign definitions, not Chinese definitions as this may imply. See "China Cloud Computing Launches the Research Phase for Cloud Computing Standards in 2012," (中国云计算标准进入调研阶段或于 2012 年推出) *Loudi [City] Economic and Information Technology Commission* (娄底市经济和信息化委员会), August 15, 2011, http://sjw.hnloudi.gov.cn/Item/377.aspx.

[15] "Cloud Computing Industry to Upgrade," (云计算产业升级) *Electronic Machinery Online* (机电在线), September 23, 2011, http://market.jdol.com.cn/newsinfo726.html.

作组) and SOA standardization (SOA; 标准工作组) under NITSTC.[16] This description included no mention of the MIIT ITSS working group or the MIIT CESI, despite MIIT's nominally central role in information technology regulation.

Major international cloud computing providers have thus far had only limited and inadequate opportunities to participate in the standards creation process, which may create challenges not only for multinational corporations doing business in China but also for the Chinese cloud computing industry. This issue is directly addressed in the MIIT 2012 Cloud Computing White Paper, which states that the relatively slow development of Chinese cloud computing standards can be partly attributed to the lack of participation in the process by mainstream cloud computing providers.[17]

This is not to say that there is a total lack of multinational corporate participation. According to the US Information Technology Office (USITO), an independent membership-based trade association of US information and communications technology corporations doing business in China, foreign corporations can participate in the CESI, NITSTC SOA, and CCSA standards groups, but often not as full voting members.[18] However, other important working groups, including some groups under NITSTC, do not allow foreign companies to participate even as observers. Even in the industry groups that do welcome foreign participation, the degree of influence exercised by foreign corporations is uncertain and unlikely to be equivalent in transparency and impartiality to the process by which international cloud computing standards are drafted and amended.

[16] "Urgent Need for Cloud Computing Standardization – International Standards Research Still Starting," (云计算亟需标准化 全球标准研究尚起步) *China Communications Standards Association*, February 21, 2013, http://www.cwts.org/article_new/show_article.php?categories_id=912a0cdc-aacb-0a21-6620-5125850dd098&article_id=cyzx_51d40d97-dee9-cb98-6166-5125baafbb0f.

[17] "2012 Cloud Computing White Paper," (云计算白皮书 2012) *China Academy of Telecommunication Research of MIIT*, April 2012, http://www.miit.gov.cn/n11293472/n11293832/n15214847/n15218338/n15224998.files/n15224997.pdf, p. 22. The White Paper does recognize significant progress in the development of some basic cloud computing technical standards, including those for virtual machine formats, data interfacing, and network technology, while noting that standards development has been slow on the whole.

[18] *United States Information Technology Office*, "China's Cloud Computing Policies and Implications for Foreign Industry," November 2012, http://cryptome.org/2012/12/usito-china-cloud.pdf.

Chapter Two: Development and Penetration Rate of Chinese Cloud Computing

This chapter outlines the history of the development of Chinese cloud computing, and then provides a relative comparison of cloud computing technical capabilities and penetration rates in China, the United States, and other leading ICT countries.

The key findings of this chapter are as follows:

- Although the Chinese government first introduced policies specifically aimed at cloud computing technology in 2010, a framework for government support for related technology and industry already existed within China's medium to long-term science and technology planning document.

- Government support and priorities for cloud computing have guided investment and development of the industry, but this appears to have produced mixed results in terms of level of technological sophistication achieved. According to materials published by the China Software Industry Association (CSIA), the development of cloud computing in China has suffered from a lack of understanding, "blind" development, inefficient organization, hastily constructed projects at cloud computing centers, and a general lack of coordination that has resulted in a waste of resources. [19]

- Penetration of cloud computing technology in China lags behind the United States, particularly in business operations, military organizations, and intelligence agencies. Concern with data security and unclear regulations regarding usage appear to be major factors in Chinese businesses' reluctance to adopt cloud computing.

- According to criticisms published by MIIT, China's technical capacity for developing cloud computing technology is limited by systemic weaknesses in the software and integrated circuit industries, which include: lack of core technology, insufficient innovation capabilities, and serious structural personnel problems due to a lack of high-level, well-rounded personnel in leadership positions.

- China's technical capacity for securing cloud computing technology is limited by structural issues in the Chinese information security industry, which MIIT rated as "relatively weak as a whole." Industry deficiencies include: a lack of high-end information security personnel who can meet the industry's development needs, a lack of core technology, too much reliance on importing foreign products and services, and an absence of large enterprises to lead the industry.

History of Cloud Computing Development in China

The Chinese government has guided the direction of cloud computing development in China through strategic investment and support, starting when it identified cloud computing as a

[19] Here, the CSIA appears to refer to a lack of understanding in all parties involved, including policy makers as well as the companies that are involved in the research and development.

strategic emerging industry in 2010. At that time, the State Council issued goals for promoting cloud computing in the 12th Five Year Plan (FYP) (covering 2011-2015), and central government ministries responded with specific plans for how the requirements would be met. Lower level administrative units and organizations (provincial governments, municipal governments, research institutes, companies, research laboratories, and supporting organizations) responded in turn with their own development plans in accordance with the central government's priorities. The development of China's cloud computing industry may thus be traced through the state and ministry-level guiding documents that map the path described above in greater detail. The most relevant documents are:

- China's Medium-To-Long Term Plan For S&T Development
- 12th FYP for Economic and Social Development
- 12th FYP for Cloud Computing
- 12th FYP for Software And Integrated Circuits
- 12th FYP for Information Security And Information Security Industries

Each of these plans is discussed below.

Support for Cloud Computing from China's Central Government

China's central planning organization, the State Council, provided support for development and investment in cloud computing technology through two major planning documents, the National Medium and Long-Term Plan for S&T Development and the 12th FYP for Economic and Social Development.

China's National Medium and Long-Term Plan for S&T Development

Although China's government began to focus on developing cloud computing capabilities in 2010, the foundation for current cloud computing development projects was established earlier, in China's National Medium and Long-Term Plan (MLP) for S&T Development (2006-2020) (国家中长期科学和技术发展规划纲要 2006—2020 年), released by the State Council in 2006. The MLP helped to support the creation of an IT infrastructure that was later employed in cloud computing development.

The MLP was created to help China become an innovation-oriented country by 2020, and to emerge as a world power in science and technology by 2050. It identified S&T challenges facing China, outlined an S&T development strategy, and defined R&D priorities for 2006 until 2020. In particular, it highlighted the importance of developing China's IT industry, and named it one of 11 priority technology sectors targeted for support. The MLP then outlined four broad development goals and seven technological goals for the industry, setting expectations for the particular areas in which the government wanted to see the most progress. The first development goal called for the industry to make breakthroughs in core technologies related to integrated circuits, large-scale software, high-performance computers, broadband and wireless communications, and next-generation networks. These were identified as the technology barriers impeding the development of the information industry. The second and third development goals

both focused on the concept of "integrated innovation" (集成创新) in technology products, with the aim to raise design and manufacturing standards and nurture new technologies and services, while at the same time shifting "integrated innovation" toward application demand. These efforts would encourage the creation of new modern service industries and promote the transformation of traditional industries. The final development idea focused on the development of network security technology and related products, and emphasized the need for trusted networks, the establishment of a system of information security technology safeguards, and technological capacity to guard against any kind of information security incident.

The three technological priorities promoted for the IT industry in the MLP that were most relevant for later cloud computing development were:

- information technology for supporting modern service industries and large-scale application software
- major next-generation information technology and services
- high performance, high confidence computing

The government's promotion of these three technology goals in particular helped support the research, development, and strategic investment in resources that fed into later cloud computing development. One of the MLP's sixteen "Mega Projects," also provided funding vehicles for early cloud computing projects under the *He Gao Ji* (核高基重大专项) Major Project, which included broad support for high-performance computing, large-scale application software, and major cutting edge information technology and services research and development.

China's 12th FYP for Economic and Social Development

China's first attempt to address cloud computing development specifically appeared in the 12th Five Year Economic and Social Development Plan, which was issued by the State Council and CCP Central Committee and ratified in 2011 by the National People's Congress. The outline for the 12th FYP prioritized transforming China from a "technology producer" to a "technology designer," while promoting "leapfrog development" in key fields. It also outlined plans to invest heavily in science and technology R&D, and called for prioritizing industrial development in key sectors, dubbed "strategic emerging industries" (SEIs). The Plan targets SEIs for heavy support with the expectation that they will form the new backbone of China's economy. The SEIs are as follows:

- Biotechnology
- New Energy
- High-End Equipment Manufacturing
- Energy Conservation and Environmental Protection

- Clean Energy Vehicles
- New Materials
- Next-Generation Information Technology

Cloud computing appears as a priority sector for development within the Next-Generation Information Technology Industry (新一代信息技术产业重). Cloud computing is also referenced as an important element of the construction of China's future national information technology infrastructure, with the expectation that it will increase the level of information technology integration.

Support for Cloud Computing From the Ministry of Science and Technology

The Ministry of Science and Technology (MOST), the PRC Central Government's chief ministry responsible for the drafting of S&T development plans and relevant laws, regulations, and rules, provided groundwork for the development of cloud computing S&T development projects within its 12th FYP.

Ministry of Science and Technology 12th FYP

As with the 12th FYP for Social and Economic Development, The 12th FYP Guidelines created by China's Ministry of Science and Technology (MOST) called particular attention to cloud computing as a part of its broader plan for developing "Next-Generation IT" (新一代信息技术). Although next-generation IT as described in the MOST Plan encompassed a wide range of technologies, the Plan highlighted cloud computing projects (中国云工程) along with the national broadband network and new display technologies as three areas of particular importance, signaling that they would receive priority support from the ministry. According to the Plan, cloud computing projects would target three priorities: 1) the development of technical solutions and construction standards for cloud computing, based on indigenously developed technology; 2) mastery of cloud computing and high-performance computing core technologies; and 3) the creation of a national cloud computing platform to guide organs, local governments, and enterprises to form cloud computing platforms of different scales and service models and to cultivate the development of cloud computing.

Support for Cloud Computing Development from the Ministry of Industry and Information Technology

MIIT, the PRC Central Government's ministry responsible for regulating and developing the postal service, Internet, wireless, broadcasting, communications, production of electronic and information goods, software industry, and the promotion of the national knowledge economy, released two FYPs to support the growth of cloud computing services within China that aimed at two specific sub-sectors of the ICT industry: the Software and Information Technology Service Industry Development Plan for the 12th FYP (软件和信息技术服务业"十二五"发展规划) and

the Information Security Industry Development Plan for the 12th FYP (信息安全产业"十二五"发展规划).

Software and Information Technology Service Industry Development Plan in the 12th FYP

The Software and Information Technology Service Industry Development Plan for the 12th FYP, which was released on November 28, 2011, provided guidelines for addressing perceived weaknesses in China's software and information industry. The Development Plan introduced broad strategies for growth, identified specific technology areas for development, and introduced a series of major projects. Broadly, the Plan encouraged the Chinese software and IT industries to seek foreign opportunities, calling on all levels of government to help "backbone," or strategically crucial, corporations set up overseas subsidiaries, establish market networks and R&D centers, and carry-out cross-border mergers and acquisitions. Further, the Plan highlighted the importance of attracting foreign direct investment (FDI) and encouraging foreign multinational corporations to establish R&D centers and headquarters in China. The Plan also encouraged software development outsourcing to support the exportation of Chinese software products and services.[20]

While not the chief focus of the Plan, cloud computing was referenced within three of the Plan's ten prioritized technology areas. MIIT highlighted the importance of research on cloud computing platforms within basic software development, research in cloud computing services as part of service outsourcing development, and research directed at services for cloud computing business models as part of development in emerging IT services. The Plan also included cloud computing innovation development as one of its eight major projects, and created goals of innovative development in cloud computing services as well as rapid industrialization of cloud-computing services. It also called for broad cloud computing demonstrations (in science, manufacturing, and health care, for example) and called for the development of relevant standards and industrial public service systems. Further, it outlined support for the formation of an internationally competitive cloud computing industrial development plan that promoted more robust industrial product chains and related services.

Information Security Industry Development Plan in the 12th FYP

At the same time that MIIT released the development guidelines for the software and information technology industry, it also outlined support for cloud computing technology within its broad information security industry development guidelines for the 12th FYP. The document called on the information security industry to pursue "two historic tasks:" to promote the strengthening of the information security industry, and to enhance its ability to support national security.

[20] Annual Report of China Software & Information Technology Service Industry," (中国软件和信息服务业发展研究报告), *China Software Industry Association* (中国软件行业协会), 2012, p 443.

Information Security Research Projects Related to Cloud Computing

Support Project for Next-Generation Information Technology Application Security (新一代信息技术应用安全支撑工程) This project aims to include research on information security system architectures for cloud computing, as well as for the development of crucial information security technology products and systems.

Information Security Demonstration Project (信息安全示范工程) This project's aims include demonstrations for safe and controlled information security for cloud computing. It also seeks to promote the formation of industry alliances to accelerate the industrialization of information security products and services.

The Plan evaluated the weaknesses within the information security industry and directed state resources towards development priorities in three areas: information security key technologies, information security products, and information security services. The Plan also outlined four major development projects for the industry that would promote its growth and improve its capabilities. Two of the four projects called for research aimed at filling requirements of cloud computing development: the Support Project for Next-Generation Information Technology Application Security (新一代信息技术应用安全支撑工程) and the Information Security Demonstration Project (信息安全示范工程). Both projects are active, but currently the results appear to be mixed. The only Chinese company to release a viable security solution aimed specifically at supporting cloud computing services in China at this time appears to be Qihoo 360.

Cloud Computing Capabilities Gaps between China and the World

Although many elements factor into the equation, the relatively low penetration rate of cloud computing technology in China appears linked to several issues that are common in China's IT sector: distrust of foreign technology (a common theme in literature discussing government requirements for indigenous innovation), a lack of crucial technology required to develop the kind of mature technological capabilities that are needed, and a lack of technical standards and requirements to drive technology development. Recent reports from Chinese government agencies indicate that they are aware of these deficiencies. For example, in January 2013, the director of the China Center for Information Industry Development described the cloud computing industry as being still only in its infancy. He cited major problems in the industry, including a lack of cloud computing services and applications.[21]

On a macro level, self-reported weaknesses in industries that are essential to cloud computing – software, integrated circuits, and information security – underscore the broad challenges facing Chinese firms as they attempt to reach or exceed the technical capacity achieved for cloud computing in other countries. For example, in the realm of information security, MIIT's assessment of China's domestic cloud computing industry published in the Information Security Industry Development Plan for the 12th FYP was that it was "relatively weak as a whole," and listed a number of the industry's key deficiencies:

[21] "Development of Cloud Computing in China Faces Obstacles," SINA.com, January 24, 2013, http://english.sina.com/business/2013/0124/552988.html.

- A reliance on importing foreign products and services
- A lack of core technology
- An absence of large enterprises to lead the development of the industry
- An inability to properly support national security needs
- An inadequate innovation capability
- A lack of high-end information security personnel who can meet the industry's development requirements

MIIT also identified several deficiencies in China's software and integrated circuits industries, some of which are similar to the problems found in the information security industry:

- A lack of enterprises with leading global positions
- At an overall level, the industries are at the low-end of the value chain
- An imperfect industrial innovation system
- A lack of core technology
- An inability to fully realize industry chain synergies
- A lack of an industry development plan supporting leading enterprises and small-to-medium enterprises (SME)
- Serious structural personnel problems – a lack of high-level, well-rounded personnel in leadership positions
- Deficiencies in the industry's capacity for sustainable development

In 2012, the China Software Industry Association (CSIA) released a report on China's software and information technology service industry, which also offered insight into issues affecting the technical capacity of Chinese cloud computing. The report cited six major problems in Chinese cloud computing development, specifically:[22]

[22]Annual Report of China Software & Information Technology Service Industry," (中国软件和信息服务业发展研究报告), *China Software Industry Association* (中国软件行业协会), 2012, p 236.

1. Cloud computing development "lacked understanding;" [23] there was uninformed "blind" development,"[24] and a hasty issuance of projects at cloud computing centers that resulted in a lack of coordination between the research organizations and policy makers involved, and a general waste of resources.

2. China still lacks a mature cloud computing development platform; key prerequisite technologies such as massive data processing and large-scale IT resource management still need to be developed.

3. There are issues that are hindering the development of cloud computing technology for the social management and public service sector. Systemic issues that must be resolved include: a lack of collaboration between government departments, inadequate sharing of government information and resources, and government services outsourcing.

4. There are no successful cases of cloud computing applications in the most important sectors of the Chinese economy, and the capabilities for organizations to integrate cloud computing applications into existing operations and infrastructure need to be improved.

5. Information security is a great challenge due to the large amount of data being collectively stored and managed.

6. There is a lack of standards for cloud computing services, and reliability and security inspection capabilities are weak. Further, user data security and privacy protection require urgent resolution.

Taken together, the CSIA criticisms suggest that the technical capacity of Chinese cloud computing is still limited and that several basic conditions must be met before cloud computing can mature. One of these is Internet speed, which is an important factor in performance for cloud computing services, and where China's cloud computing technical capacity currently lags behind the United States and other leading ICT countries. As of late 2011, the average rate of data transfer in China was 1463 kilobytes per second, five times slower than the rate in OECD countries.[25] China's network speed is further burdened by the government's network monitoring requirements, which slow the speed of Internet traffic. Deschert LLP, an international law firm founded in the United States with practices in Europe, Asia, and the Middle East, in a report on cloud computing in China, noted that "cloud computing only functions as a useful commodity when used with a high-speed broadband connection." [26] These and other infrastructure deficiencies have helped ensure that Chinese cloud computing firms are generally ill-suited to match the services that are provided in other countries with more advanced cloud industries.

[23] Although the source document does not specify which specific elements of development lacked understanding or which particular parties were at fault, in context it appears to suggest that the "lack of understanding" criticism is directed at policy makers and the groups responsible for issuing projects and resources to research organizations.
[24] Even though the source does not clarify what "blind development" refers to, here it appears to refer to the development of cloud computing focused research parks and projects. Still, it may also include a reference to "blind development" of cloud computing technologies by research organizations.
[25] Dechert LLP, "Latest Trends in Cloud Computing in China," *JD Supra Law News*, June 5, 2012, http://www.jdsupra.com/legalnews/latest-trends-in-cloud-computing-in-chin-06403/.
[26] Ibid.

Emerging cloud computing firms in other foreign markets appear to show a relatively higher technical capacity as both providers and innovators. Two companies headquartered in the Netherlands, Interexion and GoGrid, appear to have made particular headway in this area. Interexion, for instance, operates 32 cloud data centers spread across 11 countries, including the United Kingdom, Germany, and France. The Netherland's technical capacity for cloud computing technology is backed by a mature software industry that has a history of innovations and inventions (e.g. Bluetooth technology, WiFi, and Route Navigation). Further, the Netherlands currently has the ICT infrastructure needed for cloud computing and is sometimes considered the leading country for broadband capability in the world.[27] Also, Netherlands-based companies appear to operate in an industry-led, rather than government-led, standards environment, and also show low rates of software piracy, both factors which typically encourage innovation and investment in the software industry. This favorable industry environment shows similarities with that of the US, which BSA reports also enjoy relatively low-levels of software piracy and industry-led standards environment. Published US government standards for cloud computing are not mandatory for commercial systems used outside of the government, though many commercial firms voluntarily adopt these standards.

Cloud Computing Technology Penetration Rates in US and Chinese Sectors

China's rate of adoption of cloud technology in the private sector has, and continues to, lag behind the United States. At the time that China was first publishing its cloud computing priorities, few large Chinese companies were using cloud computing, according to a report by Accenture and the Chinese Institute of Electronics' Cloud Computing Expert Committee (中国电子学会云计算专家委员会). Based on surveys, they found that only 43 percent of Chinese companies were using or testing cloud computing software. Within that group, most were testing software products. The report found that only 27 percent of Chinese companies used private cloud platforms, 30 percent used cloud process services, 4 percent used cloud platform services, and 9 percent used software services. This contrasted with respondents in the United States, where 89 percent were using some form of cloud computing service at the time.[28] As such, the report portrayed a large gap between cloud computing penetration between the United States and China.

It is unclear how much this has changed since that survey was conducted in 2009, but the fact that many of the major concerns expressed within the study still hold true today suggests that cloud technology adoption in China remains relatively slow. According to the study, major concerns for Chinese business professionals included a lack of clear government standards and regulations and data privacy concerns – two issues that still have not been resolved as of July 2013. Further, compared with other countries, the joint study indicated that Chinese consumers are relatively more concerned about data security than citizens of other countries. The survey found that Chinese businesses considered their data a matter of national security and highly

[27] "The Netherlands – Digital Gateway to Europe," Netherlands Ministry of Economic Affairs, Agriculture and Innovation, modified November 2010, http://www.government.nl/files/documents-and-publications/leaflets/2010/11/01/digital-gateway-to-europe/nl-digital-gateway-to-europe.pdf.

[28] Allan E. Alter et.al, *China's Pragmatic Path to Cloud Computing*, 2010, p.33, http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture_Chinas_Pragmatic_Path_to_Cloud_Computing.pdf#zoom=50.

confidential. Similar to the Chinese officials surveyed, Chinese business leaders also appeared to express concerns that,

> "[H]ighly confidential data about the Chinese economy, military, and government, as well as crucial technology and science developments, can be stolen or accidentally disclosed to foreign competitors, or end up in the hands of groups or individuals who seek to overturn the national government."

This concern also manifests in a general distrust of foreign cloud computing technology and providers, which is expressed within the confines of the survey, and may continue to factor into the relatively low levels of cloud computing technology adoption within China as compared with other foreign countries.[29] As of May 2013, Steve Mushero, co-founder and CEO of ChinaNetCloud, claimed that China continued to lag behind the United States in terms of technology adoption, although he expected that "China will develop in a similar way as the U.S…. with more corporations choosing to forgo servers for cloud storage and cloud computing services as time marches forward."[30] Mushero noted that the Chinese government will drive the direction of the cloud computing as an early technology adopter, and the government recently published a decision that permits public organizations to now use their budgets to purchase cloud services.

Even with the support of e-government initiatives, intensive Chinese investment in cloud computing infrastructure has simply built up an excess capacity that is not being fully utilized. According to the website of *China Daily Asia Pacific*, a 2012 report by CCW Research stated that only 20 percent of China's cloud computing capabilities were in use. The report indicated that "most of the investment was used to build servers, data memories (sic) and other hardware infrastructure, but the investors failed to recognize how to facilitate the hardware and integrate cloud services to existing offline businesses."[31]

The use of cloud computing services in the United States is also more extensive in the military, as compared to China's People's Liberation Army (PLA). While the US military already began deploying a secure DOD cloud computing solution in May 2013,[32] there are no indications that China has set out a singular military-wide cloud computing solution. The PLA does not appear to employ cloud computing services within a singular service or branch, and while there is some evidence that a military district incorporated cloud computing technology into its daily operations, the penetration rate of cloud computing technology appears to occur on a limited ad-hoc basis. China may be working on military-wide cloud solutions at the General Staff Department's 61st Research Institute, but that research still appears to be in its early stages.[33] For

---

[29] Ibid.

[30] Robert O'Brian, "Cloud Computing in China, An Insider's Perspective," *Tech Rice*, June 1, 2013, http://techrice.com/2013/05/01/cloud-computing-in-china-an-insiders-perspective/.

[31] Gao Yuan, "Companies' Future is in the Cloud," *China Daily Asia Pacific*, January 21, 2013, http://www.chinadailyapac.com/article/companies-future-cloud.

[32] Zach Whittaker, "iPhones, iPads Cleared for Military Use; DOD Fortifies the Cloud," *ZDNet*, May 17, 2013, http://www.zdnet.com/iphones-ipads-cleared-for-u-s-military-use-dod-fortifies-cloud-7000015549/.

[33] The solutions are qualified as potentially military-wide because the General Staff Department's 61st Research Institute plays a chief role in the development of the PLA's Integrated Command Platform (ICP; 一体化指挥平台). See Yang Yu and Guangmin Wang, "General Staff Department Information Technology Research Institute Created

further discussion of the military implications of China's cloud computing development, see page 38.

Our Military's Unified Command System," (总参某信息化研究所建成我军一体化指挥系统), *GMW.cn*, April 24, 2012, http://mil.gmw.cn/2012-04/24/content_4028245.htm.

Chapter Three: American Exposure to Chinese Cloud Computing Infrastructure

This chapter addresses US consumer use of Chinese cloud computing infrastructure, as well as US owned or operated infrastructure located within China. At present this use is extremely limited both in scope and volume, despite some recent progress toward greater interplay between the Chinese and US cloud computing industries. This chapter explores in detail the underlying causes of this lack of integration, the extent to which any Chinese cloud services provided to US consumers would transparently convey the services' country of origin, and the potential implications of future growth in US-China cloud integration for the information security needs of US consumers.

The key findings of this chapter are as follows:

- Integration between the US and Chinese cloud computing industries and markets is likely to remain heavily limited for the foreseeable future due to both market and regulatory factors.

- At present there is a strong Chinese emphasis on private (rather than public) cloud computing. This means that cloud infrastructure deployed in China by US corporations are generally private clouds solely intended for the use of China-located corporations and consumers.

- The importance of having a nearby Point of Presence (or PoP, the physical location at which cloud computing resources are stored) in public cloud computing creates a strong disincentive for US utilization of Chinese public cloud infrastructure (and vice versa). This disincentive is exacerbated by China's Great Firewall, and recent efforts by investment-seeking provincial Chinese governments to carve out exceptions to the firewall for foreign corporations have been blocked by the central government.

- It is conceivable but highly unlikely that a US consumer might unknowingly have data stored or processed in Chinese cloud computing infrastructure, though specific jointly developed US-China cloud computing projects may carry their own unique concerns in this regard (e.g. directly benefit PLA military users, or include PRC intelligence agency oversight requirements).

US-China Cloud Linkages Are Growing But Remain Limited and Small-Scale

Cloud computing linkages between the United States and China fall largely into three interrelated categories, each with their own set of economic and security considerations. The first involves US corporations that might utilize Chinese-developed, owned, and/or operated cloud infrastructure for their own purposes. The second involves US corporations locating their cloud computing infrastructure within China. The third involves US corporate or individual consumers who *indirectly* utilize Chinese cloud computing, knowingly or unknowingly, by using the services of corporations who do.

Although the differing states of US-China interactions on cloud computing in these three categories should not be freely conflated with each other, a common trend can be observed – and the picture that emerges is of a closed door that is only gradually being opened. Despite the enormous allure of the Chinese marketplace for cloud computing and potential cost savings, US involvement in Chinese cloud computing remains relatively limited and small-scale, and while this may certainly change with time, the current trajectory of investment is not likely to change radically in the short-term. This is the result of numerous barriers to US investment and involvement in Chinese cloud computing, stemming both from restrictive Chinese regulation and the simple realities of the Chinese cloud computing marketplace (discussed in detail below).[34]

On the surface, there does appear to be some increase in the trade of cloud infrastructure and services between the United States and China. Over the past half-decade, US corporations operating in China such as IBM and Hewlett Packard have begun conducting both R&D and the direct sale of cloud computing services to the Chinese domestic market. At present these services are often owned and operated by partially or wholly-owned Chinese entities, though this may change as the industry evolves.[35] An increasing number of Western firms have entered into these partnerships in recent years, such as the recent partnerships formed by Microsoft with China Mobile and by SAP (a German multinational software corporation) with China Telecom.[36] Additional connections appear to be forming in the United States as well, albeit more slowly. One notable example of this is the Chinese national champion corporation Huawei, which has a research center in Silicon Valley partially devoted to cloud computing.[37]

Growing linkages can also be seen in smaller-scale cloud computing services such as MadeiraCloud, a Beijing-based start-up that seeks to provide cloud middleware (software for enabling communication and management of data between clients and servers) for corporations to better manage their consumption of cloud computing services such as Amazon AWS. MadeiraCloud is currently focused on development for the international market, making them a relative rarity among Chinese cloud computing start-ups, but they anticipate potentially shifting focus to the domestic market if public cloud computing were to grow in popularity in China.[38]

However, these linkages appear to be of a relatively small scale when viewed in the context of the size and growth of the Chinese and US cloud computing industries. Most major US public cloud providers such as Amazon and Rackspace do not provide public cloud services with Point-of-Presence in mainland China, whether for the Chinese domestic market or for American users. (Microsoft's Windows Azure platform is slated to become an important exception to this rule in

[34] Issues involving the competitiveness of US firms in the Chinese cloud marketplace are discussed in greater detail in Chapter Five.
[35] "Made in IBM Labs: IBM to Build First Cloud Computing Center in China," February 1, 2008, http://www-03.ibm.com/press/us/en/pressrelease/23426.wss.
[36] See Mark Lee, "Microsoft, China Mobile to Partner on Cloud Computing," *Bloomberg News*, December 17, 2010, http://www.bloomberg.com/news/2010-12-17/china-mobile-microsoft-to-collaborate-on-cloud-computing.html, and Paul Taylor, "SAP-China Telecom deal to offer cloud-based services in China," *Financial Times*, May 26, 2011, http://www.ft.com/intl/cms/s/0/1b1f345a-7fdf-11e0-b018-00144feabdc0.html.
[37] "Research and Development," Huawei Corporation, accessed July 28, 2013, http://www.huawei.com/us/about-huawei/corporate-info/research-development/.
[38] Derrick Harris, "Meet 7 startups that could define the Chinese cloud," *GigaOm*, January 4, 2013, http://gigaom.com/2013/01/04/meet-7-startups-that-could-define-the-chinese-cloud/.

the near future, and is discussed in greater detail below.) The use of Chinese cloud infrastructure by American corporations, while difficult to track, appears to be so small as to be almost nonexistent. The reasons for this limited and uneven integration between the two countries' cloud computing industries are complex, and must be understood in the context of the particular contours of China's cloud computing market and regulatory environment.

US Exposure to Chinese Cloud Computing Infrastructure is Limited by Barriers to US Entry into the Chinese Market

Chinese regulation of cloud computing poses the first major barrier to greater US involvement. The difficulties posed by these regulations stem both from their explicit content and from the varied ways in which vaguely worded regulations may be interpreted by China's powerful regulatory agencies in any given situation. These concerns are reflected in a December 2012 report on US involvement in Chinese cloud computing written by USITO and also in a May 2012 report by the United States International Trade Commission (USITC), an independent federal agency with broad trade-related investigative responsibilities, on the prospects for US-China trade in cloud computing goods and services.[39] The USITO report, intended only for distribution among its members but leaked to the public by the information dissemination website Cryptome.org, draws heavily on the experience of USITO's member companies to lay out the problems faced by US companies attempting to participate in the Chinese cloud computing marketplace. The USITC report makes similar use of contacts within the cloud computing industry, as well as the Chamber of Commerce.

The first concern that US corporations face when offering cloud computing services in China is who will exercise control of the China-based corporate entity under which they are provided. China places strict limits on foreign direct investment in its telecommunications sector, with the precise limits varying slightly according to the type of business being done. "Online data processing" and "data hosting" in particular are activities which are limited to joint ventures and unavailable to Wholly-owned Foreign Entities (WOFE). Currently, Chinese regulators appear to be classifying IaaS cloud computing as a "value-added telecommunications service," which in turn means that foreign investment is limited to 50 percent ownership of a joint venture, and that foreign firms can only partner with one of a handful of partners in the state-owned telecommunications industry.

These ownership requirements are complemented by regulatory requirements placed on hardware and software deployed in cloud computing centers, such as the Multi-Level Protection Scheme (MLPS), the Commercial Encryption Regulations, as well as other regulations concerning the hardware and software to be deployed in establishing IaaS operations.[40] These myriad regulations place onerous requirements on US corporations seeking to provide cloud services and infrastructure in China, in some cases requiring the sharing of source code and other

[39]United States Information Technology Office, "China's Cloud Computing Policies and Implications for Foreign Industry," November 2012, http://cryptome.org/2012/12/usito-china-cloud.pdf, and Renee Barry and Matthew Reisman, "Policy Challenges of Cross-Border Cloud Computing," *United States International Trade Commission Journal of International Commerce and Economics*, May 2012, www.usitc.gov/journals/policy_challenges_of_cross-border_cloud_computing.pdf.

[40] See, for example, United States Information Technology Office, "China's Cloud Computing Policies and Implications for Foreign Industry," November 2012, http://cryptome.org/2012/12/usito-china-cloud.pdf.

potentially sensitive information. Such requirements naturally raise concerns regarding the illicit appropriation of foreign intellectual property by Chinese partners, and acts as a de-facto bar to entry for US corporations who see these regulations as an unacceptable risk to their intellectual property.

In some cases, regulation explicitly bars US corporations entirely from providing certain cloud services to certain industries or types of institutions, such as in the Chinese banking sector.[41] However, the practical effect of Chinese regulations on foreign firms is not always so clear-cut. As with many other sectors of the Chinese economy, the USITC report concludes that Chinese cloud computing regulation is "flexible to the point of being unpredictable." As a result, US corporations that provide cloud computing services may take a pessimistic view both as to whether future laws and regulations will impact their commercial activity in China, and as to the likelihood that Chinese laws and regulations will be enacted and enforced impartially. As with other information technology sectors, the presence of Chinese national champion corporations such as Huawei, ZTE, and Datang in the cloud computing market raises justifiable fears among foreign corporations that after entering the Chinese market they will find themselves targeted by new regulations specifically designed to advantage those national champions at foreign expense.[42]

Concerns surrounding the establishment and ownership of cloud computing infrastructure in China are matched by the complexities involved in attempting to commercially operate that infrastructure. IaaS services in China are covered by the MIIT Internet Content Provider (ICP) licensing system, which licenses and regulates every company providing Internet content or services hosted in China. Without such a license, virtually every action taken in the normal course of conducting commercial activity on the Internet is illegal. Cloud data centers, like any other data centers in China, are required to host only clients with an ICP license, effectively banning the use of Chinese cloud computing and data centers by most foreign corporations that are not already operating inside China. The USITO report further claims that, perhaps as a result of these regulations, a number of well-known US-based cloud computing services are inaccessible from Chinese IP addresses, a claim which was unable to be independently verified or disproven.

While the concerns mentioned above are indeed substantial, the impact of these regulatory barriers is not uniform, nor are they entirely insurmountable for US corporations. The regulatory regime may even improve in the future; as discussed below, there have been efforts in recent years to carve out exceptions to these rules for certain foreign companies (contingent on participation in one of several proposed Special Cloud Computing Zones, campuses designed exclusively for investment by foreign cloud computing firms that operate under a more relaxed regulatory framework) in order to encourage multinational corporations to make use of Chinese cloud computing services. However, these efforts have not yet come to fruition (and as discussed

[41] Renee Barry and Matthew Reisman, "Policy Challenges of Cross-Border Cloud Computing," *United States International Trade Commission Journal of International Commerce and Economics*, May 2012, www.usitc.gov/journals/policy_challenges_of_cross-border_cloud_computing.pdf.
[42] See James McGregor, "The 'National Champion' Ecosystem," in the US Chamber of Commerce report "China's Drive for 'Indigenous Innovation': A Web of Industrial Policies," July 2010, http://www.uschamber.com/sites/default/files/reports/100728chinareport_0.pdf.

below, may be abandoned entirely for the foreseeable future), leaving these onerous rules as active regulations that US corporations operating in China must take into account.

These concerns may also be somewhat mitigated when American corporations are participating in the cloud market with the sole intention of serving Chinese clients. In those instances, however, additional challenges confront US companies in the Chinese domestic market. One major concern is an ongoing tendency for Chinese state regulatory agencies to establish China-specific standards and protocols that become requirements for products sold within China. These standards, even if not fully adopted or mandated, are particularly likely to be enforced for municipal and provincial government contracts, a large and important segment of the Chinese market for most forms of information and communications technology.

Such standards, which have been enacted in the past in realms such as digital visual surveillance and mobile communications, can sometimes have the effect of bifurcating the market. They often work to the advantage of domestic corporations (particularly larger and well-connected domestic corporations which may have an inside track during the development of regulations and standards), allowing them to increase their domestic market-share. For foreign corporations, however, they may dramatically increase the costs (due to the requirement to custom-design products for the Chinese market) and uncertainty (since regulations may continue to evolve without transparency or outside input) of continued foreign participation in the Chinese market.

The unique structure of the domestic Chinese market for cloud computing services, particularly the Chinese emphasis on private, rather than public cloud computing, also works to disincentivize more extensive participation by US corporations. In the United States, for example, the sale of public cloud services is a robust growth market. In China, by contrast, both the regulatory environment and the current priorities of the Chinese IT sector have resulted in the majority of sales of corporate cloud computing services involving the deployment of private clouds within domestic corporations rather than the utilization of public cloud infrastructure.[43]

This emphasis on private cloud development can be seen not only in China's private sector but also at the governmental level, as one component of China's ongoing, multi-faceted "e-government" initiatives. Within the Chinese central government, a focus on cloud computing and cloud storage arose in recent years partly as a reaction to the difficulty government agencies experienced retrieving and restoring their data in the aftermath of the Sichuan earthquake.[44] In the Chinese governmental system, broadly defined strategic priorities such as e-government generally tend to acquire more concrete definitions and mandates for action over time, as various political and regulatory bodies integrate the concepts into their strategic planning. These bodies then issue guidance as required to provincial and municipal authorities across China for broad implementation.

As a result of this 'trickle-down' dissemination of strategic guidance, procurement contracts for goods and services tied to these major government initiatives have the potential to be 'market-

[43] Derrick Harris, "Meet 7 startups that could define the Chinese cloud," *GigaOm*, January 4, 2013, http://gigaom.com/2013/01/04/meet-7-startups-that-could-define-the-chinese-cloud/.
[44] Conversation with top China-based cloud computing professional, based on his conversations with relevant government officials.

making,' with firms entering the market in order to chase a broad and stable government client-base. In cases where government procurement requirements demonstrate little variance across differing regions, jurisdictions, or government agencies, selling standardized private cloud solutions to numerous government entities can be especially lucrative. Chinese firms will generally have an advantage in markets dominated or shaped by government procurement, as a result of both their tendency to possess (through their experience and connections) a superior ability to navigate government bureaucratic channels and explicitly stated government preferences for domestic procurement in key technology areas.

The focus on private cloud computing in turn influences how US corporations interact with the Chinese market. Many of the Chinese firms that provide private cloud services claim to have partnerships with US and multinational cloud computing firms, but these partnerships appear to consist almost entirely of the purchase of foreign hardware, software, and other support infrastructure for eventual resale to their Chinese customers as part of the development and sale of cloud computing architectures. Meanwhile, US providers of cloud computing middleware and other services that have developed their businesses to interface with an industry-wide emphasis on public cloud computing often find that this strategic direction does not position them for significant growth in China's current private cloud-focused regulatory and market environment.[45]

Most Current US-China Cloud Linkages Do Not Pose Large Security Risks

Growth in the scale of private cloud services and capabilities does not generally give rise to worries regarding the security of the sensitive information of US persons and corporations, since the infrastructure in question is being installed in China for Chinese use. However, the individual US firms in question may have concerns regarding whether their intellectual property rights will be respected in these arrangements. There is reason to worry: Chinese information technology firms such as Inspur have stated publicly that they see top-end cloud computing technology in the server industry as still being in the hands of multinationals such as IBM, and in past situations the result of such disparities has often been Chinese technology firms gaining unlawful access to leading-edge technology through means such as joint ventures.[46] Nevertheless, those concerns are along the same lines as those felt by information technology firms selling all manner of enterprise-grade equipment to China, rather than being something unique to the cloud computing industry.

At present no publicly available evidence suggests that the converse scenario, in which Chinese-origin cloud computing hardware and software might hypothetically be deployed in the private cloud infrastructure of US organizations, should be an area of particular concern. It is difficult to gauge the extent to which such hardware is presently in use in US corporate private clouds, since much of the hardware can be used for purposes other than cloud computing and could be procured without corporate agreements of sufficient prominence to be touted publicly by either party. Although Chinese-developed or manufactured hardware and software could conceivably

[45] See, for example, Derrick Harris, "Meet 7 startups that could define the Chinese cloud," *GigaOm*, January 4, 2013, http://gigaom.com/2013/01/04/meet-7-startups-that-could-define-the-chinese-cloud/.
[46] Yu Dawei, "Cloud Computing on the Far Horizon," *Caixin Online*, November 17, 2010, http://english.caixin.com/2010-11-17/100199352.html.

contain 'backdoors' or other malicious code or components, the few large Chinese corporations in a sufficiently advanced position to develop and supply such products internationally would see their global market share vanish overnight if such a compromise were discovered, giving them a strong material incentive not to engage in such behavior.

Even if one conceives of an extreme hypothetical in which that incentive structure were ignored, for example as part of a Chinese state-directed espionage campaign, US private cloud infrastructure remains a relatively low-value target for such high-risk endeavors when compared with the publicly known and widely discussed vulnerabilities of the US supply chain for non-cloud defense and defense-industrial computing and electronics to reliance on China-sourced components. Simply put, any valid concerns regarding potential Chinese backdoors or malicious components in cloud computing technology purchased by US corporations constitutes a single permutation of the broader vulnerability of the US information technology supply chain, not a phenomenon unique to cloud computing.

Finally, due in part to the barriers discussed above, when Chinese and US corporations do have a need for cloud computing services located in one another's country, it is generally for the purpose of providing service to local customers, rather than for the storage and transmission of sensitive data from abroad. As an example, prominent providers of US-based cloud computing services such as Rackspace and Amazon offer US-based cloud computing services to Chinese corporations doing business in the US, and Chinese firms are increasingly offering the same for US corporations doing business in China.[47]

Some US-China Joint Cloud Ventures Do Carry Security Risks

However, some US-China joint cloud computing ventures do carry less hypothetical, more concrete security concerns. The US firm Eucalyptus has entered into an agreement with the China Electronic Technology Group Corporation 32nd Research Institute (CETC 32nd RI) to conduct joint cloud computing research.[48] The CETC 32nd RI has extensive ties to the PLA.[49] These ties are generally only acknowledged in Chinese sources and the organizations involved are not transparent about the specific project linkages. Furthermore, CETC as a broader entity explicitly follows what it terms its "3-3-3 Transform and Ascend Strategy," (三三三转型升级战略) whereby foreign trade and collaboration is described as directly fueling CETC's development of not only its civilian development, but also its military products.[50]

[47] Discussions with Rackspace and Amazon sales representatives; also see, for example, the website of the ChinaNetCloud corporation, accessed July 28, 2013, http://www.chinanetcloud.com/.
[48] "CETC32 and Eucalyptus Sign Strategic Partnership to Accelerate Cloud Computing Adoption in China," Eucalyptus Corporation, April 2, 2012, http://www.eucalyptus.com/news/cetc32-and-eucalyptus-sign-strategic-partnership-accelerate-cloud-computing-adoption-china.
[49] Matthew Luce, "A Model Company: CETC Celebrates 10 Years of Civil-Military Integration," *Jamestown Foundation China Brief,* Volume 12, No. 4, February 21, 2012, http://www.jamestown.org/single/?no_cache=1&tx_ttnews%5Btt_news%5D=39031.
[50] LeighAnn Ragland, Joe McReynolds, Debra Geary, "China's Defense Electronics and Information Technology Industry," UC Institute on Global Conflict and Cooperation Minerva Conference on Chinese Defense Research and Development, July 2012, San Diego, CA.

While the specific content of Eucalyptus' joint research with the CETC 32nd RI may not involve technologies or infrastructure specifically designated as militarily sensitive, it may nevertheless result in some form of unintended technology transfer to the PLA and thus support China's military informatization objectives. Reports in the media stating that Eucalyptus has decided to provide the CETC 32nd RI with the "full source code for its enterprise-level products" have raised additional concerns. However, taking into account the open-source nature of Eucalyptus' primary platform, it is unclear whether the source code being given to CETC 32nd RI is being described accurately in these reports, and by extension whether the provided code is in any way sensitive or proprietary.[51]

Efforts by Chinese Municipalities to Establish Special Cloud Computing Zones for Overseas Customers Have Failed

Although there is presently little use by US consumers of cloud computing infrastructure that is Chinese developed, owned, or operated, this may eventually change as the Chinese cloud computing industry and supportive provincial governments attempt to remedy some of the key issues limiting US adoption. One important recent initiative along these lines was the attempted creation of "International Offshore Special Cloud Computing Zones." Beginning with Chongqing, these zones aimed to offer cloud computing and storage services exclusively to overseas businesses. According to Chinese news reports, these services would be *explicitly exempted* from China's usual "Great Firewall" Internet monitoring systems.[52] Despite the promise of the Zones, however, these efforts have not come to fruition. They remain worthy of examination both as a guide to what future US-China cloud integration might look like, but most importantly they offer an indication of the limits of the Chinese central government's flexibility in accommodating US corporate interests.

The Chongqing Special Cloud Computing Zone, sometimes referred to as the "Liangjiang International Cloud Computing Center" (两江国际云计算中心), was the pilot project for this concept.[53] The effort dovetailed with Chongqing's larger efforts under the 12th FYP to fashion itself as "China's Model City for Service Outsourcing" (中国服务外包示范城市).[54] Chongqing is the fourth Chinese city to establish an extensive Cloud Computing infrastructure, following Hong Kong, Shenzhen, and Tianjin, though it was the first to propose opening that infrastructure up to foreign corporations for their special use.[55]

---

[51] See "CETC, Eucalyptus Systems to Establish Joint Lab in Shanghai," *SinoCast Daily Business Beat*, April 9, 2012, http://technews.tmcnet.com/news/2012/04/09/6244299.htm, and Marten Mickos, "Together We Build Cloud," Eucalyptus Corporation, June 19, 2012, http://www.eucalyptus.com/blog/2012/06/19/together-we-build-cloud.

[52] See, for example, Steven Millward, "China Plans a 'Cloud Computing' Zone, Free From Great Firewall," June 23, 2011, http://www.techinasia.com/china-cloud-zone-no-firewall/.

[53] "Liangjiang Special Investment District Will Be Available to Foreign-owned Telecommunications Services," ("两江新区将设数据特管区 电信业务外商可独资") *Chongqing Commerce Daily*, June 15, 2011, http://chongqing.mofcom.gov.cn/aarticle/sjshangwudt/201106/20110607599745.html.

[54] "Chongqing's International Offshore Cloud Computing Project Construction Shows Preliminary Success," ("重庆国际离岸云计算项目建设初战告捷") February 21, 2011, http://news.163.com/11/0221/09/6TDJ3RGH00014JB5.html.

[55] "Go-live of First Cloud Computing Internet Data Center (IDC) of Chongqing," *Chongqing Today*, April 2, 2013, http://en.cq.gov.cn/ChongqingToday/News/3913.htm.

In the end, however, the enthusiasm of Chongqing and other local governments for the Special Zone concept ran up against opposition from the central government, most notably MIIT, which effectively terminated the plan.[56] The general difficulty of obtaining central government approval for a plan to grant foreign companies an explicit exemption from certain politically sensitive censorship regulations and processes appears to have been an important factor in the plan's demise. Even if such approval were granted, however, key elements of the plan were internally contradictory. If the Zones had truly only allowed for foreign corporations and foreign data, those corporations would have been unable to serve their local Chinese clients despite the proximity of their cloud resources, lessening the appeal of participation. However, if foreign corporations were allowed to serve both Chinese and foreign customers using Special Zone assets outside the firewall, the greater freedom of action granted to them might place Chinese corporations at a disadvantage against foreign corporations in providing enterprise-level services in China. Even if the program had received strong backing from the central government, these conflicting interests might have eventually jeopardized the program's prospects.

Despite the failure of the ambitious Special Zone proposal, foreign cloud computing in China continues to expand, albeit in more modest ways. The foreign telecommunications multinational Pacnet's growing presence in Chongqing is an excellent case in point. While planning for construction of the Special Zone in 2011, Chongqing had initially selected Pacnet as its main partner for the project, with the goal of leveraging Pacnet's expertise in managing international cloud infrastructures and large Asian client-base to attract multinational companies to join the project upon its completion.[57] Pacnet is the largest independent telecommunication service provider in Asia, with a wholly-owned undersea cable network stretching across the Asia-Pacific.[58] Although it is not a US corporation and its main characteristics are not fully analogous to those of its American competitors in the cloud computing market, its operations in Chongqing, particularly in the aftermath of the demise of the 'Special Zone' concept, provide a working example of how major US cloud computing providers might one day structure their cloud computing arrangements in China.

Although the Special Zone failed to materialize, Pacnet has continued to establish cloud computing infrastructure in China along more limited and traditional lines. The Chongqing Government announced in April 2013 that Pacnet's "Pacific Telecommunication Chongqing Internet Data Center" or "Pacnet Data Center Chongqing (CQCS1)" (太平洋电信重庆数据中心) had begun operation on March 27th, 2013.[59] At CQCS1, Pacnet is primarily focusing on providing cloud data services for customers with extensive business in China. The data center itself is controlled by a foreign equity joint venture, which in turn connects with Pacnet's larger

[56] Discussion with China telecommunications industry professional with direct contact with relevant organs of the Chinese government.
[57] "Pacnet Develops Chinese Cloud Data Center," July 3, 2011, https://www.datacenterdynamics.com/tr/mobile/focus-news/story/34291.
[58] "Our Network," Pacnet Corporation, accessed July 28, 2013, http://www.pacnet.com/about-pacnet/our-network/.
[59] "Go-live of First Cloud Computing Internet Data Center (IDC) of Chongqing," *Chongqing Today*, April 2, 2013, http://en.cq.gov.cn/ChongqingToday/News/3913.htm, and Zhong Zhi and Bing She, "重庆首个云计算数据中心竣工投运," ("Chongqing's first cloud computing data center was completed and put into operation") *Chongqing Commerce Daily*, March 28, 2013, http://www.cq.xinhuanet.com/2013-03/28/c_115185793.htm, and "Pacnet Data Center Services – Chonging (CQCS1)," Pacnet Corporation, accessed July 28, 2013, http://www.pacnet.com/enterprise/hosting/pacnet-datacenter-services/chongqing/.

wholly-owned Asia-Pacific data network.[60] Perhaps in order to assuage any client worries about using cloud services based in China through a joint venture, Pacnet promises that "their hosted equipment is managed by Pacnet's own data center experts."[61] This follows on from Pacnet's construction of two cloud data centers in Hong Kong (with the second completed in 2012), which are also fully operated by Pacnet and make use of Pacnet's wholly-owned landing stations, connecting it to Pacnet's subsea cable network. The Chongqing government hopes that this development will serve as a "strong impetus for the construction of a national level offshore data processing center" and will prompt reconsideration of MIIT's earlier decision, though there are no indications of that occurring.[62]

Microsoft Deal With 21Vianet Offers Access to Chinese Cloud Computing Infrastructure[63]

The Microsoft and 21Vianet cloud computing partnership provides an avenue for customers to use China-based cloud computing resources operating a version of Microsoft's cloud computing technology. 21Vianet is a Chinese data center services provider with a NASDAQ-listed corporate vehicle incorporated in the Cayman Islands to avoid the telecommunications ownership restrictions discussed earlier in this chapter.[64] Microsoft has agreed to provide a version of its 'Office 365' SaaS and 'Windows Azure' PaaS and IaaS offerings to 21Vianet, which will then be in charge of operating them locally for Chinese consumers.[65]

This partnership, which operates under the approval of the Shanghai municipal government (and thus is potentially subject to oversight from the same), has features which cause it to stand apart from the usual cooperation agreements struck between foreign developers of cloud technology and Chinese firms importing and adapting that technology for the domestic market. It aims to use foreign technology to provide a public cloud service to Chinese consumers, in contrast with the general focus in China on private cloud development. The public cloud services provided by 21Vianet are separate instances of the Windows Azure and Office 365 cloud services from those offered by Microsoft, with customers not encountering any direct bridge or contractual linkage between the local Chinese implementation and Microsoft's global cloud computing services. Since the 21Vianet cloud is operated independently but based on essentially the same technology as Microsoft's global cloud services, global customers (assuming they sign a separate contract

[60] "Pacnet Launches Chongqing Data Center," *Street Insider*, accessed July 28, 2013, http://www.streetinsider.com/Press+Releases/Pacnet+Launches+Chongqing+Data+Center/8213537.html.

[61] "Pacnet Data Center Services – Chongqing (CQCS1)," Pacnet Corporation, accessed July 28, 2013, http://www.pacnet.com/enterprise/hosting/pacnet-datacenter-services/chongqing/.

[62] "Go-live of First Cloud Computing Internet Data Center (IDC) of Chongqing," *Chongqing Today*, April 2, 2013, http://en.cq.gov.cn/ChongqingToday/News/3913.htm.

[63] An earlier version of this report inaccurately characterized certain aspects of the Microsoft-21Vianet partnership, including an assessment that users of the China-based Windows Azure platform offered by 21Vianet and users of Microsoft's global Windows Azure platform would be technically and contractually able to fluidly move data and services between the two systems. This assessment was based on inaccurate information provided to the authors by Microsoft sales and support employees familiar with US services. The authors would like to thank Microsoft for their assistance in clarifying the details of 21Vianet's Windows Azure service.

[64] Mark Lin, "Risks Outweigh Emerging Market Opportunities For This Stock," *Motley Fool*, April 8, 2013, http://beta.fool.com/asiavalue/2013/04/08/emerging-market-opportunities-come-with-emerging-m/29565/.

[65] Lara Luo, "21Vianet Teams with Microsoft for Shanghai-based Cloud Offering," *Data Center Dynamics*, November 22, 2011, http://www.datacenterdynamics.com/focus/archive/2012/11/21vianet-teams-microsoftshanghai-based-cloud-offering.

with 21Vianet) can take applications they have written for Windows Azure and deploy them via the Chinese Windows Azure portal without having to make any major changes to the code (and vice versa).

Despite this ease of compatibility, it appears unlikely that Chinese cloud computing will be used by US corporations to store customer data from US citizens or provide them with services. The most plausible reason a US company would utilize Chinese cloud infrastructure would be to better serve Chinese consumers in the domestic market, not to store global customer data there. Furthermore, as numerous cross-border intrusion sets have demonstrated, storing sensitive data on US-based servers does not necessarily guarantee that data's security from foreign hackers. As the Chinese cloud computing market continues to evolve, however, these risk-mitigating considerations may not continue to hold true, and the frequency of China-based cloud infrastructure usage by American consumers may increase as global technology companies offer their services in China and multinational corporations decide to use them.

In addition to the uncertainties facing US companies utilizing Chinese cloud architecture, the Microsoft-21Vianet partnership raises a potential security risk for Windows Azure users who have no business in China whatsoever, a risk stemming not from technical vulnerabilities but from the Chinese government itself. Chinese national security laws give the government incredibly broad powers to make compromising demands from information and communications technology companies operating within its borders.[66] As discussed extensively in the recent Congressional hearings regarding Huawei's global operations and its ties to the Chinese state, the Chinese government could at any time demand access to virtually any information under 21Vianet's control. Such information likely would include information about how Windows Azure is deployed and administered, though since 21Vianet does not possess the Windows Azure source code, any source code access could only be provided by Microsoft.[67] Through reverse engineering and other means, such access to proprietary information could aid China's defense and intelligence services in better understanding the workings of Windows Azure deployments in order to more effectively compromise them.

The Microsoft-21Vianet deal carries another risk: since the Windows Azure and Office 365 software executables will be on servers in China, experienced Chinese software forensic experts could be able to reverse engineer the Azure source code. Some actors may be interested in finding vulnerabilities or copying the source code to create competitive products. Reverse engineering techniques are well understood within the software engineering industry, and specialized reverse engineering tools are readily available. Reverse engineering is a widely used method around the globe for discovering software vulnerabilities. The practice is so widespread that the release of a security patch by Microsoft speeds the authoring of exploits designed to utilize the vulnerability that has just been patched, likely because miscreants are reverse

[66] Article 11 of Chapter 2 of the State Security Law of the People's Republic of China states that "where State security requires, a State security organ may inspect the electronic communication instruments and appliances and other similar equipment and installations belonging to any organization or individual."

[67] In the past, Microsoft has elected to provide the Chinese government with the opportunity to view parts of the source code for Microsoft Windows and other products.

engineering the patch itself.[68] Using reverse engineering to create a copy of functionality is allowed in the US under copyright law, but is generally prohibited through software licensing terms. Enforcing these license terms in China may be difficult.

In September 2013, Microsoft Windows Azure public cloud solution (PaaS) and Microsoft's Global Foundation Services cloud infrastructure (IaaS) received "provisional authorization" for use by US government agencies by the Federal Risk and Authorization Management Program (FedRAMP), a "government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services."[69] Aside from the question of Windows Azure's "provisional authorization," increased use of Windows Azure by US government entities could increase risks to US government agencies, since any potential exploitation of the 21Vianet-controlled components of Windows Azure's operating structure by China's defense or intelligence services or other criminal elements could result in the discovery of a method of compromising Microsoft's platform in the future.

[68] Ashish Arora, Anand Nandkumar, Rahul Telang, "Does information security attack frequency increase with vulnerability disclosure? An empirical analysis," *Information Systems Frontiers,* Volume 8 Issue 5, 2006.

[69] FedRAMP is a multiagency program is made up of computer security experts from the National Institute of Standards and Technology, US General Services Administration, Department of Homeland Security, Department of Defense, National Security Agency, Office of Management and Budget, Federal Chief Information Officers Council, and private industry. "FedRAMP FAQs," *US General Services Administration*, June 29, 2012, http://www.gsa.gov/portal/category/102439; "FedRAMP Compliant CSPs," *US General Services Administration*, November 7, 2013, http://www.gsa.gov/portal/category/102375.

Chapter Four: Risks and Vulnerabilities of Chinese Cloud Computing

This chapter assesses the potential risks and security issues associated with the use of Chinese cloud infrastructure for US consumers, including whether or not the choice to use China-based (as opposed to US-based) infrastructure will be transparent to those consumers. A technical overview is then provided of China's potential uses of cloud computing technology, ranging from boosting private-sector competitiveness and the resiliency of government and military systems to more offensive applications such as cyber attacks and censorship activities. Finally, a security assessment is provided of the vulnerabilities of Chinese cloud computing infrastructure, and the extent to which those vulnerabilities would be unique to the Chinese situation or along the same lines as global cloud computing security issues.

The key findings of this chapter are as follows:

- Although risks posed to US consumers by Chinese cloud computing is limited due to low level of usage discussed in Chapter Three, hypothetical future growth in US consumer use of Chinese cloud computing would likely raise significant security concerns.
    - Regulations requiring foreign firms to enter into joint cooperative arrangements with Chinese companies in order to offer cloud computing services may jeopardize those services' information security arrangements.
    - Chinese-language news sources indicate that China's primary foreign intelligence collection organization, the Ministry of State Security, has taken an oversight role in projects aiming to bring foreign cloud computing investment to China.

- China is developing cloud computing technology for a wide range of private-sector, civilian, military, and government uses, including both increasing the resiliency of IT systems by enabling them to continue operation despite the failure of individual computing nodes, and as a component of its ongoing efforts to modernize and 'informatize' the People's Liberation Army.

- Chinese cloud computing infrastructure could be used for offensive cyber operations, but the same is true of public cloud computing platforms globally. If Chinese public cloud infrastructure were ever to become unusually popular for these purposes, it would likely be due to a relative lack of oversight and rules enforcement of users' conduct by Chinese service providers, not due to Chinese cloud infrastructure being more 'weaponized' than its American equivalent.

- By the same token, vulnerabilities in Chinese cloud infrastructure appear to be largely the same as the vulnerabilities found in other cloud infrastructure around the globe. To the extent Chinese cloud infrastructure might be on the whole less secure, it would likely result from increased use of Chinese hardware and software (which, generally speaking, tend to have more security holes than their American counterparts), not from the fundamental design of that infrastructure.

Currently, Chinese efforts to sell cloud computing services to the outside world are still in their infancy, but if these offerings were to reach maturity and eventually achieve widespread adoption, the end result might be significant amounts of US corporate data ending up on servers under Chinese control. Ideally, this process would be transparent to the US corporations and consumers involved, each of whom has individually weighed the security risks of storing data in China and knowingly chosen to use Chinese cloud services providers despite potential risks.

In practice, however, there are several potential reasons for caution and concern. Some of these fears are legitimate. Others are inflated beyond the actual threat posed, are unlikely to come to pass for any number of reasons, or are simply hazards resulting from the general characteristics of all cloud systems rather than anything specific to the use of Chinese infrastructure.

The first cause for concern is the question of whether or not it will be accurately represented to consumers of Chinese cloud computing services that China is that service's country of origin. There are many reasons why a US entity might actively desire to purchase cloud computing services in China, either on a general best-value basis or in order to obtain what is referred to by the industry as PoPs in China. However, users of Chinese cloud computing services would be unable to take appropriate security precautions if they lacked full knowledge of those services' country of origin.

One practice that might lead to such obfuscation is the business-to-business reselling of cloud computing services.[70] There is no evidence that any eventual Chinese Special Cloud Computing Zones (or other such entities) will permit resale, or that in the course of resale the cloud services' country of origin would necessarily become obscured. Nevertheless, the multiple layers of ownership would present at least a hypothetical possibility for this to occur. Ultimately, since full disclosure of the PoP for each client's data is firmly ingrained as industry-wide best practice, it appears relatively unlikely that this will grow into a major problem.

Even if a US corporation knowingly makes use of Chinese cloud computing infrastructure, that corporation's clients and customers could still conceivably have their data stored in Chinese infrastructure without their knowledge. US corporations may find both a cost incentive to purchase cloud computing and storage services from China and a public relations disincentive to publicize that fact, due to China's reputation for attempting to illicitly acquire sensitive data from US corporations. Looking beyond purely financial considerations, however, the actual likelihood of this occurring in practice is greatly reduced by the substantial degradation of service for US consumers that utilizing a Chinese Point of Presence would cause. Chinese cloud computing is much more likely to be harnessed by US corporations doing business in China to provide services to their Chinese clients.

The second and perhaps more disconcerting issue is the direct involvement of the Chinese intelligence services in government-led cloud computing development aimed at attracting foreign clients. Although the Chongqing Special Cloud Computing Zone project was being overseen by the Chongqing municipal government, the approval process for setting it up has gone through

[70] See, for example, "Cloud Computing Resellers Hosted by Rackspace," Rackspace Corporation, accessed July 28, 2013, http://www.rackspace.com/cloud/resellers/.

both MIIT and the Ministry of State Security (MSS).[71] The MSS is China's primary civilian intelligence agency focused on the collection of foreign intelligence and is publicly known to operate extensive intelligence collection efforts aimed at US corporate and government assets.[72] MIIT's involvement in the Special Cloud Computing Zone is mentioned in a number of English-language reports on the project; the involvement of the MSS is only mentioned in Chinese sources.

The MSS's planned involvement in the Chongqing Special Cloud Computing Zone did not merely consist of a one-time stamp of approval. According to a letter sent by the MSS to the Chongqing authorities regarding the project, the MSS was working to "actively support and coordinate with" the Chongqing municipal government on this project on an ongoing basis. As part of their mission of "safeguarding national information security," the MSS was to be providing "leading guidance and corresponding requirements."[73]

Even if the MSS had not explicitly acknowledged any involvement in the project, the potential for Chinese espionage would be a significant concern that any foreign corporation weighing involvement must consider. The inherently secretive nature of espionage, combined with China's history of having few qualms about targeting foreign corporations for intelligence collection, would make it difficult for the Chinese to fully assuage these fears. The MSS's decision to explicitly state their involvement, particularly under a nebulously-worded mandate allowing them broad freedom of action, can only heighten these concerns. This precedent should cause all US corporations considering participation in Chinese cloud computing projects to question their prospective Chinese partners regarding whether the MSS has any oversight role in that project.

Cloud Computing Censorship Activities

Given that one of the major information technology projects of the Chinese central government is its ongoing Internet censorship and monitoring regime, it is reasonable to question whether advances in the Chinese cloud computing industry will serve to strengthen China's ability to restrict its citizens' freedoms of speech and association. At present, however, there are no known cases of cloud computing technology being used by the Chinese government for the purposes of censoring of the Internet. The key ongoing challenges faced by the Chinese Internet censorship apparatus are human, not technological; they hinge on the government's ability or inability to monitor and shape rapidly evolving modes of popular communication, ranging from microblogs to online gaming chat. While high-performance computing may play a role in the future of Chinese censorship, particularly in performing sophisticated predictive analysis of immense quantities of data, there is no particular advantage to employing cloud computing in these

[71] "Chongqing's International Offshore Cloud Computing Project Construction Shows Preliminary Success," ("重庆国际离岸云计算项目建设初战告捷") February 21, 2011, http://news.163.com/11/0221/09/6TDJ3RGH00014JB5.html.

[72] Peter Mattis, "Beyond Spy vs Spy: The Analytic Challenge of Understanding Chinese Intelligence Services," *Studies in Intelligence*, Volume 56, No. 3, September 2012, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-56-no.-3/pdfs/Mattis-Understanding%20Chinese%20Intel.pdf.

[73] "Chongqing's International Offshore Cloud Computing Project Construction Shows Preliminary Success," ("重庆国际离岸云计算项目建设初战告捷") February 21, 2011, http://news.163.com/11/0221/09/6TDJ3RGH00014JB5.html.

endeavors beyond the generalized advantages and disadvantages of utilizing cloud computing for highly intensive computing tasks.

Military Uses for Cloud Computing

Military-use cloud services are an important area of potential future development for Chinese cloud computing. Cloud computing and virtualization technology could enable more effective and flexible development and deployment of military equipment, while at the same time improving the survivability of the PLA's information systems by endowing them with greater redundancy (allowing a system's capabilities to survive the disabling or destruction of any individual node). Chinese military analysts are keenly aware of this potential, and it is likely that military cloud computing technology will see greater use in the PLA in the years to come. Although cloud computing technology has not yet achieved broad usage in the PLA, it appears to be in active development and has even been fielded for testing by certain military units. Chinese military analysts have followed the US military's cloud computing developments with great interest.[74]

As an essential component of its overall modernization efforts, the Chinese military is currently embarking on a process it terms "informatization," whereby the PLA is attempting to connect and integrate its numerous systems (many of which overlap with one another or are of greatly varying vintages) into a unified, harmonized information technology framework.[75] One major part of this informatization effort is the development of Integrated Command Platforms (ICPs). ICPs are information systems designed to allow battlefield commanders and soldiers to share information and utilize specialized battlefield command automation software in real-time across various military and civilian information networks. Cloud computing technology directly supports the deployment and operation of ICPs, and the PLA organization most responsible for ICP development, the General Staff Department's 61st Research Institute, is also actively conducting research into military cloud computing.[76] (See page 21 for additional discussion of the military implications of China's cloud computing development.)

Cloud Computing as a Tool for Cyber Attacks

In addition to its commercial, governmental, and military applications, public cloud computing services can be used as a tool or launch pad by malicious actors to launch attacks against non-cloud targets. Many of the benefits of cloud computing that give it wide appeal to corporations and end-users also make it attractive to actors with hostile intent. Generally, this consists of malicious actors misusing legitimate services for their own activities. For example, recent Distributed Denial of Service (DDoS) attacks against Sony Corp. were partially launched from

[74] See, for example, Chen Yan and Dai Wei, "Applications of Cloud Computing in Military Informatization," ("云计算在军队信息化建设中的应用") *Sichuan Ordinance Journal*, Vol. 31, Issue 9, September 2010, http://wenku.baidu.com/view/9a133514866fb84ae45c8d6f.html.

[75] See Joe McReynolds and James Mulvenon, "The Informatization of the PLA Under Hu Jintao," Strategic Studies Institute/US Army War College and US Pacific Command/National Bureau of Asian Research 23rd Annual People's Liberation Army Conference, October 2012, Carlisle, PA.

[76] Yang Yu and Guangmin Wang, "General Staff Department Information Technology Research Institute Created Our Military's Unified Command System," (总参某信息化研究所建成我军一体化指挥系统), *GMW.cn*, April 24, 2012, http://mil.gmw.cn/2012-04/24/content_4028245.htm.

Amazon.com's Elastic Computer Cloud (EC2) IaaS platform.[77] Such attacks can be carried out through cloud infrastructure based in any country, but since there has been an observable pattern of Chinese information technology infrastructure providers (such as domain registrars and Internet service providers) tending not to aggressively police abusive use of their consumer services against foreign targets, one can speculate that malicious use of Chinese cloud services may eventually take place at a higher rate than the cloud computing industry's global norm.

Aside from direct attacks launched through the cloud, cloud software and platforms may be leveraged by malicious cyber actors to indirectly serve their goals. For example, SaaS-type solutions like Pastebin.com (a popular site allowing users to easily make plain-text documents publicly available) are frequently used as dumping grounds for stolen data by hackers and other malicious actors from all over the world, including Chinese hackers.[78] Commercial password-breaking software from Passware includes built-in functionality to leverage Amazon's EC2 services as a distributed computing cluster, which can dramatically decrease the time needed to brute-force (that is, break a password by having a computer try out millions or billions of possible passwords until it finds one that works) any of hundreds of different encryption methods.[79] While the software is intended for law enforcement and corporate security personnel, its commercial nature ensures availability to all, regardless of intent.

Security Assessment of Vulnerabilities in Chinese Cloud Systems

The Chinese emphasis on private (rather than public) cloud computing means that the ability of outsiders to provide a comprehensive security assessment of vulnerabilities in specific Chinese cloud systems is greatly restricted. Any given organization's private cloud computing infrastructure, assembled wholly or partly with international hardware, may be as secure as any other elsewhere in the world, or it may be particularly insecure owing to idiosyncratic factors such as lax password policies or poorly configured servers. A dedicated hacker will extensively scan and probe a specific target's public exterior (including web interfaces and network ports that indicate they are open for communication with external systems) prior to attacking in search of these vulnerabilities. The hacker will then select a particular vulnerability to exploit, typically choosing the attack vector that will most easily enable them to successfully penetrate the system. As for the public cloud computing that does exist in China, most notably services offered by domestic market leaders Tencent and Alibaba, it appears to adhere to roughly the same security practices as global cloud computing providers.

Nevertheless, China's cloud computing infrastructure, as with all cloud computing, does potentially contain vulnerabilities that can be exploited, and these vulnerabilities are best understood in the broader context of global cloud security and vulnerability.

---

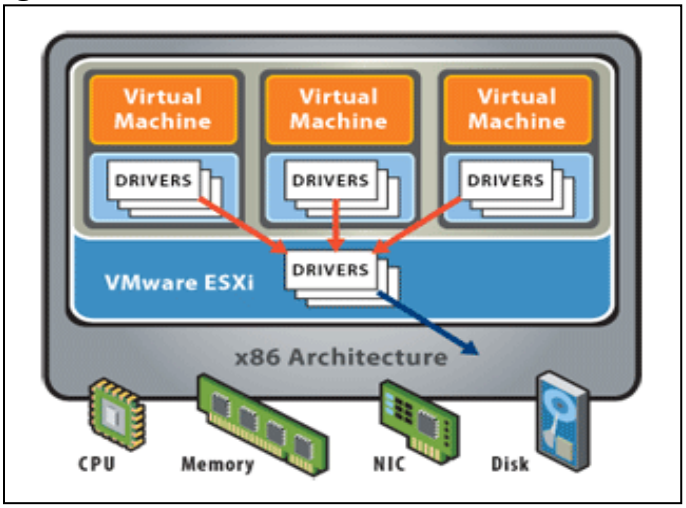
[77] Joseph Galante, Olga Kharif, and Pavel Alpeyev, "Sony Network Breach Shows Amazon Cloud's Appeal for Hackers," *Bloomberg News*, May 15, 2011, http://www.bloomberg.com/news/2011-05-15/sony-attack-shows-amazon-s-cloud-service-lures-hackers-at-pennies-an-hour.html.

[78] Matt Brian, "Pastebin: How a popular code-sharing site became the ultimate hacker hangout," *The Next Web*, June 5, 2011, http://thenextweb.com/socialmedia/2011/06/05/pastebin-how-a-popular-code-sharing-site-became-the-ultimate-hacker-hangout/.

[79] "Cloud Computing Acceleration HowTo," Passware Inc., accessed April 14, 2013, http://www.lostpassword.com/cloud-computing-acceleration-howto.htm.

At the most basic level, one sees vulnerabilities in Infrastructure as a Service (IaaS) provided through the cloud that are similar in nature to traditional IT infrastructure vulnerabilities. Regardless of whether a server is a physical or a virtual resource, it provides a similar target to an attacker, since even a virtualized system (a temporary system generated dynamically by a physical cloud computing infrastructure) may under certain conditions provide a conduit to its physical host.[80] In the case of IaaS, virtualization is provided to the user by using a specialized piece of software referred to as a "hypervisor." Since software coding is by definition an imperfect art rather than a perfectible science, a hypervisor's code may be subject to the same sorts of probing, reverse engineering, and attacks as any other piece of software. In the case of exploiting a hypervisor, the host system may contain additional virtualized resources in addition to the host's own resources, opening an avenue for attacks. One example of such a relationship, in the 'ESXi' virtualization platform offered by the VMWare corporation, is shown in Figure 2 below. There have been a number of documented exploits against particular hypervisors that involve "breaking out" from the constraints of a virtualized system. Virtual network segmentation mechanisms aimed at maintaining a wall between individual virtualized machines do not always provide full and absolute segmentation in practice, and attackers may exploit these inadequacies.[81]

Figure 2: VMware's ESXi Virtualization Platform[82]



Platform as a Service (PaaS) also opens a new dimension of vulnerability for attackers to exploit. Historically, middleware platforms like databases, computing clusters, and other traditionally "back-end" systems have been operated behind a network's perimeter, where they were generally inaccessible via the Internet. Using a PaaS architecture to fulfill these needs means that the services are no longer protected behind that perimeter, which increases an application's or

[80] Piotr Bania, "VMware CloudBurst - VMware Guest to Host Escape Exploit," *Piotr Bania Chronicles*, September 16, 2009, http://blog.piotrbania.com/2009/09/vmware-cloudburst-vmware-guest-to-host.html.
[81] Neil MacDonald, "Yes, Hypervisors Are Vulnerable," January 26, 2011, http://blogs.gartner.com/neil_macdonald/2011/01/26/yes-hypervisors-are-vulnerable/. See also "NetTop Fact Sheet," National Security Agency, accessed April 11, 2013, http://www.nsa.gov/research/tech_transfer/fact_sheets/nettop.shtml.
[82] "VMware Virtual Security Basics, Secure Virtual Machines, Embedded Virtualization," VMWare Inc., accessed April 13, 2013, http://www.vmware.com/technical-resources/security/overview.html.

company's "attack surface."[83] Under the PaaS model, proper configuration and access controls are imperative to the integrity of the overall application. Where a traditional enterprise network would require an attacker to "pivot" through a system exposed to both the Internet and the target's intranet, a cloud-based PaaS architecture may eliminate that buffer.

Another aspect of this increased attack surface is the use in PaaS of Application Programming Interfaces (APIs). An API is a data protocol that enables unlike programs to communicate and interact using a shared 'language'. One particularly common example of API usage is a simple online credit card transaction:

1) The consumer enters their purchase card information at a vendor site, and the vendor creates an API request containing the consumer's information. The API request expresses the information in a shared language that the payment processor's applications will be able to understand.

2) The vendor then sends that API request to the payment processor, and the processor performs the interaction with Visa, MasterCard, etc.

3) The vendor site waits for a response that is also formatted according to the aforementioned API specification and takes the proper action (such as providing a good or service to the consumer) based on the payment processor's response.

PaaS providers generally expose their services' functionality through these APIs, with which users can send requests, receive results, and even exert total control over the services or platforms they have purchased. Currently, most APIs use text-based data interchange standards such as Extensible Markup Language (XML) or Javascript Object Notation (JSON) for data formatting and the Hypertext Transfer Protocol (HTTP) that forms the foundation of the World Wide Web for data exchange. Examples of XML and JSON are in Figure 3. While they are text-based constructs, both require machine parsing to extract the data items of interest. Data parsers have historically been frequent targets for exploitation due to the complexity involved in parsing arbitrary data.[84] Since the protocols themselves are generally passed over HTTP, their use is also subject to all typical HTTP vulnerabilities, such as cross-site scripting or insufficient encryption of data.

[83] "Cisco Cloud Security Accelerates Cloud Adoption," Cisco Systems, accessed April 13, 2013, http://www.cisco.com/en/US/solutions/collateral/ns170/ns896/ns1066/white_paper_c11-674558.pdf.
[84] "CVE-2011-2481: Apache Tomcat information disclosure vulnerability," Apache Tomcat Security Team, August 12, 2011, http://mail-archives.apache.org/mod_mbox/www-announce/201108.mbox/%3C4E4526A7.60109@apache.org%3E., and Adi Cohen, "JSON-based XSS Exploitation," *IBM Application Security Insider*, October 24, 2011, http://blog.watchfire.com/wfblog/2011/10/json-based-xss-exploitation.html.

Figure 3: Same Source Data as seen in XML and in JSON

It should be noted that APIs are sometimes used with the IaaS and SaaS service models as well. For example, the Amazon EC2 API allows users to create and start entire new virtual systems using API calls, while many SaaS providers expose some or all of their datasets through an API.[85] Regardless of the functionality and/or data exposed through an API, the vulnerabilities are much the same. However, because the PaaS tier consists primarily of machine-to-machine services, APIs establish the foundation of such services.

The SaaS model, in which an entire application is outsourced to a third party provider through cloud services, creates a complex security structure. Users of such outsourced services are fully dependent on the service provider's ability to design, develop, operate, and maintain that service in a way that properly addresses the user's security requirements and policies. When a SaaS provider is breached, its users stand to lose invaluable data through no fault of their own. In one recent incident of this type, a misconfiguration of Microsoft's cloud-based business productivity suite exposed data records to customers other than their respective owners.[86] Other large breaches at payment processing companies have clearly demonstrated the risks that come with reliance on such outsourced services. The recent breach at Global Payments, Inc., for example, exposed the credit card data of 1.5 million customers, most of whom had likely never even heard of the company before the theft.[87]

Regardless of service tier, all cloud computing solutions share a common vulnerability – their users. The ubiquity of the web browser as a primary client for cloud computing providers and their services broadens their respective attack surfaces to include every user on any platform. Even the most security-conscious cloud provider is only as secure as the inevitable web-based

[85]"Amazon AWS Auto-Scaling," Amazon Corporation, acccessed April 11, 2013, http://aws.amazon.com/autoscaling/, and "Web Services API Developer's Guide," Salesforce.com, accessed April 11, 2013, http://www.salesforce.com/us/developer/docs/api/index.htm.
[86] Andreas Udo de Haes, "Microsoft BPOS Cloud Service Hit With Data Breach," *PC World*, December 22, 2010, http://www.pcworld.com/businesscenter/article/214591/microsoft_bpos_cloud_service_hit_with_data_breach.html.
[87] Brian Krebs, "Global Payments: Rumor and Innuendo," *Krebs on Security*, April 2, 2012, http://krebsonsecurity.com/2012/04/global-payments-rumor-and-innuendo/.

login to the provider's control panel or similar site. In the pre-cloud era, it was widely known that physical security was the lowest common denominator for any technology solution. If someone with malicious intent could gain access to the system itself, almost all technical means of security could be thwarted. As the industry has shifted to cloud-based providers, we see a striking corollary to the administrative interfaces used to manage those services.

In one recent example, an attacker accessed the web-based management interface at linode.com, a large IaaS provider. Though formal reporting on the incident is thin, information security experts claim that the attacker used the intended features of the management interface to reset the password(s) for several users' virtual machines and proceeded to steal data from those virtual machines (VMs).[88] This password reset feature is common with many hosting providers, often allowing users to change the VM's root or Administrator password via the web with no additional authentication.[89]

One important trend in Chinese cloud security is that an increasing number of Chinese cloud infrastructure projects are moving toward using domestically-developed network equipment. Since examinations by information security professionals have often shown Chinese network equipment to be more vulnerable and open to exploitation than comparable equipment developed by market-leading international corporations, it logically follows that use of this equipment may constitute an additional vulnerability in some Chinese cloud infrastructure, beyond the standard 'baseline' level of vulnerability.[90]

[88] "Manager Security Incident," Linode.com, March 01, 2012, http://status.linode.com/2012/03/manager-security-incident.html.
[89] Julian Yap, "The story of the compromised Linode VPS and further analysis," March 1, 2012, http://julianyap.com/2012/03/01/compromised-linode-vps.html.
[90] See, for example, Elinor Mills, "Expert: Huawei Routers are Riddled With Vulnerabilities," *CNet*, July 30, 2012, http://news.cnet.com/8301-1009_3-57482813-83/expert-huawei-routers-are-riddled-with-vulnerabilities/.

Chapter Five: Prospects for Cloud Computing in China

This chapter identifies the prospects for cloud computing technology in China, based on a number of qualitative factors. Assessments are included regarding the adoption of public and private cloud computing technology, the current potential of the Chinese cloud marketplace, the ability of Chinese firms to innovate in the cloud marketplace, and the level of government support for the Chinese cloud industry through both direct R&D funding and preferential regulatory and legal policies.

The key findings of this chapter are:

- Chinese industry analysis projects that China's cloud computing industry will continue to grow, with the overall value chain reaching between 750 billion and 1 trillion RMB by 2015 ($122 to $163 billion USD).

- China's cloud computing industry faces challenges of reliability and energy inefficiency in domestic data centers, as well as a lack of innovation in core chips and virtualization support.

- Some Chinese companies have shown an ability to innovate in this market. Alibaba Cloud Computing's cloud-based operating system for smart phones was the first of its kind, and Baidu has designed data centers that claim to be far more energy efficient than others in China.

- Limits and restrictions on foreign investment in value-added telecommunications services mean that US companies must enter into joint ventures with Chinese companies in order to provide cloud computing services to Chinese consumers from data centers in China.

- It is unclear how competitive US cloud computing firms will be in China's government procurement market. The percentage of foreign software and hardware procured for the central government's e-government services is high but appears to be decreasing. Government policy directs agencies to buy domestic if Chinese products can meet agencies' demands. And obstacles remain before China will accede to the World Trade Organization's Agreement on Government Procurement.

- Despite challenges to foreign participation in China's cloud computing market, Microsoft and other US companies are actively pursuing partnerships and opportunities there. However, questions remain as to whether or not US companies will benefit in the short- and long-term from market participation.

What Is The Market Potential For Cloud Computing Technology In China?

The 2012 *Annual Report of China Software & Information Technology Service Industry*, edited by the China Software Industry Association (中国软件行业协会), projects that the value of China's cloud computing market will grow from 16.7 billion RMB in 2010 to 117.4 billion RMB in 2013, while the size of the industry's overall 'value chain' will grow to between 750 billion and 1 trillion RMB ($122 to $163 billion USD) by 2015. The report suggests that government, telecommunications, education, finance, petrochemicals, electricity, and health care are among

the main sectors of the economy in which the use of cloud computing will likely increase over the next several years.[91] The penetration of cloud computing into the Chinese marketplace extends far beyond the individuals and firms directly utilizing it, with many Chinese e-mail services, mobile apps, and social networking sites storing data in the cloud automatically.[92]

Of the growth sectors listed above, e-governance applications in particular appear likely to help drive growth in China's cloud market, since the Chinese government is actively pushing the adoption of cloud computing technology at all administrative levels. In 2012, the State Council published the "Opinions of the State Council on Vigorously Advancing Informatization Development and Thoroughly Ensuring Information Security" (国务院关于大力推进信息化发展和切实保障信息安全的若干意见), which encourages the migration of e-government service applications to the cloud computing model as a means of enhancing China's e-government service capabilities.[93] In recent years, numerous e-governance cloud computing initiatives have been launched within central, provincial, and municipal government organs.

The government also supports a market for cloud computing applications oriented toward public services. One example of the use of cloud computing in the education sector in China is the National Public Service Platform for Educational Resources (国家数字教育资源公共服务平台), also known as the "National Education Cloud" (国家教育云). Established by China's Ministry of Education, the National Education Cloud is a platform that provides resources for teachers, students, and parents.[94] Its adoption is being driven by places like Wuhan (Hubei province), where all 972 elementary and middle schools in the city are reported to have achieved not only a seamless connection with the Internet, but also access to the National Education Cloud in June 2013. China Mobile's local subsidiary in Hubei Province is providing infrastructure and operational support for this project.[95]

Although the public sector appears to have embraced cloud computing in China and will continue to emphasize this technology, China's private sector has been more hesitant about purchasing cloud computing services.[96] Whether Chinese companies will come to welcome

---

[91] Annual Report of China Software & Information Technology Service Industry," (中国软件和信息服务业发展研究报告), *China Software Industry Association* (中国软件行业协会), 2012, p.237.

[92] See "The Cloud Floats Above All In Storm Of Tech Disruptions," in *Mobilizing Innovation: The Evolving Landscape Of Disruptive Technologies*, KPMG, September 4, 2012, http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/technology-innovation-survey/Pages/cloud-floats-above-all.aspx.

[93] "State Council Opinions on Vigorously Promoting the Development of Informatization and Effectively Protecting Information Security," (国务院关于大力推进信息化发展和切实保障信息安全的若干意见) *Central People's Government of the People's Republic of China*, modified July 17, 2012, http://www.gov.cn/zwgk/2012-07/17/content_2184979.htm.

[94] "Ministry of Education Ten Year Development Plan for Informatization 2011-2020," (教育信息化十年发展规划 2011-2020 年), *Ministry of Education*, modified March 2012, http://www.moe.gov.cn/ewebeditor/uploadfile/2012/03/29/20120329140800968.doc.

[95] "Hubei Mobile Invested 23.13 Million Yuan to Help Build Wuhan Cloud Computing Project," (湖北移动投入 2313 万元 助建武汉市教育云工程) *SINA.com*, June 6, 2013, http://tech.sina.com.cn/t/2013-05-06/23418309563.shtml.

[96] Liau Yun Qing, "China's Cloud Deployment Dampened by Nascent Enterprise Demand," *ZDNET*, March 15, 2013, http://www.zdnet.com/cn/chinas-cloud-deployment-dampened-by-nascent-enterprise-demand-7000012662/.

cloud computing with the same fervor as Chinese officials may depend in part on the availability of reliable network infrastructure in China and whether or not cloud providers and the central government can convince companies that their data will be secure.[97]

MIIT's 2012 Cloud Computing White Paper, discussed earlier in this report, outlines several challenges facing China's cloud computing industry that may hamper its growth prospects and damage its long-term competitiveness. One of those challenges is the lack of large data centers, which the white paper defined as centers containing more than 500 cabinets. In addition, the white paper stated that weaknesses in design, construction, operations, and maintenance have caused China's data centers to use energy inefficiently. The white paper noted that "[Power Usage Effectiveness (PUE) in China's data centers] is commonly between 2.2 and 3, whereas the level in the majority of developed countries is between 1.5 and 2."[98] Google's website explains that "a PUE of 2.0 means that for every watt of IT power, an additional watt is consumed to cool and distribute power to the IT equipment." It adds that "a PUE closer to 1.0 means nearly all of the energy is used for computing."[99]

Chinese Government Support for Cloud Computing

The Chinese government has supported the development of China's cloud computing industry through grants from the Electronic Information Industry Development Fund (电子信息产业发展基金) and the *He Gao Ji* Mega Project.[100] The government also implemented a value-added tax (VAT) to support the country's software industry, a measure that may extend to Chinese cloud computing service providers. Two important documents detailing the Chinese government's support for the country's software industry since 2000 are "A Number of Policies for Promoting the Development of the Software and Integrated Circuit Industries" ("鼓励软件产业和集成电路产业发展的若干政策"), also known as "Document 18," and "Several Policies for Further Promoting the Development of the Software and Integrated Circuit Industries" ("进一步鼓励软件产业和集成电路产业发展若干政策"), or "New Document 18."[101] Document 18 implemented a 17-percent VAT on software products developed and produced in China, with "taxes collected that exceed an actual tax burden of 3 percent to be refunded" to the producer, a policy continued by New Document 18. Document 18 states that companies will use these refunds to conduct R&D and "expand re-production." These documents also state that qualifying

[97] Ibid.
[98] "2012 Cloud Computing White Paper," (云计算白皮书 2012) *China Academy of Telecommunication Research of MIIT*, April 2012, http://www.miit.gov.cn/n11293472/n11293832/n15214847/n15218338/n15224998.files/n15224997.pdf, p. 37.
[99] "Efficiency: How we do it," *Google.com*, accessed May 24, 2013 http://www.google.com/about/datacenters/efficiency/internal/.
[100] Annual Report of China Software & Information Technology Service Industry," (中国软件和信息服务业发展研究报告), *China Software Industry Association* (中国软件行业协会), 2012, p. 234.
[101] Annual Report of China Software & Information Technology Service Industry," (中国软件和信息服务业发展研究报告), *China Software Industry Association* (中国软件行业协会), 2012, p.49. See also Li Ying, ed., "Report on China's Software and Information Service Industry (2011)," p.36-37, 39-43.

software companies can be granted two years during which they will not be charged corporate income tax, followed by three years during which they are taxed at half the usual rate.[102]

The Chinese government also offers Chinese companies preferential government procurement policies for cloud computing services. According to the "The State Council Office's Opinions on the Further Strengthening of Government Procurement Management Work" ("国务院办公厅关于进一步加强政府采购管理工作的意见"), published in 2009, "the procurement of imported products should be strictly examined, and where domestic products can meet the demands, domestic products should always be purchased."[103] As of 2011, 48 percent of software and hardware procured for China's central government e-government services were foreign products. However, this number appears to be decreasing, as 70 percent of these products were foreign in 2003.[104] As the Chinese government seeks to rely more on cloud computing for e-government services, foreign companies may have an opening to sell cloud computing products to government ministries, but that window may be closing rather than widening.

One challenge to China's preferential treatment is that it is in the process of negotiating accession to the World Trade Organization's Agreement on Government Procurement, under which parties agree not to favor domestic products or services over the products or services of other parties in government procurement.[105] While major obstacles currently block China's accession, if China were to finally accede to the agreement, US companies may encounter lower barriers to entry into China's cloud computing market as a result.[106]

The 2011 *Report on China's Software and Information Service Industry*, by MIIT's Electronics Science and Technology Information Institute (电子科学技术情报研究所), makes some assertions about China's cloud computing services market and the competitiveness of foreign companies. The report states that "even if a company is a large foreign cloud computing provider, the company's influence in China's cloud computing market is not as great as it is in the international market." It adds that "the cloud products and services that [these companies] provide in China's market are also not as plentiful as in other countries." The reason for this may lie in the fact that these foreign firms are primarily working through "cooperative arrangements with local government agencies, universities or other organizations to enter China's market,"[107] rather than being allowed to operate autonomously.

---

[102] "State Council Issued Notice of a Number of Policies for Further Promoting Development of the Software and Integrated Circuit Industries," (国务院关于印发《鼓励软件产业和集成电路产业发展的若干政策》的通知) *National Development and Reform Commission*, June 24, 2000, http://www.ndrc.gov.cn/cyfz/zcfg/t20050805_39059.htm.

[103] "State Council Office Notice Advice on Further Strengthening Management of Government Procurement," (国务院办公厅关于进一步加强政府采购管理工作的意见) *State Council*, modified April 13, 2009, http://www.gov.cn/zwgk/2009-04/13/content_1283914.htm.

[104] "E-Gov PPT Template," *Advisory Council for State Informatization*, accessed May 21, 2013, http://www.acsi.gov.cn/WebSite/ACSI/UpFile/File626.pdf.

[105] "Government Procurement: Parties and Observers," *WTO.org*, accessed June 3, 2013, http://www.wto.org/english/tratop_e/gproc_e/memobs_e.htm#memobs;"Agreement on Government Procurement," www.wto.org, accessed June 3, 2013, http://www.wto.org/english/docs_e/legal_e/gpr-94_e.pdf.

[106] "Europe Says China's Latest Bid To Join Procurement Agreement 'Highly Disappointing,'" *Reuters*, December 6, 2012, http://www.reuters.com/article/2012/12/06/us-china-eu-trade-idUSBRE8B50G720121206.

[107] "Report on China's Software and Information Service Industry (2011)," 2011, p. 204.

China's 2008 "Regulations on the Management of Foreign Companies' Investment in Telecommunications Enterprises" ("外商投资电信企业管理规定") states that enterprises operating in China in the area of basic telecommunication services can only contain foreign investment up to 49 percent. Enterprises in the field of value-added telecommunications services can only contain up to 50 percent foreign investment.[108] According to the law firm Cadwalader, Wickersham & Taft LLP, "cloud computing is theoretically classifiable as a value-added service" or VAS. The firm adds that "this is because cloud computing may fall under one of two broadly defined categories: 'Internet Access Services,' or 'Information Services,' both of which are subsumed within the category of VAS."[109]

How Will Government Support Through Funding, Policies, and Regulations Impact Cloud Computing In China?

In recent years the Chinese government has invested heavily in the development of cloud computing infrastructure. As of August 2012, there were 46 public cloud projects underway in all four of China's municipalities under the central government (Beijing, Tianjin, Shanghai, and Chongqing), and in 18 out of China's 27 provinces and autonomous regions. These projects have been established as far west as the Xinjiang Uyghur Autonomous Region, and as far south as the island province of Hainan. Jiangsu Province is home to the most projects, with six, and Guangdong Province has the second most, with four.[110] As reported in the 2012 *Annual Report of China Software & Information Technology Service Industry*, Beijing alone has received state and municipal government support for 30 public and private projects, with total investment reaching 50 billion RMB (8.2 billion USD) and 300 million RMB (48.9 million USD).

The Chinese government has taken some beginning steps to address data security issues. In December 2012, the Standing Committee of the National People's Congress issued a resolution on "Strengthening the Protection of Information on the Internet" ("全国人民代表大会常务委员会关于加强网络信息保护的决定"), which aims to improve network and information security practices by providers of consumer computing services (including cloud computing).[111] Most recently, in April 2013, MIIT published a draft of the "Regulations on Telecommunications and Internet User Personal Information Protections" ("电信和互联网用户个人信息保护规定").[112] The Business Software Alliance (BSA) notes that the resolution "includes some very basic

[108] "Regulation on Foreign Investment in the Telecommunications Industry," (外商投资电信企业管理规定) *Legislative Affairs Office of the State Council*, September 16, 2008, http://www.chinalaw.gov.cn/article/fgkd/xfg/xzfg/200809/20080900033197.shtml.

[109] "Cloud Computing In China: Impact of a Complex Environment," (云计算在中国: 复杂环境的影响) *Cadwalader.com*, accessed May 22, 2013, http://www.cadwalader.com/CN/assets/client_friend/ 云计算在中国：复杂环境的影响.pdf.

[110] "Number of Public Cloud Projects," *China Daily Asian Pacific*, accessed May 23, 2013, http://www.chinadailyapac.com/sites/default/files/imagecache/400xY/images/20130121/13-3.jpg.

[111] "Country Report: China," in *2013 BSA Cloud Computing Scorecard*, 2013, p. 2, http://cloudscorecard.bsa.org/2013/assets/PDFs/country_reports/Country_Report_China.pdf

[112] "Send Your Feedback: Draft on Telecommunications and Internet Users Individual Information Protection Regulations," (意见征集：《电信和互联网用户个人信息保护规定（征求意见稿）》、《电话用户真实身份信息登记规定（征求意见稿）》) *Ministry of Industry and Information Technology*, April 10, 2013, http://www.miit.gov.cn/n11293472/n11293832/n11293907/n11368223/15333978.html.

security requirements for ISPs and organizations processing personal information online" and adds that "these requirements are likely to cover cloud service providers."[113] However, there are still gaps in China's laws. The BSA further states that China does not have "specific security laws relating to data hosting infrastructure," companies in China that provide data hosting or storage services are not required by law to inform customers of data breaches, and there are no "security audit requirements in Chinese law" to which these and other cloud service companies are subject.[114]

Foreign Participation Improves Prospects for Chinese Cloud Computing

In China, Inspur, Baidu, Alibaba, and SNDA are considered representative firms for Internet service enterprise based cloud computing solutions in search engines, electronic commerce, and enterprise management service. ZTE, Huawei, UFIDA, and Kingdee are considered the representative Chinese manufacturers and developers of cloud related software, hardware, and cloud computing system solutions.[115] However, the industry is not limited to these companies. The China Cloud Computing Technology and Industry Alliance (中国云计算技术与产业联盟) recently released three lists of Chinese companies involved in the cloud computing industry. Despite being an incomplete picture of the industry, the list contains 15 companies providing cloud platforms, 174 companies providing cloud applications, and 64 companies providing cloud hosting and storage.[116] Other industry representative groups are participating in this space as well; in one recent example, representatives from more than 150 companies have come together to support the China Coalition of Cloud Computing Applications (中国云计算应用联盟), which held its founding meeting in the city of Hangzhou (Zhejiang Province).[117]

Despite potential obstacles to foreign participation in the cloud computing market, it appears to improve the level of technology and services that will be offered in China. 21Vianet Group's recent partnership with Microsoft, introduced previously in the report, is illustrative. 21Vianet's first cloud initiative CloudX failed and went out of business.[118] Since then, 21Vianet has signed a partnership with Microsoft to license Microsoft's Office 365 and Windows Azure cloud computing platform. Domestic users in China will have access to these products through 21Vianet's domestic data centers.[119] The public was able to sign-up to use Azure on June 6, 2013, as part of a preview of the cloud computing technology. The offering of a mature cloud computing solution such as Windows Azure, instead of the CloudX prototype, could encourage more business customers to adopt cloud computing solutions.

[113] "Country Report: China," in *2013 BSA Cloud Computing Scorecard*, 2013, p. 2
[114] Ibid.
[115] "Report on China's Software and Information Service Industry (2012)," 2012, p. 236.
[116] "Build China Cloud Computing Ecosystem," *China Software Developer Network*, May 20, 2013, http://www.csdn.net/article/2013-05-20/2815362-2013-Build-China-CloudComputing-Ecosystem-3.
[117] "China Cloud Computing Alliance Established in Hangzhou," (中国云计算应用联盟在杭州成立) *Ministry of Science and Technology*, November 1, 2012, http://www.most.gov.cn/dfkj/zj/zxdt/201210/t20121031_97518.htm.
[118] Robert O'Brian, "Cloud Computing in China, An Insider's Perspective," *Tech Rice*, June 1, 2013, http://techrice.com/2013/05/01/cloud-computing-in-china-an-insiders-perspective/.
[119] "Cloud OS is Coming to China," *Windows Azure Team Blog*, November 1, 2012, http://blogs.msdn.com/b/windowsazure/archive/2012/11/01/cloud-os-is-coming-to-china.aspx.

Similarly, HP and Microsoft participation in other areas of the Chinese market may improve the overall technology level of products for Chinese businesses. Microsoft first partnered with Jiangsu Feng Yun Network Services Co. Ltd. (江苏风云网络服务有限公司), and in 2008 Feng Yun Network released a SaaS platform called cnsaas.com.[120] This platform has been directed toward SMEs in China.[121] In 2011 Microsoft signed an agreement with China Standard Software Co. Ltd. (C2SC/中标软件有限公司) to "jointly develop, market and sell solutions" for China's cloud computing market. The two companies also agreed to establish a joint laboratory in Beijing for developing and testing cloud computing solutions.[122] Furthermore, Microsoft established the China Cloud Innovation Center (CCIC) in Shanghai. The center has engaged in projects such as providing the Microsoft Virtual Desktop Infrastructure for around 200 employees at Shanghai's Shibei High & New Technology Zone (市北高新技术服务业园区).[123] In June 2011, Hewlett Packard (HP) opened its HP Cloud Executive Briefing Center in the city of Tianjin. The center's purpose is to "provide customers in China and the region with hands-on experience in building, enabling and operating HP-led cloud environments." HP describes the center as giving "customers an opportunity to create a blueprint for a seamless, secure, context-aware cloud environment, whether it is private, public or hybrid…"[124] Taken together, joint-research facilities and commercial partnerships between leading cloud firms and Chinese cloud firms may raise the prospects for cloud computing technology in China.

Are Chinese Cloud Computing Firms Making Innovations in Cloud Computing?

Although a number of major Chinese cloud computing firms claim and have received awards for innovation, independent critical technical reviews are unavailable to support these claims. The current state of China's overall cloud computing technical capacity makes these claims questionable. As of 2012, MIIT's cloud computing white paper had stated that China's companies "still urgently need a breakthrough in critical products and technology, such as core chips for large-scale cloud computing systems management, and support for virtualization."[125] Lacking breakthroughs in critical products and technology for cloud computing, how can companies expect to achieve true innovation? Most of the Chinese products reviewed appear to offer incremental design improvements at this time and misuse the term "innovation."

The Chinese government has tried to address known problems in innovation by introducing policies that support innovation among the country's cloud computing providers. In 2010, the National Development and Reform Commission (NDRC) and MIIT released the "Circular

[120] "Company Introduction," (公司简介) *Fengyun.com*, accessed May 18, 2013, http://fengyun.cnsaas.com/about/introduction.html; "Microsoft Share News," *ADFN.com*, accessed May 18, 2013, http://www.advfn.com/nasdaq/StockNews.asp?stocknews=MSFT&article=44395023.
[121] "Report on China's Software and Information Service Industry (2012)," 2012, p. 204.
[122] "Microsoft Formalizes Cross-Platform Collaboration With CS2C in China," *Microsoft.com*, August 11, 2008, http://www.microsoft.com/en-us/news/press/2011/aug11/08-22CS2CPR.aspx.
[123] "Corporate Citizenship," *Microsoft.com*, accessed May 18, 2013, http://www.microsoft.com/china/mscorp/citizenship/yzcx.aspx.
[124] "HP Deepens Commitment to China," *HP.com*, June 29, 2011, http://www8.hp.com/us/en/m/hp-news/details.do?id=1002900&articletype=news_release.
[125] "2012 Cloud Computing White Paper," (云计算白皮书 2012) *China Academy of Telecommunication Research of MIIT*, April 2012, http://www.miit.gov.cn/n11293472/n11293832/n15214847/n15218338/n15224998.files/n15224997.pdf, p.37.

Regarding Successfully Conducting Cloud Computing Services Innovation and Development Pilot Demonstration Work" ("关于做好云计算服务创新发展试点示范工作的通知"). The circular directed this work to begin in five cities: Beijing, Shanghai, Shenzhen, Hangzhou, and Wuxi. It explained that the pilot development will be "linked to regional industry development advantages" and the "building of innovative cities."[126] However, it is unclear whether the Chinese government's support for innovation in cloud computing has accomplished its intended effect. Cloud computing technology may be developing too quickly for government assistance to have an impact on innovation in China.[127]

In order to identify innovation in China's leading cloud computing firms, DGI analysts identified Chinese cloud products and services that received particular recognition for their ostensibly innovative qualities. However, a review of dozens of products failed to identify clear indicators of innovation. Further investigation failed to identify technical reviews from independent experts that would suggest innovation. The following list provides examples of products claimed to be innovative from China's leading cloud computing firms:

- Baidu has achieved progress with cloud computing technology, particularly in data centers and with the design of a new Solid State Disk (SSD). In one Nanjing center, it claims to have achieved significant reductions in data center ownership costs, while at the same time increasing the center's ability to store data by 70 percent.[128] In the process of developing this system, Baidu obtained 10 invention patents.[129] Baidu also designed its own SSD, which Baidu asserts is six times more effective and 10 percent less expensive than Serial ATA SSD (SATASSD), another competing SSD product.[130]

- Alibaba Group Holding Ltd.'s subsidiary Alibaba Cloud Computing may have developed an innovative product: a smartphone operating system that is located in the "cloud" instead of on the phone.[131] Although this product exists as the first cloud-based operating smartphone operating system, Google has alleged that Aliyun OS incorporates elements of Android and runs

[126] "National Development and Reform Commission: MIIT's "Notice On Doing Cloud Computing Service Innovation Pilot and Demonstration Project Work," (国家发展改革委工业和信息化部关于做好云计算服务创新发展试点示范工作的通知) *National Development and Reform Commission*, October 25, 2010, http://www.ndrc.gov.cn/zcfb/zcfbtz/2010tz/t20101025_376673.htm.
[127] "Cloud Computing in China: An Insider's Perspective on the Chinese Attempt to Catch up to Amazon," *Content China*, May 2013, http://contextchina.com/2013/05/cloud-computing-in-china-an-insiders-perspective-on-the-chinese-attempt-to-catch-up-to-amazon/.
[128] Lara Luo, "21Vianet Teams with Microsoft for Shanghai-based Cloud Offering," *Data Center Dynamics*, November 22, 2011, http://www.datacenterdynamics.com/focus/archive/2012/11/21vianet-teams-microsoft-shanghai-based-cloud-offering.
[129] "Baidu's Nanjing Data Center, Data Center Computing and Reform," (百度南京数据中心: 数据中心计算与变革) *InfoQ*, January 2013, http://www.infoq.com/cn/news/2013/01/baidu-data-center.
[130] Lara Luo, "21Vianet Teams with Microsoft for Shanghai-based Cloud Offering," *Data Center Dynamics*, November 22, 2011, http://www.datacenterdynamics.com/focus/archive/2012/11/21vianet-teams-microsoft-shanghai-based-cloud-offering.
[131] "Alibaba Introduces Its Own Mobile Cloud System," *Cloud Times*, July 6, 2011, http://cloudtimes.org/2011/07/06/alibaba-introduces-its-own-mobile-cloud-system/.

in an Android runtime environment, essentially providing users with a heavily customized version of Android.[132] If true, this product should be considered an incremental innovation.

- In 2011, Inspur revealed a Smart Cloud Container Data Center, for which Inspur personnel obtained over 60 patents, the majority of which are invention patents.[133] According to Li Deyi, the chairman of the China Electronics Society's Cloud Experts Committee, this product involved "structural innovations" in power distribution and configuration control, among other areas.[134] Some Chinese experts have claimed that at the time of its release, Inspur's "Cloud Sea" (云海) Operating System was "overall a world leader" due to the system's method of combining cloud computing and cloud storage.[135] However, such claims cannot be corroborated without detailed technical specifications that do not appear to be publicly available.

When examining claims of innovative product and service development by Chinese cloud computing firms, there are a number of likely factors that lead to many of these offerings providing less innovation than meets the eye. In addition to the obvious market incentive for corporations to exaggerate their own achievements, the strong Chinese funding for 'innovation' may paradoxically encourage cloud computing companies to describe their products as 'innovative' in a bid to attract government support and funding regardless of their actual content.

Assessments of the state of Chinese cloud computing innovation by knowledgeable foreign participants in the Chinese cloud marketplace offer a unique and valuable perspective regarding the extent to which Chinese firms are in fact producing cutting-edge cloud innovations. In one such recent interview, Steve Mushero, the co-founder and CEO of the Chinese public cloud provider ChinaNetCloud, explained that despite a proliferation of cloud service providers and Chinese government investment in cloud computing as a "strategic emerging industry," the Chinese cloud computing industry lags technologically behind the world in general and Amazon's advanced cloud infrastructure in particular.[136] Mushero is skeptical that Chinese government funding can play a significant role in spurring cloud computing innovation, since the bureaucratic mechanisms for determining and dispensing funding in such schemes are unlikely to be able to keep pace with the rapid innovations occurring in the global cloud computing market.

---

[132] "Google: Alibaba's OS is an incompatible version of Android," *CNET*, September 14, 2012, http://news.cnet.com/8301-1035_3-57513559-94/google-alibabas-os-is-an-incompatible-version-of-android/.
[133] "Inspur Small to Medium Enterprises Cloud Computing Solutions," (浪潮中小企业云解决方案) *Inspur.* accessed 31 May, 2013, http://www.inspur.com/products/channel_cloud/qyy_23499.shtml.
[134] Zhang Guilin, "Li Deyi: Call for Chinese Cloud Computing Indigenous Innovation," (李德毅: 呼吁中国云计算自主创新) *SINA.net*, April 7, 2011, http://server.chinabyte.com/296/11898796.shtml.
[135] "China's Breakthrough of Core Technology in the Cloud Computing Industry," (中国突破云计算产业核心技术) *Qiu Shi Theory*, June 1, 2011, http://www.qstheory.cn/kj/zzcx/201106/t20110601_84454.htm.
[136] Robert O'Brian, "Cloud Computing in China, An Insider's Perspective," *Tech Rice*, June 1, 2013, http://techrice.com/2013/05/01/cloud-computing-in-china-an-insiders-perspective/.

Conclusions

China has prioritized the development of cloud computing technology with the goal of providing efficient and resilient information technology resources for Chinese end-users while also nurturing an internationally competitive cloud computing services industry. A review of relevant trends suggests that China aims to protect this growth and development through preferential policies toward "indigenously developed" technologies, as well as other benefits for domestic Chinese firms. Although some major US firms such as Microsoft and Hewlett Packard have entered into partnerships with domestic Chinese firms in order to gain access to the Chinese market, it is unclear whether these partnerships will result over the long term in transfers of key technology to Chinese partner firms.

The rise of China-based cloud computing services and solutions raises important concerns for US consumers, who may find themselves knowingly or inadvertently processing and storing sensitive data using cloud infrastructure located within Mainland China. This infrastructure may suffer from a relatively wide range of security gaps, likely due more to the use of insecure and bug-ridden Chinese hardware and software than to any weakness inherent to Chinese cloud computing systems. Another cause for concern is the involvement of China's premiere foreign intelligence collection organization, the Ministry of State Security, in the oversight of China-based data centers aimed exclusively at foreign cloud computing users. These factors, taken together with the growing list of military applications for cloud computing technology envisioned by the PLA, combine to ensure that future Chinese advancements in this field will remain a topic of interest to the US and other foreign governments for the foreseeable future.