Digital Expansionism: Exploring the U.S.-China Technology Dynamic Through Cybersecurity Policy and International Marketing Strategies in the Cloud Computing Sector

Julien Isaacs

Working Paper CISL# 2019-14

June 2019

Cybersecurity Interdisciplinary Systems Laboratory (CISL)
Sloan School of Management, Room E62-422
Massachusetts Institute of Technology
Cambridge, MA 02142

Digital Expansionism:
Exploring the U.S.-China Technology Dynamic Through Cybersecurity Policy and International Marketing Strategies in the Cloud Computing Sector

By

Julien Isaacs

BSFS Georgetown University, 2012

SUBMITTED TO THE MIT SLOAN SCHOOL OF MANAGEMENT IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE IN MANAGEMENT STUDIES AT THE MASSACHUSETTS INSTITUTE OF TECHNOLOGY

JUNE 2019

©2019 Julien Isaacs. All rights reserved.

The author hereby grants to MIT permission to reproduce and to distribute publicly paper and electronic copies of this thesis document in whole or in part in any medium now known or hereafter created.

Signature of Author:

_____

Julien Isaacs
MIT Sloan School of Management
May 10, 2019

Certified by:

_____

Stuart Madnick
John Norris Maguire Professor of Information Technologies, Sloan School of Management & Professor of Engineering Systems, School of Engineering
Thesis Supervisor

Accepted by:

_____

Jake Cohen
Senior Associate Dean, MIT Sloan Undergraduate & Masters Programs
MIT Sloan School of Management

Digital Expansionism:
Exploring the U.S.-China Technology Dynamic Through Cybersecurity Policy and International Marketing Strategies in the Cloud Computing Sector

By

Julien Isaacs

**Submitted to MIT Sloan School of Management
on May 10, 2019 in Partial Fulfillment of the
requirements for the Degree of Master of Science in Management Studies.**

ABSTRACT

The U.S. and China remain largely separated from one another in terms of technological market access, with both sides implementing policy regimes serving as official or unofficial barriers to international trade, especially evident in data-sensitive industries, such as cloud computing. The result is a very low market share for American cloud computing providers in China, and vice-versa. This paper explores the U.S.-China dynamic insofar as government policy and action are concerned, the U.S. and China markets, and private enterprise's response and strategy in the cloud computing industry, which is notable not only given its value, $278.3 billion worldwide by 2021, but also its central position in the flow of global data.[1]

The paper arrives at a number of conclusions. Firstly, given China's techno-nationalist policy regime, U.S. cloud computing firms, and by extension, all U.S. technology companies, will face increasingly limited market share and opportunity in China. Conversely, Chinese cloud computing providers, and by extension Chinese technology products, in general, may be able to successfully garner market share in the U.S. by offering innovative products with little to no substitutes, for which Americans will potentially waive their data privacy concerns in order to access (which may lead to unintended consequences). Lastly, the U.S. and China should work together to form, articulate and implement cybersecurity and data norms, enhancing international cooperation on a government and private enterprise level, effectively removing international trade barriers and promoting and enhancing market access. Cooperation, however, remains a challenge, given the differing policy objectives of the U.S. and China.

Thesis Supervisor: Stuart Madnick
Title: John Norris Maguire Professor of Information Technologies, Sloan School of Management & Professor of Engineering Systems, School of Engineering

---

[1] "Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.3 Percent in 2019." *Gartner IT Glossary*, Gartner, Inc., 2018, www.gartner.com/en/newsroom/press-releases/2018-09-12-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-17-percent-in-2019.

Table of Contents

List of Tables

List of Figures

1. Introduction

The U.S. and China represent two of the most important global economies and political heavyweights in the world today, both increasingly focused on the development and adoption of cutting-edge technologies, including cloud computing. In the increasingly digitized, plugged in and automated age, inarguably, the technology dynamic between the United States and China will be a crucial relationship of greater future consequence and economic effect. Yet, especially in the technology space, the two remain separated by the Great Firewall, each relying on its own increasingly unique ecosystem, informed by government policies, consumer preferences, public perception and historical variables. Numerous American technology titans have headed to China. Once they arrive, their superstar status seems to fade. Similarly, Chinese technology superpowers struggle to find footing and traction with consumers in the American market. This leads to two core questions: (1) Why do American technology firms have so much trouble in the China market? and (2) Why do Chinese technology companies have an inability to make it big in America?

Perhaps in no sector are the bilateral issues more emblematic than in the cloud computing services business, which touches on many big-ticket issues such as Big Data (upon which AI is so dependent), consumer privacy, and localization requirements. The cybersecurity issue is especially salient here, as cybersecurity concerns have impacted governmental policies and, by extension and via reaction, the international strategy for cloud computing service firms in the U.S. and China. Summarily, this thesis, through an analytical framework centered on dissecting challenges around institutional, technological, social and managerial factors, and comprehensive case study analyses, will examine the current U.S.-China cloud dynamic and ultimately provide actionable strategies for how American cloud technology platforms can maximize their China market share, and vice-versa. However, serious challenges abound on both sides, much of which can only be remedied by substantial overhaul to current policy regimes.

Interestingly, both the U.S. and China cite “state security” as the motivation for limiting, either officially or unofficially, market access for foreign technology players, effectively serving as a barrier to international trade in the digital economy. In China, it seems, the Chinese Community Party (the “CCP” or “the Party”), primarily utilizes the notion of state security as a justification to grow its domestically Chinese national champions, such as Tencent and Huawei, under the pretense of economic and political stability. The CCP correlates indigenous technological innovation as central to China’s long terms strategic interests and, as a result, has implemented a “techno-nationalist” policy regime that has severely limited American technology companies’ ability to succeed in the China market. This phenomenon is especially prevalent in the cloud services business, where American corporations such as Amazon and Microsoft that provide public cloud services in China were sent scrambling given a 2017 cybersecurity

law that mandated localized data storage for Chinese user generated data. Though other countries or nation-states also have data localization requirements, which, for instance, in the EU serve to protect consumer privacy, China's data localization remains unique as a mechanism for the Chinese State to retain social control, ensuring political and economic stability. In the United States, state security is also cited as a reason to limit Chinese technological access, with the goal of preventing economic espionage and the theft of intellectual property. Huawei and ZTE are especially useful precedents here. Governing bodies such as Congress have issued reports and passed legislation barring the governmental purchase and dissuading the private adoption of Chinese telecommunications equipment. However, a less formalized policy regime exists against Chinese companies in America compared to American companies in China. A key factor in the U.S. is consumer preference. In other words, given the data security issues associated with Chinese technology products and services, American consumers will be less likely to adopt a Chinese technology product or service, such as cloud storage, compared to a perceived more secure American product, such as Amazon Web Services ("AWS"). However, American consumers, in the future, will likely be willing to adopt Chinese technology products and services, despite data security concerns, if there exists no direct domestic substitute, with current examples such as Bytedance's AI-informed viral short video app Tic Tok and DJI's drone technology.

The paper is organized as follows. In section two, cloud computing as a technology will be explained and the relevant security issues informing government policy and consumer adoption will be explored. A global market analyses will then be performed, followed by more specific examinations into the cloud markets in the U.S. and China, respectively. In section three, a cybersecurity overview will then be introduced. Frameworks to understand cybersecurity issues, international trade and consumer adoption preferences will be explored, for later application. Additionally, a discussion on cloud, data and consumer data privacy will be employed. Section four will detail and analyze the America to China cloud expansion dynamic, with a focus on examining the local market landscape, relevant policies and a select firm case study. Issues regarding China & the WTO and techno-nationalism will also be carefully examined. Microsoft Azure in China will serve as the America to China cloud expansion case study. Following that, section five will explore the China to America dynamic for cloud computing services, which will then be analyzed, with a focus, again, on examining the local market landscape, relevant policies and a select company case study. Issues regarding Huawei & ZTE, FIRRMA & CFIUS and U.S.-China cybertensions will be explored. Alibaba's Alicloud (or Aliyun 阿里云) in America will serve as the China to America cloud expansion case study. Analyses will be provided using an updated Parkerian Hexad and Porter's 5 Forces methodology for the two case studies. Finally, the paper will conclude by offering international strategy recommendations for U.S. and Chinese cloud computing operators, policy

recommendations for the U.S. and China, and a current and future analysis of the sector for foreign actors.

2. Cloud Computing

2.1 Cloud Computing Technology Overview

Since its inception, cloud computing has inexorably altered the software landscape, introducing a new paradigm in terms of data storage and distribution. The term “cloud computing” appeared as early as 1996, cited first in the Compaq Computer offices in Houston, Texas, as employees envisioned the future of the Internet and software transmission.[2] Later in the mid 2000s, the term was popularized by major players such as Amazon and Google. Amazon, especially, contributed to the mainstream adoption of the term with the release of Amazon Elastic Compute Cloud (Amazon EC2) in 2006.[3]

For the past decade, cloud has remained a buzzword in the technology industry, but an understanding of the fundamentals may remain vague for many. Below, formal definitions are provided.

Microsoft, via the Microsoft Azure service site, describes cloud computing as “the delivery of computing services--servers, storage, databases, networking, software, analytics, intelligence and more--over the Internet ("the cloud") to offer faster innovation, flexible resources, and economies of scale.”[4] According to the National Institute of Standards and Technology (NIST), cloud computing enables ubiquitous access to a shared pool of computing resources.[5] Cloud computing technologies have five main characteristics: on demand self-service, broad network access, resource pooling, rapid elasticity and measured service. The nature of the cloud allows for computing resources, such as networks, storage, services, etc., to be rapidly provisioned to users with minimal management and limited interaction with the service provider. The official NIST cloud computing definition is as follows:

> Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g.

---

[2] Regalado, Antonio. “Who Coined 'Cloud Computing'?” *MIT Technology Review*, MIT Technology Review, 30 Dec. 2013, www.technologyreview.com/s/425970/who-coined-cloud-computing/.

[3] “Announcing Amazon Elastic Compute Cloud (Amazon EC2) - Beta.” *Amazon*, Amazon, 2006, aws.amazon.com/about-aws/whats-new/2006/08/24/announcing-amazon-elastic-compute-cloud-amazon-ec2---beta/.

[4] “What Is Cloud Computing? A Beginner's Guide | Microsoft Azure.” *A Beginner's Guide | Microsoft Azure*, azure.microsoft.com/en-us/overview/what-is-cloud-computing/.

[5] Mell, Peter and Timothy Grance. “The NIST Definition of Cloud Computing.” *National Institute of Standards and Technology*, 2011, nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

> networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.[6]

Though some elements of this definition have become slightly outdated as the technologies powering cloud computing continue to advance and new service mechanisms have been introduced, in general, the NIST definition of cloud computing remains the gold standard worldwide. NIST provides a more official and technical version than Microsoft, which reads more as a consumer friendly and easy to understand definition of the cloud.

In terms of service models, three main models compose the cloud service infrastructure: SaaS (software as a service), PaaS (platform as a service) and IaaS (Infrastructure as a service).[7] Arguably the most ubiquitous, SaaS (software as a service) allows users to access provider applications running on a cloud infrastructure. Examples of SaaS include Google Docs, Siri and Dropbox. PaaS (platform as a service) enables users to create or acquire applications via utilizing the cloud service provider's resources, including programming languages and libraries. Examples of PaaS include Openshift, Google App Engine and Heroku. IaaS (Infrastructure as a service) enables users to create operating systems, storage, deployed applications and other fundamental computing resources on the cloud service provider's underlying cloud infrastructure. The primary features of IaaS are elasticity and virtualization. Examples of IaaS include Rackspace and Cisco Metapod.[8] To note, both Amazon Web Services and Microsoft Azure have PaaS, and Iaas functionalities. IaaS is the base for all cloud services, and the foundation upon which PaaS and SaaS applications are built.

Virtualization technology is essential to cloud computing, acting as the fundamental technology powering cloud computing. According to Madnick and Donovan (1973), virtualization "enables a single system to concurrently run multiple isolated virtual machines (VMs), operating systems or multiple instances of a single operating system (OS)."[9] There are two main types of virtualization: application virtualization and server virtualization. Application virtualization allows for the delivery of an application, that is typically hosted on one or a few main servers, to be simultaneously delivered to a large number of users. Server virtualization hosts virtual machines using common physical hardware, such as networks, storage or computing machines.[10] In effect,

---

[6] Ibid

[7] "Types of Cloud Computing." *Amazon*, Amazon Web Services, aws.amazon.com/types-of-cloud-computing/.

[8] Watts, Stephen. "SaaS vs PaaS vs IaaS: What's The Difference and How To Choose." *BMC Blogs*, 2017, www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/.

[9] Madnick, Stuart, and John Donovan. "Application and Analysis of the Virtual Machine Approach to Information System Security and Isolation." Contents: Using the Digital Library, ACM, 1973, dl.acm.org/citation.cfm?id=803961.

[10] Ruparelia, Nayan. *Cloud Computing*. The MIT Press, 2016.

virtualization allows for the software manipulation of the hardware, which enables cloud computing technology to function effectively.

Beyond the more traditional SaaS, PaaS and IaaS service models, three new service models have been more recently introduced: BPaaS (business process as a service), INaaS (information as a service), and DBaaS (database as a service).[11] BPaaS (business process as a service) involves business processes outsourcing via a cloud service model, effectively reducing labor count, the traditional goal of business process outsourcing, through increased cloud automation. Examples of BPaaS include HR functions such as payroll and benefit administration.[12] BPaaS usually sits on one of the three more foundational cloud service models, SaaS, PaaS or IaaS. INaaS (information as a service) allows any application to access information, often via an API, referring to the ability to access any remotely hosted information via the cloud.[13] Examples could include accessing the latest tax code and accounting regulations or stock price information. INaaS is unique from IaaS since it not just involves the storage of data, but also requires the manipulation of data to present it in a meaningful and useful way. DBaaS (database as a service) enables users to provision, configure and operate database software via the cloud of a remotely hosted database. Examples of DBaaS include Xeround, which provides applications via the open source MySQL database, and Amazon Web Services' Amazon Relational Database Service (Amazon RDS), which helps scale computing resources and scale capacity for relational databases.[14] BPaaS, INaaS and DBaaS represent three additional cloud service models which are used widely but which do not fall within the NIST cloud computing definition. Table 1 below details the various cloud service models

Cloud Service Model	Description
SaaS (software as a service)	Allows users to access provider applications running on a cloud infrastructure
PaaS (platform as a service)	Enables users to create or acquire applications via utilizing the cloud service provider's resources, including programming languages and libraries
IaaS (Infrastructure as a service)	Allows users to create operating systems, storage, deployed applications, etc. on the cloud service provider's underlying cloud infrastructure

[11] Ibid

[12] Rouse, Margaret. "What Is BPaaS (Business Process as a Service)? - Definition from Whatls.com." *SearchERP*, searcherp.techtarget.com/definition/BPaaS-Business-Process-as-a-Service.

[13] Mosbah Magdy, Mohamed, et al. "CURRENT SERVICES IN CLOUD COMPUTING: A SURVEY." *International Journal of Computer Science, Engineering and Information Technology (IJCSEIT)*, 2013, pdfs.semanticscholar.org/3594/79fbca56b4b1295734b8c4c16af0d17273f2.pdf.

[14] Ibid

BPaaS (business process as a service)	Involves business processes outsourcing via a cloud service model
INaaS (information as a service)	Enables any application to access remotely hosted information, often via an API
DBaaS (database as a service)	Allows for users to provision, configure and operate database software via a remotely hosted database

Table 1: Cloud Service Models

Distribution-wise, there are four main deployment models: private cloud, community cloud, public cloud and hybrid cloud. Private cloud indicates that the cloud is to be used exclusively by a single institution. Community clouds are created to a serve a certain group of individuals that may share an objective, a mission or security requirements. Public clouds are for the general public's open use, but may be owned by a company, government or academic institution. Lastly, hybrid clouds are a mix of two or more of the aforementioned cloud deployment models that are bound by either standardized or proprietary technology.

Four distinct participants, or actors, are involved in the chain of creation, delivery and consumption of cloud services: the cloud service creator, the cloud service provider, the cloud service broker and the cloud service consumer. The cloud service creator optimizes the supply of resources that underpin a cloud service, and then provides those resources to a cloud service provider. Occasionally, cloud service creators also act as cloud service providers. Cloud service providers are the entities that provide cloud computing services to the user. The service provider maintains the service catalogue, sets the price and handles the contractual matters. The cloud service broker acts as an agent between numerous cloud service providers and the service consumer, ensuring optimum cost (and payment), quality and timeliness parameters. The cloud service consumer is the user of the cloud services, often concerned with service cost, quality and timeliness. Note that not all four entities must be present in every cloud service supply chain; it is possible to have just two entities, the cloud service provider and cloud service consumer.

With respect to cloud security, which will be discussed in more detail below, key issues include data privacy and service availability.[15] Security problems can include issues such as data security and user data privacy protection. Service availability concerns includes maintenance of platform stability and cloud computing administration. Traditional cybersecurity issues such as security vulnerabilities, exposure to viruses and hacking threats are also applicable to cloud computing, especially the threat of hacking,

[15] Liu, Wentao. "Research on Cloud Computing Security Problem and Strategy ." *2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)*, 2012, ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6202020.

as malicious intruders may try to hack into cloud accounts and steal potentially sensitive data. Protection strategies can include data encryption, security authentications and access control policies. For the purposes of this paper, issues concerning data privacy and information security are the most salient and will be explored more thoroughly in the next section.

2.2 Cloud Computing: Market Analyses

Cloud computing is a rapidly growing market, globally, projected to grow to at least $278.3 billion by 2021 and, in many ways, has introduced a new paradigm for software, in terms of its distribution, and computing resources, including data storage and development tools, in terms of access. Many digital businesses today rely on cloud services for internal operations, such as data management, hosting services and remote storage and, increasingly, modern enterprises utilize cloud services to provide services to their customers. As shown in Table 2, the public cloud services market is arguably the biggest and most valuable market, especially compared to the other deployment models such as private and community cloud. In 2017, the worldwide cloud public cloud services market generated revenues of worth $145.3 billion, growing 21% in 2018 to $175.8 billion. The market is projected to grow to $206.2 billion in 2019, a 17% increase.[16] By contrast, in the fourth quarter of 2017, public cloud generated revenues of $8.5 billion and private cloud $4.3 billion in revenue.[17] Of the different service models, IaaS is the fastest growing in the 2018 to 2019-time range, growing 27.6% from $31.0 billion in 2018 to $39.5 billion in 2019. Sid Nag, research director at Gartner, believes that PaaS and IaaS will be instrumental in driving the next wave of cloud infrastructure adoption and key drivers of future demand.[18] However, today, SaaS still remains the largest cloud market segment, occupying 41% of the total public cloud service market in 2018. As enterprises have gone increasingly digital in the past ten years, the cloud service ecosystem has grown exponentially in revenues, in value and in size.

---

[16]"Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.3 Percent in 2019." *Gartner IT Glossary*, Gartner, Inc., 2018, www.gartner.com/en/newsroom/press-releases/2018-09-12-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-17-percent-in-2019.

[17] "Public Cloud Expansion Drives Double-Digit Growth of Worldwide Cloud IT Infrastructure Revenues in the Fourth Quarter of 2017, According to IDC." *IDC: The Premier Global Market Intelligence Company*, 2018, www.idc.com/getdoc.jsp?containerId=prUS43705018.

[18] Ibid

Table 1. Worldwide Public Cloud Service Revenue Forecast (Billions of U.S. Dollars)

	2017	2018	2019	2020	2021
Cloud Business Process Services (BPaaS)	42.2	46.6	50.3	54.1	58.1
Cloud Application Infrastructure Services (PaaS)	11.9	15.2	18.8	23.0	27.7
Cloud Application Services (SaaS)	58.8	72.2	85.1	98.9	113.1
Cloud Management and Security Services	8.7	10.7	12.5	14.4	16.3
Cloud System Infrastructure Services (IaaS)	23.6	31.0	39.5	49.9	63.0
Total Market	**145.3**	**175.8**	**206.2**	**240.3**	**278.3**

BPaaS = business process as a service; IaaS = infrastructure as a service; PaaS = platform as a service; SaaS = software as a service

Table 2: Worldwide Public Cloud Services Revenue Forecast September 2018[19]

Of the cloud service providers, Amazon, Microsoft, Alibaba, Tencent and IBM are the current industry heavyweights worldwide, especially in terms of infrastructure services such as IaaS and PaaS. As shown in Figure 1, Amazon, with its Amazon Web Services suite of cloud computing services, currently dominates the public cloud market, and has an estimated 33% of the cloud infrastructure market share, almost 2.5 times greater than its closest competitor, Microsoft. Amazon has held its roughly ⅓ worldwide market share for roughly twelve consecutive quarters; however incumbents such as Microsoft, which offers cloud services via Microsoft Azure, IBM, which offers cloud services via IBM Cloud, Google, which offers cloud services via Google Cloud Platform, and Alibaba, which offers cloud services via Alicloud, have all grown their market shares, without reducing that of Amazon's as the cloud market has boomed in the past few years. The graph below illustrates this trend. It is worth noting that small to medium-size operators are the ones who have seen their market share and revenues diminish.[20]

[19] Columbus, Louis. "Roundup Of Cloud Computing Forecasts And Market Estimates, 2018." *Forbes*, Forbes Magazine, 24 Sept. 2018, www.forbes.com/sites/louiscolumbus/2018/09/23/roundup-of-cloud-computing-forecasts-and-market-estimates-2018/#55bc055e507b.

[20] Coles, Cameron. "AWS vs Azure vs Google Cloud Market Share 2018 Report." *Skyhigh*, Skyhigh Networks, 12 Sept. 2018, www.skyhighnetworks.com/cloud-security-blog/microsoft-azure-closes-iaas-adoption-gap-with-amazon-aws/.

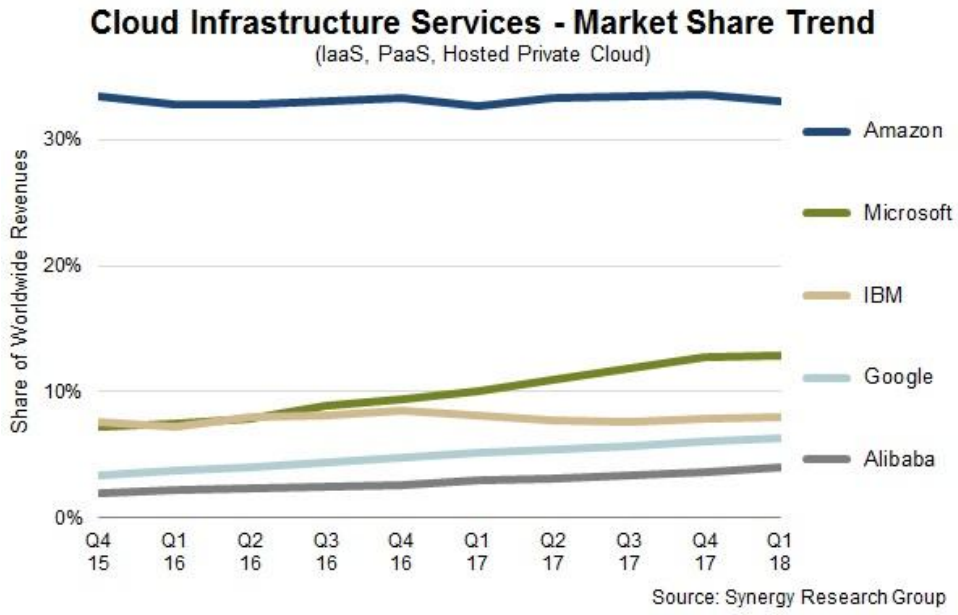

Figure 1: Cloud Infrastructure Services Market Share Trends[21]

Unique to the cloud industry in the technology sector is the notion of scope and the importance of economies of scale. Essential to the concept of cloud computing is "resource pooling," where cloud computing service providers can serve multiple customers using a multi-tenant model that dynamically assigns resources according to demand.[22] The significant cost savings for consumers and profit for cloud service providers are realized only after a certain level of scale have been achieved by the cloud service providers, especially given the initial cost of the data center which hosts the physical IT equipment. The price of data centers can be in the multi-millions and thus, a meaningful level of capital is needed to start hosting cloud services (which can explain why so many Internet companies have invested their extra cash into cloud services businesses). The inherent nature of cloud computing resource sharing, amplified by the cost of building and maintaining expensive data centers results in a market where typically there are a few strong market players in public cloud services, with often one "monopoly-like" player who has successfully exploited economies of scale, which can be seen in Table 3, where a few Internet companies dominate the global landscape. Therefore, there are likely to be only a few dominant players in the cloud computing for any given local. Below, this will play out in both the U.S. and China markets and remains a unique feature of cloud computing markets worldwide.

---

[21] Synergy Research Group. "Cloud Growth Rate Increased Again in Q1; Amazon Maintains Market Share Dominance." *Synergy Research Group*, 2018, www.srgresearch.com/articles/cloud-growth-rate-increased-again-q1-amazon-maintains-market-share-dominance.

[22] Jackson, Kevin. "The Economic Benefit of Cloud Computing." *Forbes*, Forbes Magazine, 12 May 2012, www.forbes.com/sites/kevinjackson/2011/09/17/the-economic-benefit-of-cloud-computing/#2a93d6f5225c.

Public Cloud Leadership by Region – Q1 2018

Rank	Worldwide	North America	EMEA Region	APAC Region	Latin America
Leader	AWS	AWS	AWS	AWS	AWS
#2	Microsoft	Microsoft	Microsoft	Alibaba	Microsoft
#3	Google	Google	Google	Microsoft	Google
#4	Alibaba	IBM	IBM	Google	Salesforce
#5	IBM	Salesforce	Salesforce	Tencent	IBM

Source: Synergy Research Group

Table 3: Regional Public Cloud Leadership in North America, EMEA (Europe, Middle East and Africa), APAC (Asia Pacific) and Latin America[23]

Since IaaS is the backbone of both PaaS and SaaS, using IaaS as a benchmark to analyze market share for the top cloud providers appears to be the most logical choice. The top five IaaS service providers in 2016 and 2017 worldwide remained constant, as illustrated by Table 4. Amazon is the number one IaaS provider, followed by Microsoft, Alibaba, Google and IBM. These five giant titans represent the heavyweights for cloud computing service providers. Notably, four of these companies are based in the U.S. Only Alibaba is Chinese based.

[23] Panettieri, Joe. "Cloud Market Share 2018." *ChannelE2E*, 2018, www.channele2e.com/event/google-cloud-next-2018/.

Vendor	2016	2017	2017 Market Share (%)	Annual Growth Rate (AGR)
Amazon	9,775	12,221	54.1%	25.0%
Microsoft	1,579	3,130	8.7%	98.2%
Alibaba	670	1,090	3.7%	62.7%
Google	500	780	2.8%	56.0%
IBM	297	457	1.6%	53.9%
Other Vendors	5,245	5,699	29.0%	8.6%
Total Market	**18,066**	**23,377**	**100.0%**	**29.4%**

Table 4: IaaS Only Market Share of the Top Five Providers, June 2018

2.3 Cloud Computing: U.S. Market

Cloud computing originated in the United States, and today, the United States remains one of the most robust, innovative and largest cloud markets. At the present time, the U.S. is the most valuable public cloud services market worldwide, with an estimated value of $97 billion in 2018, accounting for more than 60% of the global market.[24] Cloud computing officially came into existence in 2006 when Amazon created its Amazon Web Services subsidiary and released its Elastic Compute Cloud (EC2), a platform that provided developer computing capacity.[25] Between 2008 and 2012, a variety of U.S. Internet companies and start-ups entered the market, including Google (Google App Engine released in 2008, Google Compute Engine live in 2013), Microsoft (Microsoft Azure released in 2010), Rackspace (via Rackspace Hosting in 2010), IBM (IBM SmartCloud announced in 2011) and Oracle (Oracle Cloud released in 2012). Amazon, today, remains the market leader in both the U.S. and worldwide, especially given its first mover advantage in the field, aggressive expansion strategy and its leverage of the economies of scale inherent for success in cloud computing. Revenues and market value from the U.S. region are hard to pinpoint exactly, since cloud computing providers don't typically report on region to region performance metrics publicly. However, Amazon is by far the market leader, followed by Microsoft and

[24] McLaughlin, Kevin. "Alibaba Puts the Brakes on U.S. Cloud Expansion." *The Information*, 2018, www.theinformation.com/articles/alibaba-puts-the-brakes-on-u-s-cloud-expansion?jwt=eyJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJtcmp1bGllbmlzYWFjc0BnbWFpbC5jb20iLCJleHAiOjE1Nzk0OTE5MTksIm4iOiJHdWVzdCIsInNjb3BlIjpbInNoYXJlIl19.hZYDYKeQGrrbbnQgSsIE5WEO1gT8JK_w1LHunxcqqNc&unlock=fbcd594fcdd32d70.

[25] "Announcing Amazon Elastic Compute Cloud (Amazon EC2) - Beta." *Amazon*, Amazon,

Google. One can view the annual revenue run, a metric used to project future financial performance based on current revenue, from Q4 2017 rate in Table 5 to get a good idea of their financial performance. Though Amazon remains the market leader, Microsoft is catching up fast and quickly growing its Azure business.

Cloud vendor	Annual revenue run rate
Microsoft commercial cloud	$21.2 billion
Amazon Web Services	$20.4 billion
IBM	$10.3 billion
Oracle	$6.08 billion
Google Cloud Platform/G Suite	$4 billion
Alibaba	$2.2 billion

Table 5: Annual Run Rate Q4 2017[26]

In terms of the policy regime, during the advent of cloud computing the U.S. government took a rather passive approach to governance, support or intervention, preferring to let the Silicon Valley corporations largely self-regulate and self-innovate. Perhaps the first cloud-focused and cloud-specific policy that the American government passed was the CLOUD (Clarifying Lawful Overseas Use of Data) Act. Introduced in February 2018 and signed into law March 2018, the CLOUD Act, initiated at the behest of the FBI, allows U.S. federal law enforcement agencies to warrant or subpoena data stored on servers of U.S. companies no matter if the data is stored domestically in the U.S. or internationally.[27] However, this bill remains rather light-handed in terms of government intervention and is solely targeted at U.S.-based technology entities. Moreover, the bill was introduced a full 12 years after the introduction of cloud computing services in 2006. Especially compared to China, which has introduced a bevy of domestic policy and regulatory initiatives directed at cloud computing, the U.S. governmental approach remains non-interventionist, with only slight policy aimed primarily at intelligence gathering.

2.4 Cloud Computing: China Market

As the digital economy in China has grown exponentially in the past decade, so too has cloud computing. China is the 5th largest public cloud market globally, with an

[26] Dignan, Larry. "Top Cloud Providers: How AWS, Microsoft, Google, IBM, Oracle, Alibaba Stack Up." *ZDNet*, ZDNet, 16 Jan. 2019, www.zdnet.com/article/top-cloud-providers-2018-how-aws-microsoft-google-ibm-oracle-alibaba-stack-up/.

[27] "H.R.4943 - 115th Congress (2017-2018): CLOUD Act." *Congress.gov*, 6 Feb. 2018, www.congress.gov/bill/115th-congress/house-bill/4943.

estimated value of $5.4 billion in 2018.[28] By 2019, the value of the China cloud computing market is projected to reach 430 billion RMB.[29] By 2021, China is expected to become the second most valuable cloud market, after the U.S.[30] Cloud was originally adopted in China around 2009/2010, with the introduction of four pilot test cities in the Mainland to determine the efficacy of the technology. Government subsidies and partnerships, combined with policies that limit foreign competitors with equity caps and data localization requirements, have resulted in a robust, cloud computing service ecosystem that doesn't much match any other market in the world. All of the dominant firms in the China market are local. Moreover, the government has placed strategic importance on the development of the cloud, through initiatives such as the Made in China 2025 Plan and the 13th 5 year plan, both of which identify cloud technologies as an essential backbone for the development and advancement of the Chinese IT industry, the foundation for key industries such as AI and IoT, and, by extension, as essential to cementing China's superpower status as an international technology force. Even the Ministry of Industry and Information Technology regularly issues plans and reports, such as the Cloud Development Three Year Action Plan (2017-2019) (《云计算发展三年行动计划（2017 - 2019年）》解读), illustrating specific measures intended to grow the cloud computing industry and technological development on a national level.[31] In China, robust cooperation exists between the public and private sector, in a sui generis manner to the Chinese economy and State.

The biggest player in the Chinese market is Alibaba's Alicloud (or Aliyun 阿里云), a cloud subsidiary of Alibaba, founded in 2009. Similar to its fellow e-commerce giant Amazon, Alibaba began to sell its extra data storage capacity, much of which was originally used to power its core e-commerce business. Since 2015, Alicloud has successfully captured 30-45% of the cloud computing market share, especially the IaaS market, in China, and remains the dominant market player, enabled by the economies of scale inherent in the cloud computing industry. Aliyun has a unique advantage in the China market, given its ability to successfully meet China's compliance, administrative, legal and financial requirements.

Table 6 illustrates the state of the Chinese cloud market in 2015. Alicloud is the dominant player, with approximately 31% of the market share. Major Chinese telecom operators, China Telecom and China Unicom, had the next biggest market shares, at

---

[28] McLaughlin, Kevin. "Alibaba Puts the Brakes on U.S. Cloud Expansion."

[29] 姜 维. "2018中国云计算产业竞争格局分析 阿里云占市场近半份额." *PCOnline*, 8 Mar. 2018, servers.pconline.com.cn/1091/10917424.html.

[30] McLaughlin, Kevin. "Alibaba Puts the Brakes on U.S. Cloud Expansion."

[31] "《云计算发展三年行动计划（2017 - 2019年）》解读." *中华人民共和国工业和信息化部*, 2017, www.miit.gov.cn/n1146295/n1652858/n1653018/c5570632/content.html.

13% and 8%, respectively and approximately. Microsoft, via its partnership with 21Vianet, had an approximate 7% share of the market. Other foreign cloud service providers, such as Amazon, IBM, and Oracle, combined had not more than 5% of the market. From the 2015 perspective, Chinese domestic companies already dominated the local landscape, and this trend continues into 2016 and 2017.

云服务供应商	2015年市场份额	2015年营收(百万美元)	年增长率
Alicloud阿里	31.0%	259.0	80.7%
China Telecom中国电信	13.1%	109.8	59.9%
China Unicom中国联通	7.6%	63.5	21.1%
21Vianet世纪互联（微软云授权实体）	7.3%	61.1	102.5%
Kingsoft金山	4.5%	37.9	251.6%
Amazon.com亚马逊	4.3%	36.1	157.9%
CaptialOnline Data Service首都在线	1.2%	10.2	69.6%
ChinaCache蓝汛	0.9%	7.9	17.0%
Dr.Peng Group鹏博士	0.6%	4.8	41.2%
Fujitsu富士通	0.5%	4.4	60.2%
IBM	0.1%	1.1	27.9%
Oracle甲骨文		0.0	
VMware		0.0	
Others	28.8%	241.0	59.5%

Table 6: Chinese Cloud Service Providers: 2015[32]

According to research firm IDC, the 2016 China cloud IaaS market had four leaders: Aliyun, Chinese Telecom, Tencent and Kingsoft (Jinshan) Cloud. With $588 million USD in revenues, Aliyun had a market share of over 40% for the 2016 China IaaS market. China Telecom had an 8.51% market share, with revenues of $122 million USD. Tencent, via Tencent Cloud, had revenues of $100 million USD, with a 7.34% market share. Tencent Cloud began in 2013 and by 2016 was a major force in the domestic Chinese market. Lastly, Kingsoft Cloud had a 6.02% market share with $87 million USD. Table 7 illustrates the 2016 China IaaS market.

Cloud Service Provider	**Domestic Market Share**	**Revenue**

[32] “IDC：2015年中国公有云计算报告 阿里云市场份额达31%.” *199it*, 2016, www.199it.com/archives/508703.html.

Aliyun (阿里云)	40%+	$4 billion RMB ($588 million USD)
China Telecom (中国电信)	8.51%	$122 million USD
Tencent (腾讯云)	7.34%	$100 million USD
Kingsoft Cloud (金山云)	6.02%	$87 million USD

Table 7: Chinese Cloud Service Providers: 2016

Two notable conclusions can be gleaned from the 2015 to 2016 market for China cloud computing. One is that local, domestic companies cemented their market dominance from 2015 to 2016. In 2015, 21Vianet, via its partnership with Microsoft, still had a sizeable market share, acting as the four biggest cloud service providers in China. Come 2016, the top four IaaS providers were all local Chinese companies, with no foreign joint venture partners present. Second, Aliyun increased its market share from 2015 to 2016, further solidifying the notion that cloud companies benefit from economies of scale.

In 2017, Aliyun continued to dominate the China cloud IaaS market, increasing its market share to 47.6%. Once again, foreign cloud service providers were notably absent from the list, with no mention of Amazon, Microsoft or IBM. Tencent, Kingsoft, and China Telecom were once again the top providers, as well as start-up Ucloud. Figure 2 shows this phenomenon.

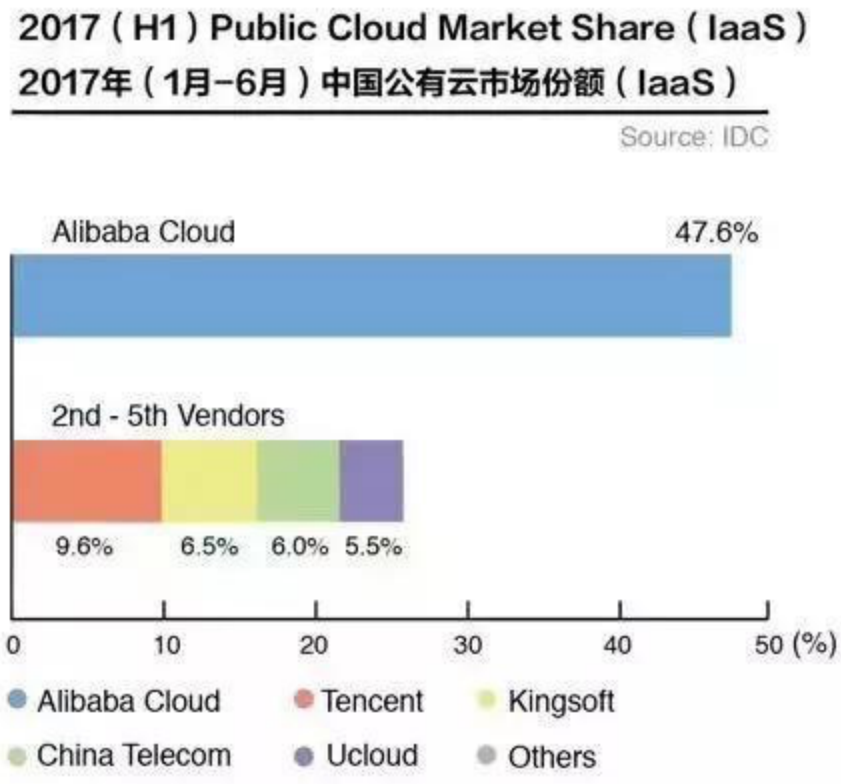

Figure 2: Chinese Cloud Service Providers: 2017

In terms of the policy regime, China, and the Chinese government, has enacted a long-term strategic push towards not only indigenous innovation, but also towards the control of data, viewing both as primary to its political and economic interests. China has long used policy, including foreign equity caps, joint venture partnership requirements and local subsidies, for Chinese telecommunications and, more recently, digital services. For instance, the 2017 Cybersecurity Law mandated that all data generated by Chinese users had to be stored in China and could not be sent out of the country without government consent, sending American companies scrambling to either construct extremely expensive local data centers with joint venture partners, such as Apple, or sell their China cloud business to their local partner, such as Amazon. One can view data localization as am international trade barrier which, combined with localization and operational difficulties, can largely explain the paucity of successful foreign technology companies in the cloud services business. The China market, unlike any other cloud market today, is wholly dominated by domestic Chinese firms with little market share from the major U.S. technology players.

Above is a brief overview of cloud computing as a technology, an introduction to key service models and operational processes and information on cloud security, market and computing resources. This background will help provide the necessary context for the analyses discussed below.

3. Cybersecurity

3.1 Cybersecurity; Overview & Framework

Cybersecurity is becoming an increasingly invoked and focal aspect of “national security.”[33] Labeled as the 'fifth domain,' cybersecurity has become an important part of national security and governments worldwide have responded accordingly with policy. Foreign economic and industrial espionage represent a significant threat to today’s nations. Cyberspace remains the preferred operational domain for a variety of malicious actors, from rogue hackers to state-sponsored commercial enterprises. Advanced, development economies with corporations who engage in expensive and costly R&D with expensive IP are a particular target for developing economies hoping to advance on the global stage. The U.S. and China, currently, fit into this dialectical relationship, with China ostensibly hoping to access a variety of critical technologies, IP and trade secrets to help leap-frog and spur its economic advancement and transition from a manufacturing to a more services-oriented economy. Moreover, China has a complicated and multi-pronged strategy to support its strategic development goals, including science and technology advancement and military modernization, among others.[34] China employs both licit and illicit methods. Licit methods can include joint venture partnerships that mandate technology transfer, which is legal under WTO guidelines, while illicit means include hacking, cyber-espionage and cyber-theft. Thus, issues regarding data security are of foremost concern to data-sensitive U.S.-China cloud computing technologies and services.

Three key questions regarding data security, cloud computing and international trade will be explored through case studies and the lens of cybersecurity:

(1) Cybersecurity Risk: Whether the "cloud" increases or decreases the risks related to cybersecurity?

(2) Policy Implications: Whether and how countries construct barriers to cloud computing originating from other countries due to concerns about cybersecurity?

(3) Strategy Reactions: If restrictive international trade policies do exist, how can business entities navigate these barriers, or not, to effectively form a viable strategy?

---

[33] Huang, Keman, et al. *How Can Cybersecurity and International Trade Impact Each Other: A Systematic Framework*. 2018.

[34] “Foreign Economic Espionage in Cyberspace.” *NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER*, 2018, www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf.

3. 2 Cybersecurity; International Trade

Cybersecurity concerns have increasingly impacted national security policy, both politically and economically, affecting international trade in the global, digital economy. As Huang, Madnick and Jonson (2018) explore via a systemic framework linking the relations between cybersecurity and international trade, cybersecurity is no longer solely a policy or regulatory issue, but increasingly a business strategy issue, irrevocably tied into geopolitics.[35] Moreover, cybersecurity concerns impact national and organization action, which reshapes the international trade environment and forms the nature of a given country's domestic market. We will see this dynamic play out, where cybersecurity concerns impact international trade for digital services access in cloud computing, in the U.S. and China case studies discussed below.

Cybersecurity concerns that impact international trade emerge from two different perspectives, national security concerns and supply chain concerns.[36] For the purposes of this paper, national cyber security concerns will be mostly explored, though supply chain concerns are certainly applicable, especially in terms of hardware for cloud computing data center equipment. Khetri (2016) details categories to understand national cybersecurity concerns: military security, political security, economic security and cultural security.[37] For the majority of regulation in the U.S. and China, political security and economic security are the most salient dimensions, though cultural security certainly factors into the CCP's decision making process regarding how to create a healthy cyberspace environment, in line with the public morals of China that maintains their public order.[38] Political security includes preventing political espionage, such as a malevolent actor obtaining sensitive political or military information, and thereby ensuring political stability, where the use of cyberspace could potentially undermine a government's political authority. In terms of economic security, economic espionage and economic stability are key concerns. Economic espionage refers to the stealing of economic related trade information, and economic stability refers to the use of cyberspace that could lead to economic instability in a country. For the U.S. policy regime affecting cloud computing and data privacy, the U.S. government seems most concerned with preventing political espionage and economic espionage. For the Chinese policy regime affecting cloud computing and data privacy, the Chinese government seems most concerned with ensuring political and economic stability. Table 8 below highlights the respective governments national cyber security concerns which impacts digital trade in the country.

---

[35] Huang, Keman, et al. *How Can Cybersecurity and International Trade Impact Each Other: A Systematic Framework*.
[36] Ibid
[37] Ibid
[38] Ibid

National Cybersecurity Concern: Category	National Cybersecurity Concern: Type	Relevant Country Policies
Political Security	Political Espionage	U.S.
	Political Stability	China
Economic Security	Economic Espionage	U.S.
	Economic Stability	China

Table 8: National Cybersecurity Concern Policy Motivations in the U.S. and China

Based upon these national cybersecurity concerns, governments tend to impose different policies and regulations, often in the form of trade regulations or barriers.[39] According to the United Nations Conference on Trade & Development (UNCTAD) in 2012, non-tariff trade barriers exist relevant to cybersecurity and the digital economy. For the purposes of this paper, the following trade barriers are relevant to the discussion: authorization or registration requirements, local content measures, foreign direct investment barriers, restrictions on post-sales/digital services and intellectual property. In particular, restrictions on post-sales/digital services, especially data localization regulations in China passed in 2017 via the Cybersecurity Law, are a major trade barrier in cloud computing, as identified by the United States Trade Representative (USTR) in 2017.[40]

Thus, in summary, national cybersecurity concerns, especially those of political or economic natures, have implications on the drafting and implementation of trade policy that results in international trade barriers in the digital economy. These national cybersecurity concerns will be used to explore why U.S. cloud service operators have such a low market share in China, and vice-versa.

3.3 Cybersecurity; The Cloud

The Cloud Security Alliance (CSA) released its "Treacherous Twelve" in March of 2016, detailing the top 12 threats to cloud security. Foremost on the list is data breaches. Cloud computing has transformed the ease with which to access and delivery technology globally, and use has skyrocketed in the past decade. However, the rise of cloud has also created new security vulnerabilities and has amplified pre-existing issues, problems and concerns. Traditional cybersecurity threats, such as phishing, the

[39] Ibid
[40] Ibid

use of malware, the installation of backdoors, are all applicable to the cloud. Other cloud-specific threats include attacks on virtualization and invasions of user data privacy, often by the cloud service provider itself, either knowingly or unknowingly. Liu (2013) identifies four main new security problems introduced by the advent of cloud computing. Summarily, they are: data security, user data privacy protection, cloud computing platform stability and cloud computing administration.[41] For the purposes of this paper, however, problems regarding cloud computing platform stability and cloud computing administration are assumed to be non-factors. Especially given the technological advancement in the U.S. and China and the engineering skill from the main cloud computing service providers in the U.S. and China, such as Microsoft and Alibaba, cloud computing service offerings in the two countries are assumed to be stable and competently administered. Difference, though, will emerge, in terms of data security and user data privacy, especially impacted by government policy at a national level. Therefore, the key cybersecurity issues explored with respect to cloud will be data security and user data privacy, through an updated Parkerian Hexad model.

3.4 Parkerian Hexad

The Parkerian Hexad model is a useful tool by which to analyze information security for cloud computing operators. In 1998, information security researcher and consultant Donn B. Parker introduced the Parkerian Hexad in *Fighting Computer Crime*.[42] Building on the classic CIA triad, consisting of confidentiality, integrity and availability, Parker introduced three new elements, possession, authenticity and utility, to form a more comprehensive and complete security model.[43] While the CIA model primarily focused on the technological security risks, Parker sought to introduce the human element, honing in on the role that people play in defending and perpetuating information compromise. Parker suggested that the elements be understood in the following groupings: confidentiality and possession, integrity and authenticity, and availability and utility. A visual representation of the Parkerian Hexad is provided below in Figure 3.

[41] Liu, “Research on Cloud Computing Security Problem and Strategy .”

[42] Parker, Donn. *Fighting Computer Crime: A New Framework for Protecting Information*. ACM, 1998, dl.acm.org/citation.cfm?id=286060.

[43] Pender-Bey, Georgie. “THE PARKERIAN HEXAD.” *Information Security Program at Lewis University*, cs.lewisu.edu/mathcs/msisprojects/papers/georgiependerbey.pdf.

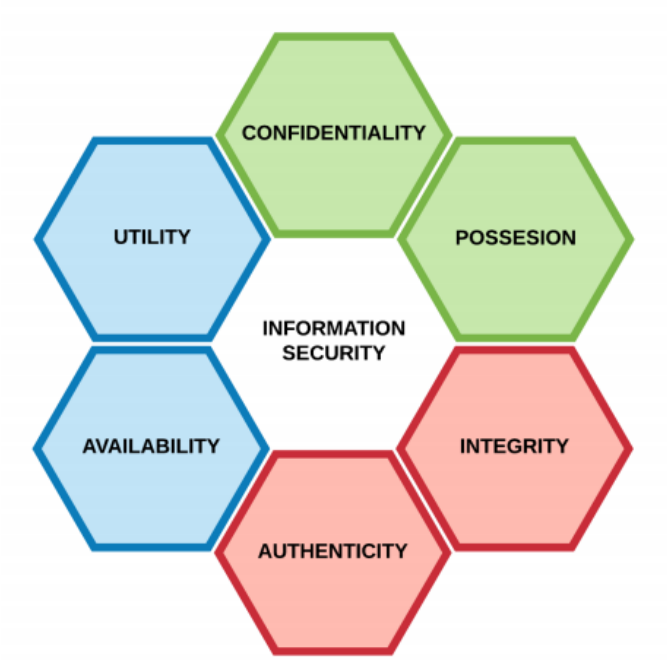

Figure 3: Cybersecurity & The Parkerian Hexad[44]

The six elements of the Parkerian Hexad, confidentiality, possession/control, integrity, authenticity, availability and utility, form a useful lens for understanding the main concerns of IT security. *Confidentiality*, arguably the most important, refers to who can access what kind of information. Information should not be made available or disclosed to unauthorized entities, individuals or processes. *Possession* or *control* define who or what systems can possess information or have control over information use. Confidential data can be accessed or controlled by unauthorized users without violating confidentiality; thus, Parker introduced the concept of possession/control to cover breaches when confidentiality is both salient yet non-existent.[45] *Integrity* is the ability for data to be correct and consistent with its original use. That is, the data has not been altered or changed in an unauthorized manner. If data is modified, either intentionally or unintentionally, that would constitute a breach in data integrity. *Authenticity* involves the notion of proof of identity, assuring the validity and accuracy of the information's origin and creation. *Availability* is the ability to access information in a timely manner, maintaining and ensuring resource availability when required for intended use. Though simple to describe, guaranteeing availability is one of the key challenges to IT security. Lastly, *utility* refers to the concept of usefulness, ensuring that the information is useable and useful in a manner so intended by the user. Table 9 below summarizes the key concepts and definitions of the Parkerian Hexad model.

[44] Marks, Paul. "Cybersecurity and the Parkerian Hexad." *European Niche Technology Recruitment - StaffHost*, 2018, www.staffhost.co.uk/blog/2018/10/cybersecurity-and-the-parkerian-hexad.
[45] Pender-Bey, "THE PARKERIAN HEXAD."

Parkerian Hexad Element	Component Definition
Confidentiality	Information is only available or disclosed to authorized users.
Possession/Control	Only designated users or systems may possess or control information.
Integrity	Information must be correct and consistent with its original use; information cannot be altered in an unauthorized manner.
Authenticity	The origin and creation of the information must be valid and accurate.
Availability	Access to information is available in a timely manner.
Utility	Information is in a useable and useful manner for the intended user.

Table 9: The Parkerian Hexad: Component Definitions

In *Cloud Computing* by Nayan B. Ruparelia, the Parkerian Hexad is discussed as it relates to cloud security.[46] Since cloud user data storage may involve data being stored in a different country than the country in which the user generated the data, the notion of international jurisdiction with regards to data protection mechanisms is crucial. Thus, Ruparelia proposes to add a seventh dimension to the Parkerian Hexad: jurisdiction. The addition of jurisdiction helps account for the legal or regulatory requirements, an increasingly important element in information security. The result is an updated Parkerian Hexad, now with seven critical information security elements, as shown in Table 10.

Updated Parkerian Hexad Element	Component Definition
Confidentiality	Information is only available or disclosed to authorized users.
Possession/Control	Only designated users or systems may possess or control information.

[46] Ruparelia, *Cloud Computing*.

Integrity	Information must be correct and consistent with its original use; information cannot be altered in an unauthorized manner.
Authenticity	The origin and creation of the information must be valid and accurate.
Availability	Access to information is available in a timely manner.
Utility	Information is in a useable and useful manner for the intended user.
Jurisdiction	Local laws or regulatory requirements which allow for untampered access to information.

Table 10: The Updated Parkerian Hexad: Component Definitions

Table 10 detailing the updated Parkerian Hexad will be used in later analysis of U.S. and China cloud computing operators expanding internationally into China and the U.S., respectively, and to explore how information security concerns impact downstream consumer adoption.

3.5 A Discussion on Cloud, Data and Consumer Data Privacy

A discussion is required regarding the intersection between data privacy practices, data privacy laws and cloud computing solutions, especially as it relates to the consumer. The notion of "consent" is a key concept in most global data privacy laws, pursuant to which data users must obtain the data owners consent to use a given piece of information. Most users have to give express permission if their data is to be used, except in the case of legal action or in intelligence operations. However, users generally have the expectation that their data is private and secure. Recent scandals such as Cambridge Analytica and Facebook, where user data was unknowingly granted to third parties, challenge this expected norm and can have a negative effect on user experience and long-term, sustained customer use of the technology product.

Moreover, this issue is compounded by the transnational nature of cloud computing storage. Since cloud companies such as Amazon and Alibaba store user data at data centers throughout the world, their cloud computing network can be thought of as typically "transcending national boundaries" by facilely moving data to and from the various centers depending on internal operational directives and needs.[47] The reality

[47] Eustice, John C. "Understanding Data Privacy and Cloud Computing." *Legal Cases - Westlaw | Thomson Reuters Legal*, legal.thomsonreuters.com/en/insights/articles/understanding-data-privacy-and-cloud-computing.

of the current world is that such data storage networks inevitably touch upon countries with restrictive data privacy and protection laws, such as Europe or China. Thus, for users, understanding where the data is actually stored will have a great impact on data control, data oversight and data security, since different locations will have different rules regarding how and when data can be accessed and used.

One of the biggest concerns for users of cloud computing is that the data stored in the cloud may end up being stored in a different country than the one in which the users reside. This situation begets a critical question: Should the data be compromised; which country's laws or data protection mechanisms should apply? Such an issue relates to the legal and regulatory jurisdiction of data storage within an international and cross-border dimension. This worry is further exacerbated by the inherently elastic nature of cloud computing, which can easily shuttle computing resources, including the storage of data, from one location to another.[48]

In the U.S., data protection laws are rather nascent. Despite some intelligence-related legislation, the U.S. government often leaves the particulars to the technology companies, who detail the data protection provisions in their terms of service or SLA agreements. There is no unifying data protection law in the U.S. Instead, the various States themselves usually mandate privacy protection for individuals, especially involving sensitive information such as biometric information and social security numbers. In general, in the U.S., users are quite sensitive about the use of their personal data. The Edward Snowden and Wikileaks controversies caused quite a stir, and Americans, in general, seem more protective over their data privacy then their Chinese counterparts. In general, the American attitude towards data privacy can be traced back to the Fourth Amendment, which protects against unreasonable searches or seizures by government authorities and, by modern extension, the Electronic Communications Privacy Act of 1986 (ECPA), which heavily restricts the ability of the government to access stored digital communications or data on the Internet without just cause (which may require a formal search warrant).

In China, by contrast, users have grown accustomed to a laxer sense of control over their personal data. Since so much of average Chinese life is controlled by the State in any event, such as where one can go to school, where one can legally live, whether one can go abroad or not, the expectation, somewhat, follows by extension that data too would be able to be monitored and not entirely secure or private. Indeed, the CCP engages a massive surveillance and censorship campaign of its citizens, spending billions annually to monitor its citizens. This has created a different norm regarding data privacy than in Western countries such as the United States. Chinese "netizens" are more likely to be less sensitive regarding their data and privacy usage rights. Moreover, the comparatively weak intellectual property environment in China also contributes to the sense that information is often public and rarely proprietary. Though things in China

[48] Ruparelia, *Cloud Computing*.

are certainly evolving as IP laws get enforced more and more, the general attitude of Chinese individuals remains less concerned than their American counterparts about the protection of their private information.

Data users in the U.S. and China, thus, have differing attitudes regarding data privacy. In America, there is an expectation that user data is private, protected and controlled. In China, consumers expect most data to be monitored and user privacy data is viewed less as an inherent right.

Logically following, Chinese companies in America will, subsequently, face challenges when selling data sensitive products in America given both differing attitudes about data privacy and the lingering effects of the lack of control over domestic Chinese data from government parties. American companies will not face such a challenge in China for data sensitive products, offering those that are comparatively more secure and trustworthy. However, their challenge will stem from restrictive Chinese policy for foreign players, fierce local competition in a quickly evolving market, and growing techno-nationalistic sentiments within China, both in terms of the people and the Party.

3.6 Porter's Five Forces

Especially when examining a company's strategy within a market, Porter's Five Forces is a useful tool to help understand relative comparative advantage. Michael Porter, of Harvard University, first published the framework in the Harvard Business Review in 1979.[49] Porter wanted to identify the key factors that impact the competitive business environment which determines a firm's profitability. Summarily, as shown in Figure 4, the five forces are: 1) Competitive Rivalry; 2) Supplier Power; 3) Buyer Power; 4) Threat of Substitution; and 5) Threat of New Entry.

[49] Porter, M. (1980). Competitive strategy. New York: Free Press.

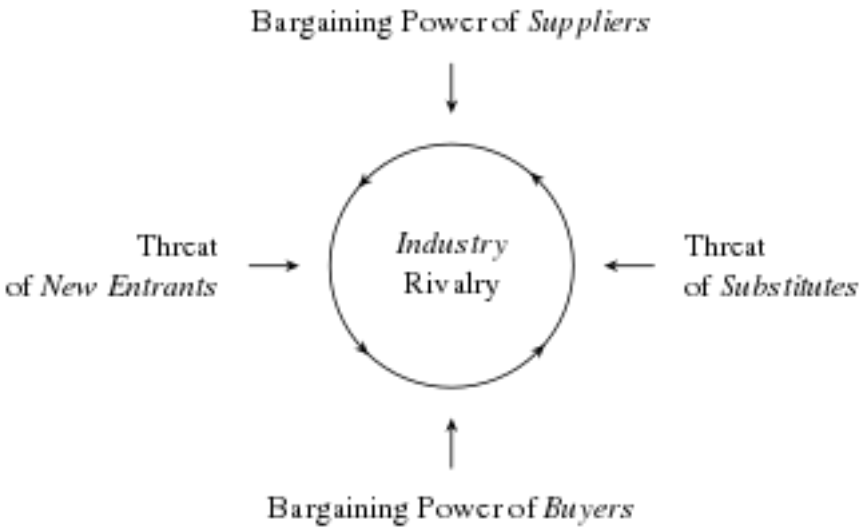

Figure 4: Porter's Five Forces

Competitive Rivalry looks at the number and strength of competitors in the market. Intense rivalries cause companies to slash prices and engage in aggressive marketing. A lack of Competitive Rivalry can result in monopoly-like profits. Supplier Power refers to the ease by which suppliers can increase their prices. More suppliers mean that switching for cost benefits can be easier and cheaper. Note: since most cloud service providers are also the "supplier," this element of Porter is not as salient within the cloud computing industry context, though it can be relevant for more outsourced parts, such as chips that are manufactured by third parties. Buyer Power indicates the extent to which buyers can drive prices down. If there are only a few buyers, they may be able to negotiate prices down. A larger number of buyers will likely be unable to accomplish this control over price. Threat of Substitution, which is very critical to cloud computing, is the ability or likelihood that customers may find a different way or method of receiving the product or service. Threat of New Entry refers to the relative ease by which a company or competitor can enter your market. If entry is easy, then one's strategic advantage position can be weakened. New Entry is typically more difficult for cloud computing, since the initial capital investment for a data center network is quite costly. Porter's five forces are summarized in Table 11 below.

Force	Details
Competitive Rivalry	• Number and strength of competitors, quality differences, switching costs, customer loyalty
Supplier Power	• Number and size of suppliers, uniqueness of service, switching costs

Buyer Power	● Number of customers, price sensitivity, ability to substitute, cost of changing
Threat of Substitution	● Substitute performance, cost of change
Threat of New Entry	● Time and cost of entry, economies of scale, barriers to entry

Table 11: Porter 5 Forces

Porter's Five Forces framework will be later used to explore companies' competitive advantage, or relative disadvantage, in the U.S. and China in the cloud computing context.

3.7 A Comprehensive Framework

We can witness how the flow of how policy is created with regards to cloud computing and data protection in the U.S. and China in the framework presented in Figure 5. Initially, cybersecurity concerns or alternative policy motivations such as the desire for technological access play a role in the formation of government policy. International cloud computing operators can either comply or oppose local law, with a variety of outcomes which will have implications for adoption. Customers will either adopt or not, but their decision may be informed by authoritarian based policy that results in data being not as secure. Specifically, entities may choose to not adopt Alibaba's Alicloud in the U.S. given the possibility that the data might not be secure and audited by the Chinese government in a non-transparent manner. Policy and corporate actions will affect the market: domestic firms will likely dominate, with a few key players having a large market share, given the economies of scale that comes will cloud storage infrastructure costs. This dynamic will be explored, in detail, below.

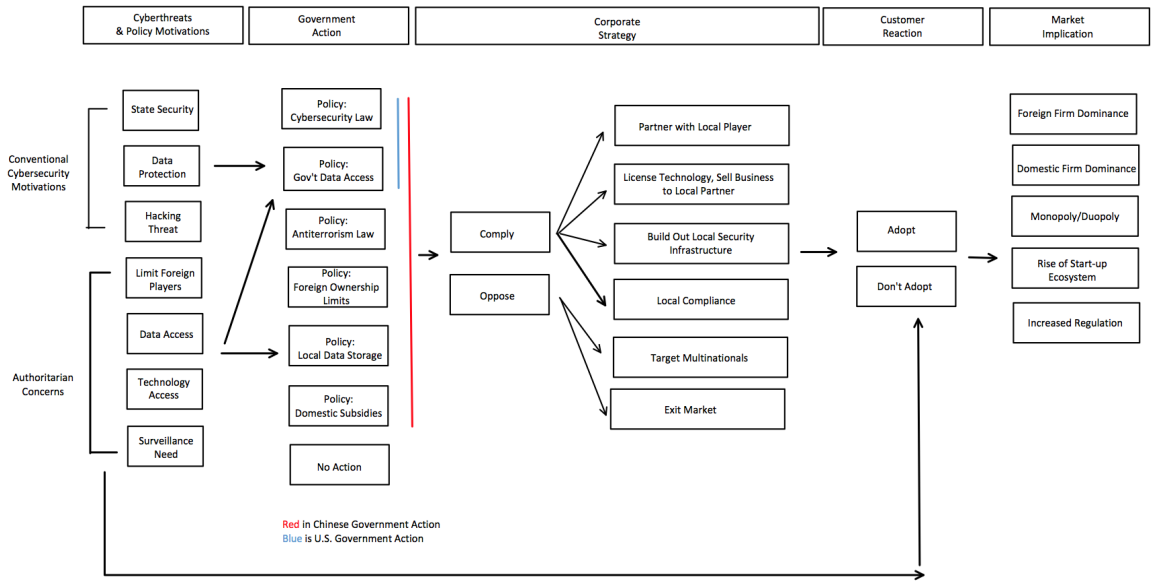

Figure 5: A Systems Dynamic Framework for U.S.-China Cybersecurity Policy & Cloud Computing Business Expansion

In terms of cyber threats and policy motivations, global governments conventionally are concerned with ensuring state security, protecting data protection and preventing hacking. Additionally, authoritarian governments, such as China, are also hoping to limit foreign players, increasing the market share of domestic companies, ensuring unfettered access to data, allowing for access to foreign technology, through licit and illicit means, and enabling the government to conduct surveillance on its netizens. Notably, surveillance is different categorically from state security, which encompasses traditional intelligence gathering law enforcement activities. From there, governments form policies around these concerns, which can take the shape of cybersecurity laws, government data access laws, anti-terrorism laws, foreign ownership limit laws, local data storage requirements, or domestic subsidies for local companies. Alternatively, governments may take no action given their cybersecurity concerns. Companies, as a result, can either comply or oppose these regulations. If they oppose, companies will often be forced to exit the international target market, or contract with multinational companies that have business entities in other locals. If they comply, companies can form a partnership with a local company in the form of a joint venture partnership, license its technology or sell its business to the local partner, build out its local security infrastructure, or conduct other activities to ensure local compliance. By reaction, customers will either choose to adopt or not adopt these products or services, informed, indirectly, by government policy and, directly, by corporate action. This will, in turn, have a noted effect on the market, where foreign or domestic firms will come to dominate, often in a monopoly-like or duopoly-like manner,

cause a rise in start-ups that hope to disrupt the market, or create an environment of increased government concern and regulation, from which the cycle would start again.

4. America to China: Cloud Expansion

For American technology companies, China represents a highly desirable market in terms of potential revenue generation and population user base, yet remains elusive in terms of effective long-term strategy. In 2017, China boasted a 751 million internet users, with a 96.3% mobile internet penetration rate. On Single's Day (11/11) alone, consumers spent over 168.2 billion RMB on Alibaba's platforms. Yet for Silicon Valley giants, China often remains out of reach, with challenges including China market entry, brand building, localization, government compliance, swiftly adapting to ecosystem shifts, and ethical concerns. For instance, as a result of new regulations issued by the Cyberspace Administration of China (CAC) in February 2017, entitled "Inspection Measures on Network Products & Services" 《个人信息和重要数据出境安全评估办法（征求意见稿）》, Amazon sold its public cloud business, Amazon Web Services, to its local partner, Beijing Sinnet Technology. The deal, struck for $301.1 million in November 2017, helps Amazon achieve better compliance with respect to local data storage requirements, but in some ways represents a setback. Companies whose future success hinges, in part, on their ability to continually woo Chinese consumers have adapted, while other companies, less successful in making economic progress in China, have not. For example, Apple recently announced that it will open its first data center in Guizhou, China. The move is part of Apple's $1 billion investment in the province and, adroitly, it will be operated in partnership with a local data management business, the Guizhou-Cloud Big Data Industry. All in all, successfully navigating through local compliance laws still remains a key factor to achieve success for American cloud technology companies in China. For the American to China cloud expansion analysis, the following companies will be examined as case studies: Google, Microsoft, Amazon, and Apple.

4.1 America to China: Context & Background

The Chinese government, via a complex ecosystem of government bodies, research institutes, private-sector companies, state-owned enterprises and military organizations, has prioritized the development of cloud computing technology and the cloud computing industry in China. For instance, the Ministry of Industry and Information Technology (MIIT) released the Software and Information Technology Service Industry

Development Plan for the 12th Five Year Plan (软件和信息技术服务业"十二五"发展规划) in 2011, which referenced cloud computing in three of the ten priority technological areas.[50] Thus, unlike in the U.S. where the government takes a more hands-off approach to technological innovation, especially in recent decades, the Chinese government has taken, and will undoubtedly continue to take, an activist stance, working directly with private and state-owned enterprises to spur previously identified key technological development.

To grow its domestic sector and protect national security interests, China limits foreign investment in value-added telecommunications services, such as cloud. U.S. companies must enter into joint venture partnerships with Chinese companies in order to effectively provide cloud computing services to Chinese consumers. Joint venture partnerships typically involve aspects of technology transfer. In China, since foreign firms are barred from competing directly against Chinese domestic firms, the only choice American companies have to access the large Chinese market is to enter into joint venture partnerships with Chinese firms. Thus, this de facto requirement demonstrates that an unequal playing field is already emerging, where Chinese domestic firms benefit disproportionately in the local market. This imbalance is further exacerbated by government support for “domestic” national champions, which can take the form of subsidies, research and development funding or economic performance incentives.[51] The influx of American technology (by whatever means) combined with robust and protective government policy has enabled the cloud computing industry in China to boom since 2010.

It is useful to understand China’s specific, strategic goals in this sense. China hopes to become an economic heavyweight on the global stage, bolstered by advanced technology that is indigenously innovated and a military that is state-of-the-art and modernized. In order to achieve such aims, the Chinese state has issued a variety of plans, such as China 2025, and specific policies. Mechanisms China has traditionally used to achieve such goals include a legal and regulatory environment, joint venture partnerships, M&A, international talent recruitment and many more. Figure 6 illustrates how China’s strategic goals are operationalized.

[50] Ragland, Leigh Ann, et al. “Red Cloud Rising: Cloud Computing in China.” *U.S.-China Economic and Security Review Commission*, 2013, www.uscc.gov/sites/default/files/Research/DGI_Red%20Cloud%20Rising_2014.pdf.
[51] Ibid

Figure 6: Understanding China's Strategic Goals[52]

China, through a variety of plans and policies issued by the most central corridors of state government, hopes to achieve comprehensive national power through an innovation-driven economic growth model (with a focus on services rather than manufacturing) and a modernized military. China has implemented a variety of mechanisms to achieve such ends, such as M&A activities, a talent recruitment program, a unique legal and regulatory environment, joint venture partnerships, etc.

4.2 A Discussion on China & the WTO

At this point, a discussion regarding China and the WTO is warranted. China joined the WTO in 2001, leading to a boom in international trade. The entry was instrumental in the realization of the China economic miracle and its double-digit GDP

[52] "Foreign Economic Espionage in Cyberspace." *NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER*, 2018.

growth in the following decades. As a condition for WTO entry, China was supposed to revise hundreds of laws, regulations and other measures, including opening the economy to foreign investment, lifting restrictions in foreign ownership, especially in the financial sector, and stop providing unfair advantages to domestic Chinese firms. Yet, China's entry into the WTO has been marred by controversy and has presented fundamental challenges to the contemporary global economy that the WTO often is unequipped to handle.

Law professor Mark Wu in his paper *The "China, Inc." Challenge To Global Trade Governance,* argues that China's rise presents a major challenge to the WTO's multilateral trade regime given the nature of China's unique governing structure.[53] In effect, the issues that China presents to the WTO skew political in nature and, thus, beyond the jurisdiction of the simplified economic squabbles that the WTO is equipped to properly handle. The core of the challenge that China presents to the WTO stems from the sui generis nature of China's economic structure, which, idiosyncratically, has evolved in a manner not only unforeseen by those who negotiated its entry into the WTO, but also outside the purview of what the WTO can rule on. When China joined the WTO in 2001, key state-sponsored elements of the Chinese economy did not exist. Six unique factors of the Chinese economy, which Wu dubs "China Inc.", separate China from traditional state capitalist economies. These factors are detailed in Table 12 below. Summarily, Wu concludes that with the unique economic nature of China and its correlated rise on the world stage will exacerbate the diminishing centrality of WTO law for global trade governance.

Element Number	Distinct Economic Structural Element	Detailed Information
Element 1	The State as a Corporate Holding Entity: SASAC	● Chinese State Owned Enterprises (SOEs) controlled by single government agency, State-owned Assets Supervision and Administration Commission (SASAC) of the State Council. ● Organized in 2003, SASAC oversees over 106 SOEs as the controlling shareholder. ● Shareholder metric for SASAC companies is not pure profit, but rather the state's interest, which is broadly defined.
Element	State Control of	● Central Huijin Investment Ltd., also founded

[53] Wu, Mark. "The 'China, Inc.' Challenge to Global Trade Governance." *Harvard International Law Journal*, 2016, http://www.harvardilj.org/wp-content/uploads/HLI210_crop.pdf.

2	Financial Institutions: Central Huijin and Other Vehicles	in 2003, acts as the controlling shareholder for China's banks, especially the big four: Bank of China, the Industrial and Commercial Bank of China, China Construction Bank, and the Agricultural Bank of China. ● Central Huijin allows banks to compete against each other to stay market competitive, but also retains ultimate control. ● China's sovereign wealth fund, the China Investment Corporation, manages the Central Huijin, and further control is exerted via SASAC's use of holding companies.
Element 3	State Control over Planning & Inputs: NDRC	● The National Development and Reform Commission (NDRC), which oversees the creation of China's Five Year Plan, has broad power to affect market supply, market capacity and state investment allocation. ● NDRC also sets utility pricing and approves infrastructure investment. ● NDRC reports independently to the State Council, often dubbed China's "super-ministry."
Element 4	Chinese-Style Corporate Groups & Affiliated Networks	● Beyond central authority structures (Central Huijin, SASAC, etc.), Chinese state-owned networks are vertically integrated yet horizontally connected. ● Salient concepts here include "network hierarchy" (subservient to Central Huijin) and "institutional bridging" (connected companies, universities and state bodies). ● Structure allows the State to redirect resources as needed in a facile manner and retain control over market forces.
Element	Communist Party	● Chinese Communist Party (CCP) maintains

5	Involvement and Control	control over the State, but both the Party and the State's mechanisms can be used to advance each other's ends. ● The Party's Central Organization Department appoints all positions within the state including leadership of SASAC, Central Huijin and SOEs. ● Private corporations must form a Party committee, allowing the Party greater insight and control over private enterprises. ● Party deeply entrenched in business interests with broad control levers.
Element 6	The Intertwined Nature of Private Enterprises and the Party-State	● Blurred boundary between State and private ownership in contemporary China - the State is also often a shareholder. ● Entrepreneurs actively forge links with the Party-State.

Table 12: Unique Elements of the Chinese State

Uniquely, China effectively blurs the line between public and private enterprise, government and business. Entities such as the Central Huijin, SASAC and other control mechanisms, such as the Party as a corporate shareholder, ensure that the Party is able to advance its agenda, when desired, and let the free market impact price and demand, when desired. The structural nature of the Chinese economy, bolstered by sui generis government control mechanisms, have created greater problems for China's trading partners; the WTO's oversight and governing rules are insufficient to rein in China's market distorting behavior. The manipulation of the Chinese domestic economy, specifically the Party's interventionist policies that offer substantial government guidance, subsidies and regulatory support to Chinese industries, and the subsequent effects on trade and foreign market access that a state-led economy creates are outside the WTO jurisdiction. Thus, the main international governing body for dealing with these kinds of international trade disputes has been essentially rendered null and void by the rise of the "China, Inc." uniquely state-run economy.

4.3 A Discussion on Techno-nationalism

Some of the policies explored below, such as restrictions on ownership limits for foreign enterprises in China, seem unnecessarily and unfair to non-Chinese companies. It is helpful to view such policies, as well as the alleged IP theft and acquisition of

sensitive technological R&D globally, via the lens of Chinese techno-nationalism. What is Chinese techno-nationalism? Summarily, Chinese techno-nationalism is the Chinese own notion that China's indigenous innovation, mastery, leadership and even dominance in strategic technologies, such as AI, Quantum Computing or even Cloud, is essential to China's future strategic interest and, in some ways, an element of the destiny of China's rise.

This concept manifests itself heavily in the area of policy, where China's strategic interests in terms of technological dominance have deep roots in China's policy landscape.[54] Evidence of Chinese techno-nationalism can be found especially in the China 2025 plan. Formulated in 2015 by the Ministry of Information and Information Technology, the Made in China 2025 plan pushes for leadership in robotics, artificial intelligence, information technology, clean energy, and other key energy sectors.[55] According to some, the ultimate aim of the China 2025 plan, via the careful crafting of state policies, is to exclude foreign firms and technologies from the Chinese marketplace. This not only helps grow the Chinese domestic economy, but allows for the rise of technological national champions, who can go on to be central figures in the global technological economy, akin to the likes of Microsoft internationally. Moreover, this reduces any dependencies on foreign technology, which China views as a strategic threat to its national sovereignty. In other words, China cannot grow its domestic technology capabilities without, in a sense, knocking out foreign players early, if possible, or at least eventually - there is only so much market share. Thus, foreign businesspeople view the Chinese effort to make domestic technology companies self-sufficient as creating an unfair playing field in the Chinese market, with favor heavily tilting towards domestic Chinese firms via favorable government policies.

China 2025 and techno-nationalism play into China's long-standing worldview. Dating back to the 1950s, China views 1) technology as a source of national power; 2) the nature of competition with foreigners as a threat to its long-term goals and 3) the subsequent need for indigenous Chinese capability to thrive. While foreign technology transfers via joint venture partnerships were popular before, and also acceptable under WTO guidelines which stipulate the responsibility of developed economies (such as the U.S.) to transfer technology to developing economies (such as China, which is still classified by the WTO as a developing economy), Beijing is increasingly focused on indigenizing technological innovation and capabilities.

---

[54] Feigenbaum, Evan A. "The Deep Roots and Long Branches of Chinese Technonationalism." *Carnegie Endowment for International Peace*, 2017, carnegieendowment.org/2017/08/12/deep-roots-and-long-branches-of-chinese-technonationalism-pub-72815.

[55] Erdenebileg , Zolzaya, and Weining Hu. "Made in China 2025: Implications for Foreign Businesses." *China Briefing News*, 24 Oct. 2018, www.china-briefing.com/news/made-in-china-2025-implications-for-foreign-businesses/.

4.4 America to China: Policy Background

China's regulatory approach to the development of cloud computing presents significant challenges for foreign companies. The Chinese State has implemented an aggressive policy regime that not only has sought to rapidly develop key technologies, such as cloud computing, but also has given the State ultimate authority in terms of access and control. Moreover, Chinese policies have notably created a situation that many deem equivalent to unfair market access to foreign players. Political and economic national cyber security concerns, especially regarding maintaining stability through economic and political control, factor in heavily to the State's policy making processes and motivations. Table 13 below details the policy motivations stemming from the national cybersecurity concern from Khetri (2016), as discussed above.

National Cybersecurity Concern: Category	National Cybersecurity Concern: Type	Relevant Country Policies
Political Security	Political Stability	China
Economic Security	Economic Stability	China

Table 13: National Cybersecurity Concern Policy Motivations in China

Early policies based on government sponsorship will be examined, as well as the Telecom Law. In addition, the 2012 NPC Standing Committee Decision, the 2015 National Security Law, and, arguably most importantly, the 2017 Cybersecurity Law will be analyzed. From the exploration of these policies, one can see a that the Chinese government, as opposed especially to the U.S. government, takes an activist and interventionist stance towards key technology development, and has embarked on implementing a techno-nationalist regime, aimed at limiting foreign market access and maximizing the potential for indigenous innovation. Interestingly, as opposed to the West, little regulation regarding consumer data privacy has been passed. Rather, most data-related regulation involves ensuring government access to a variety of data and restricting the flow of data, containing it within China's borders, in line with the China "Internet sovereignty" concept.

4.41 2006 - 2012: Early Policies & Initiatives

China officialized the importance of national cloud computing development in the 12th Five Year Plan (第十二个五年计划), covering 2011-2015, in 2010. However, 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), which supported the creation of an IT infrastructure that later was employed as a foundation for cloud computing technology development.[56] As early as 2010, the State Council and other central government ministries released plans, policies and initiatives aimed at cultivating cloud computing. In late 2010, the State Council released State Council Circular 32: Decisions of State Council on Accelerating the Cultivation and Development of Emerging Strategic Industries (国务院关于加快培育和发展战略性新兴产业的决定国发〔2010〕32号), which extrapolated on the 12th Five Year Plan's strategic IT initiative.[57] Specifically, State Council Circular 32 assigned cloud computing as an a priority sector for next generation IT (新一代信息技术产业重) and outlined detailed goals for 2015 and 2020, cementing its strategic importance in China's economic and technological development. Shortly after in 2010, the National Development & Reform Commission (NDRC) and the Ministry of Industry and Information Technology put forward the Cloud Services Pilot Cities Notification, which outlined the development of five cloud computing pilot cities. The cities were Beijing, Shanghai, Shenzhen in Guangdong province, Hangzhou in Zhejiang province and Wuxi in Jiangsu province.[58] In Beijing, for instance, Baidu utilized cloud storage services for its search functions. Goals, plans and definitions were further formalized in 2012. The Ministry of Industry and Information Technology (MIIT) released the 12th Five Year Plan for the Development of the Software & IT Service Industry, which further clarified cloud computing development goals. The China National Information Security Standards Technical Committee released the Information Security Techniques -- Basic Requirements for Security for Government Department Cloud Computing Service Providers, which proposed security standard for companies providing cloud services to the Chinese government, and the National Development & Reform Commission issued the Establishment of Cloud Computing Guiding Documents Drafting Experts' Committee, which formulated the scope of cloud computing, organized experts, and established a working standards group.[59] These early policies demonstrate how, from the very beginning, the cloud computing industry was jointly developed between government forces, public entities and private corporations in China.

---

[56] Ragland, Leigh Ann, et al. "Red Cloud Rising: Cloud Computing in China."

[57] "国务院关于加快培育和发展战略性新兴产业的决定." *中华人民共和国中央人民政府*, 2010, www.gov.cn/zwgk/2010-10/18/content_1724848.htm.

[58] Bundy, Todd, and Michael Haley. "China's Cloud Cities." *ISEMAG*, 7 June 2016, www.isemag.com/2016/05/chinas-cloud-cities/.

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

4.42 2009 China Telecom Law

Another relevant piece of legislation came earlier in 2009 with the advent of the Telecom Law (中华人民共和国电信条例), which was updated in 2016 to include providers of cloud services.[60] Issued by the Standing Committee of the National People's Congress, the Telecom Law limited foreign direct investment to 49% to basic services and to 50% for value added services in the telecom sector, and only Chinese domestic companies could receive permits with less than 50% foreign ownership for value-added telecom services. As cloud computing technology developed, Chinese authorities included these new information technology applications into existing regulatory frameworks.[61] Thus, the cloud computing sector was similarly regulated by the structure of the 2009 Telecom Law equity caps, evidenced in the 2016 revision of the law. IaaS and PaaS service providers were classified as value added telecom services, forcing companies like Microsoft to partner with local 21Vianet in order to provide Azure's IaaS and PaaS services to Chinese consumers.

4.43 ICP & ISP Licenses

Another relevant policy designed to benefit the Chinese cloud companies and other domestic technology firms included the need to obtain Internet Content Provider (ICP) & Internet Service Provider (ISP) licenses. Both ICP and ISP licenses are issued by the Ministry of Industry and Information Technology. An ICP License is required for any company providing content or services over the Internet. For instance, a data center in China would be required to have an ICP license in order to operate locally. An ISP License is required for value-added telecommunications businesses and, in the past, was limited to China's major carriers such as China Unicom and China Telecom.[62] Both licenses necessitate a Chinese domestic entity as the named licensee, which can be subject to equity caps, as mentioned above via the 2009 Telecom Law. Both practices can be seen as limiting foreign competitiveness in order to grow the Chinese domestic information technology industry.

---

[60] "中华人民共和国电信条例." *中华人民共和国工业和信息化部*, 2016, www.miit.gov.cn/n1146295/n1146557/n1146619/c4860613/content.html.

[61] "China's Cloud Computing Policies and Implications for Foreign Industry ." *United States Information Technology Office*.

[62] Ibid.

4.44 2012 Decision of the Standing Committee of the National People's Congress on Strengthening Information Protection on Networks

Up until 2012, issues regarding data access and control did not factor heavily into Chinese policy making decisions regarding IT regulation. According to Sun Ping, professor of law at Shanghai Jiaotong University, the turning point occurred in 2012 with the introduction of the Decision of the Standing Committee of the National People's Congress on Strengthening Information Protection on Networks (全国人大常委会关于加强网络信息保护的决定) by the National People's Congress Standing Committee.[63] The Decision formalized that the unregulated flow of data was now an issue of paramount national security, and the policy introduced measures by which the Chinese government could control data, but also introduced some basic data protection rights for consumers. For instance, the Decision implemented fundamental user data protection, guaranteeing that data cannot be illegally sold or provided.

> The state protects electronic information by which individual citizens can be identified and which involves the individual privacy of citizens. All organizations and individuals may not obtain electronic personal information of citizens by theft or any other illegal means and may not sell or illegally provide others with electronic personal information of citizens.[64]
>
> 国家保护能够识别公民个人身份和涉及公民个人隐私的电子信息。任何组织和个人不得窃取或者以其他非法方式获取公民个人电子信息，不得出售或者非法向他人提供公民个人电子信息。[65]

While this language seems positive for user data protection, and, indeed, does provide a basic framework for illegal use protecting user data, the law also ensures the Party's control over cyberspace. The law was likely implemented after a fight between two Internet giants in China, Tencent and Qihoo360, where a war for market share involved a potential infringement on customer rights in 2010. Tencent stopped service to QQ users, a Tencent chat product, who had a Qihoo360 antivirus product on their computer, forcing users to choose between the two companies' service offerings.[66] After that, the

---

[63] Sun, Ping. "Interview with Sun Ping." 15 Nov. 2018.

[64] " Decision of the Standing Committee of the National People's Congress on Strengthening Information Protection on Networks [Effective] 全国人大常委会关于加强网络信息保护的决定 [现行有效]." *Peking University Center for Legal Information* , 2012, en.pkulaw.cn/display.aspx?cgid=191975&lib=law.

[65]"全国人大常委会关于加强网络信息保护的决定." *中华人民共和国中央人民政府*, 2012, www.gov.cn/jrzg/2012-12/28/content_2301231.htm.

[66] Ye, Juliet. "QQ-360 Battle Escalates into War." *The Wall Street Journal*, Dow Jones & Company, 5 Nov. 2010, blogs.wsj.com/chinarealtime/2010/11/05/qq-360-battle-escalates-into-war/.

Chinese government began to issue policy about user data protection, albeit in a qualified manner, with the State still very much in control over data flow and oversight.

4.45 2015 National Security Law

In mid-2015, China's legislature launched a new national security law, entitled the National Security Law of the People's Republic of China (中华人民共和国国家安全法). Though the new law proved to be the most comprehensive national security legislation in modern China, the notion of national security is, potentially by design, inherently vague in the law. National security, ostensibly, includes threats to China including food security, religious security, border security and, importantly, cybersecurity.[67] Like many laws in China, the law provides a framework for safeguarding China's interests; however, how the actual law would be actually implemented remained unclear at the time of ratification. Like most legislation in China, there is a gap between the actual law and its implementation.

The law calls for greater protection of the security of Chinese cyberspace. Article 25, in particular, discusses the necessity to establish a safeguarded network system, with goals including "elevating the capability to protect network and information security," "achieving the security and controllability of core network and information techniques, key infrastructure, information systems in important fields and data," "preventing and punishing unlawful and criminal activity on networks," and "maintaining cyberspace sovereignty, security, and the development interests of the State."[68]

Additionally, of note, the national security law also calls for China to accelerate the development of "autonomous and controllable" key technologies in areas of strategic import. Specifically, Article 24 states that China should "strengthen its capability to keep technical secrets confidential, and to safeguard the security of important technologies and projects."[69] The emphasis on indigenous innovation relates back to the techno-nationalism discussion earlier, where China views technological power as focal to its national security and national power interests.

In many ways, the 2015 national security law laid the foundational framework for the 2017 cybersecurity law, which built on the notion of Chinese cyber sovereignty, coupled with the emphasis on "autonomous and controllable" strategically important technology networks.

---

[67] Boehler, Patrick. "What You Need to Know About China's New National Security Law." *The New York Times*, The New York Times, 1 July 2015, sinosphere.blogs.nytimes.com/2015/07/01/what-you-need-to-know-about-chinas-new-national-security-law/?mtrref=undefined&gwh=BE1B95C6C87990A5A04494F949EEA45A&gwt=pay.

[68] "China Enacts New National Security Law." *Covington*, 2015, www.cov.com/~/media/files/corporate/publications/2015/06/china_passes_new_national_security_law.pdf.

[69] Ibid

4.46 2017 Cybersecurity Law

In 2017, China issued a new cybersecurity law with vast implications for foreign-owned U.S. businesses in the technology, data storage and software businesses, with noted implications for network operators that engage in data management. The Cybersecurity Law (中华人民共和国网络安全法) was adopted by the National People's Congress (NPC) in 2016 following a year of legislative proceedings and was officially effective June 1st, 2017.[70] The new law effectively restricted the sales of foreign information and communication technology (ICT). The law also required foreign firms operating in China to store their China user data in China. The data cannot be transferred outside of China without government approval and foreign companies must submit ICT for government review.

Containing 79 articles within seven chapters, the Cybersecurity Law details numerous new cybersecurity requirements: protection of critical information infrastructure, safeguards for Chinese national cyberspace sovereignty, and stipulations on data protection, access and privacy. In terms of national sovereignty, that law builds on a notion first introduced in a 2010 government white paper that stated the domestic Internet in China is under Chinese control.[71] The law can be viewed through two lenses. First, the law is an attempt to bring Chinese law up to date with global cybersecurity best practices and norms, serving as the fundamental or basic law in the cybersecurity field, including mandating data safeguards and stipulating data storage requirements, in one comprehensive piece of legislation. On the other hand, the law can be understood as a continued effort by the Party to control content and data on the Internet, giving the Party greater access to all data within China through spot-checks and certifications. Notably, the law requires that all data generated or collected in China must be stored in China, which has implications for multinational technology companies who previously stored Chinese data in their international data centers located outside of China. According to KMPG's *Overview of China's Cybersecurity Law*, the Cybersecurity Law contains six key elements that have important implications for enterprises in China, as shown in Table 14.

Cybersecurity Law Highlights	Details
Protection of Personal Information	● Clear requirements for personal information data collection, use and protection.

[70] "Overview of China's Cybersecurity Law." *KPMG China*, 2017, https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf.

[71] Wagner, Jack. "China's Cybersecurity Law: What You Need to Know." *The Diplomat*, The Diplomat, 1 June 2017, thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/.

Notion of “Critical Information Infrastructure”	• Critical Information Infrastructure (CII) Operators security and protection requirements detailed. • Scope of what constitutes a Critical Information Infrastructure (CII) Operator not clearly defined - open to interpretation.
Definition of Network Operators	• Definition of what constitutes a network operator and their responsibilities are delineated.
Preservation of Sensitive Information	• Personal data, characterized as sensitive information, collected or generated in China must be stored in China.
Certification of Security Products	• Critical network equipment, products and services must be certified by a national security review.
Explanation to Legal Liabilities	• Network operators, CII operators and sellers of network products and services may face penalties if they violate certain articles of the Cybersecurity Law. • Violation fine can be up to RMB 1,000,000.

Table 14: Key Highlights from China’s 2017 Cybersecurity Law

The law draws the distinction between “network operators” and “Critical Information Infrastructure (CII) Operators.” Network operators are defined as any system or equipment that gathers, stores, transmits, exchanges or processes data. CII operators refer to enterprises in communications, information services, energy, transportation, water, financial services, and electronic services. Cloud computing operators, therefore, would likely be classified as a CII operator, under the umbrella of information services. However, CII operators are not explicitly defined in the law and this important issue remains open to interpretation. The government has stated that relevant ministries will follow-up with more concrete definitions.

The Cybersecurity Law requires network operators to comply with best practices in cybersecurity management, as well as requiring network operators in critical sectors to store data in China. Under the new law, network operators must allow full access of their data to authorities, as well as submit to mandatory equipment testing and certification. Additionally, network operators are required to adopt a variety of best-in-practice security measures, via Article 21, such as the implementation of network

security protections, data classification, encryption and security management systems. Article 37 requires network operators in critical industries to store data generated and collected in China domestically. The data may not be transferred abroad without explicit government permission. Article 37 provides as follows:

> Personal information and important data collected and generated by critical information infrastructure operators in the PRC must be stored domestically. For information and data that is transferred overseas due to business requirements, a security assessment will be conducted in accordance with measures jointly defined by China's cyberspace administration bodies and the relevant departments under the State Council. Related provisions of other laws and administrative regulations shall apply.[72]
>
> 关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。[73]

The new law brings about a variety of business and data security risks for foreign companies in China. As the U.S. chamber of commerce pointed out, foreign companies are forced to localize a valuable set of data in China, which can result in huge cost. More than 50 U.S., Japanese and European business lodged complaints, penning a letter to Premier Li Keqiang stating that the law impeded foreign entry and innovation in China.[74] Pundits pointed to the fact that the law adds another layer of regulation in China in the Internet and technology sectors, which are already heavily controlled, further preventing, potentially, the ability of foreign businesses in China to be efficient and remain market competitive. Furthermore, the data may not be secured - with opaque government access, data may be misappropriated or misused. The discussion that follows and Figure 7 details the necessary steps that U.S. companies must comply with in order to be legally compliant to do business in China.

American companies have responded in a variety of ways, and their reactions will be examined in greater detail in the next sections. Responses ranged from Apple announcing the creation of a new data center in Guizhou, China, to Amazon selling its

---

[72] "Overview of China's Cybersecurity Law." *KPMG China*.

[73] "中华人民共和国网络安全法." *度小法-百度智能法律产品*, 2017, duxiaofa.baidu.com/detail?searchType=statute&from=aladdin_28231&originquery=%E7%BD%91%E7%BB%9C%E5%AE%89%E5%85%A8%E6%B3%95&count=79&cid=f66f830e45c0490d589f1de2fe05e942_law.

[74] Wagner, Jack. "China's Cybersecurity Law: What You Need to Know."

public cloud computing unit to its local Chinese partner, Beijing Sinnet Technology Co Ltd., for 2 billion RMB in November 2017.[7576]

In February 2018, as a result of the 2017 cybersecurity law, Apple officially transferred its China iCloud operations and encryption keys to its local partner, Guizhou Big Cloud Data, in Southern China.[77] Interestingly, Guizhou Big Cloud Data corporate governance structure includes a board primarily run by government-owned businesses.[78] The ties to the Chinese government and the CCP are numerous, leading to the question: was Apple effectively forced to turn over its data management operations to the Chinese government in order to stay in the China market? The answer, more likely than not, is yes.

Amazon has long struggled in China; however, after the implementation of the Cybersecurity Law in 2017, Amazon decided to sell its Amazon Web Services (AWS) public cloud computing unit to its Chinese partner, Beijing Sinnet Technology Co. Ltd in November 2017 for 2 billion RMB. Though AWS technically still owns the intellectual property behind its services, Amazon sold the physical infrastructure and the business management to Sinnet. Amazon cited the Cybersecurity Law as the reason for the sale, hoping to better comply with Chinese law. Indeed, many experts in the field agreed that the move was mainly motivated by the need for regulatory compliance.[79] However, during a 2018 Bloomberg report on Supermicro, it came to light that Amazon, who long struggled in the China cloud market, was looking to offload its China business given a potential security compromise on its servers.[80] The new legislation provided the perfect opportunity to "exit" the market in a strategic and PR-friendly manner. Allegedly, Amazon launched an internal investigation into its SuperMicro-built servers in the AWS Beijing facilities and discovered motherboards altered with malicious chips.[81] One source at Amazon cited the sales as "hacking off a diseased limb."[82] Though, after the report came to light, Amazon vehemently refuted the claims publicly. However, the possibility of a potential hardware compromise, compounded by mediocre performance

---

[75] "Establishing a Data Center in China." *China Briefing News*, 28 Nov. 2018, www.china-briefing.com/news/setting-shop-guide-chinas-data-centers/.

[76] Cadell, Cate. "Amazon Sells off China Cloud Assets as Tough New Rules Bite." *Reuters*, Thomson Reuters, 14 Nov. 2017, www.reuters.com/article/us-china-amazon-cloud/amazon-sells-off-china-cloud-assets-as-tough-new-rules-bite-idUSKBN1DE0CL.

[77] Liao, Shannon. "Apple Officially Moves Its Chinese ICloud Operations and Encryption Keys to China." *The Verge*, The Verge, 28 Feb. 2018, www.theverge.com/2018/2/28/17055088/apple-chinese-icloud-accounts-government-privacy-speed.

[78] "Introduction to Guizhou-Cloud Big Data Industry Co., Ltd." *Guizhou-Cloud Big Data*, english.gzdata.com.cn/c101/index.html.

[79] Cadell, "Amazon Sells off China Cloud Assets as Tough New Rules Bite."

[80] Robertson, Jordan, and Michael Riley. "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies." *Bloomberg.com*, Bloomberg, 2018, www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies.

[81] Russell, Jon. "Amazon Reportedly Offloaded Its Chinese Server Business Because It Was Compromised." *TechCrunch*, TechCrunch, 4 Oct. 2018, techcrunch.com/2018/10/04/amazon-aws-china-server-business/.

[82] Ibid

given inadequate localization, entrenched competitors such as Alicloud. An increasingly hostile to foreign business Internet regulatory regime provided the perfect storm of reasons for Amazon to sell its hardware to Sinnet.

The 2017 Cybersecurity Law effectively made the required steps for U.S. companies to do business in China quite complex. The required steps, summarily, for U.S. cloud computing operators are: 1) pass national security reviews for technology and services; 2) store all data physically in China; 3) form a joint venture partnership to open a data center; 4) obtain government approval for data transfers; and 5) buy government approved encryption and virtual private networks (VPNs). The sequence is detailed in Figure 7.

Figure 7: Required Steps for Data/Software U.S. Businesses in China as of 2017[83]

All in all, and without a doubt, the policy should be viewed as clearly techno-nationalist, encouraging the dominance of domestic players in the marketplace, while disincentivizing foreign players through onerous and costly hoops, including expensive compliance mechanisms, in order to succeed in the China market. The 2017 Cybersecurity Law has proven to be one of the most profound pieces of legislation with vast financial and market share implications for the foreign business community in China.

[83]"Foreign Economic Espionage in Cyberspace." *NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER*.

4.5 America to China: Cloud Computing Case Study: Microsoft

Microsoft entered the China market in 1992, establishing an office in Beijing.[84] As with most foreign companies in China, Microsoft engaged a variety of local partners to innovate and localize Microsoft technologies to the Chinese consumer. Microsoft is notable in terms of American companies operating in China - unlike Facebook and Google, Microsoft has never been blocked by Chinese authorities (though, Microsoft was primarily hardware and operating systems, not an information-sensitive platform for much of its history).[85] Back in 2007, Bill Gates predicted that China would be Microsoft's largest market revenue-wise. As of 2016, the prediction has yet to materialize, with an estimation that China contributes less than 10% to Microsoft's overall revenues.[86]

For cloud computing offerings, Microsoft formed a partnership with 21Vianet, a Chinese data center that is registered in the Cayman Islands. Microsoft, in the early 2010s, partnered with 21Vianet to offer a variety of cloud computing services to Chinese users, officially launching in June 2013 and including 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.[87] Specifically, in 2012, Microsoft partnered with the Shanghai Municipal government and 21Vianet to offer cloud computing services in the New Pudong area of Shanghai, leveraging 21Vianet's local data center in Shanghai.[88]According to Microsoft's website, Microsoft achieved regulatory compliance in China through its partnership with 21Vianet:

> Microsoft Azure is the first foreign public cloud service provider offered in China in compliance with government regulations. Microsoft meets those requirements by authorizing 21Vianet to operate a public cloud business in mainland China.[89]

Microsoft licensed its technology to 21Vianet to comply with the Telecom Regulation, discussed earlier, where IaaS and PaaS services must have value-added telecom permits, which are only available to domestic Chinese companies (or locally registered companies with less than 50 percent foreign owned investment). Moreover, Microsoft, on its Azure operations in China website, lists the reasons why Microsoft Azure in China has an advantage over other foreign public cloud service providers in China. Advantages include a well-experienced global operation model, trusted cloud services

---

[84] "About Microsoft's Presence in China." *Microsoft*, news.microsoft.com/about-microsofts-presence-in-china/.

[85] "Microsoft in China: 20 Years of Playing By The Rules." *Sampi.co*, 2016, sampi.co/microsoft-in-china-20-years/.

[86] Ibid.

[87] Ragland, Leigh Ann, et al. "Red Cloud Rising: Cloud Computing in China."

[88] Jones, Penny. "21Vianet Teams with Microsoft for Shanghai-Based Cloud Offering." *DCD*, 22 Nov. 2012, www.datacenterdynamics.com/news/21vianet-teams-with-microsoft-for-shanghai-based-cloud-offering/.

[89] "Azure Operations in China vs. Global Azure." *Microsoft Docs*, docs.microsoft.com/en-us/azure/china/china-overview-operations.

with full compliance with the requirements of the Chinese government, world-class data privacy, advanced intelligent cloud solutions, and hybrid cloud options.[90] However, the world-class data privacy is certainly brought into question by Microsoft's partnership with 21Vianet. The Microsoft Azure China site details its arrangements with 21Vianet:

> Microsoft Azure operated by 21Vianet (Azure China 21Vianet) is a physically separated instance of cloud services located in mainland China, independently operated and transacted by Shanghai Blue Cloud Technology Co., Ltd. ("21Vianet"), a wholly owned subsidiary of Beijing 21Vianet Broadband Data Center Co., Ltd. The services are based on the same Azure, Office 365, and Power BI technologies that make up the Microsoft global cloud service with comparable service levels. Agreements and contracts, where applicable, are signed between customers and 21Vianet, given that 21Vianet is the official legal entity for Microsoft Azure.[91]

The Azure cloud services in China are wholly operated by 21Vianet and represent a physically separate entity, infrastructure and network. Given China's data regulations, especially the data audits and access required by the Chinese government, it is unlikely that the data services provided by Azure in China is as secure as it is in the U.S. Sensitive data stored in China in the Azure 21Vianet network may very well be compromised, especially in terms of confidentiality, integrity and possession/control, potentially provided to the Chinese government or malicious actors without user consent or knowledge.

Moreover, and this applies to all cloud service providers in China, the Microsoft 21Vianet-Partnership has potential implications and risks for Azure users in China, stemming from the risks posed by the Chinese government rather than technical risks. Since Article 11 of Chapter 2 of the State Security Law of the People's Republic of China allows 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."[92] The Chinese government, thus, can ostensibly demand any information at any time under 21Vianet's control, potentially leading to compromised information and communications for global enterprises and consumers. There may also be implications for Azure users outside of China, where their information security could be put at risk by the 21Vianet partnership and network.

Many of Microsoft's cloud customers in China are multinational companies, such as Adobe, Coke, Costco, P&G, and Toyota, who may already employ Azure in their

---

[90] Ibid.
[91] Ibid.
[92] Ragland, Leigh Ann, et al. "Red Cloud Rising: Cloud Computing in China."

international cloud strategy.[93] In this sense, Microsoft has been largely limited to multinational corporations, with only such an effective strategy at penetrating the local market, who prefer domestic services such as Alicloud or Tencent Cloud.

Looking at Microsoft Azure's market share, one can discern a definite trend downwards over time. In 2016, Microsoft Azure was estimated to have 6.2% of the Chinese IaaS market.[94] However, in 2017, Azure all but disappeared from the top of the China IaaS revenue list. This was likely caused in large part by the 2017 Cybersecurity Law, the increasing preference of Chinese enterprises towards Chinese-made technology, and fierce competition from domestic competitors such as Alibaba.

4.6 America to China: Analysis

Using an updated Parkerian Hexad, one can conclude that although the information security elements ranks relatively high, there are still issues regarding the local partnership with 21Vianet for Microsoft Azure, as shown in Table 15. Elements of the Parkerian Hexad for Chinese consumer perceptions of Microsoft Azure in China are ranked 1-5, with 1 being the lowest (or least secure) and 5 being the highest (or most secure). Explanations for the ranking are provided in the rightmost column. Most of the information security issues stem not from technical risks, but rather from the risks posed by the Chinese government. There are serious consumer risks for Microsoft Azure in China, especially in terms of confidentiality, possession/control, integrity and jurisdiction. However, Microsoft's global standards, which inform its partnership 21Vianet, help bolster the information security for authenticity, availability and utility.

Updated Parkerian Hexad Element	**Consumer Information Security: American Cloud Computing Operators in China, Microsoft Azure (1-5)**	**Details**
Confidentiality	2	The requirement to provide data to the Chinese government in a non-transparent manner poses a serious risk to consumer

[93] Lardinois, Frederic. "Microsoft Launches Two New Azure Regions in China." *TechCrunch*, TechCrunch, 27 June 2018, techcrunch.com/2018/06/27/microsoft-launches-two-new-azure-regions-in-china/.

[94] "IDC发布，中国公有云市场份额排名！." *搜狐网*, 19 May 2017, www.sohu.com/a/141983144_258957.

		confidentiality.
Possession/Control	2	Non-transparent auditing of data by the Chinese government potentially compromises user possession/control.
Integrity	3	Information may be scrubbed or altered if deemed malicious to the Chinese state, though not entirely likely.
Authenticity	4	Information creation and origin likely authentic, given Microsoft global standards.
Availability	4	The partnership with 21Vianet conforms to Microsoft's global standards - information should likely be readily available, though maybe not to the extent of information stored on Microsoft's own network.
Utility	4	Information likely readily available and useful in form, given Microsoft's global standards.
Jurisdiction	2	Local laws do not allow for access to untampered information; Chinese government hand omni-present and non-transparent.

Table 15: The Updated Parkerian Hexad: Chinese Consumer Risks for Microsoft Azure in China

To note, many of the risks and low marks in the Parkerian Hexad will also be applicable to other Chinese cloud operators in China, both domestic and foreign, given the Chinese government's regulations on providing access to data and technology.

The main issue from Microsoft Azure in China, though, is not technical information security risks inasmuch as policy barriers that have enabled robust domestic competition. Using Porter's 5 Forces, one can see that the competitive rivalry of competitors such as Tencent and Alibaba, enabled by government support and adroit localized leadership, combined with a policy regime that favors local players, have severely hampered Azure's competitiveness in China. This is shown below in Table 16. Porter's 5 forces are ranked 1 to 5, with 5 posing the highest threat and 1 posing the

lowest. Competitive rivalry and threat of substitution, here, have proven significant as factors that have diminished Azure's China market share, compounded especially by the Chinese consumers tendency towards nationalistic technology service selection and fierce domestic competition that is optimized to the local market.

Force	Microsoft Azure in the Chinese Market (1-5)	Details
Competitive Rivalry	5	Azure's main weakness in China is the strength of its rivals, such as Alibaba and Tencent, who can leverage their existing customer base and strong localized models and protective policies.
Supplier Power	2	Since Microsoft supplies much of its cloud infrastructure, supplier power is low, though 21Vianet may be subject to supplier power.
Buyer Power	3	Buyer power is stronger than supplier power; however, the vast number of buyers in China render the number lower.
Threat of Substitution	4	Threat of substitution is high - people can easily substitute out Azure offerings for other products, services or companies, unless it is a unique product/service.
Threat of New Entry	2	Given the economies of scale and the initial investment involved in cloud computing, threat of new entry is unlikely.

Table 16: Porter 5 Forces for Microsoft Azure in China

One can understand the low performance of Azure of China, thusly, as a combined result of policy that puts Azure at a disadvantage compared to its local competitors and the entrenched strength of such competitors, who are able to leverage existing customer bases (in a platform strategy), tap into economies of scale, and leverage good relationships with government entities. Moreover, it seems that Chinese consumers prefer to consume Chinese goods and services, potentially out of a sense of

nationalist pride, hoping to support the growth of local champions. In China, we can see observe that the strong hand of the government actually results in a situation where policy forms downstream consumer attitudes, leading to a preference to select local cloud operators such as Alibaba and Tencent. Microsoft Azure may remain in China for years, catering especially to multinational corporations using their services on a global scale, but it will likely never be able to break a certain threshold of market share, limited by policy, local players and consumer preferences.

5. China to America: Cloud Expansion

For Chinese technology companies, especially as they reach key inflection points in terms of their local market saturation, America represents the ultimate prestige market, the epicenter of global innovation and a population with high purchasing power and global consumptive clout. The S&P 500 closed at a record high in 2017, up over $1.5 trillion in value since the start of the calendar year, with 37% of that growth attributed to Apple, Alphabet, Facebook, Amazon and Microsoft. Though in terms of establishing themselves in the U.S, legal issues, here too, remain a significant roadblock for Chinese technology firms, coupled with a bevy of operational problems and managerial decisions. Alicloud, the cloud computing business of the Alibaba group, opened its first data center in the United States in 2015, promising to overtake Amazon's cloud computing business in a period of 3-4 years. Three years later, Alibaba still lags behind, with the vast majority of its revenue coming from its home market, despite providing steep discounts in the U.S. market to attract a larger customer base. American companies, especially concerned about their data privacy (and how best to protect it) in the context of a Chinese cloud company, have been extremely hesitant to adopt the platform. With respect to Chinese companies' international expansion efforts into the American market, products that work well at home often get lost in translation with American consumers. For the China to America cloud expansion analysis, Alibaba’s Alicloud will be used as the primary case study.

5.1 China to America: Context & Background

5.11 A Discussion on Huawei & ZTE: A Helpful Precedent

At this point, a discussion on Huawei Technologies Co. Ltd (Huawei) and their past efforts and troubles regarding American expansion is warranted. The Huawei case helps establish a useful precedent to better understand the lens through which the U.S. government and, by extension, the U.S. business community, views Chinese

technology giants, particularly those whose products involve a critical role in infrastructure safety and national security, on American soil.

To provide a brief background on the company, Huawei was founded in 1987 in Shenzhen, China by Ren Zhengfei, a former deputy director of the People's Liberation Army engineering corp. Ren Zhengfei hoped to reverse engineer foreign technology with local researchers, breaking the dependency Chinese firms had at the time on joint venture partnerships with foreign players.[95] Huawei hit its stride in 1993, launching the C&C08 program controlled telephone switch in China, which began Huawei's dominance in creating telecommunications equipment and consumer electronic products, first in China and then expanding globally. The Chinese government, according to many, was a key catalyst that helped accelerate Huawei's growth. In 1994, the People's Liberation Army granted Huawei the contract to build the first military national telecommunications network, a partnership of noted strategic importance.[96] Furthermore, in 1996, the Beijing government announced a policy in support of domestic telecommunications manufacturing, effectively boosting Huawei to the status of "national champion" and limiting access to foreign competition. Today, Huawei operates in more than 170 countries and reported a 2017 revenue of $92.55 billion.[97]

Counterintelligence efforts against Huawei began by U.S. agencies as early as 2010; however, in 2012, the U.S. House of Representatives Permanent Select Committee on Intelligence released the authoritative *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*.[9899] Authored by Chairman Mike Rogers and Representative Dutch Ruppersberger, this seminal report involved a comprehensive investigation into the counterintelligence and security threats posed by virtue of the U.S. operations of Huawei and ZTE, the largest Chinese telecommunications companies. Specifically, the committee wanted to better ascertain how companies like Huawei and ZTE are influenced by the Chinese state, what is the relationship between the Chinese state and Chinese telecommunications companies in terms of corporate governance, and what is the connection between Chinese intelligence services and Chinese telecommunications companies, especially in terms of cyber-espionage? To evaluate the potential threats to

---

[95] Garsd, Jasmine. "The History Of Tech Giant Huawei And The Chinese Government." *NPR*, NPR, 7 Dec. 2018, www.npr.org/2018/12/07/674467994/huawei-and-the-chinese-government.

[96] Gilley, Bruce (28 December 2000). "Huawei's Fixed Line to Beijing". Far Eastern Economic Review: 94--98.

[97] "Huawei's 2017 Annual Report: Solid Performance and Lasting Value for Customers - Huawei Press Center." *Huawei*, 30 Mar. 2018, www.huawei.com/en/press-events/news/2018/3/Huawei-2017-Annual-Report.

[98] Goldstein, Matthew, et al. "How a National Security Investigation of Huawei Set Off an International Incident." *The New York Times*, The New York Times, 14 Dec. 2018, www.nytimes.com/2018/12/14/business/huawei-meng-hsbc-canada.html.

[99] "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE." *U.S. House of Representatives*, 2012, intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf.

U.S. security interests, the investigation involved: 1) a review of open-source corporate information including histories, financials and corporate governance structures and 2) a review of classified information via the U.S. intelligence community.

During the course of the investigation, it came to light that Huawei was likely in violation of United States law. Through conducting interviews with numerous former and current Huawei employees, multiple, credible reports cited frequent instances of the following unethical and illegal corporate behavior: 1) immigration violations; 2) bribery and corruption; 3) discriminatory behavior; and 4) copyright infringement. To note, some of these practices may be considered more commonplace in China, given its unique development of its view of the rule of law and informal institutions dictating business practices.

The committee also explored Chinese government motivations for explorations and the various controls in place to leverage telecommunications companies for malicious purposes. China not only has the technological capabilities to access data worldwide, via hacking, insertion of malicious hardware or software implants, but also has the political motivation to do so. By accessing valuable global information, China is able to spur its economic development and hasten its rise on the world stage: “The capacity to maliciously modify or steal information from government and corporate entities provides China access to expensive and time-consuming research and development that advances China’s economic place in the world.”[100] Malicious Chinese hardware and software implants, functioning as a tool for espionage, allow access to corporate American trade secrets, advanced R&D data and even litigation positions that the Chinese state could use in economic and diplomatic arenas. This has proven to be an issue in the past and remains a threat in the future. Moreover, Chinese companies have little ability to refuse Beijing’s requests/instructions. China can cite State security laws to force corporate cooperation. In other words, the Chinese government could request to add a malicious implant into a Huawei or ZTE component, functioning as a back-door to access critical or sensitive information, and the company would have little bargaining or agency to refuse such a request. The committee also finds that even if executive leadership were to refuse such a request, all Chinese intelligence services would need would be the compliance of a working-level technician or manager in order to engage in hardware tampering.

Unfortunately, a noted theme throughout the report is the unwillingness of Huawei to provide clear and comprehensive answers to the U.S. inquiries. Overall, Huawei was deemed uncooperative, evasive and even non-responsive in the investigation by Congress, casting doubt on Huawei’s ability to abide by international rules. Especially in terms of its formal relationship or regulatory interaction with Chinese authorities, both companies were non-forthcoming and unwilling to provide detailed responses, at times citing a potential violation of China’s state-secret laws and related

[100] Ibid.

criminal liability. In particular, Huawei failed to provide “information about its corporate structure, history, ownership, operations, financial arrangements and management.”[101] Below, Table 17 details the 5 key recommendations and implementation details from the U.S. Investigative Report.

Recommendation Number	High-Level Content	Additional Details
Recommendation 1	The U.S. should view Chinese telecommunications companies with suspicion.	● U.S. Intelligence community should remain wary ● Committee of Foreign Investment in the United States (CFIUS) should block all acquisitions, mergers and takeovers involving Huawei and ZTE ● U.S. government systems should not include Huawei or ZTE parts
Recommendation 2	U.S. private sector actors are encouraged to not use Chinese telecommunications companies.	● Huawei and ZTE cannot be trusted to be free of Chinese state influence and pose a security threat to domestic actors
Recommendation 3	U.S. Congress should investigate unfair trade practices in the Chinese telecommunications sector.	● Congress should investigate China’s financial support for key companies
Recommendation 4	Chinese companies should become more open, transparent and compliant.	● Chinese companies should list on Western stock exchanges, given the advanced transparency requirements. ● Chinese companies should be subject to independent third-party review

[101] Ibid.

		• Chinese companies must comply with U.S. legal standards of information and intellectual property protection
Recommendation 5	U.S. Congress should consider legislation around state-influenced telecommunications companies.	• U.S. Congress should introduce legislation to better mitigate risk from state-influenced telecommunications companies. • Legislation can include increased information sharing and expanded CFIUS oversight and control.

Table 17: Summary of Recommendations from Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE

Key takeaways from the U.S. House Report are numerous and manifold. First, the report explicitly lays out the suspicion that critical infrastructure operators, such as Chinese telecommunications companies, have explicit links to the Chinese government, both in terms of the military and intelligence services. Such ties could potentially result in (or have potentially resulted in) espionage, spying and even potential intellectual property theft. Moreover, the companies' reluctance to disclose their specific relationship with the Chinese government and, at times, Huawei and ZTE's evasive responses further heighten the sense of an opaque yet tangible connection. Second, beyond the scope to which Huawei and ZTE are "compromised" by their dealings with the Chinese government from a cybersecurity perspective, the Report also details the various criminal and unethical behavior conducted by the companies, especially Huawei. Compounded by both the companies' reluctance to cooperate with the investigation in a transparent, willing and compliant manner, the results seems to conclude that both Huawei and ZTE do not follow international standards of business behavior and have a tendency towards the illegal and the unethical. Third, the committee investigated the motivations of the Chinese government and Chinese intelligence collection, exploring how Chinese law requires Huawei and ZTE to cooperate with any request made upon them by the Chinese government, often under the guise of state security, concluding that these companies have little agency and bargaining power to refuse even the most sensitive request. Lastly, the Report concludes that the U.S. government should not utilize any Huawei or ZTE equipment in a critical infrastructure capacity, recommends that private enterprises find other suppliers with less potentially compromising nation-state relations and seeks increased investigation and regulatory oversight into these kind of operators by U.S. governmental bodies, such as Congress, the department of Justice and CFIUS.

Huawei has long faced scrutiny in its internationalization efforts, by not just the U.S. but from a variety of global governments. However, the U.S. has remained one of the most vocal critics and alarm raisers. Huawei is effectively banned in the U.S., especially in terms of M&A opportunities and hardware distribution. Security concerns, and, as Head of M16 Alex Younger recently put it, China's legal and ethical framework regarding data use make the adoption of Huawei technologies difficult in the West.[102] For instance, in early 2018, the U.S. Federal Communications Commission (FCC) pressured AT&T to drop its planned deal with Huawei to distribute phones in the U.S., citing security issues, with espionage concerns and Huawei's role in such espionage at the top of the list.[103] Huawei planned on entering the U.S. market even as recently as early 2018, with plans to partner with AT&T to sell its flagship Mate 10.[104] However, the venture was subsequently blocked given political pressure applied by the U.S. government, again, with espionage, spying and national security concerns at the center of the block.[105]

Serious trouble began for ZTE in 2017, when the U.S. government, citing that ZTE had violated sanctions that prevented sales in Iran and North Korea, introduced a massive fine and a subsequent ban forbidding American companies from selling components to ZTE, beginning in April of 2018.[106] Heavily dependent on American-made microchips and the Android operating system, ZTE was effectively forced to shut down operationally until the ban was lifted. The ban was ultimately lifted and ZTE paid a $1 billion penalty. In addition, ZTE had to fire any leadership member who was senior vice president or above and somehow involved in the sanction evasion case. What exactly happened? ZTE shipped a later revealed $32 million of telecommunication equipment to Iran, which included U.S. components, despite the sanctions and without U.S. authorization. To make matters worse, ZTE then lied to U.S. investigators, stating that dealings and shipments to Iran had stopped, which was untrue. Many of the themes mentioned in the 2012 House report are equally applicable in the 2018 ZTE ban, including unethical business behavior, a lack of transparency in terms of operations and an unwillingness to cooperate with U.S. law enforcement processes in an honest and non-deceptive manner.

Sanction evasion issues also plagued Huawei. Meng Wanzhou, Huawei CFO and daughter of founder Ren Zhengfei, was arrested while changing planes in Canada

---

[102] Bond, David. "Head of MI6 Warns of Huawei Security Concerns." *Financial Times*, Financial Times, 3 Dec. 2018, www.ft.com/content/40b35b84-f6ff-11e8-af46-2022a0b02a6c.

[103] Jiang, Sijia. "Huawei's AT&T U.S. Smartphone Deal Collapses." *Reuters*, Thomson Reuters, 9 Jan. 2018, www.reuters.com/article/us-at-t-huawei-tech/huaweis-att-u-s-smartphone-deal-collapses-idUSKBN1EX29E.

[104] Chigne, Jean-Pierre. "Huawei Planning On Entering US Market In February Through AT&T." *Tech Times*, 29 Dec. 2017, www.techtimes.com/articles/217706/20171229/huawei-planning-entering-u-s-market-february-through-t.htm.

[105] Cheng, Roger. "Some of the Hottest Android Phones Aren't Coming to the US..." *CNET*, CNET, 27 Mar. 2018, www.cnet.com/news/why-some-of-the-flashiest-huawei-android-p20-p20-pro-mate-10-pro-phones-arent-in-the-us/

[106] Stolyar, Brenda, and Christian de Looper. "ZTE Resumes Business Once Again as U.S. Lifts Ban on Suppliers." *Digital Trends*, Digital Trends, 13 July 2018, www.digitaltrends.com/mobile/commerce-bans-zte-from-exporting-technology-from-the-us/.

in late 2018 at the request of the U.S., which was seeking extradition of Meng. The U.S. government cited that Huawei, and specifically Meng, defrauded U.S. investors, including the banks HSBC and Standard Charter, by lying about the relationship between Huawei and subsidiary Skycom, which effectively served as Huawei's Iran-based affiliate to circumvent sanctions.[107] HSBC is said to have cleared more than $100 million in Skycom transitions between 2010 and 2014. Meng, during 2013 presentations to HSBC investors, purposefully mislead bankers about the Huawei and Skycom connection and ensured that HSBC transactions would not be used for any dealings in Iran. In an internal document later released, ZTE officials allegedly cited the Huawei model (referring to the company as "F7") of creating a "cut-off" company to do business with places like Iran and North Korea.[108]

The situation for Huawei boiled over in January 2019, when the U.S. Department of Justice unveiled sweeping sanctions against Huawei's U.S. branch, charging Huawei officially with fraud and IP theft.[109]

Beyond the clear illegality of the sanction violations and investor defrauding by Meng and Huawei, another salient issue at the core of the recent Huawei scandal rests upon the rise of China's "military-civilian integration," which has caused great alarm in the halls of Washington.[110] In China's context, military-civilian integration refers to the practice of incorporating advanced technologies of private entities (companies such as Huawei, Tencent and Alibaba) and public entities (the PLA, the national government and state-run enterprises). The initiative was spearheaded by Xi Jinping himself, creating the Central Commission for Integrated Military and Civilian Development in 2017. The body, overseen by the CCP's Central Committee, overseas the development of military-civilian integration. Politically, the rise of the Chinese private-military complex presents a challenge to Washington's power not to mention its comfort level, which it may seek to curb in order to protect its own perceived national security interests.

This 2012 House Report, and the subsequent issues with Huawei have critical implications for Chinese cloud computing operators in the U.S. There are clear parallels between telecommunications equipment and services and cloud computing services and data storage technologies. In essence, one can be seen as the evolution of the other. In other words, telecommunications equipment predated the advent of cloud computing, which went on to replace or complement traditional telecommunications

---

[107] Horowitz, Julia. "How Huawei's CFO Ended up in a Jail in Canada." *CNN*, Cable News Network, 11 Dec. 2018, www.cnn.com/2018/12/11/business/huawei-cfo-arrest-details/index.html.

[108] Mozur, Paul. "ZTE Document Raises Questions About Huawei and Sanctions." *The New York Times*, The New York Times, 21 Dec. 2017, www.nytimes.com/2016/03/19/technology/zte-document-raises-questions-about-huawei-and-sanctions.html.

[109] "United States V. Huawei Device Co. Ltd." *UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF WASHINGTON 8 AT SEATTLE* , 2018, www.justice.gov/opa/press-release/file/1124996/download.

[110] Nakazawa, Katsuji. "Xi, Huawei and China's Powerful Military-Industrial Complex." *Nikkei Asian Review*, Nikkei Asian Review, 13 Dec. 2018, asia.nikkei.com/Editor-s-Picks/China-up-close/Xi-Huawei-and-China-s-powerful-military-industrial-complex.

infrastructure with more high-tech channels. In both cases, critical information is transmitted, and in the case of cloud, the United States' security interests are at stake and face a variety of threats. Some may actually conclude that cloud services are actually more vulnerable to compromise than the traditional telecommunications supply chain, especially if the data storage center is hosted non-locally and governed by different laws. Moreover, control over data will be critical to AI in the future, further highlighting the importance of the cloud. All in all, the conclusions by the U.S. House Report regarding Chinese telecommunications operators have clear implications for Chinese cloud operators in the United States, which, by extension, can be attributed to limiting their market share in order to discourage government purchasing and private adoption. Of course, to note, Huawei also currently has cloud computing service offerings, especially notable for providing e-Government cloud solutions for cities such as Beijing, Shanghai, and Tianjin, though it is all but absent from the U.S. market.

5.12 FIRRMA & CFIUS

In 2018, in response to the perceived threat posed by the Made in China 2025 plan, U.S. Congress passed the Foreign Investment Risk Review Modernization Act (FIRRMA). FIRRMA expands the ability of CFIUS to evaluate and address national-security concerns related to foreign investment in the U.S., especially that from China.[111] The bill introduced major operational and institutional changes in the structure of CFIUS, mandating CFIUS to consider, including: 1) the national security effects of cumulative market share by foreign powers; 2) the extent to which a transaction is likely to expose sensitive data of U.S. citizens by exploitation of foreign actors; and 3) whether a transaction involves a country of concern that has a strategic goal of acquiring technologies that would affect U.S. technological leadership.[112] Given the history of CFIUS blocking China-based investment in the U.S., and given the rhetoric of the measure itself, the bill is a not so subtle move to curb Chinese investment in key technologies in the U.S.[113]

One of the most high-profile U.S.-China fallouts from the CFIUS review process was the failed takeover of Moneygram International Inc., a U.S.-based money transfer platform, by Ant Financial, the financial services fin-tech subsidiary of Alibaba in January of 2018. Upon review, CFIUS rejected the merger, citing concerns over the safety of data that could be used to identify U.S. citizens and their financial transactions. The deal, valued at $1.2 billion, represented a huge blow to both companies. According

[111] Segal, Adam. "Year in Review: Huawei and the Technology Cold War." *Council on Foreign Relations*, Council on Foreign Relations, 2018, www.cfr.org/blog/year-review-huawei-and-technology-cold-war.
[112] Zable, Stephanie. "The Foreign Investment Risk Review Modernization Act of 2018." *Lawfare*, 6 Aug. 2018, www.lawfareblog.com/foreign-investment-risk-review-modernization-act-2018.
[113] To note, Chinese companies often prefer investing to acquire U.S. companies or technologies rather than directly manage given localized operational and managerial challenges.

to Scott Kennedy, a fellow at the Center for Strategic and International Studies in Washington, D.C., "[t]his deal fell apart because Ant Financial is from China, a country that has little credibility when it comes to protecting personal data. Add to that the lack of reciprocity -- China would never countenance such a deal in reverse -- and one could ask why Alibaba would expect to find a sympathetic hearing in Washington." In the global technology arena, the inability of an American company to purchase Ant Financial, in a theoretical reciprocal sense, also proved to be a block that caused the deal to collapse.[114] The rejection of the takeover by Ant Financial represents a growing trend of trade tension between the U.S. and China. The U.S. cited data privacy and cybersecurity concerns as the core rationale behind its ruling, wary of exposing sensitive U.S. citizen data to China. As noted before, behind the veil of data privacy and cybersecurity, an undercurrent of the Moneygram-Ant Financial fallout is the desire to curb China's technological rise and the goal to keep the U.S. as the global leader in technology production and innovation. These two motivating issues, more often than naught, seemed irrevocably tied when it comes to U.S. formulation of policy or regulations when it comes to creating a framework for dealing with China.

The end of 2018 saw the introduction of future measures by the U.S. government to monitor and enforce Chinese trade theft cases. Then-acting Attorney General Jeff Sessions announced a China Initiative in 2018, which would allow the U.S. Department of Justice to identify priority Chinese trade theft cases and, with ample resources, pursue them to an appropriate and swift conclusion.[115] Shortly after, U.S. officials charged two Chinese nationals, Zhu Hua and Zhang Shilong, with alleged extensive ties to the PLA as part of APT10, for long-term and systemic illegal hacking operations.[116] Prosecutors stated that Zhu and Zhang, working for the Huaying Hatai Science and Technology Development Company via the Chinese Ministry of State Security's Tianjin State Security Bureau, breached the computers of more than 45 companies since 2006 and accessed sensitive business information, including trade-secret sensitive companies such as NASA's jet propulsion lab, the Navy, U.S. Department of Energy's Lawrence Berkeley National Laboratory and an additional other 25 technology-related companies.[117] The move dampened the already fraught state of U.S.-China relations

---

[114] Isaacs, Julien. "CFIUS: The Failed Takeover of MoneyGram by Ant Financial." *Julien Isaacs U.S.-China Global Brand Consultancy中美品牌咨询公司*, 14 June 2018, julienisaacs.com/index.php/2018/06/14/cfius-the-failed-takeover-of-moneygram-by-ant-financial/.

[115] "Attorney General Jeff Sessions Announces New Initiative to Combat Chinese Economic Espionage." *The United States Department of Justice*, 7 Nov. 2018, www.justice.gov/opa/speech/attorney-general-jeff-sessions-announces-new-initiative-combat-chinese-economic-espionage.

[116] Sanger, David E., and Katie Benner. "U.S. Accuses Chinese Nationals of Infiltrating Corporate and Government Technology." *The New York Times*, The New York Times, 20 Dec. 2018, www.nytimes.com/2018/12/20/us/politics/us-and-other-nations-to-announce-china-crackdown.html.

[117] "Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information." *The United States Department of*

but also represents a further important setback for Chinese actors in the U.S. Unintentionally, the actions of the Chinese government via international hacking have implications for Chinese technology, especially software operators in the U.S., such as Huawei, Alibaba, Tencent, Xiaomi and others. **In essence, given the knowledge that the Chinese government has engaged in a targeted campaign to access business-sensitive data, any Chinese owned platform or service involving data storage or data transfer will be immediately treated with suspicion by U.S. consumers and the U.S. government given the Chinese owned companies' opaque and likely submissive relationship with the Chinese State and with Chinese regulators, which has clear impact on adoption and future revenues.**

5.13 Exposing PLA Unit 61398 (总参三部二局)

To note, awareness of Chinese state-sponsored hacking first came to public light as early as the early 2000s; however, a 2013 report released by Mandiant entitled *APT1: Exposing One of China's Cyber Espionage Units* proved especially groundbreaking.[118] APT1, or PLA Unit 61398 (总参三部二局), located in the Pudong district in China, engaged in a systematic campaign to steal hundreds of terabytes of data, especially sensitive IP, from roughly 141 organizations. Their actions were likely government-sponsored - the industries that APT1 targeted matched the strategic emerging industries identified in the Chinese government's 12th Five Year Plan. Below, Figure 8 illustrates how APT1 or PLA Unit 61398 fits into the greater Chinese military-government organization.

Justice, 20 Dec. 2018, www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion.

[118] "APT1 Exposing One of China's Cyber Espionage Units." *Mandiant*, 2013, www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

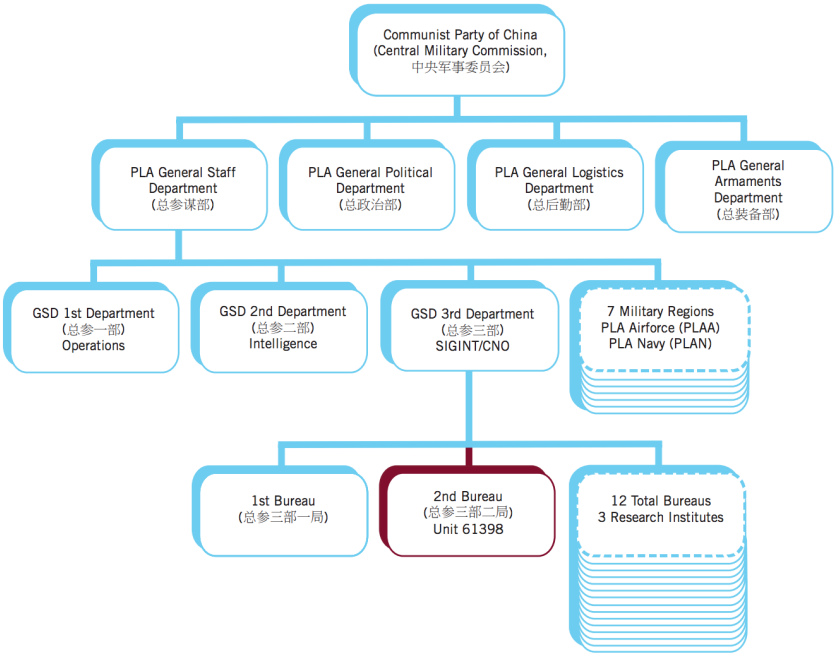

Figure 8: Unit 61398: Position Within in the PLA

The 2013 Report and the exposing of specific hackers and hacking actions by the Mandiant Report caused a bit of a firestorm in Washington and in the U.S. business community. Specifically, it provided concrete proof between the Chinese government had engaged in international espionage and cyber theft activities.

5.14 Increased U.S.-China Cyber Tension

Further accusations of China state-supported economic espionage continued after the Mandiant Report, leading to arrests, indictments, executive orders and further reports. In May 2014, the U.S. Department of Justice indicted five Chinese nationals, Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, and Gu Chunhui, who were officers in Unit 61398 of the People's Liberation Army (PLA), for computer hacking and economic espionage towards six American targets in the nuclear power, solar and metals industries.[119] The charges were noteworthy because they represented the first instance that U.S. criminal charges were knowingly filed against Chinese state actors for hacking. The U.S. Department of Justice also indicted another Chinese national shortly after, Su Bin, for orchestrating cyber-enabled economic espionage in the aerospace industry, helping Chinese military officers hack into computer networks of

[119] Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information." *The United States Department of Justice.*

major U.S. defense contractors. Bin later plead guilty and was sentenced to 46 months in federal prison.[120]

Subsequently, the Obama Administration issued an Executive Order, enabling the freezing of U.S. controlled property and interests for individuals engaged in malicious cybersecurity activities threatening U.S. national security.[121] The Executive Order, entitled *"Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities,"* was released in April 2015. The measure can be understood in the building trend of disincentivizing foreign hackers from assailing critical American infrastructure or compromising American computer networks, this time with increased punishment and economic loss on behalf of the indicted parties. Finally, the American media began reporting that the Obama Administration was considering sanctions against China given the administration's increasing frustration with China's continued state-sponsored cyber hacking. Obama, himself, announced the threat of sanctions, saying that the U.S. was "preparing a number of measures that will indicate to the Chinese that this is not just a matter of us being mildly upset, but is something that will put significant strains on the bilateral relation if not resolved."[122] The announcement came just before the visit of President Xi to the United States to meet with President Obama in Washington and, may be seen, in retrospect, as crucial to the creation of the *U.S.-China Cyber Agreement*, which was instituted later that month, ratified by both President Obama and Xi, with both the U.S. and China promising increased cooperation in cyberspace and decreased state-supported cyber-theft.

5.15 2015 The U.S.-China Cyber Agreement

Amid the proof of Chinese state-sponsored cyber-campaigns aimed at economic espionage on U.S. and international actors, the growing hacking threat, the possibility of sanction against China, and the increasing advanced techniques employed by Chinese malicious cyber operators, President Xi and President Obama signed a landmark cyber agreement in 2015. Entitled the *U.S.-China Cyber Agreement,* the treaty was signed during a state visit to the U.S. by President Xi in September 2015. As shown in Table 18, the Agreement contained four major tenets, detailed below, including providing assistance concerning malicious cyber activities, promoting norms of behavior in

---

[120] "Chinese National Who Conspired to Hack into U.S. Defense Contractors' Systems Sentenced to 46 Months in Federal Prison." *The United States Department of Justice*, 11 Aug. 2016, www.justice.gov/opa/pr/chinese-national-who-conspired-hack-us-defense-contractors-systems-sentenced-46-months.

[121] "Executive Order -- 'Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities.'" *National Archives and Records Administration*, National Archives and Records Administration, 2015, obamawhitehouse.archives.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m.

[122] Davis, Julie Hirschfeld. "Obama Hints at Sanctions Against China Over Cyberattacks." *The New York Times*, The New York Times, 21 Dec. 2017, www.nytimes.com/2015/09/17/us/politics/obama-hints-at-sanctions-against-china-over-cyberattacks.html.

cyberspace and establishing high-level joint dialogues between the U.S. Secretary of Homeland Security and China's Ministry of Public Security, Ministry of State Security, Ministry of Justice, and the State Internet and Information Office.

Tenet Number	Tenet Details
Tenet 1	Provide timely responses to requests for information and assistance concerning malicious cyber activities.
Tenet 2	Refrain from conducting or knowingly supporting cyber-enabled theft of intellectual property.
Tenet 3	Pursue efforts to further identify and promote appropriate norms of state behavior in cyberspace within the international community.
Tenet 4	Establish a high-level joint dialogue mechanism on fighting cybercrime and related issues.

Table 18: Tenets from the U.S.-China Cyber Agreement[123]

Key among the tenets is the second tenet, which states that both parties will refrain from conducting cyber-enabled theft, which is clearly directed at the PLA supported hacking activities such as those from PLA Unit 61398. This provision from the Agreement proved to be quite effective, reducing the instances of Chinese state supported economic cyber espionage for a three year period, especially the kind that concerned the Obama Administration, mainly the use of limiting hacking efforts design to appropriate U.S. IP for commercial purposes in China.[124] According to a June 2016 FireEye iSight Intelligence Report, the number of network compromises started by Chinese hacking groups dropped by 60 from February 2013, two years or so before the Agreement, to just under 10 by May 2016, roughly a year after the Agreement was signed.[125] Indeed, cyber-attacks by China reduced significantly. Figure 9 below, assembled by FireEye, shows 262 network compromises by 72 suspected China based groups. Of the 262 incidents, 182 occurred on U.S. networks. This 86% decrease in state-sponsored hacking instances can likely be attributed to the *U.S.-China Cyber*

[123] "FACT SHEET: President Xi Jinping's State Visit to the United States." *National Archives and Records Administration*, National Archives and Records Administration, obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.
[124] Farley, Robert. "Did the Obama-Xi Cyber Agreement Work?" *The Diplomat*, The Diplomat, 11 Aug. 2018, thediplomat.com/2018/08/did-the-obama-xi-cyber-agreement-work/.
[125] Segal, Adam. "The U.S.-China Cyber Espionage Deal One Year Later." *Council on Foreign Relations*, Council on Foreign Relations, 2016, www.cfr.org/blog/us-china-cyber-espionage-deal-one-year-later.

Agreement, coupled with PLA cyber operations reorganizations and other domestic reforms under the Xi Administration.[126]

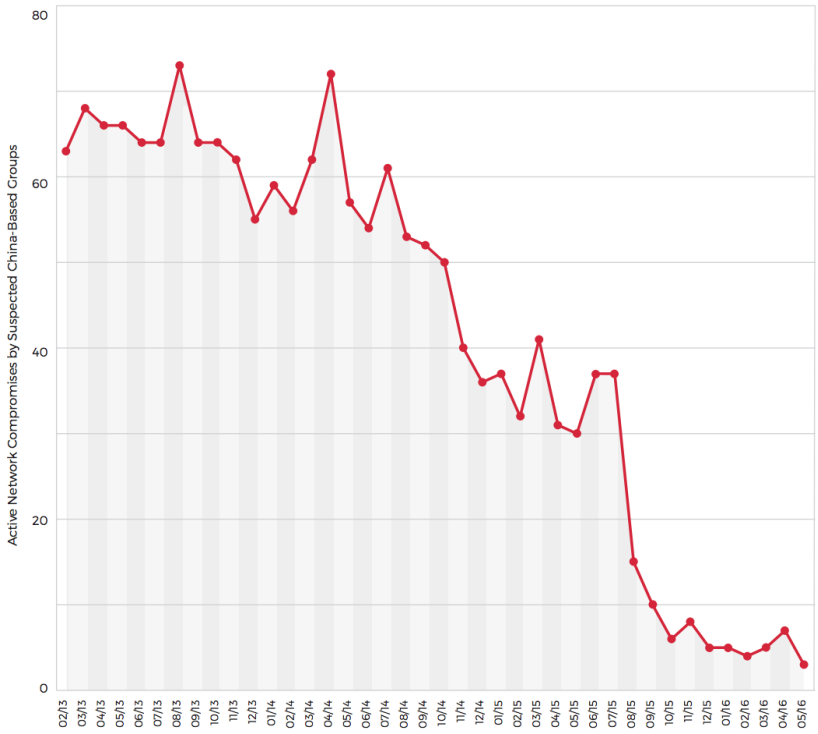

Figure 9: Active Network Compromises Conducted by 72 Suspected China-Based Group: 2013-2016[127]

However, as the Trump-Xi U.S.-China trade war ramped up, instances of Chinese hacking into U.S. governments and businesses once again started to rise. In late 2018, U.S. officials went on public record and stated that China had violated the *U.S.-China Cyber Agreement* and that China had resumed state-sponsored hacking activities, one such which including a giant hack of the U.S. federal government's personnel office, compromising the data of over 20 million individuals.[128] Rob Joyce, National Security Agency official, did note that even though China was currently in violation of the Agreement, the quantity and number of attacks had nevertheless dropped "dramatically" since the 2015 agreement.[129]

---

[126] "Red Line Drawn: China Recalculates Its Use of Cyber Espionage." *Fireeye ISight Intelligence*, 2016, www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf.
[127] Ibid.
[128] "U.S. Accuses China of Violating Bilateral Anti-Hacking Deal." *Reuters*, Thomson Reuters, 9 Nov. 2018, www.reuters.com/article/us-usa-china-cyber/u-s-accuses-china-of-violating-bilateral-anti-hacking-deal-idUSKCN1NE02E.
[129] Ibid.

5.2 China to America: Policy Background

The U.S. policy regime regarding cloud, data privacy, foreign access and technology in general remains, from the 1980s to today, strikingly non-interventionist. Seemingly, the U.S. has adopted a hands-off approach to regulating technology, preferring to let the giants of Silicon Valley self-regulate and self-innovate. The primary policy trend that has emerged has mostly been intelligence based in nature, allowing the federal government access to information for use in criminal investigations and counter-terrorism efforts. Oversight authority has been granted to CFIUS (The Committee on Foreign Investment in the United States), especially via FIRRMA (Foreign Investment Risk Review Modernization Act) to curb foreign and, in the recent years, Chinese technological access to purchasing American technology companies that are deemed sensitive and pose a potential national security risk. However, there exists little direct policy explicitly banning Chinese companies from selling in the U.S. The expectation and precedent here are Huawei and ZTE, the Chinese telecommunication giants, as Congress launched an in-depth investigation, resulting in the banning of the purchase of Huawei and ZTE products by the U.S. government and a dissuasion of the use of Huawei and ZTE products for private enterprise. This ban, combined with the reports on Chinese hacking efforts, have created a norm where Americans have grown mis-trusting of Chinese technology products, especially those that are data sensitive. Political and economic national cyber security concerns, especially regarding preventing espionage through economic and political channels, factor in heavily to the U.S. government's policy making process and motivations. Table 19 details the policy motivations stemming from the national cybersecurity concern from Khetri (2016), as discussed above.

National Cybersecurity Concern: Category	National Cybersecurity Concern: Type	Relevant Country Policies
Political Security	Political Espionage	U.S.
Economic Security	Economic Espionage	U.S.

Table 19: National Cybersecurity Concern Policy Motivations in the U.S.

The 1986 Stored Communications Act (SCA), 1986 Electronic Communications Privacy Act (ECPA), 1994 Communications Assistance for Law Enforcement Act (CALEA), 2011 Patriot Act, 2018 CLOUD Act are likely the most relevant official policies affecting Chinese cloud computing operators in the U.S. Most of these laws enact standard intelligence compliance regulations. In the U.S., political and economic

national cyber security concerns factor in most relevantly when creating policy, with the political concerns of paramount importance.

As discussed below, the key challenge for Chinese cloud operators in China is winning consumer trust and ensuring data integrity for their users.

5.21 1986 Stored Communications Act (SCA) & 1986 Electronic Communications Privacy Act (ECPA)

In terms of official legislation affecting cloud computing providers in the U.S., the Stored Communications Act (SCA), introduced in 1986, is likely the first in the modern regime of intelligence-centric policy.[130] The SCA allows for privacy protection of a user's digital communication and data on the Internet, and limits the ability of the government to force an Internet Service Provider (ISP) from turning over relevant data without just cause and the proper due process.

The SCA is part of a broader Electronic Communications Privacy Act (ECPA)[131] that enhanced consumer protections from government surveillance, such as wire tapped phone calls or electronic data transmission. The ECPA can be viewed as an extension of the Fourth Amendment, which protects people's rights to be secure against unreasonable search or seizures by government authorities, updated for the modern technology of our times.

The ECPA and SCA have been instrumental in informing American user's understanding of data privacy and protection rights in the modern era. With the expectation that the government is restricted in its access to personal data from Internet Service Providers, users can logically assume data privacy and protection from other third party actors in society. This has become the unofficial norm, but fully expected, in American society.

5.22 1994 Communications Assistance for Law Enforcement Act (CALEA) & 2011 Patriot Act

Since the enactment of the ECPA and SCA, several pieces of additional legislation, including the 1994 Communications Assistance for Law Enforcement Act (CALEA) & 2011 Patriot Act and the 2018 CLOUD Act, have been introduced that slightly eroded consumer data privacy and enhanced the purview of the government to access and monitor digital data.

---

[130] "18 U.S. Code Chapter 121 - STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS." *LII / Legal Information Institute*, Legal Information Institute, www.law.cornell.edu/uscode/text/18/part-I/chapter-121.

[131] "Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510-22." *Justice Information Sharing*, it.ojp.gov/PrivacyLiberty/authorities/statutes/1285.

The Communications Assistance for Law Enforcement Act (CALEA, introduced in 1994, required that telecommunications companies must modify their equipment or services to allow for better government surveillance under appropriate circumstances.[132] The law was later expanded to include the Internet and Broadband. At the request of the FBI, CALEA was created to better allow the intelligence and justice wings of the U.S. government to conduct electronic surveillance under appropriate circumstances, while still protecting the privacy of information.

The Patriot Act (USA PATRIOT expanded or Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) was introduced in 2001 following the 9/11 terrorist attacks.[133] The law is broad and vague, though the consensus is that the Act expands the ability of the government to conduct surveillance, to search and seize, and to conduct a variety of acts under the moniker of state security under appropriate circumstances. Many of the provisions were eventually sunset, but the expanded power to surveil data is still of note today.

5.23 2018 CLOUD Act

Arguably the only policy issued by the U.S. specifically aimed at the cloud and data storage, the CLOUD (Clarifying Lawful Overseas Use of Data) Act was enacted in March 2018. The CLOUD Act allows U.S. federal enforcement agencies to warrant or subpoena access to data that U.S. technology companies have stored either domestically or abroad under appropriate circumstances. The bill was introduced at the request of the FBI, when SCA warrants no longer proved viable for obtaining intelligence information stored outside of the U.S. Specifically, an issue arose when Microsoft refused the FBI's request to hand over emails between U.S. drug traffickers stored in its Ireland data servers, resulting in the 2015-2016 legal action entitled *Microsoft Corp. v. United States.*[134] The case spurred the U.S. government to update the law and pass the CLOUD Act, with the Justices noting that Congress was better equipped to address foreign conflicts regarding technology and the law.[135]

The case had important implications for data privacy security. Microsoft argued that providing U.S. authorities with emails might scare off foreign customers, who may

---

[132] "Communications Assistance for Law Enforcement Act." *Federal Communications Commission*, 6 Oct. 2017, www.fcc.gov/public-safety-and-homeland-security/policy-and-licensing-division/general/communications-assistance.
[133] "The USA PATRIOT Act: Preserving Life and Liberty ." *The United States Department of Justice*, www.justice.gov/archive/ll/highlights.htm.
[134] Williams, Pete. "Supreme Court Seems Set to Rule against Microsoft in Email Privacy Case." *NBCNews.com*, NBCUniversal News Group, 2018, www.nbcnews.com/politics/supreme-court/gov-t-battles-microsoft-email-privacy-case-supreme-court-n851216.
[135] "The CLOUD Act, Bridging the Gap between Technology and the Law." *The National Law Review*, National Law Review, 2018, www.natlawreview.com/article/cloud-act-bridging-gap-between-technology-and-law.

prefer to use local hosting services outside of the reach of U.S. law enforcement.[136] This, potentially, could impact consumer trust, and compromise the "authenticity" and "possession/control" elements of the Parkerian Hexad model, resulting in consumers choosing a more secure, local cloud substitute over the U.S. owned technology company. Moreover, such legislation conflicts with international law, such as the China 2017 Cybersecurity Law, which states that data may not be transferred outside of the country without express governmental permission. All in all, though, the CLOUD Act represents a not surprising piece of legislation by the U.S., as it indicates, from the judicial and intelligence point of view, a necessary updating of previous legislation and the SCA, in order to achieve the same end result, access to information for the Department of Justice. In a way, such a piece of legislation is inevitable. While U.S.-based cloud computing operators may lose out to local substitutes, likely, the effects of such a data privacy legislation are minimal given the largely transparent nature of U.S. law enforcement processes and the limited scope by which the U.S. government is permitted to access information.

5.3 China to America: Main Case Study: Alibaba

Alibaba launched its cloud services subsidiary, Alicloud or Aliyun (阿里云), in 2009. However, Alibaba got more serious about its cloud business in 2015, investing $1 billion USD.[137] The majority of Alicloud's business is in China and in greater Asia; however, Alicloud entered the U.S. market in 2015 and currently has two data centers in the U.S., one in Silicon Valley and one in Virginia.

Though Alicloud experienced success in the China market, its cloud business in the U.S. has struggled to take hold. Alibaba entered the U.S. market with the hopes of taking on incumbents such as Amazon Web Services and Microsoft Azure. After three years, Alibaba failed to gain much market share. In August 2018, The Information revealed that Alibaba planned to put its cloud U.S. infrastructure expansion plans on hold.[138] A spokesperson from Alibaba shortly thereafter responded, denying the claim:

> Alibaba Cloud's U.S. strategy has always been primarily focused on working with U.S. companies who need cloud services in China and Asia and helping Chinese companies with cloud services in the US, not competing head to head with local

[136] Mak, Aaron. "Congress Put the Controversial CLOUD Act in Its Spending Bill. What Does That Mean For Data Privacy?" *Slate Magazine*, Slate, 22 Mar. 2018, slate.com/technology/2018/03/cloud-act-microsoft-justice-department-omnibus-spending-bill.html.
[137] Miller, Ron. "Alibaba Cloud Growing like Gangbusters, but Still Far behind AWS and Other Market Leaders." *TechCrunch*, TechCrunch, 6 Feb. 2018, techcrunch.com/2018/02/06/alibaba-cloud-growing-like-gangbusters-but-still-far-behind-aws-and-other-market-leaders/.
[138] McLaughlin, "Alibaba Puts the Brakes on U.S. Cloud Expansion."

> players," a spokesman said. "Our commitment to this market remains unchanged. On a global level, Alibaba Cloud is already the #3 cloud provider, and we aim to be the industry leader in both scale and technology. While still relatively early days for our cloud business, we are growing aggressively and have significant runway in China and in many markets around the world.[139]

Alibaba had run up against two main hurdles in the U.S. market. The first involved competition from incumbent players. Amazon, Microsoft and Google all had established presence already in the cloud market, able to tap into economies of scale, an existing customer base that trusted them, and valuable brand equity.

Additionally, Alibaba allegedly feared the potential of greater regulatory backlash from Washington if it continued to aggressively expand, citing the ban on ZTE products earlier in 2018 and increased regulatory scrutiny of Chinese companies stateside. Alibaba stated that it would refocus its efforts on serving multinational companies with business in China. Even though Alicloud offered steep discounts to incentive users to switch to their products and services, the strategy in the U.S. did not pan out as expected. The move to stop aggressively competing in the U.S. market represents somewhat of a failure, having implications for Alicloud's ability to become a powerhouse in the global cloud market outside of Asia. Simon Hu, the president of Alicloud, predicted that Alicloud cloud overtake or at least match Amazon Web Services in the global cloud market in 2019 - much of that success hinged on its ability to sell into the large U.S. market. The prediction, therefore, will remain largely unrealized.

A third hurdle, in addition to the two cited above, was U.S. companies resisting the idea of storing data with a Chinese cloud provider. Though not mentioned by Alibaba publicly, this was likely the core factor leading to Alibaba's failure to gain traction in the U.S. market. Given the history of Chinese state-sponsored hacking, intellectual property theft and the non-transparent relationship between the government and technology companies such as Alibaba, American companies, especially those with sensitive or proprietary data, certainly had valid concerns about storing data with a Chinese cloud service provider. In the end, the steep price cuts, with Alicloud offering customers as much as 30% savings on the cloud bills, proved not enough to allay data privacy and data security concerns for U.S. businesses.[140]

The question arises: Why hasn't the US government been even more aggressive (such as banning and asking other countries to do so) against Alicloud, like it has with Huawei and ZTE? Simply put, Alicloud doesn't pose the same threat. U.S. consumers have effectively mitigated the information security threat posed by Alicloud by not choosing this solution, informed by the knowledge of Chinese products and their

---

[139] Deutscher, Maria. "Report Says Alibaba Halted U.S. Cloud Expansion, Company Denies Change." *SiliconANGLE*, 3 Sept. 2018, siliconangle.com/2018/08/31/report-alibaba-quietly-halted-u-s-cloud-expansion/.
[140] McLaughlin, "Alibaba Puts the Brakes on U.S. Cloud Expansion."

security ramifications. However, if Alicloud became a major market force, it would likely attract the ire of Washington and create a situation where regulatory action became highly probably. To outright ban Alibaba, though, would be politically sensitive, causing a backlash and potential retaliation by China. In other words, the political calculus is simply not worth it, especially given that Alibaba has a rather small business in the U.S. (mainly working with U.S. brands for its e-commerce platform or shipping to U.S. consumers)

5.4 China to America: Analysis

Though the U.S. remains a relatively open market to foreign technology, Chinese technology firms pay the price for the CCP leaders' political miscalculation, using these companies as potential conduits for espionage, perfectly illustrated by Huawei, and Alicloud as well.[141] Using an updated Parkerian Hexad model, one can see that information security elements are of focal concern to U.S. companies, as shown in Table 20. Unlike companies in China, which are mandated to share information with the government by law in an often non-transparent manner, there exists no such compulsion in the U.S. and, often, tech companies clash with Washington over issues of protecting user privacy. Elements of the Parkerian Hexad for American consumer risk of Alicloud in the U.S. are ranked 1-5, with 1 being the lowest (or least secure) and 5 being the highest (or most secure). Explanations for the ranking are set forth in the rightmost column. Again, most of the information security issues stem not from technical risks, but rather the risks posed by the Chinese government itself. There are serious consumer risks for Alicloud in China, especially in terms of confidentiality, possession/control and integrity.

Updated Parkerian Hexad Element	**Consumer Information Security: Chinese Cloud Computing Operators in America, Alicloud (1-5)**	**Details**
Confidentiality	1	The requirement to provide data to the Chinese government in a non-transparent manner poses a serious risk to consumer confidentiality, even for cross-

[141] Zaagman, Elliott. "Meng Wanzhou: China's 'Tantrum Diplomacy' and Huawei." *The Interpreter*, The Interpreter, 14 Dec. 2018, www.lowyinstitute.org/the-interpreter/china-tantrum-diplomacy-huawei.

		border information. Data stored in Alicloud servers in the U.S. may still end up with the Chinese government.
Possession/Control	1	Non-transparent auditing of data by the Chinese government potentially compromises user possession/control, even in a cross-border scenario.
Integrity	3	Information may be scrubbed or altered if deemed malicious to the Chinese state, though this would be somewhat rare in an international context.
Authenticity	3	Information creation and origin likely authentic.
Availability	4	Alicloud's global standards and advanced technology likely ensures a high level of availability.
Utility	4	Information likely readily available and useful in form, given Alibaba's technical capacity.
Jurisdiction	3	U.S. laws relatively open in terms of data flows, with minimal interference for intelligence and counterterrorism.

Table 20: The Updated Parkerian Hexad: American Consumer Risks for Alicloud in the U.S.

Given the laws in China, American businesses are right to worry about data privacy and control with Chinese cloud operators. Confidentiality, control, integrity and authenticity might be compromised given China's rule of law and opaque nature of the Party's control over enterprises. On that note, in 2013, the American Chamber of Commerce in Shanghai reported that only 10% of its members trusted data security

enough to consider cloud computing services in China.[142] That same mindset can be applied to Chinese cloud computing services in America, demonstrating the lack of trust Americans have towards data sensitive Chinese products and services.

The main issue for Alibaba is not only security risks, which are considerable, but also the relative merits of the Alicloud service compared to competitors that are not only entrenched, but also offer a more secure service, perceived or real, such as Amazon Web Services, Microsoft Azure, and IBM Cloud, as shown in Table 21. There is little policy in the U.S. restricting Alicloud's operations - instead, the issue rests upon consumers' preference for other cloud operators, who are perceived as more trustworthy. Using Porter's 5 Forces, one can see that the competitive rivalry of more trusted competitors such as Microsoft and Amazon, who have not only an existing customer base in the U.S., but brand equity and effective scope leveraging, have severely hampered Alibaba's competitiveness in America and its ability to attract local consumers. Porter's 5 forces are ranked 1 to 5, with 5 posing the highest threat and 1 posing the lowest. Competitive rivalry and threat of substitution, here, have proven significant as factors that have diminished Alicloud's U.S. market share.

Force	Alicloud in the U.S. Market (1-5)	Details
Competitive Rivalry	5	Amazon, Microsoft, Google and other big players have proven to be entrenched competitors in the U.S. cloud industry.
Supplier Power	2	Supplier power is a rather non-factor here, as Alicloud likely has leverage over its own supply chain.
Buyer Power	3	Buyer power is stronger than supplier power; however, the vast number of buyers in America render the number lower.
Threat of Substitution	5	Threat of substitution is high - people can easily substitute out Alicloud offerings for other products, services or companies.
Threat of New Entry	2	Given the economies of scale and the initial investment involved in cloud computing, threat

[142] Areddy, James T. "American Entrepreneurs Who Flocked to China Are Heading Home, Disillusioned." *The Wall Street Journal*, Dow Jones & Company, 7 Dec. 2018, www.wsj.com/articles/american-entrepreneurs-who-flocked-to-china-are-heading-home-disillusioned-1544197068.

		of new entry is unlikely.

Table 21: Porter 5 Forces for Alicloud in the U.S.

Alicloud has failed to gain much traction in the U.S. given the attractiveness of its competitors' offerings. Companies like Amazon, Microsoft and Google offer more secure solutions at scale than Alicloud. In other words, most U.S. businesses simply prefer to use providers who are unhampered by policy that mandates government data sharing back home. Chinese companies with direct domestic competition, especially for a data-sensitive industry such as cloud, will likely be passed over for local alternatives given security issues. However, as will be shown below, if Chinese companies can sell products with no direct substitutes, either given a certain amount of technical innovation or unique engineering, they might be able to capture U.S. market share despite security concerns. For the future though, unless Alicloud can somehow assuage U.S. consumers worries about security, its market share will likely flatline in the U.S., or may even shrink as its stops building out physical infrastructure in the market.

6. Conclusions

The hurdles and opportunities surrounding the internalization of the cloud services business are emblematic of many of the core themes that global managers will have to face in the future, including data privacy, localization strategies, and governmental compliance. Thus, a comprehensive managerial framework for navigating evolving business models with cybersecurity concerns will prove invaluable to future leaders on both sides of the Pacific. Due to poor localization, management and local compliance strategies, U.S. and China cloud service companies historically have faltered in their international expansion into each other's markets. Yet, as the world becomes increasingly interconnected digitally, and China and America emerge as the global superpowers, cloud service platforms can greatly benefit from maximizing their market shares in both markets.

6.1 International Strategy Recommendations

6.11. America to China

For American companies in China, compliance is key. As discussed, the regulations for foreign companies in China can be complex and ever-changing. Therefore, not only complying but understanding the law is crucial to a foreign firm's success in China. American companies should **seek joint venture partnerships** with

local Chinese enterprises and governments, though this can sometimes involve unwanted or unintended technology transfers. American companies must also lobby the U.S. government to work with the Chinese government to try to **remove policy that serve as blocks to China market access**, especially in industries that touch upon critical infrastructure, such as cloud. Without such policy removal, U.S. firms will forever be limited to a sliver of market share. Lastly, U.S. firms should **adequately localize** to often idiosyncratic Chinese market by hiring a local team, empowering them to make quick decisions and tailoring products to local consumer preferences.

6.12 China to America

For Chinese companies in America, winning over consumer trust in an operationally efficient way is key, but will be difficult to attain. Given the history of consumers and governments associating Chinese companies with economic and political espionage, Chinese companies need to **convince American consumers of their trustworthiness** and reliability. Additionally, Chinese companies must e**nsure that plans and operations are capital efficient**, as there can be a tendency towards financial waste and mismanagement, often stemming from a lack of understanding the local market. Chinese companies in America should readily **employ and empower a local team** that understands the American market and consumer to help them localize marketing strategies. Policy-wise, Chinese firms should lobby government bodies such as CFIUS to allow for greater Chinese M&A in the States. Lastly, Chinese companies should seek to **provide innovative products** with little to no substitutes in America, such as Bytedance's AI-informed viral short video app Tic Tok and and DJI's camera drones and quadcopters.

6.2 Policy Recommendations

In terms of policy, the U.S. and China should work together to formulate policy mechanisms to deal with cybersecurity concerns, especially as they relate to international trade. Examples exist today such as the WTO's Technical Barriers to Trade (TBT) Committee, the 2015 The *U.S.-China Cyber Agreement* and the 2017 U.S.-China Law Enforcement and Cybersecurity Dialogue (LE&CD).[143] Maintaining cooperation between the two nations is of paramount importance, to prevent situations like the current Trade War from occurring. Moreover, China and the U.S. should work together to innovate technologies of the future, such as quantum computing and AI,

[143] "U.S.-China Law Enforcement and Cybersecurity Dialogue." *U.S. Department of State*, U.S. Department of State, 3 Oct. 2017, www.state.gov/r/pa/prs/ps/2017/10/274590.htm.

focused on partnership and collaboration, particularly in terms of standard creation, rather than adopt an adversarial or rival-like stance towards technology development.

Challenges, however, are present, especially given how divergent the U.S. and Chinese interests are regarding policy and national development. Below, Table 22 details policy recommendations to further U.S. and Chinese cooperation. Keeping differing interests in mind, the policy recommendations are then explored from the U.S. perspective, the Chinese perspective, and the "common good" or global benefit. Five types of policy-focused cooperation mechanisms are recommended, with respect to cybersecurity and data, anti-IP theft, increased market access, WTO compliance, technology standards and technology development cooperation.

Policy Type	Details	U.S. Perspective	Chinese Perspective	Common Good
Cybersecurity & Data Flow Agreement	Agree to stop state-sponsored hacking, allowing for clear enforcement mechanisms, consensus on international data flow regulations that do not conflict, and more clear norms for operations in cyberspace.	Prevents hacking and IP theft by Chinese actors; positive effect on U.S. companies and government	May derail China's short-term interests, in the long-term allows for greater global respect, not viewed as a malicious cyberspace agent	Increases the common good by establishing cybersecurity and data flow norms globally
Anti-IP Theft Agreement	Agree to stop IP theft, reduce technology transfer requirements, build norms to protect IP between the U.S. and China, implement actionable punishment for actors who violate IP	Beneficial to many American businesses and government entities who are a target of IP stealing, allows for access to China market for U.S. firms by increasing the potential value of licensing	Increased IP protections in the rule of law in China, better for Chinese society as a whole. In the short term may have a negative impact on R&D efforts, but in the long run will encourage a sustainable	Better IP protections increase global technological innovation, improving trade and enhancing competitiveness

	protections		R&D infrastructure in China	
Increased Market Access Legislation	Allow for better market access in the U.S. and China, for instance removing equity caps in China for foreign enterprises and allowing for greater Chinese M&A in America	Positive effect on American firms who want to access and gain revenue from the China market, security implications for Chinese firms who conduct more business in America	Positive effect for Chinese firms who wish to deploy capital in America, potential perceived negative effective by the Chinese government if American firms can dominate a sector in the Chinese economy	Increases global market efficiency, does not allow for redundant technological innovation in the U.S. and China in the future
WTO Compliance Assurance	Ensure both the U.S. and China are living up to their WTO commitments (overlaps with market access recommendation above)	American economy more efficient via WTO compliance and American firms can gain more revenue from China	American economy more efficient via WTO and Chinese firms can gain more revenue from the U.S.	Increased global market efficiencies, better access to both markets for international economies
U.S.-China Technology Standard Creation Body	Working group between U.S. and Chinese government standard creation entities and U.S. and Chinese private corporations to create technology standards to strive for	American firms benefit from a standard body creation by not wasting resources on technology that proves to be of little market value	Chinese firms benefit from a standard body creation by not wasting resources on technology that proves to be of little market value	Global firms benefit from a standard body creation by not wasting resources on technology that proves to be of little market value

	interoperability			
U.S.-China Frontier Technology Development Fund	U.S. and Chinese government and private corporations invest together to develop frontier technologies, such as AI and Quantum computing	U.S. benefits from working with China on technological advancements, though security challenges remain	Chinese benefit from working with U.S. on technological advancements, though conflicts slightly with techno-nationalist sentiments around indigenous innovation	Prevents redundant technology development, increases global technology efficiency and diffuses U.S.-Chinese tensions around technology development

Table 22: U.S.-China Policy Recommendations & Perspectives

6.3 Current & Future Analysis

Answering the questions posed at the beginning of the paper, we can, through the above comprehensive policy, and by case study analysis, arrive at conclusions regarding cloud, cybersecurity risks and international trade as follows:

(1) Cybersecurity Risk: Whether "cloud" increases or decreases the risks related to cybersecurity?

- Cloud clearly increases the risks related to cybersecurity, especially if that consumer data is stored abroad. In the U.S., companies like Amazon and Microsoft ostensibly offer a safer alternative to an in-house data storage center, but for companies engaging in cloud hosting in China, this clearly poses a serious cybersecurity risk. In addition to traditional cybersecurity issues such as hacking, malevolent entrance, phishing, etc., technologies surrounding the cloud touch on many issues regarding data: where the data is stored, how is the data secured, which nation's laws have jurisdiction over the data, how can government access data, will consumers know their data has been surveilled in a manner in which the company is complicit with (i.e. a Chinese cloud service provider giving an American multinational company's data to the Chinese government on request). The issues regarding the international flow and control of data bring about a new level of

cybersecurity concerns for cloud technologies, which are considerably amplified by economic and political tensions between nations.

(2) Policy Implications: Whether and how countries construct barriers to cloud computing originating from other countries due to concerns about cybersecurity?

- Countries, especially China and the U.S. to a certain degree, do certainly construct barriers to cloud computing given concerns about cybersecurity. China, concerned with not only maintaining political and economic stability, but also hoping to grow its domestic economy and bolster indigenous innovation, has employed a long-term strategic and techno-nationalistic policy regime aimed at controlling data flows in China via data localization requirements, limiting the ability of foreign cloud computing providers to operate without a joint venture partner, and other such measures that have resulted in a completely idiosyncratic market. There is no other market, other than China, that have the same top cloud service providers. Even countries in Southeast Asia, where Alicloud has a robust presence, still have enabled large market shares for AWS, Azure and Google Cloud. In that respect, it is unique and the motivation for this policy is centered in protecting China's cyber state security.

(3) Strategy Reactions: If restrictive international trade policies do exist, how can corporations navigate these barriers, or not, to effectively form a viable strategy?

- Restrictive international trade policies do exist in both the U.S. and China, with direct implications for corporate strategy. Unfortunately, as the case studies with Microsoft and Alibaba, who in many ways are the most successful examples of foreign cloud operators in the U.S. and China, illustrate, it is extremely difficult to succeed when a) there exists a hostile policy regime to foreign competition (China); or b) data is perceived as not secure to domestic consumers given the corporate entities requirement or willingness to violate data autonomy and control by providing it to 3rd parties such as foreign governments for potentially malicious purposes. So far, no company has been able to execute a winning, long-term strategy for a data-sensitive product in the U.S.-China technology expansion arena. However, there are best practices to keep in mind for the future. For U.S. companies going into China, compliance is key. Maintaining good government relations, in line with government objectives, is a strategy to ensure continued access. However, the U.S. political and business community must seek high-level dialogues to change the policy regime in China in order to truly realize a healthy market

share for U.S. companies. On the other hand, Chinese companies don't face as many official policy barriers as in the U.S. Much of the Chinese companies' failures stems from operational or managerial missteps, combined with large privacy concerns American consumers have about Chinese products. If China can innovate products that have no American substitutes, American consumers may be more willing to waive their privacy concerns in order to adopt a novel technology. Companies like Bytedance, with its AI-informed viral short video app Tic Tok, and DJI, with its unique drone technology, represent beginnings of this trend. In the future, one can imagine a situation where Chinese companies that provide innovative AI, autonomous driving, clean energy or automated health software could perform well in the American market. However, the lingering issue of CCP access to corporate data will remain and continue to be a block for Chinese companies abroad, especially in terms of cloud and data storage.

6.4 In Summation: An Evolving Dynamic

Academics, policy hawks and leaders in the business community alike have cited that the U.S. and China may be headed into a technology cold war, supported by two separate Internet ecosystems, each supported by a bifurcated set of standards, regulations and dominant players. As the paper above has demonstrated, technological success for Chinese cloud companies in America and American cloud companies in China remains unrealized and, to a certain extent, unfeasible given government regulation, consumer preference for substitutes and a preference for locally created software. In recent years, Xi and Trump have embraced policies that have put the U.S. and China on an increasingly adversarial path. The outcome may be the eventual separation of the two technology systems, with companies, individuals and governments having to decide whether to integrate into the U.S. or Chinese technology platforms, software and systems.[144]

There are ways to prevent this future, and primarily, the role hinges on governments working together to cooperate on the creation of global technology standards, and international bodies such as the UN and the WTO, to ensure "fair" technological market access for developed economies. As we approach the ABC (AI, Big Data and Cloud) era, greater connectedness is essential for retaining global competitiveness. Only by integrating into the world stream of innovation, research and advancement can countries maintain their competitive edge and keep at the forefront of the briskly changing high-tech landscape.

[144] Segal, Adam. "Year in Review: Huawei and the Technology Cold War."

The techno-nationalist policy formed by the Chinese government remains a huge challenge for both the American government and American technological enterprises in China. These policies touch into the deepest roots of the Chinese state, and persuading China to abandon these policies will be met with incredible pushback from the Party. China views the ability to have technological self-sufficiency, created by national champions and domestic firms that can subsequently prosper internationally, as the key to its long-term strategic interests. Any attempt to thwart or contain such a strategy will be met with resistance, taking the form of nationalism. The concept of technological strength and national power are core concepts to the Chinese state. Thus, it is all too likely a possibility that American technology firms, especially those touching on sectors mentioned in the China 2025 plan, such as information technology, including Cloud and AI, will face a policy regime that increasingly squeezes their market share. Combined with the localization difficulties of the Chinese market for American firms given the speed, ferocity and determination of the local competition, the prospects for American technology firms in China are likewise not bright.

The future of Chinese technology companies in America is more unclear. While cybersecurity concerns have marred much of Chinese companies' entry into the U.S., most notably Huawei and ZTE in the past, there doesn't exist as much official policy barring them or restricting them from the American market long-term. Many of the issues that Chinese firms face in the U.S. are in terms of operational issues or more attractive substitutes, especially in light of cybersecurity concerns. In the short-term, it is likely that CFIUS will have a heavy hand in restricting Chinese M&A for sensitive technologies, which will impede Chinese expansion in the U.S. market, certainly. Currently, companies such as Alicloud and Tencent are not as attractive given the lack of data security these products offer, especially in terms of the opaque and often predatory nature of the Chinese intelligence system. Thus, American substitutes, such as Amazon Web Services or Microsoft Azure, are attractive options. However, there remains a huge amount of market potential for Chinese products in the U.S. with no direct substitutes. A good example recently is DJI drones. Despite any lingering cybersecurity concerns, there is no direct substitute for DJI drones in the domestic American market and the company has seen brisk sales in the U.S. market given its unique technology, becoming the number two selling drone in the U.S. American consumers, therefore, are likely to suspend much of their cybersecurity concerns in order to access a novel product. However, DJI has recently begun to experience a government backlash in the U.S., which could trickle down and shape consumer preferences. The same, hypothetically, could be applied to a novel software product, such as advanced AI analytics or hyper-cheap cloud computing storage options. All in all, Chinese technology products face a more lucrative future in the American market than American technology products in China, unless the U.S. begins to also embark on

executing a techno-nationalistic policy regime. For Chinese companies, today, however, challenges around security and adoption still abound.

Cybersecurity, still, remains a key challenge in a U.S.-China relation marred by mistrust, suspicion and often violation, and this issue has been compounded by the introduction of contradictory legislation regarding data access. The 2015 Xi-Obama Cybersecurity Agreement was landmark and represents an important viable path and mold that the two governments can follow in the creation of future cooperative policy. More such cooperation is needed to sort out disputes in cyberspace, especially when there exist policies that conflict with one another. For instance, the 2017 Cybersecurity Law in China states that data stored in China may not be transferred outside of the country without express permission. However, the 2018 CLOUD Act in the U.S. states that the U.S. government may access any data stored domestically or internationally by a U.S. based company. A hypothetical situation could occur where an American company in China is required by the U.S. to provide information and simultaneously restricted by China from transferring that same information. This happens occasionally in the international space, but key is to have cooperative mechanisms to smooth over such situations, or, even better, anticipate them in advance and work policy working groups to fix them head on. International cooperation between the U.S. and China and the creation of bilateral cyberspace working groups are needed in the future to discuss and formulate actual operational mechanisms to handle such situations in a diplomatic and fair manner.

Moreover, the U.S. and China should, ideally, work together to create mutually beneficial cybersecurity policy, aligned with safeguarding both their national interests, though the chances of this seem less likely given different policy making and implementation styles and the adversarial nature of U.S.-China relations today.

Works Cited

"18 U.S. Code Chapter 121 - STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS." *LII / Legal Information Institute*, Legal Information Institute, www.law.cornell.edu/uscode/text/18/part-I/chapter-121.

"About Microsoft's Presence in China." *Microsoft*, news.microsoft.com/about-microsofts-presence-in-china/.

"Announcing Amazon Elastic Compute Cloud (Amazon EC2) - Beta." *Amazon*, Amazon, 2006, aws.amazon.com/about-aws/whats-new/2006/08/24/announcing-amazon-elastic-compute-cloud-amazon-ec2---beta/.

"APT1 Exposing One of China's Cyber Espionage Units." *Mandiant*, 2013, www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

Areddy, James T. "American Entrepreneurs Who Flocked to China Are Heading Home, Disillusioned." *The Wall Street Journal*, Dow Jones & Company, 7 Dec. 2018, www.wsj.com/articles/american-entrepreneurs-who-flocked-to-china-are-heading-home-disillusioned-1544197068.

"Attorney General Jeff Sessions Announces New Initiative to Combat Chinese Economic Espionage." *The United States Department of Justice*, 7 Nov. 2018, www.justice.gov/opa/speech/attorney-general-jeff-sessions-announces-new-initiative-combat-chinese-economic-espionage.

"Attorney General Jeff Sessions Announces New Initiative to Combat Chinese Economic Espionage." *The United States Department of Justice*, 7 Nov. 2018, www.justice.gov/opa/speech/attorney-general-jeff-sessions-announces-new-initiative-combat-chinese-economic-espionage.

"Azure Operations in China vs. Global Azure." *Microsoft Docs*, docs.microsoft.com/en-us/azure/china/china-overview-operations.

Boehler, Patrick. "What You Need to Know About China's New National Security Law." *The New York Times*, The New York Times, 1 July 2015, sinosphere.blogs.nytimes.com/2015/07/01/what-you-need-to-know-about-chinas-new-national-security-law/?mtrref=undefined&gwh=BE1B95C6C87990A5A04494F949EEA45A&gwt=pay.

Bond, David. "Head of MI6 Warns of Huawei Security Concerns." *Financial Times*, Financial Times, 3 Dec. 2018, www.ft.com/content/40b35b84-f6ff-11e8-af46-2022a0b02a6c.

Bundy, Todd, and Michael Haley. "China's Cloud Cities." *ISEMAG*, 7 June 2016, www.isemag.com/2016/05/chinas-cloud-cities/.

Cadell, Cate. "Amazon Sells off China Cloud Assets as Tough New Rules Bite." *Reuters*, Thomson Reuters, 14 Nov. 2017, www.reuters.com/article/us-china-

amazon-cloud/amazon-sells-off-china-cloud-assets-as-tough-new-rules-bite-idUSKBN1DE0CL.

Cheng, Roger. “Some of the Hottest Android Phones Aren't Coming to the US...” *CNET*, CNET, 27 Mar. 2018, www.cnet.com/news/why-some-of-the-flashiest-huawei-android-p20-p20-pro-mate-10-pro-phones-arent-in-the-us/.

Chigne, Jean-Pierre. “Huawei Planning On Entering US Market In February Through AT&T.” *Tech Times*, 29 Dec. 2017, www.techtimes.com/articles/217706/20171229/huawei-planning-entering-u-s-market-february-through-t.htm.

“China Enacts New National Security Law.” *Covington*, 2015, www.cov.com/~/media/files/corporate/publications/2015/06/china_passes_new_national_security_law.pdf.

“China’s Cloud Computing Policies and Implications for Foreign Industry.” *United States Information Technology Office*, 2012, cryptome.org/2012/12/usito-china-cloud.pdf.

“Chinese National Who Conspired to Hack into U.S. Defense Contractors' Systems Sentenced to 46 Months in Federal Prison.” *The United States Department of Justice*, 11 Aug. 2016, www.justice.gov/opa/pr/chinese-national-who-conspired-hack-us-defense-contractors-systems-sentenced-46-months.

Coles, Cameron. “AWS vs Azure vs Google Cloud Market Share 2018 Report.” *Skyhigh*, Skyhigh Networks, 12 Sept. 2018, www.skyhighnetworks.com/cloud-security-blog/microsoft-azure-closes-iaas-adoption-gap-with-amazon-aws/.

Columbus, Louis. “Roundup Of Cloud Computing Forecasts And Market Estimates, 2018.” *Forbes*, Forbes Magazine, 24 Sept. 2018, www.forbes.com/sites/louiscolumbus/2018/09/23/roundup-of-cloud-computing-forecasts-and-market-estimates-2018/#55bc055e507b.

“Communications Assistance for Law Enforcement Act.” *Federal Communications Commission*, 6 Oct. 2017, www.fcc.gov/public-safety-and-homeland-security/policy-and-licensing-division/general/communications-assistance.

Davis, Julie Hirschfeld. “Obama Hints at Sanctions Against China Over Cyberattacks.” *The New York Times*, The New York Times, 21 Dec. 2017, www.nytimes.com/2015/09/17/us/politics/obama-hints-at-sanctions-against-china-over-cyberattacks.html.

“Decision of the Standing Committee of the National People's Congress on Strengthening Information Protection on Networks [Effective] 全国人大常委会关于加强网络信息保护的决定 [现行有效].” *Peking University Center for Legal Information* , 2012, en.pkulaw.cn/display.aspx?cgid=191975&lib=law.

Deutscher, Maria. “Report Says Alibaba Halted U.S. Cloud Expansion, Company Denies Change.” *SiliconANGLE*, 3 Sept. 2018, siliconangle.com/2018/08/31/report-alibaba-quietly-halted-u-s-cloud-expansion/.

Dignan, Larry. “Top Cloud Providers: How AWS, Microsoft, Google, IBM, Oracle, Alibaba Stack Up.” *ZDNet*, ZDNet, 16 Jan. 2019, www.zdnet.com/article/top-cloud-providers-2018-how-aws-microsoft-google-ibm-oracle-alibaba-stack-up/.

“Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510-22.” *Justice Information Sharing*, it.ojp.gov/PrivacyLiberty/authorities/statutes/1285.

Erdenebileg , Zolzaya, and Weining Hu. “Made in China 2025: Implications for Foreign Businesses.” *China Briefing News*, 24 Oct. 2018, www.china-briefing.com/news/made-in-china-2025-implications-for-foreign-businesses/.

“Establishing a Data Center in China.” *China Briefing News*, 28 Nov. 2018, www.china-briefing.com/news/setting-shop-guide-chinas-data-centers/.

Eustice, John C. “Understanding Data Privacy and Cloud Computing.” *Legal Cases - Westlaw | Thomson Reuters Legal*, legal.thomsonreuters.com/en/insights/articles/understanding-data-privacy-and-cloud-computing.

“Executive Order -- ‘Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities.’” *National Archives and Records Administration*, National Archives and Records Administration, 2015, obamawhitehouse.archives.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m.

“FACT SHEET: President Xi Jinping's State Visit to the United States.” *National Archives and Records Administration*, National Archives and Records Administration, obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

Farley, Robert. “Did the Obama-Xi Cyber Agreement Work?” *The Diplomat*, The Diplomat, 11 Aug. 2018, thediplomat.com/2018/08/did-the-obama-xi-cyber-agreement-work/.

Feigenbaum, Evan A. “The Deep Roots and Long Branches of Chinese Technonationalism.” *Carnegie Endowment for International Peace*, 2017, carnegieendowment.org/2017/08/12/deep-roots-and-long-branches-of-chinese-technonationalism-pub-72815.

“Foreign Economic Espionage in Cyberspace.” *NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER*, 2018, www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf.

Garsd, Jasmine. “The History Of Tech Giant Huawei And The Chinese Government.” *NPR*, NPR, 7 Dec. 2018, www.npr.org/2018/12/07/674467994/huawei-and-the-chinese-government.

“Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.3 Percent in 2019.” *Gartner IT Glossary*, Gartner, Inc., 2018, www.gartner.com/en/newsroom/press-releases/2018-09-12-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-17-percent-in-2019.

Goldstein, Matthew, et al. “How a National Security Investigation of Huawei Set Off an International Incident.” *The New York Times*, The New York Times, 14 Dec. 2018, www.nytimes.com/2018/12/14/business/huawei-meng-hsbc-canada.html.

“H.R.4943 - 115th Congress (2017-2018): CLOUD Act.” *Congress.gov*, 6 Feb. 2018, www.congress.gov/bill/115th-congress/house-bill/4943.

Horowitz, Julia. “How Huawei's CFO Ended up in a Jail in Canada.” *CNN*, Cable News Network, 11 Dec. 2018, www.cnn.com/2018/12/11/business/huawei-cfo-arrest-details/index.html.

Huang, Keman, et al. *How Can Cybersecurity and International Trade Impact Each Other: A Systematic Framework*. 2018.

“Huawei's 2017 Annual Report: Solid Performance and Lasting Value for Customers - Huawei Press Center.” *Huawei*, 30 Mar. 2018, www.huawei.com/en/press-events/news/2018/3/Huawei-2017-Annual-Report.

“IDC发布，中国公有云市场份额排名！.” *搜狐网*, 19 May 2017, www.sohu.com/a/141983144_258957.

“IDC：2015年中国公有云计算报告 阿里云市场份额达31%.” *199it*, 2016, www.199it.com/archives/508703.html.

“Introduction to Guizhou-Cloud Big Data Industry Co., Ltd.” *Guizhou-Cloud Big Data*, english.gzdata.com.cn/c101/index.html.

“Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE.” *U.S. House of Representatives*, 2012, intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf.

Isaacs, Julien. “CFIUS: The Failed Takeover of MoneyGram by Ant Financial.” *Julien Isaacs U.S.-China Global Brand Consultancy中美品牌咨询公司*, 14 June 2018, julienisaacs.com/index.php/2018/06/14/cfius-the-failed-takeover-of-moneygram-by-ant-financial/.

Jackson, Kevin. “The Economic Benefit of Cloud Computing.” *Forbes*, Forbes Magazine, 12 May 2012, www.forbes.com/sites/kevinjackson/2011/09/17/the-economic-benefit-of-cloud-computing/#2a93d6f5225c.

Jiang, Sijia. “Huawei's AT&T U.S. Smartphone Deal Collapses.” *Reuters*, Thomson Reuters, 9 Jan. 2018, www.reuters.com/article/us-at-t-huawei-tech/huaweis-att-u-s-smartphone-deal-collapses-idUSKBN1EX29E.

Jones, Penny. “21Vianet Teams with Microsoft for Shanghai-Based Cloud Offering.” *DCD*, 22 Nov. 2012, www.datacenterdynamics.com/news/21vianet-teams-with-microsoft-for-shanghai-based-cloud-offering/.

Kazim, Muhammad, et al. *Security Aspects of Virtualization in Cloud Computing*. HAL, 2017, hal.inria.fr/hal-01496070/document.

Lardinois, Frederic. “Microsoft Launches Two New Azure Regions in China.” *TechCrunch*, TechCrunch, 27 June 2018, techcrunch.com/2018/06/27/microsoft-launches-two-new-azure-regions-in-china/.

Liao, Shannon. “Apple Officially Moves Its Chinese ICloud Operations and Encryption Keys to China.” *The Verge*, The Verge, 28 Feb. 2018, www.theverge.com/2018/2/28/17055088/apple-chinese-icloud-accounts-government-privacy-speed.

Liu, Wentao. “Research on Cloud Computing Security Problem and Strategy .” *2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)*, 2012, ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6202020.

Madnick, Stuart, and John Donovan. "Application and Analysis of the Virtual Machine Approach to Information System Security and Isolation." Contents: Using the Digital Library, ACM, 1973, dl.acm.org/citation.cfm?id=803961.

Mak, Aaron. “Congress Put the Controversial CLOUD Act in Its Spending Bill. What Does That Mean For Data Privacy?” *Slate Magazine*, Slate, 22 Mar. 2018, slate.com/technology/2018/03/cloud-act-microsoft-justice-department-omnibus-spending-bill.html.

Marks, Paul. “Cybersecurity and the Parkerian Hexad.” *European Niche Technology Recruitment - StaffHost*, 2018, www.staffhost.co.uk/blog/2018/10/cybersecurity-and-the-parkerian-hexad.

McLaughlin, Kevin. “Alibaba Puts the Brakes on U.S. Cloud Expansion.” *The Information*, 2018, www.theinformation.com/articles/alibaba-puts-the-brakes-on-u-s-cloud-expansion?jwt=eyJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJtcmp1bGllbmlzYWFjc0BnbWFpbC5jb20iLCJleHAiOjE1Nzk0OTE5MTksIm4iOiJHdWVzdCIsInNjb3BlIjpbInNoYXJlIl19.hZYDYKeQGrrbbnQgSslE5WEO1gT8JK_w1LHunxcqqNc&unlock=fbcd594fcdd32d70.

Mell, Peter, and Timothy Grance. “The NIST Definition of Cloud Computing.” *National Institute of Standards and Technology*, 2011, nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

“Microsoft in China: 20 Years of Playing By The Rules.” *Sampi.co*, 2016, sampi.co/microsoft-in-china-20-years/.

Miller, Ron. “Alibaba Cloud Growing like Gangbusters, but Still Far behind AWS and Other Market Leaders.” *TechCrunch*, TechCrunch, 6 Feb. 2018, techcrunch.com/2018/02/06/alibaba-cloud-growing-like-gangbusters-but-still-far-behind-aws-and-other-market-leaders/.

Mosbah Magdy, Mohamed, et al. “CURRENT SERVICES IN CLOUD COMPUTING: A SURVEY.” *International Journal of Computer Science, Engineering and Information Technology (IJCSEIT)*, 2013, pdfs.semanticscholar.org/3594/79fbca56b4b1295734b8c4c16af0d17273f2.pdf.

Mozur, Paul. “ZTE Document Raises Questions About Huawei and Sanctions.” *The New York Times*, The New York Times, 21 Dec. 2017, www.nytimes.com/2016/03/19/technology/zte-document-raises-questions-about-huawei-and-sanctions.html.

Nakazawa, Katsuji. “Xi, Huawei and China's Powerful Military-Industrial Complex.” *Nikkei Asian Review*, Nikkei Asian Review, 13 Dec. 2018, asia.nikkei.com/Editor-s-Picks/China-up-close/Xi-Huawei-and-China-s-powerful-military-industrial-complex.

“Overview of China’s Cybersecurity Law.” *KPMG China*, 2017, https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf.

Panettieri, Joe. “Cloud Market Share 2018.” *ChannelE2E*, 2018, www.channele2e.com/event/google-cloud-next-2018/.

Parker, Donn. *Fighting Computer Crime: a New Framework for Protecting Information*. ACM, 1998, dl.acm.org/citation.cfm?id=286060.

Pender-Bey, Georgie. “THE PARKERIAN HEXAD.” *Information Security Program at Lewis University*, cs.lewisu.edu/mathcs/msisprojects/papers/georgiependerbey.pdf.

Porter, M. (1980). Competitive strategy. New York: Free Press.

“Public Cloud Expansion Drives Double-Digit Growth of Worldwide Cloud IT Infrastructure Revenues in the Fourth Quarter of 2017, According to IDC.” *IDC: The Premier Global Market Intelligence Company*, 2018, www.idc.com/getdoc.jsp?containerId=prUS43705018.

Ragland, Leigh Ann, et al. “Red Cloud Rising: Cloud Computing in China.” *U.S.-China Economic and Security Review Commission*, 2013, www.uscc.gov/sites/default/files/Research/DGI_Red%20Cloud%20Rising_2014.pdf.

“Red Line Drawn: China Recalculates Its Use of Cyber Espionage.” *Fireeye ISight Intelligence*, 2016, www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf.

Regalado, Antonio. “Who Coined 'Cloud Computing'?” *MIT Technology Review*, MIT Technology Review, 30 Dec. 2013, www.technologyreview.com/s/425970/who-coined-cloud-computing/.

Robertson, Jordan, and Michael Riley. “The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies.” *Bloomberg.com*, Bloomberg, 2018, www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies.

Rouse, Margaret. “What Is BPaaS (Business Process as a Service)? - Definition from WhatIs.com.” *SearchERP*, searcherp.techtarget.com/definition/BPaaS-Business-Process-as-a-Service.

Ruparelia, Nayan. *Cloud Computing*. The MIT Press, 2016.

Russell, Jon. “Amazon Reportedly Offloaded Its Chinese Server Business Because It Was Compromised.” *TechCrunch*, TechCrunch, 4 Oct. 2018, techcrunch.com/2018/10/04/amazon-aws-china-server-business/.

Sanger, David E., and Katie Benner. “U.S. Accuses Chinese Nationals of Infiltrating Corporate and Government Technology.” *The New York Times*, The New York Times, 20 Dec. 2018, www.nytimes.com/2018/12/20/us/politics/us-and-other-nations-to-announce-china-crackdown.html.

Segal, Adam. “The U.S.-China Cyber Espionage Deal One Year Later.” *Council on Foreign Relations*, Council on Foreign Relations, 2016, www.cfr.org/blog/us-china-cyber-espionage-deal-one-year-later.

Segal, Adam. “Year in Review: Huawei and the Technology Cold War.” *Council on Foreign Relations*, Council on Foreign Relations, 2018, www.cfr.org/blog/year-review-huawei-and-technology-cold-war.

Stolyar, Brenda, and Christian de Looper. “ZTE Resumes Business Once Again as U.S. Lifts Ban on Suppliers.” *Digital Trends*, Digital Trends, 13 July 2018, www.digitaltrends.com/mobile/commerce-bans-zte-from-exporting-technology-from-the-us/.

Sun, Ping. “Interview with Sun Ping.” 15 Nov. 2018.

Synergy Research Group. “Cloud Growth Rate Increased Again in Q1; Amazon Maintains Market Share Dominance.” *Synergy Research Group*, 2018, www.srgresearch.com/articles/cloud-growth-rate-increased-again-q1-amazon-maintains-market-share-dominance.

“The CLOUD Act, Bridging the Gap between Technology and the Law.” *The National Law Review*, National Law Review, 2018, www.natlawreview.com/article/cloud-act-bridging-gap-between-technology-and-law.

“The USA PATRIOT Act: Preserving Life and Liberty .” *The United States Department of Justice*, www.justice.gov/archive/ll/highlights.htm.

“Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information.” *The United States Department of Justice*, 20 Dec. 2018, www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion.

“Types of Cloud Computing.” *Amazon*, Amazon Web Services, aws.amazon.com/types-of-cloud-computing/.

“U.S. Accuses China of Violating Bilateral Anti-Hacking Deal.” *Reuters*, Thomson Reuters, 9 Nov. 2018, www.reuters.com/article/us-usa-china-cyber/u-s-accuses-china-of-violating-bilateral-anti-hacking-deal-idUSKCN1NE02E.

“U.S.-China Law Enforcement and Cybersecurity Dialogue.” *U.S. Department of State*, U.S. Department of State, 3 Oct. 2017, www.state.gov/r/pa/prs/ps/2017/10/274590.htm.

"United States V. Huawei Device Co. Ltd." *UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF WASHINGTON 8 AT SEATTLE* , 2018, www.justice.gov/opa/press-release/file/1124996/download.

Wagner, Jack. "China's Cybersecurity Law: What You Need to Know." *The Diplomat*, The Diplomat, 1 June 2017, thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/.

Watts, Stephen. "SaaS vs PaaS vs IaaS: What's The Difference and How To Choose." *BMC Blogs*, 2017, www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/.

"What Is Cloud Computing? A Beginner's Guide | Microsoft Azure." *A Beginner's Guide | Microsoft Azure*, azure.microsoft.com/en-us/overview/what-is-cloud-computing/.

Williams, Pete. "Supreme Court Seems Set to Rule against Microsoft in Email Privacy Case." *NBCNews.com*, NBCUniversal News Group, 2018, www.nbcnews.com/politics/supreme-court/gov-t-battles-microsoft-email-privacy-case-supreme-court-n851216.

Wu, Mark. "The 'China, Inc.' Challenge to Global Trade Governance." *Harvard International Law Journal*, 2016, http://www.harvardilj.org/wp-content/uploads/HLI210_crop.pdf.

Ye, Juliet. "QQ-360 Battle Escalates into War." *The Wall Street Journal*, Dow Jones & Company, 5 Nov. 2010, blogs.wsj.com/chinarealtime/2010/11/05/qq-360-battle-escalates-into-war/.

Zaagman, Elliott. "Meng Wanzhou: China's 'Tantrum Diplomacy' and Huawei." *The Interpreter*, The Interpreter, 14 Dec. 2018, www.lowyinstitute.org/the-interpreter/china-tantrum-diplomacy-huawei.

Zable, Stephanie. "The Foreign Investment Risk Review Modernization Act of 2018." *Lawfare*, 6 Aug. 2018, www.lawfareblog.com/foreign-investment-risk-review-modernization-act-2018.

"《云计算发展三年行动计划（2017 - 2019年）》解读." *中华人民共和国工业和信息化部*, 2017, www.miit.gov.cn/n1146295/n1652858/n1653018/c5570632/content.html.

"中华人民共和国电信条例." *中华人民共和国工业和信息化部*, 2016, www.miit.gov.cn/n1146295/n1146557/n1146619/c4860613/content.html.

"中华人民共和国网络安全法." *度小法-百度智能法律产品*, 2017, duxiaofa.baidu.com/detail?searchType=statute&from=aladdin_28231&originquery=%E7%BD%91%E7%BB%9C%E5%AE%89%E5%85%A8%E6%B3%95&count=79&cid=f66f830e45c0490d589f1de2fe05e942_law.

"全国人大常委会关于加强网络信息保护的决定." *中华人民共和国中央人民政府*, 2012, www.gov.cn/jrzg/2012-12/28/content_2301231.htm.

“国务院关于加快培育和发展 战略性新兴产业的决定.” *中华人民共和国中央人民政府*, 2010, www.gov.cn/zwgk/2010-10/18/content_1724848.htm.

姜 维. “2018中国云计算产业竞争格局分析 阿里云占市场近半份额.” *PCOnline*, 8 Mar. 2018, servers.pconline.com.cn/1091/10917424.html.