Excerpts from SEC488

Doing Cloud in China

SANS Cloud Security Summit 2020

ABSTRACT:
China is the only country in the world that does not permit foreign cloud service providers to own and operate their own data centers in the country. To operate a data center in China, a locally registered company that has less than 50% foreign investment must obtain a value-added telecom permit. This talk looks at how Amazon Web Services (AWS) and Microsoft Azure have modified their services to gain entry to the cloud market space in China and compares their service offerings to local Chinese cloud service providers. We will cover specific considerations for foreign companies using cloud services in China. The Chinese company, Alibaba Cloud, is the fourth largest global Infrastructure-as-a-Service provider following AWS, Azure, and Google Cloud Platform. We end the session taking a test drive of Alibaba Cloud and discuss why this CSP should be on your watchlist. NOTE: This talk provides a preview of some content from *SANS SEC488: Cloud Security Essentials*.

About Me

"I help my clients earn and maintain the trust of their customers"

Kenneth G. Hartman

- BS Electrical Engineering, Michigan Technological University
- MS Information Security Engineering, SANS Technology Institute
- Multiple Security Certifications: CISSP, GIAC Security Expert, etc.
- Certified SANS Instructor – SEC545 Cloud Security Architecture & Operations
- Co-Author – SEC488 Cloud Security Essentials

www.kennethghartman.com
@kennethghartman

The content and opinions in this presentation are my own and do not necessarily reflect the positions, strategies, or opinions of any current or previous employer.

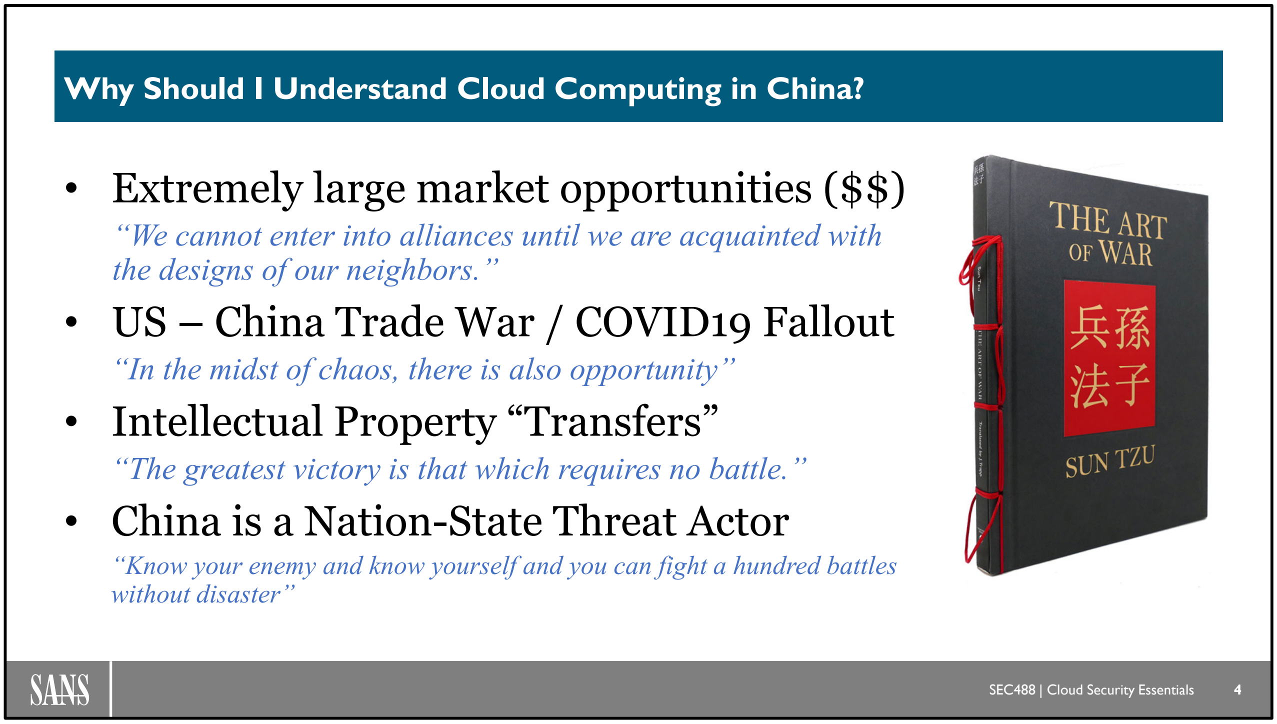
SANS

Kenneth G. Hartman - BIO

Kenneth G. Hartman is a security engineering leader in Silicon Valley and teaches the "Security 545 - Cloud Security, Architecture, and Operations" Course for the SANS Institute. Ken has worked for a variety of Cloud Service Providers in Architecture, Engineering, Compliance, and Security Product Management roles. From 2002-2011, Ken helped launch and lead a company called Visonex into a profitable, nation-wide dialysis-specific electronic medical record using a software-as-a-service (SaaS) business model. Ken holds a BS Electrical Engineering from Michigan Technological University and a Masters Degree in Information Security Engineering from SANS Technology Institute. Ken has earned the CISSP, as well as multiple GIAC security certifications, including the GIAC Security Expert.

Topics

- Why China?
- Global Market Data
- Cloud Service Providers in China
- Operational Requirements & Permits
- AWS China
- Azure China
- Alibaba – Hands On
- Going Further



Why Should I Understand Cloud Computing in China?

- Extremely large market opportunities ($$)

  “We cannot enter into alliances until we are acquainted with the designs of our neighbors.”

- US – China Trade War / COVID19 Fallout

  “In the midst of chaos, there is also opportunity”

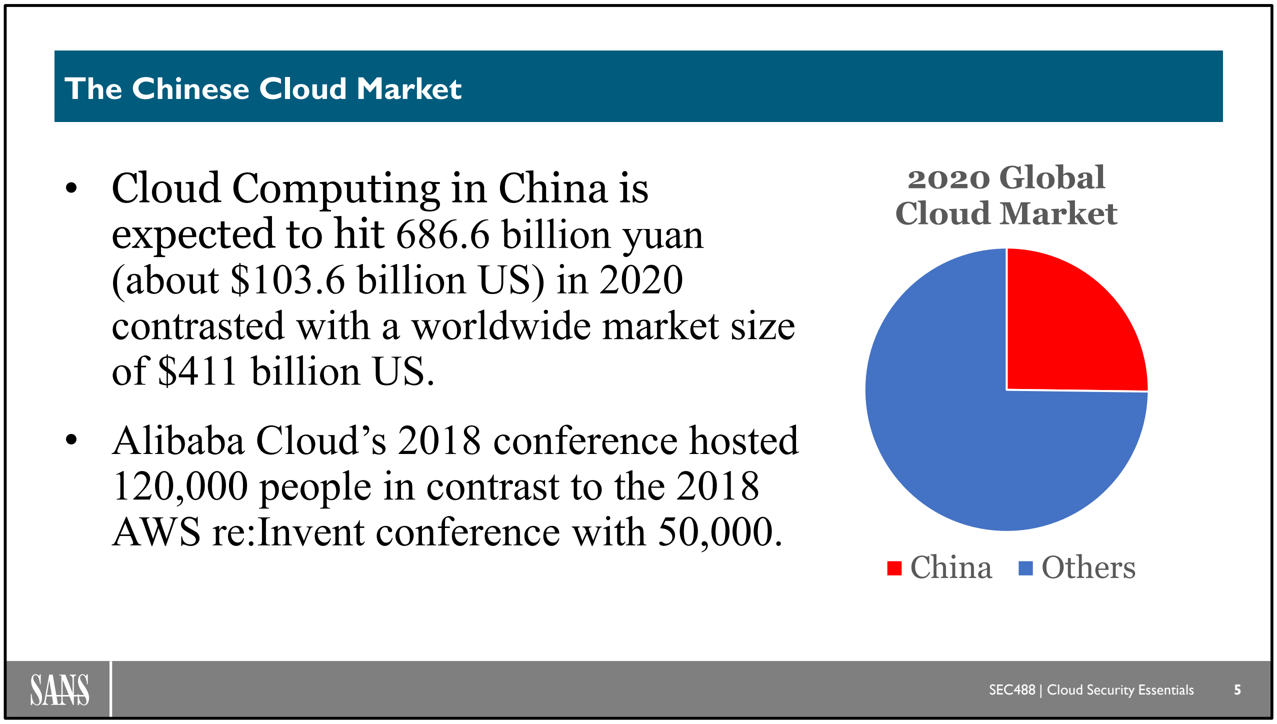
- Intellectual Property “Transfers”

  “The greatest victory is that which requires no battle.”

- China is a Nation-State Threat Actor

  “Know your enemy and know yourself and you can fight a hundred battles without disaster”

[1] Quotes of Sun Tzu - https://www.goodreads.com/author/quotes/1771.Sun_Tzu



The Chinese Cloud Market

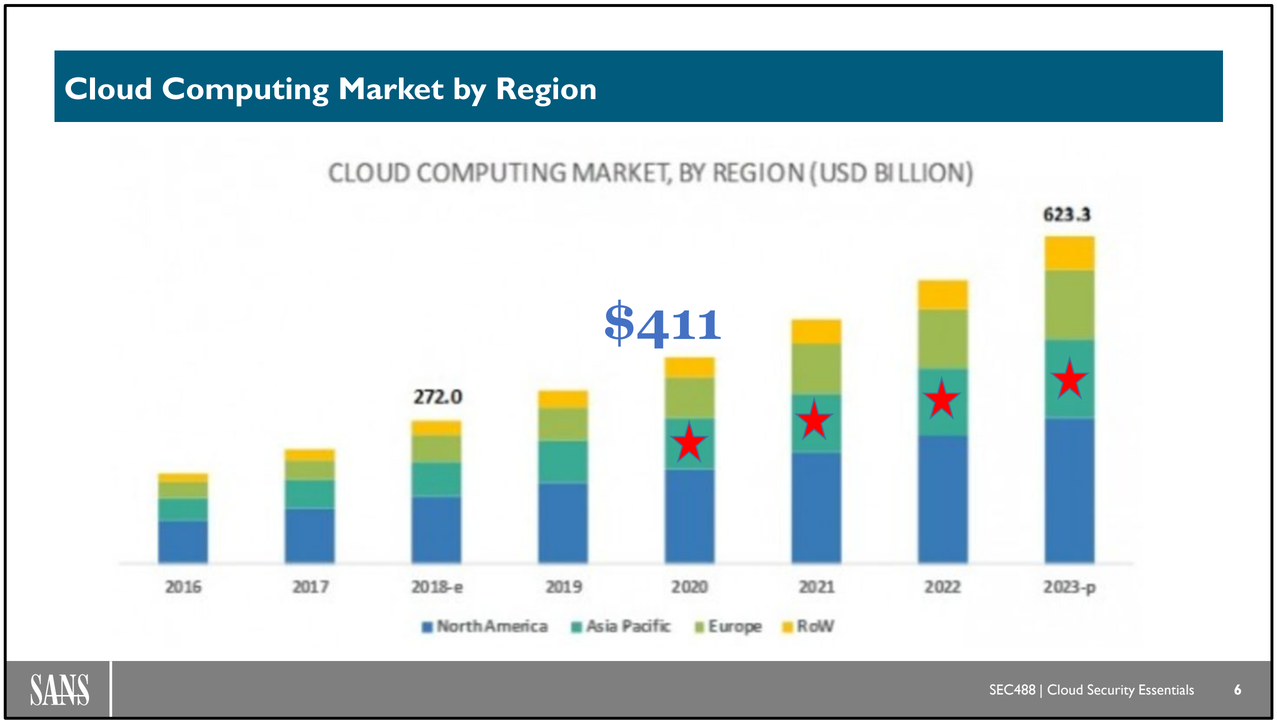
- Cloud Computing in China is expected to hit 686.6 billion yuan (about $103.6 billion US) in 2020 contrasted with a worldwide market size of $411 billion US.
- Alibaba Cloud's 2018 conference hosted 120,000 people in contrast to the 2018 AWS re:Invent conference with 50,000.

Without a doubt, everyone has their eyes on the Chinese Cloud Services market. A 2017 report [1] forecasted the China market to grow to 686.6 billion yuan (about $103.6 billion) in 2020. This is a quarter of the projected worldwide market of $411 billion.

One indicator of the keen interest in the cloud in China is the 120,000 attendee that gathered at Alibaba's 2018 cloud conference. For reference, the attendance at AWS re:Invent (the largest US conference) was 50,000 that same year [2]. NOTE: No attendance numbers available for the 2019 Alibaba Cloud Computing Conference.

While the opportunities are great, so are the challenges. Chinese companies' biggest concerns with moving to the cloud are focused on the costs and difficulties of moving to the cloud followed closely with concerns around security, according to the 2018 McKinsey China Cloud Survey [3].

[1] https://url.sec488.com?id=74
[2] https://url.sec488.com?id=73
[3] https://url.sec488.com?id=83
[4] https://url.sec488.com?id=84 (Link deprecated)

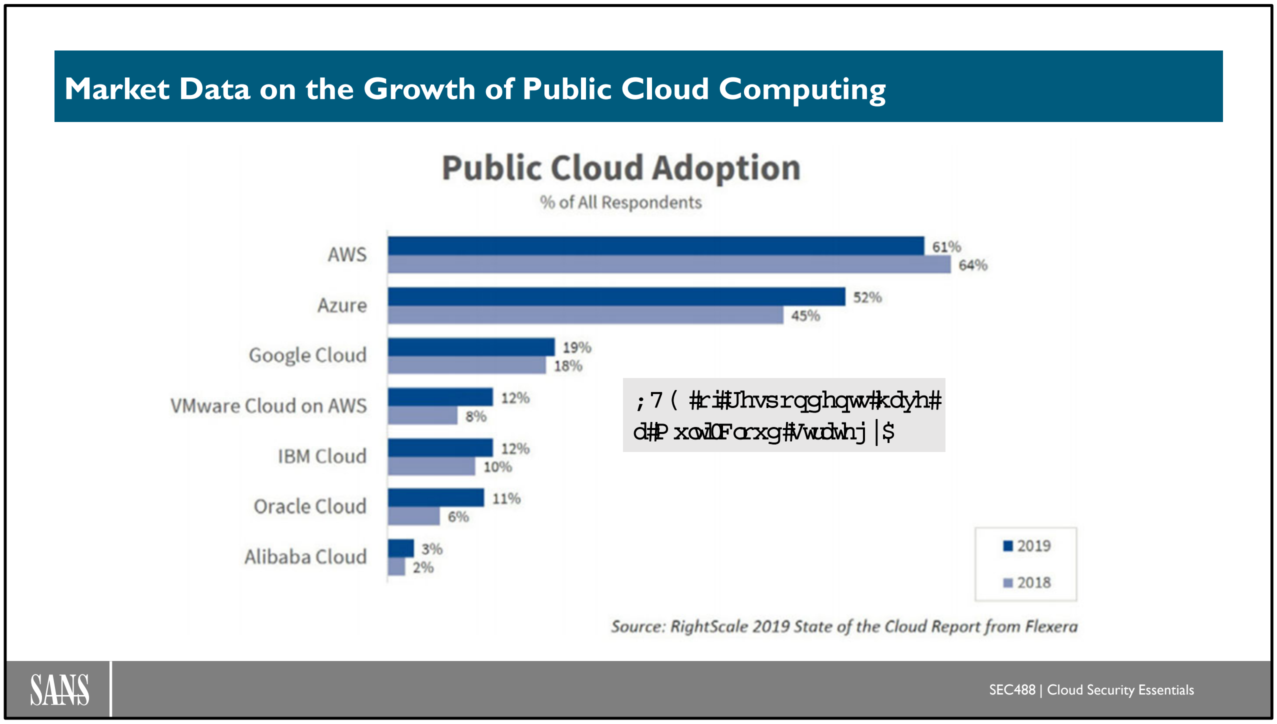


Cloud Computing Market by Region

SANS

According to a September 2019 report, The global market for cloud computing is expected to exceed $623 Billion US Dollars by 2023 [1,2]. The chart above breaks down the growth by region of the world.

[1] https://url.sec488.com?id=63
[2] https://url.sec488.com?id=64



Market Data on the Growth of Public Cloud Computing

;7(#ri#Uhvsrqghqw#kdyh#
d#Pxowl0Forxg#Vwudwhj|$

Source: RightScale 2019 State of the Cloud Report from Flexera

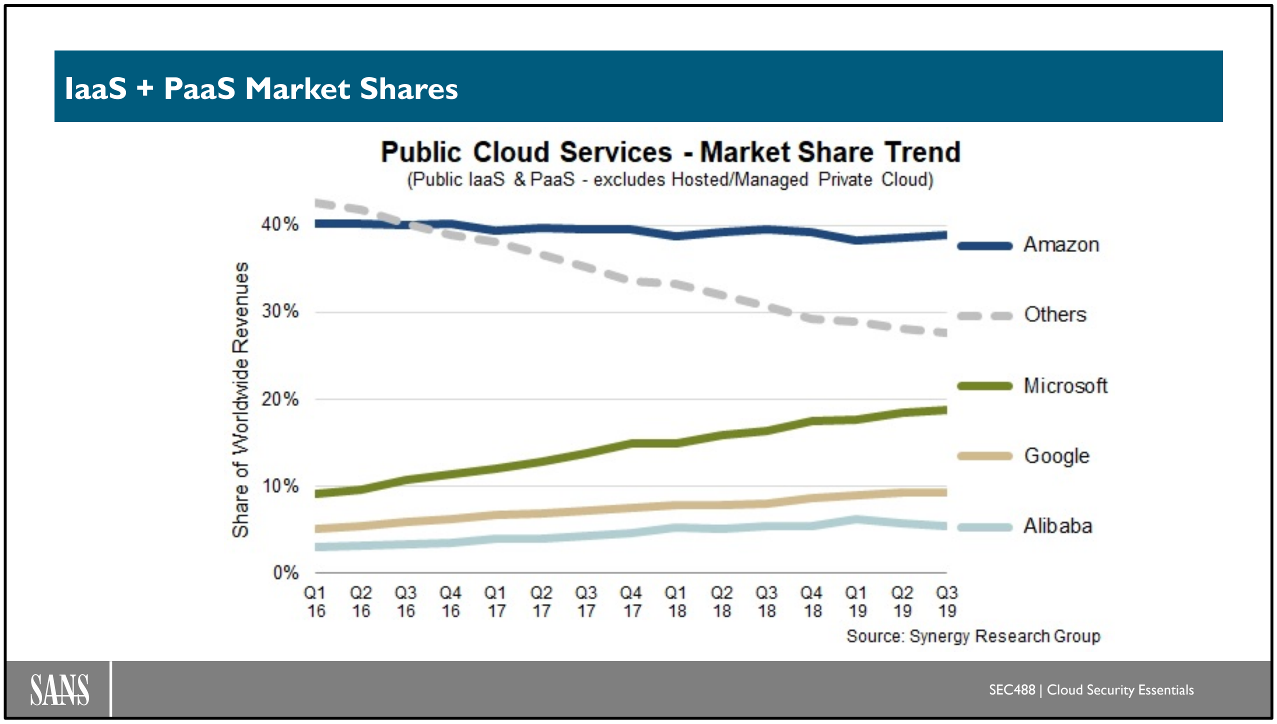
This slide shows data from the RightScale 2019 State of the Cloud Report [1].

Interestingly, in 2017 AWS Had 57% adoption, Azure had 34%, and GCP had 15%
This 2019 survey found that 84% of respondents had a multi-cloud strategy and were running applications in an average of 3.4 clouds and experimenting with 1.8 more for a total average of 4.9 clouds!

This slide shows which cloud service providers are being used, while the slide on the next page shows how much each provider is being used.

[1] https://url.sec488.com?id=57

[1] https://url.sec488.com?id=58



IaaS + PaaS Market Shares

Source: Synergy Research Group

SANS

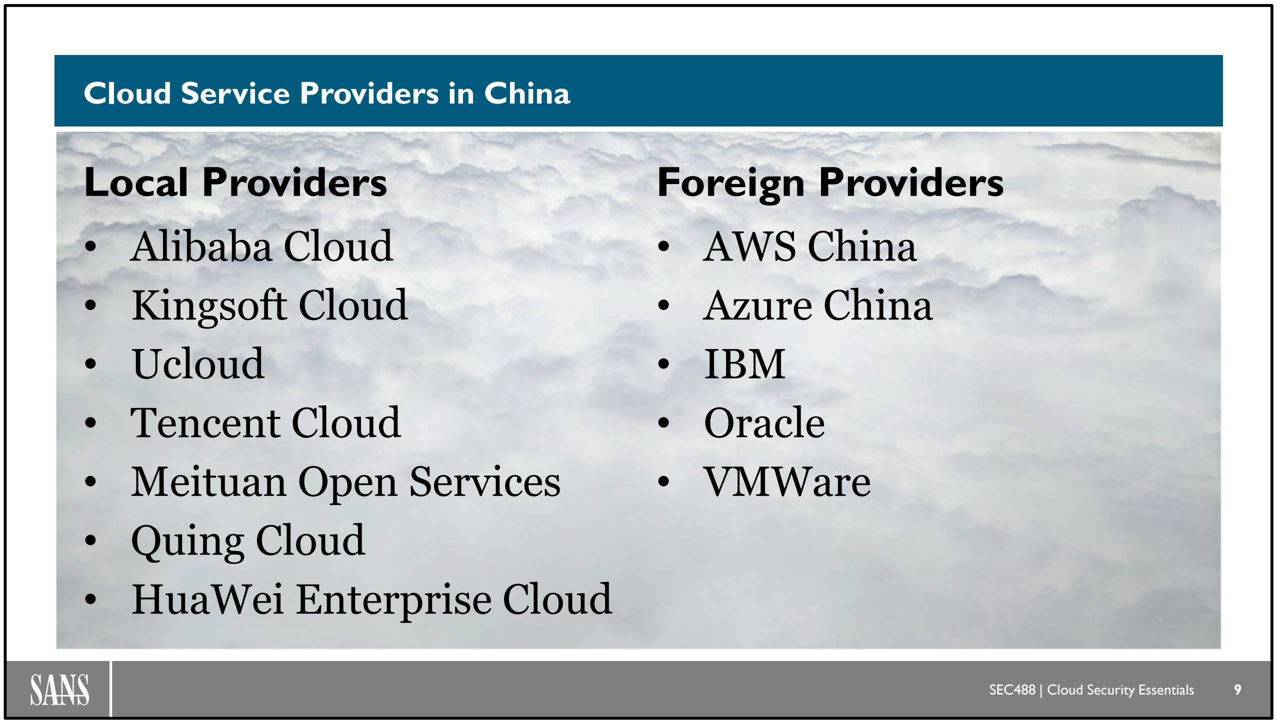
SEC488 | Cloud Security Essentials

According to the Synergy Research Group [1], Amazon is still the market leader by a significant margin. Microsoft is aggressively ramping up its cloud campaign in terms of maturing its cloud offerings as well as its and marketing efforts.

Google is definitely a player with solid cloud products and loyal customers, however it has made a strategic decision not to compete in China

Alibaba will be certainly important to track as well, particularly as they expand their footprint outside of China.

[1] https://url.sec488.com?id=59



Cloud Service Providers in China

Local Providers

- Alibaba Cloud
- Kingsoft Cloud
- Ucloud
- Tencent Cloud
- Meituan Open Services
- Quing Cloud
- HuaWei Enterprise Cloud

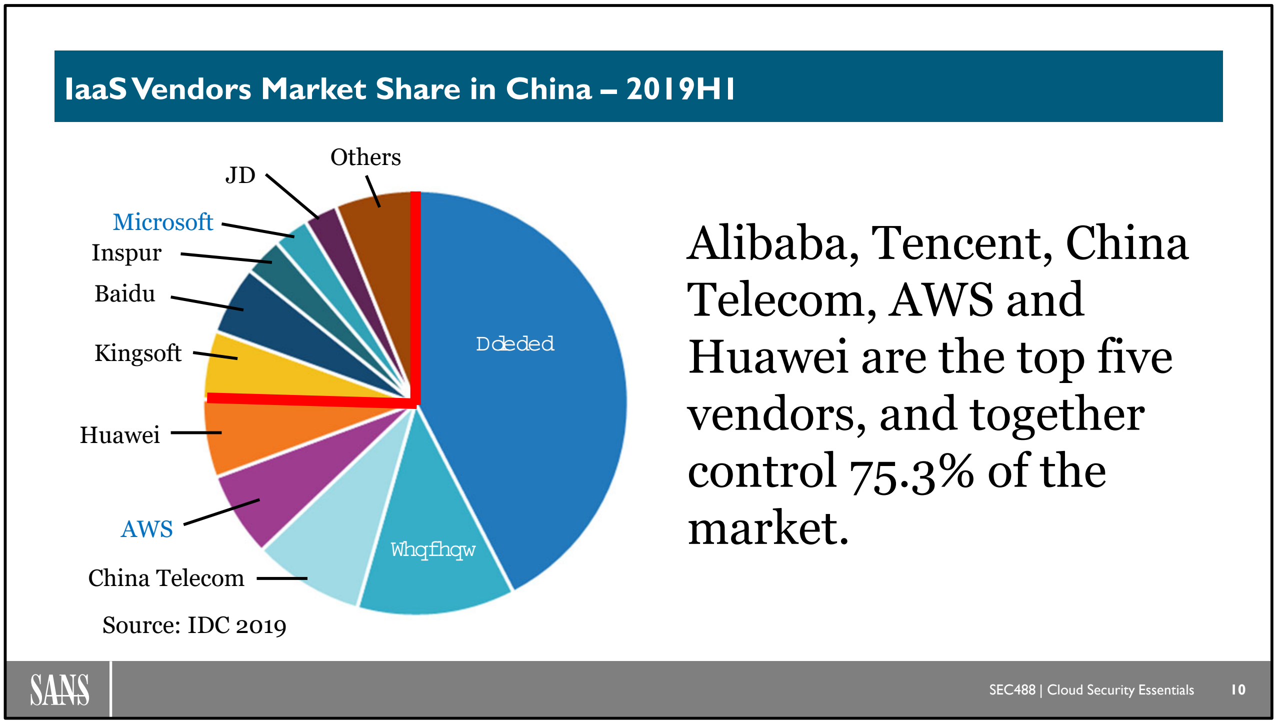
Foreign Providers

- AWS China
- Azure China
- IBM
- Oracle
- VMWare

Alibaba Cloud is the largest provider in China, but there are several domestic CSP's including Tencent (the creator of WeChat) and Kingsoft Cloud. [1,2]. According to a 2015 report [3], AWS is the sixth largest provider in China, with about 4.3% market share. This same report put IBM in the 11th position at 0.1% market share. Oracle and VMWare are referenced in [3] but no market data is provided.

At the present time, Google does not have a cloud service offering in China. Google has had a troubled relationship with China from the Operation Aurora Attack [5] to its attempt to offer a search engine that complies with China's censorship requirements [6].

[1] https://url.sec488.com?id=77
[2] https://url.sec488.com?id=78 {Link is deprecated}
[3] https://url.sec488.com?id=79
[5] https://url.sec488.com?id=81
[6] https://url.sec488.com?id=82

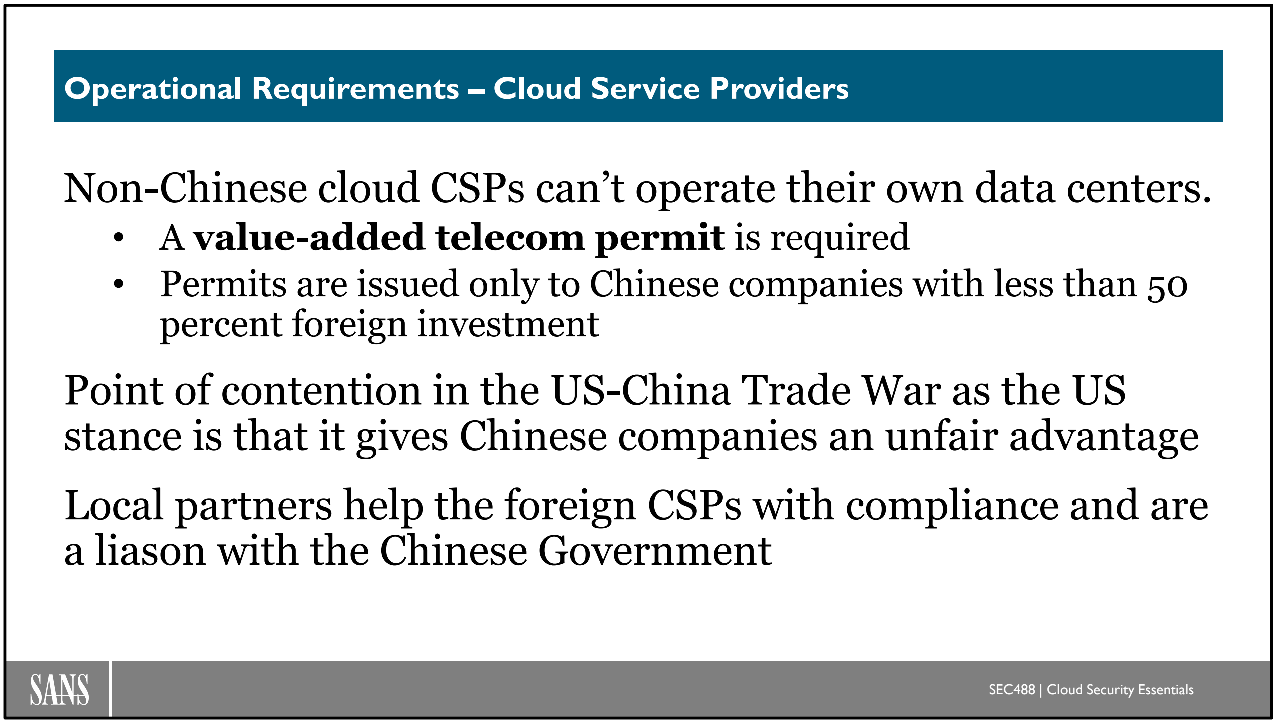


IaaS Vendors Market Share in China – 2019H1

Source: IDC 2019

Alibaba, Tencent, China Telecom, AWS and Huawei are the top five vendors, and together control 75.3% of the market.

[1] https://www.idc.com/getdoc.jsp?containerId=prCHE45761819
[2] https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/public-cloud-in-china-big-challenges-big-upside



Operational Requirements – Cloud Service Providers

Non-Chinese cloud CSPs can’t operate their own data centers.

- A **value-added telecom permit** is required
- Permits are issued only to Chinese companies with less than 50 percent foreign investment

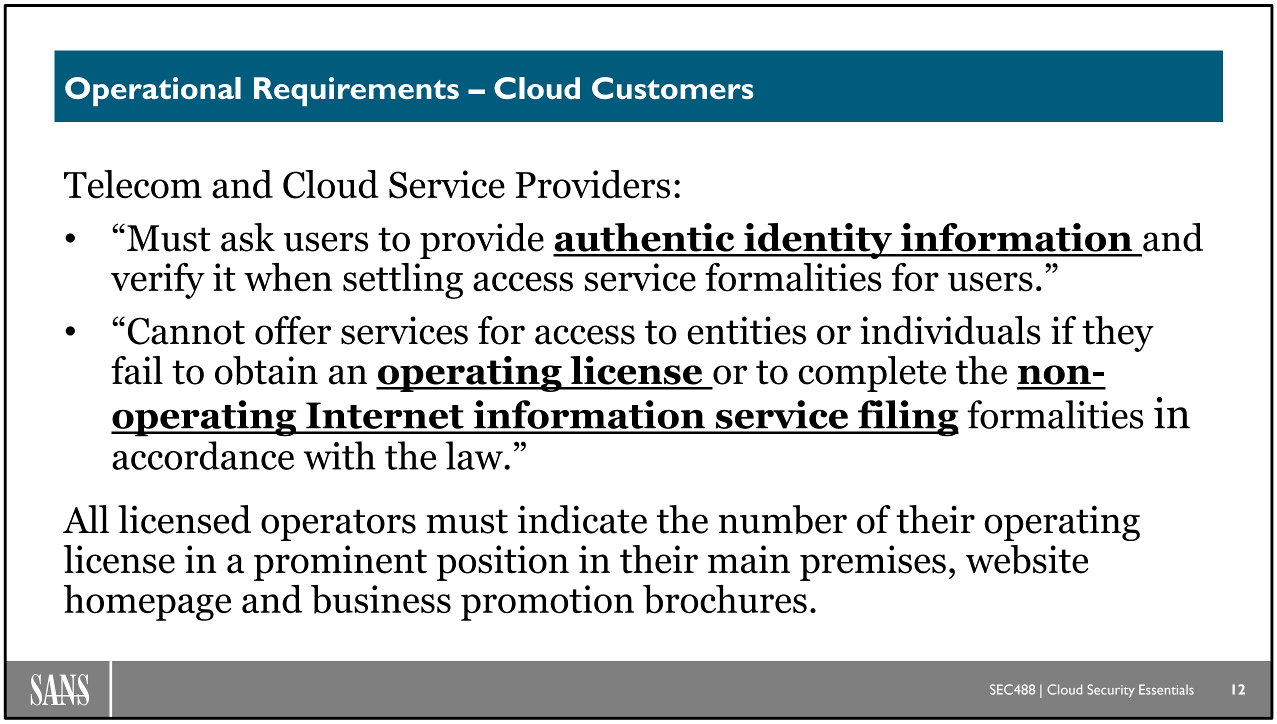
Point of contention in the US-China Trade War as the US stance is that it gives Chinese companies an unfair advantage

Local partners help the foreign CSPs with compliance and are a liason with the Chinese Government

China is the only country in the world that does not permit foreign cloud service providers to own and operate their own data centers in the country. To operate a data center in China, a locally registered company that has less than 50% foreign investment must obtain a value-added telecom permit. This permit requirement is a point of contention in the US-China trade war as the US has taken the position that it gives Chinese companies and unfair competitive advantage [1]. The local partners own the physical infrastructure and are the “seller of record,” although the foreign cloud service providers retain their intellectual property rights and trademarks [2]. These local partners in China control the relationships between the CSP’s suppliers and customers [2].

Some experts believe that the deep cultural and technical links that the local companies have with the Chinese government create nearly insurmountable advantages, especially when it comes to regulations and requirements around cybersecurity and data protection [2].

[1] https://url.sec488.com?id=72
[2] https://url.sec488.com?id=73
[3] https://url.sec488.com?id=74
[4] https://url.sec488.com?id=75
[5] https://url.sec488.com?id=76



Operational Requirements – Cloud Customers

Telecom and Cloud Service Providers:

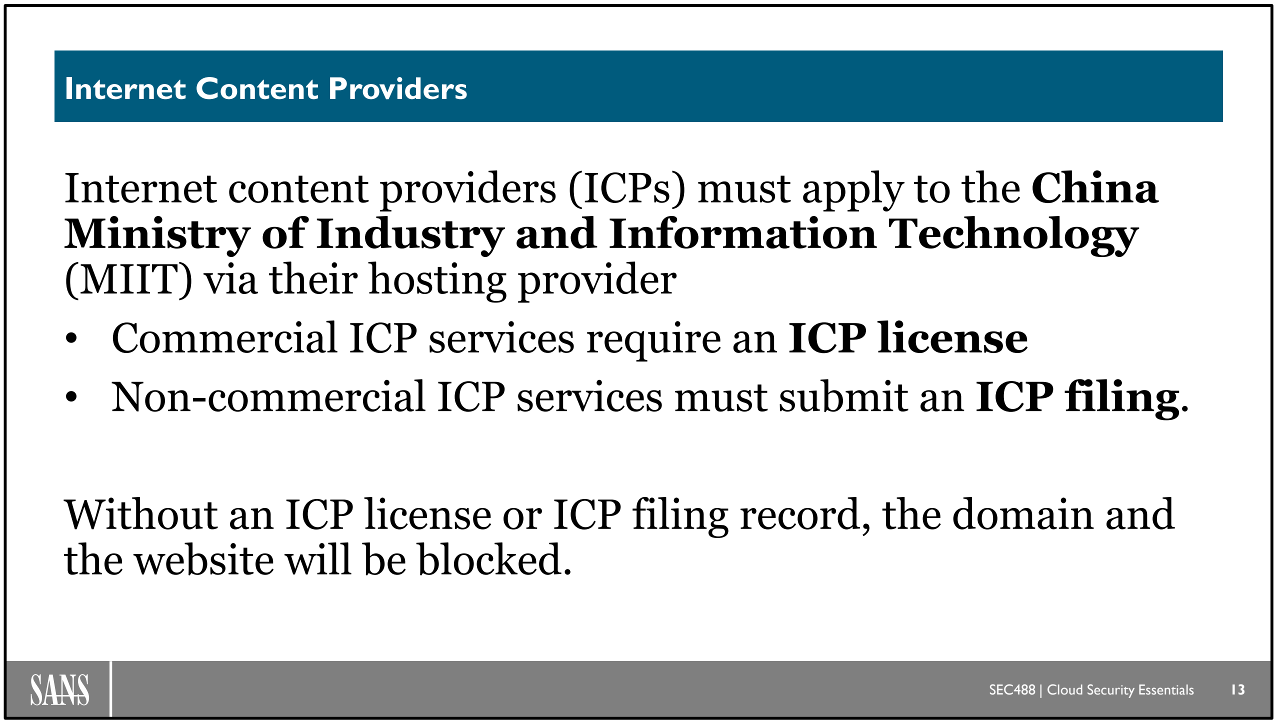
- “Must ask users to provide **authentic identity information** and verify it when settling access service formalities for users.”
- “Cannot offer services for access to entities or individuals if they fail to obtain an **operating license** or to complete the **non-operating Internet information service filing** formalities in accordance with the law.”

All licensed operators must indicate the number of their operating license in a prominent position in their main premises, website homepage and business promotion brochures.

In accordance with Chinese law and regulations, the State subjects non-commercial internet information services to a record-filing system and commercial internet information services to a permit system. No one may engage in the provision of internet information services without having carried out record-filing procedures or obtained permission [3].

Companies that want to register for a cloud account need to provide a valid Chinese business license issued by the Bureau of Industry and Commerce and valid contact information [4].

[1] https://uk.practicallaw.thomsonreuters.com/w-013-7289
[2] https://www.alibabacloud.com/help/doc-detail/52595.htm
[3] https://www.amazonaws.cn/en/about-aws/china/
[4] https://www.amazonaws.cn/en/about-aws/china/faqs/

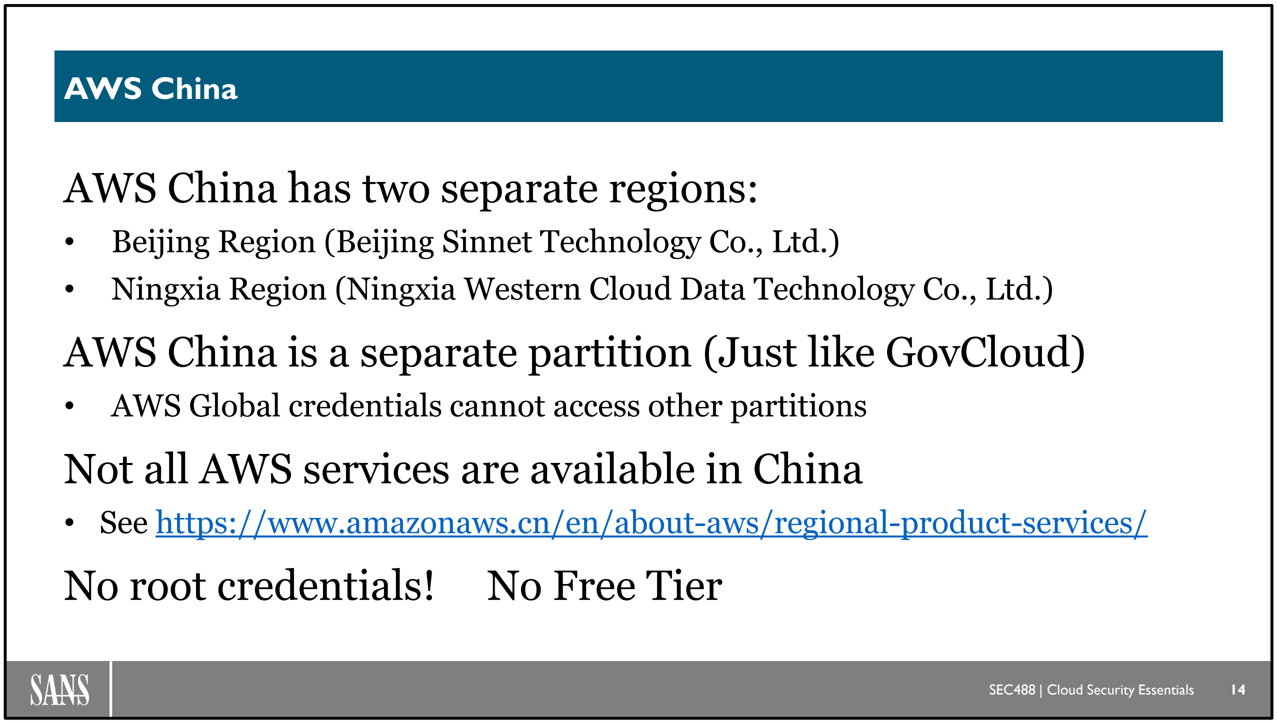


Internet Content Providers

Internet content providers (ICPs) must apply to the **China Ministry of Industry and Information Technology** (MIIT) via their hosting provider

- Commercial ICP services require an **ICP license**
- Non-commercial ICP services must submit an **ICP filing**.

Without an ICP license or ICP filing record, the domain and the website will be blocked.



AWS China

AWS China has two separate regions:

- Beijing Region (Beijing Sinnet Technology Co., Ltd.)
- Ningxia Region (Ningxia Western Cloud Data Technology Co., Ltd.)

AWS China is a separate partition (Just like GovCloud)

- AWS Global credentials cannot access other partitions

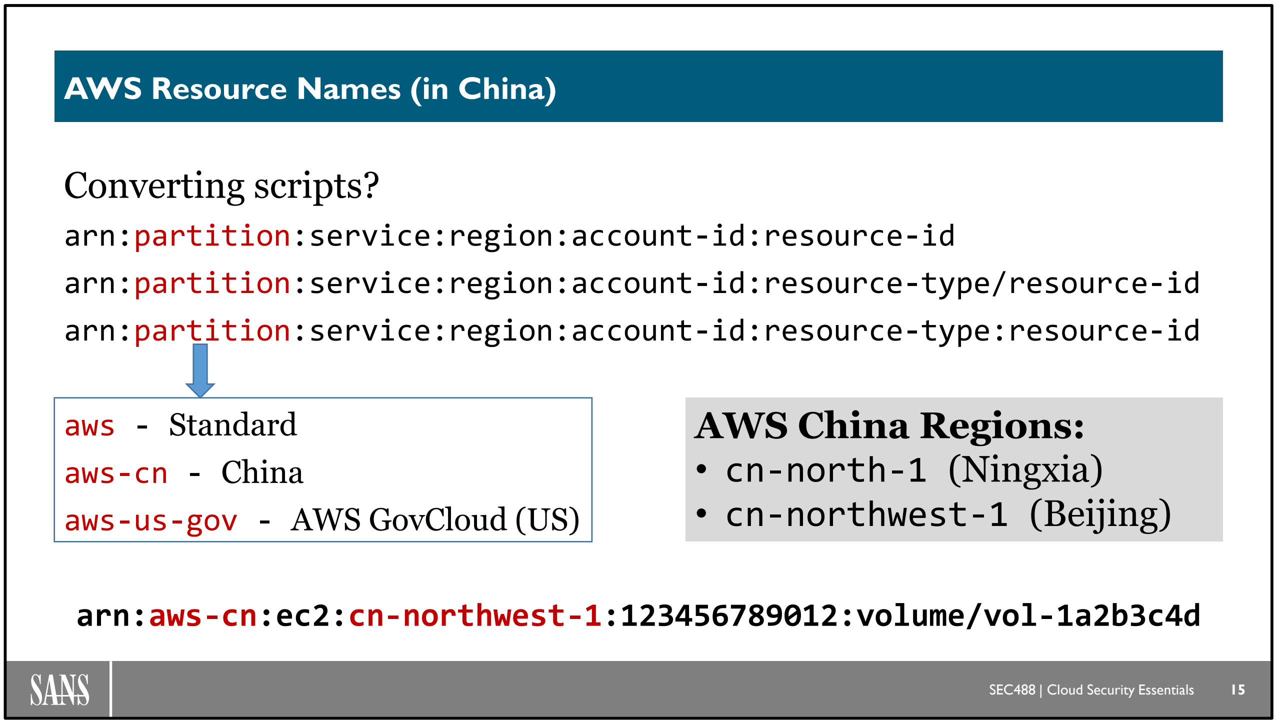
Not all AWS services are available in China

- See https://www.amazonaws.cn/en/about-aws/regional-product-services/

No root credentials!   No Free Tier

AWS China has two separate regions [1], each operated by a separate local partner:
Beijing Region (Beijing Sinnet Technology Co., Ltd.)
Ningxia Region (Ningxia Western Cloud Data Technology Co., Ltd.)

[1] https://url.sec488.com?id=80
[2] https://aws.amazon.com/blogs/enterprise-strategy/getting-started-with-aws-services-in-aws-china-beijing-region-and-aws-china-ningxia-region/



AWS Resource Names (in China)

Converting scripts?

```
arn:partition:service:region:account-id:resource-id
arn:partition:service:region:account-id:resource-type/resource-id
arn:partition:service:region:account-id:resource-type:resource-id
```

`aws` - Standard

`aws-cn` - China

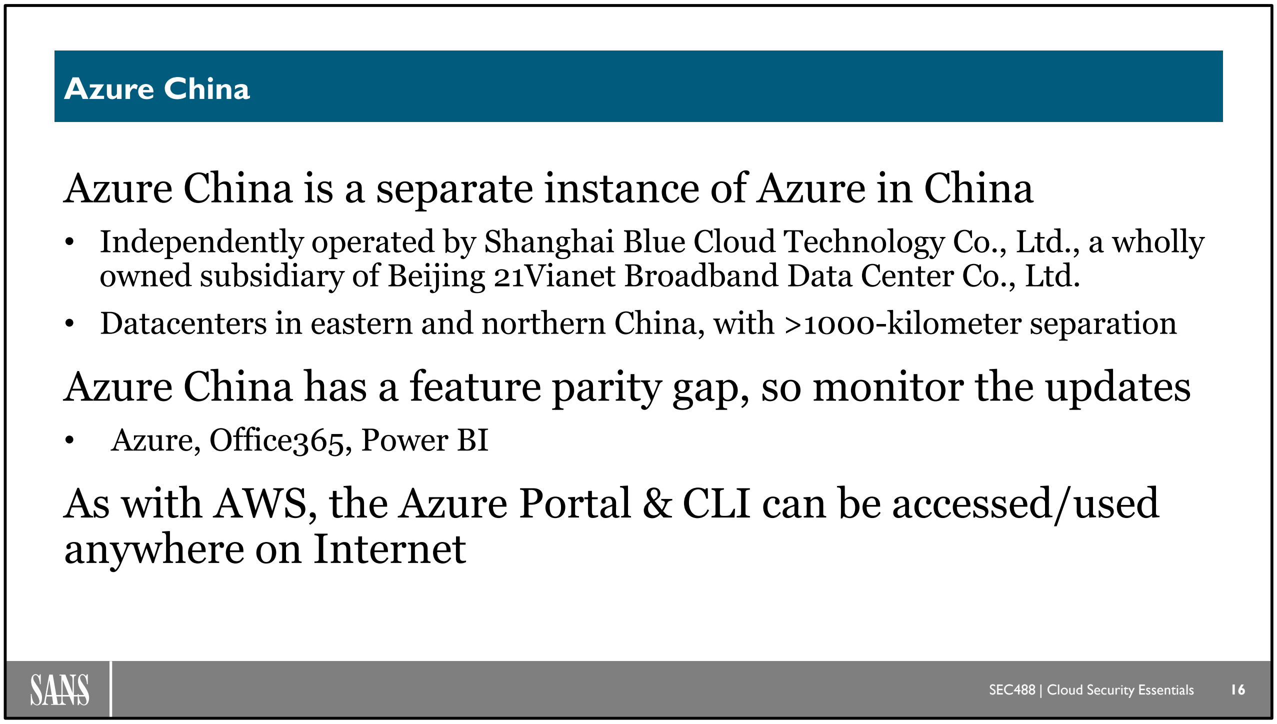
`aws-us-gov` - AWS GovCloud (US)

AWS China Regions:

- `cn-north-1` (Ningxia)
- `cn-northwest-1` (Beijing)

```
arn:aws-cn:ec2:cn-northwest-1:123456789012:volume/vol-1a2b3c4d
```

Implications: Test your scripts!!



Azure China

Azure China is a separate instance of Azure in China

- Independently operated by Shanghai Blue Cloud Technology Co., Ltd., a wholly owned subsidiary of Beijing 21Vianet Broadband Data Center Co., Ltd.
- Datacenters in eastern and northern China, with >1000-kilometer separation

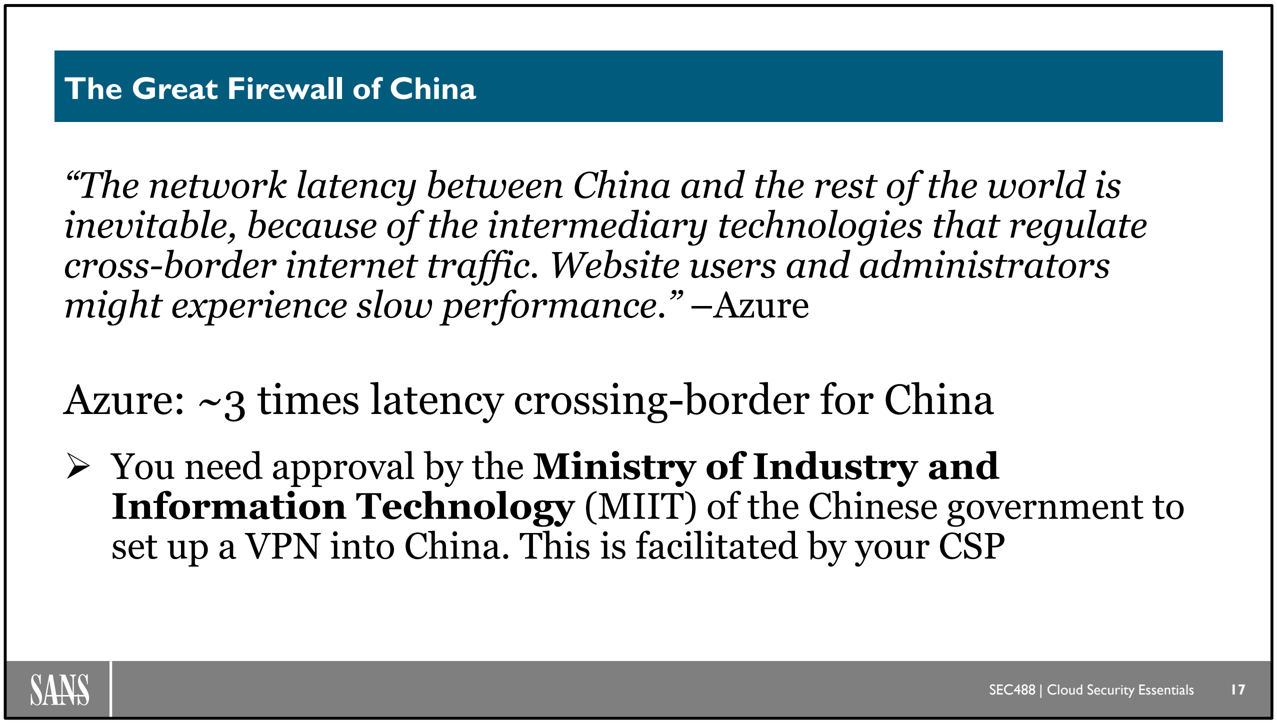
Azure China has a feature parity gap, so monitor the updates

- Azure, Office365, Power BI

As with AWS, the Azure Portal & CLI can be accessed/used anywhere on Internet

In China, the Microsoft Azure offering is called “Azure China” and is operated by operated by Shanghai Blue Cloud Technology Co., Ltd. , a wholly owned subsidiary of Beijing 21Vianet Broadband Data Center Co., Ltd. [1]

[1] https://docs.microsoft.com/en-us/azure/china/



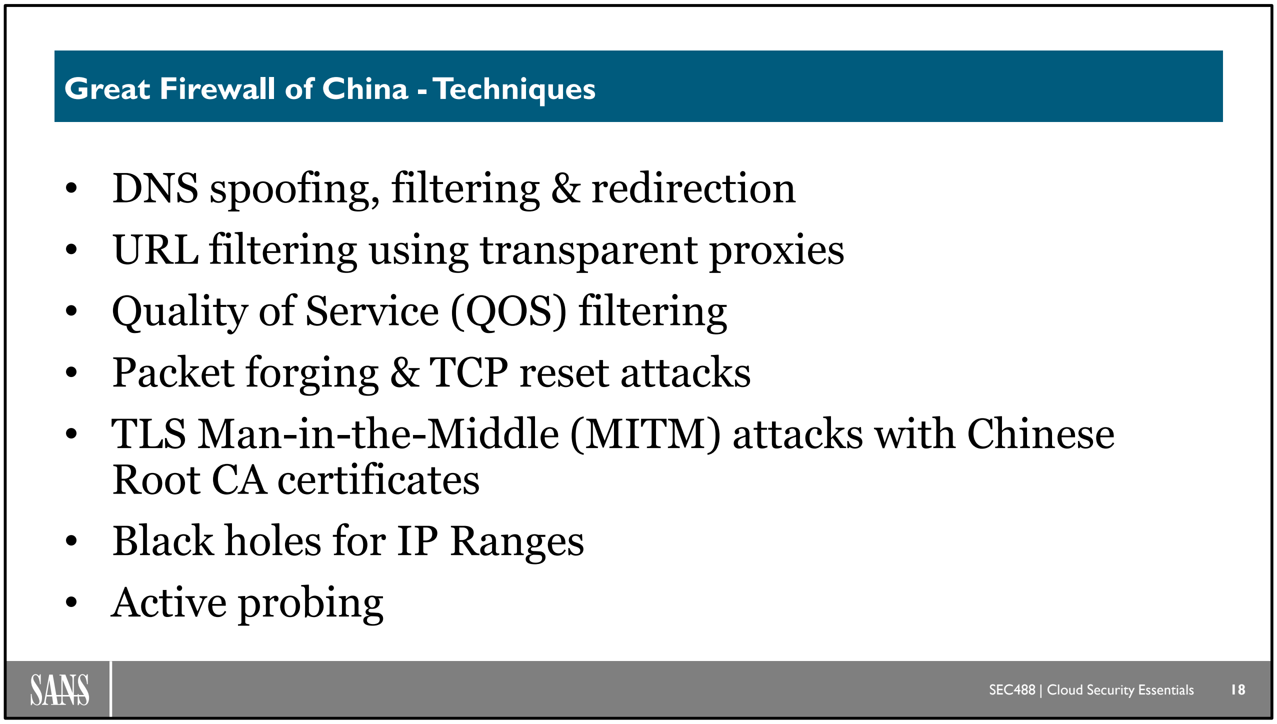
The Great Firewall of China

"The network latency between China and the rest of the world is inevitable, because of the intermediary technologies that regulate cross-border internet traffic. Website users and administrators might experience slow performance." –Azure

Azure: ~3 times latency crossing-border for China

- ➢ You need approval by the **Ministry of Industry and Information Technology** (MIIT) of the Chinese government to set up a VPN into China. This is facilitated by your CSP

[1] https://docs.microsoft.com/en-us/azure/china/



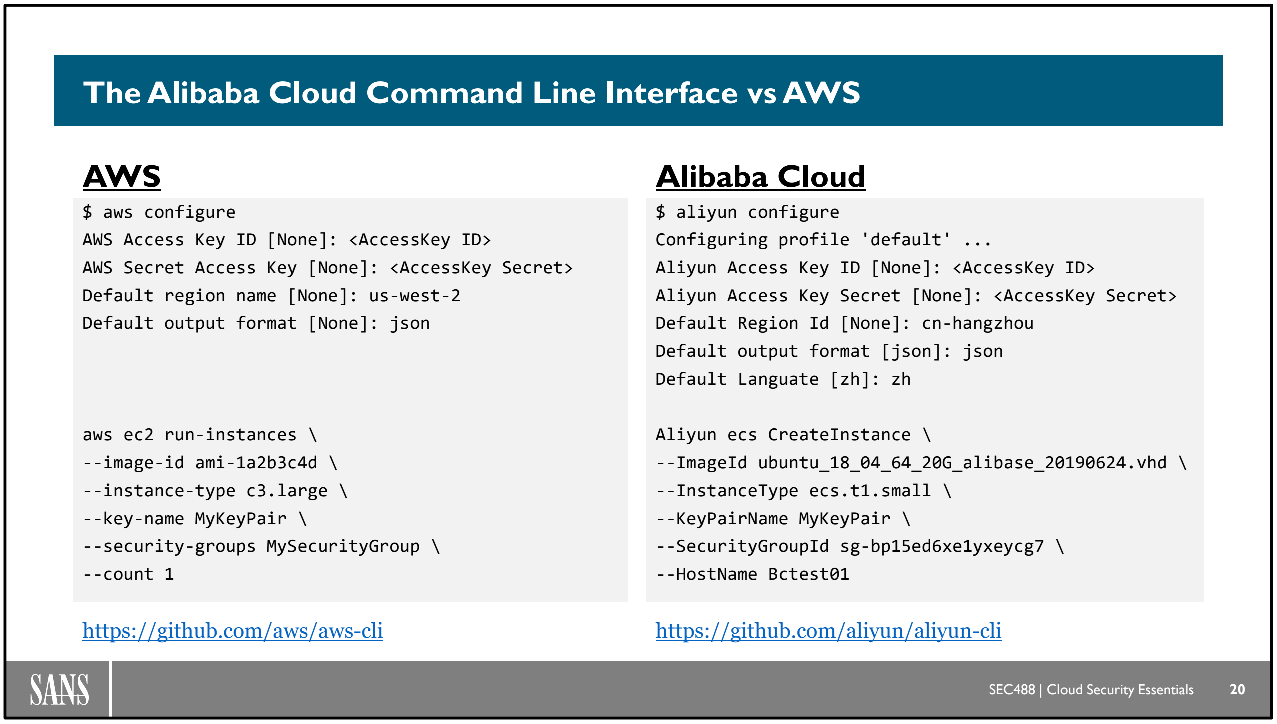
Great Firewall of China - Techniques

- DNS spoofing, filtering & redirection
- URL filtering using transparent proxies
- Quality of Service (QOS) filtering
- Packet forging & TCP reset attacks
- TLS Man-in-the-Middle (MITM) attacks with Chinese Root CA certificates
- Black holes for IP Ranges
- Active probing

[1] http://pcwizardpro.com/how-to-unblock-websites-in-china/
[2] https://www.usenix.org/system/files/conference/foci14/foci14-anonymous.pdf
[3] https://www.eecs.yorku.ca/course_archive/2014-15/W/3482/Team13_presentation.pdf
[4] https://www.theguardian.com/technology/2012/dec/14/china-tightens-great-firewall-internet-control

Hands-on Demo of Alibaba Cloud

- All products – https://www.alibabacloud.com/product
- Documentation – https://www.alibabacloud.com/help
- Real-name registration - https://account-intl.console.aliyun.com/#/secure
- Resource Access Management - https://ram.console.aliyun.com/overview
- Launch an Instance - https://ecs.console.aliyun.com/#/home
- Connect to an Instance – via console and SSH
- Terminate an Instance via the Console
- Look at the Security Group Configuration
- Attempt to launch an instance in mainland China



The Alibaba Cloud Command Line Interface vs AWS

AWS

```
$ aws configure
AWS Access Key ID [None]: <AccessKey ID>
AWS Secret Access Key [None]: <AccessKey Secret>
Default region name [None]: us-west-2
Default output format [None]: json


aws ec2 run-instances \
--image-id ami-1a2b3c4d \
--instance-type c3.large \
--key-name MyKeyPair \
--security-groups MySecurityGroup \
--count 1
```

https://github.com/aws/aws-cli

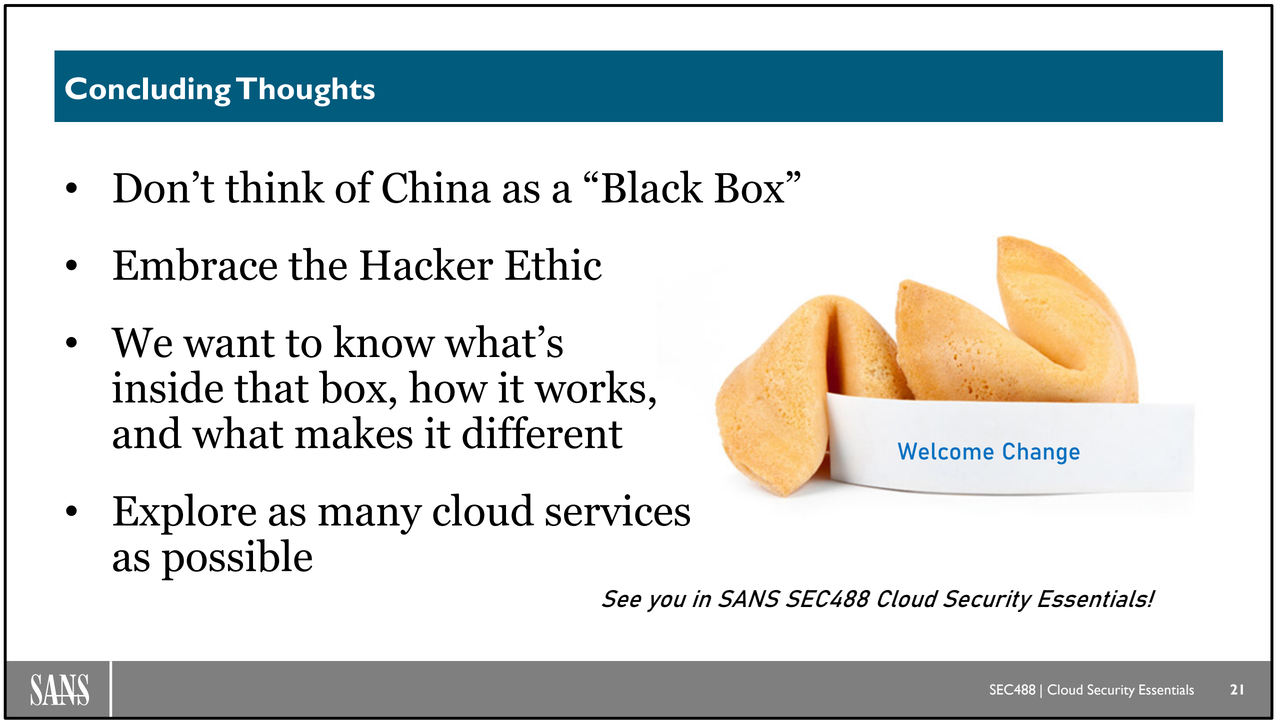
Alibaba Cloud

```
$ aliyun configure
Configuring profile 'default' ...
Aliyun Access Key ID [None]: <AccessKey ID>
Aliyun Access Key Secret [None]: <AccessKey Secret>
Default Region Id [None]: cn-hangzhou
Default output format [json]: json
Default Languate [zh]: zh

Aliyun ecs CreateInstance \
--ImageId ubuntu_18_04_64_20G_alibase_20190624.vhd \
--InstanceType ecs.t1.small \
--KeyPairName MyKeyPair \
--SecurityGroupId sg-bp15ed6xe1yxeycg7 \
--HostName Bctest01
```

https://github.com/aliyun/aliyun-cli

https://www.alibabacloud.com/help/doc-detail/110244.htm



Concluding Thoughts

- Don’t think of China as a “Black Box”
- Embrace the Hacker Ethic
- We want to know what’s inside that box, how it works, and what makes it different
- Explore as many cloud services as possible

Welcome Change

See you in SANS SEC488 Cloud Security Essentials!

Be aware, however of China’s Cybersecurity Laws: https://www.dezshira.com/library/legal/cyber-security-law-china-8013.html