Excerpts from SEC488

SANS

Doing Cloud in China

SANS Cloud Security Summit 2020

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.

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?

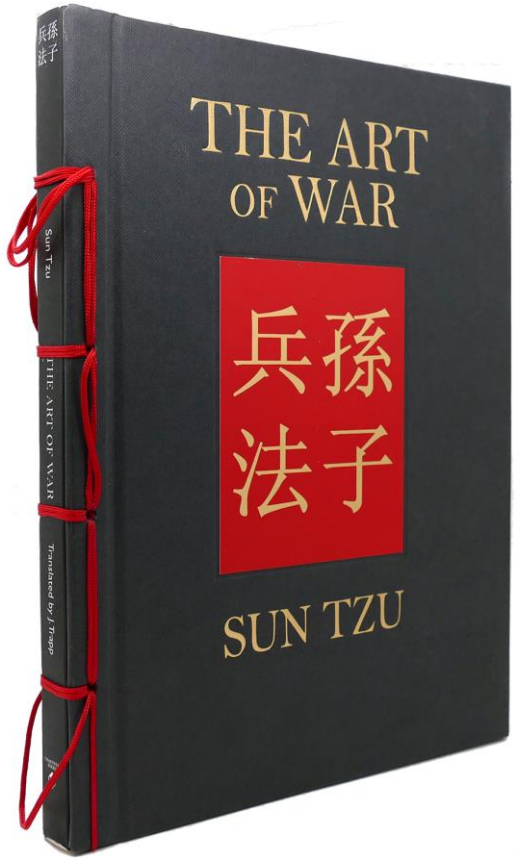
- Extremely large market opportunities ($$)

  "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"

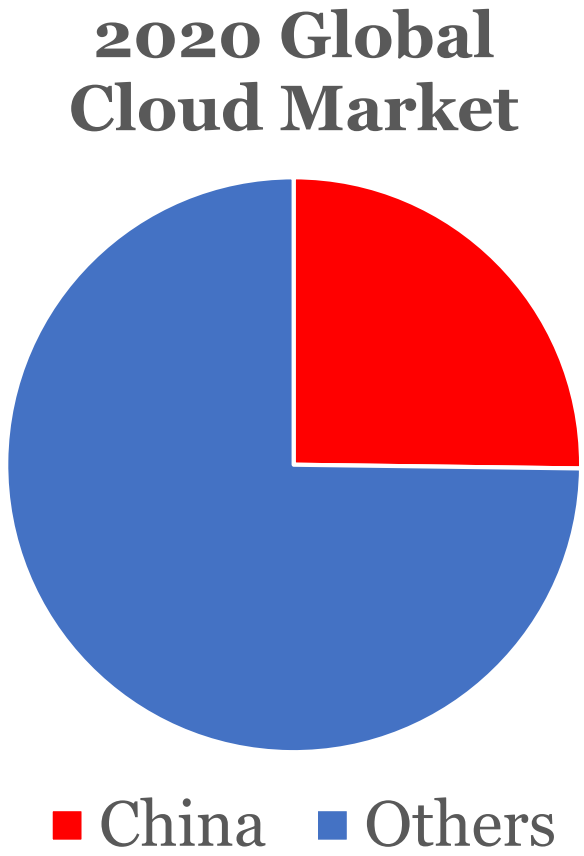
  "The greatest victory is that which requires no battle."
- China is a Nation-State Threat Actor

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

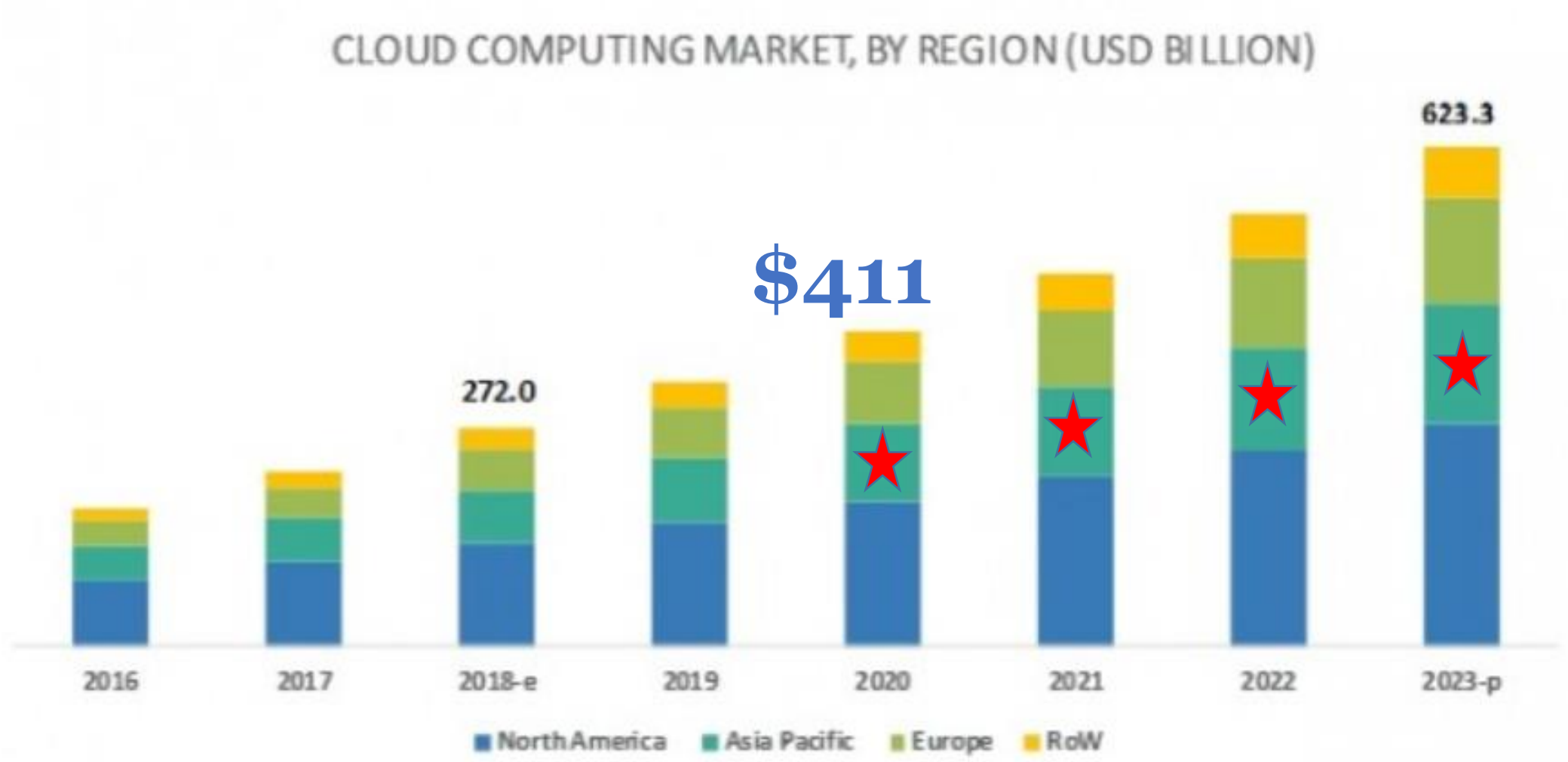


The Chinese Cloud Market

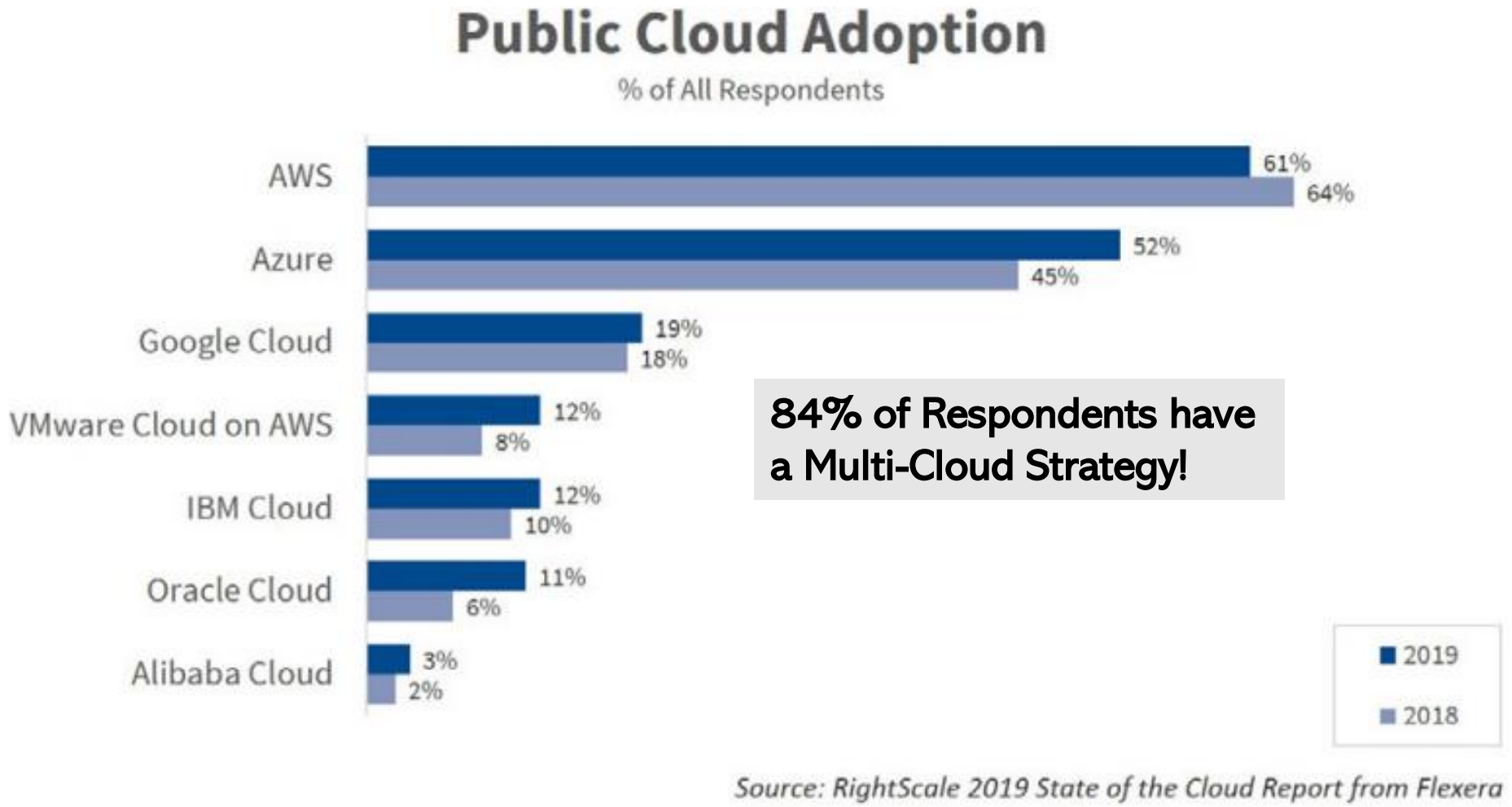
- Cloud Computing in China is expected to hit 686.6 billion yuan (about $103.6 billion US) in 2020 contrasted with a worldwide market size of $411 billion US.
- Alibaba Cloud's 2018 conference hosted 120,000 people in contrast to the 2018 AWS re:Invent conference with 50,000.



Cloud Computing Market by Region



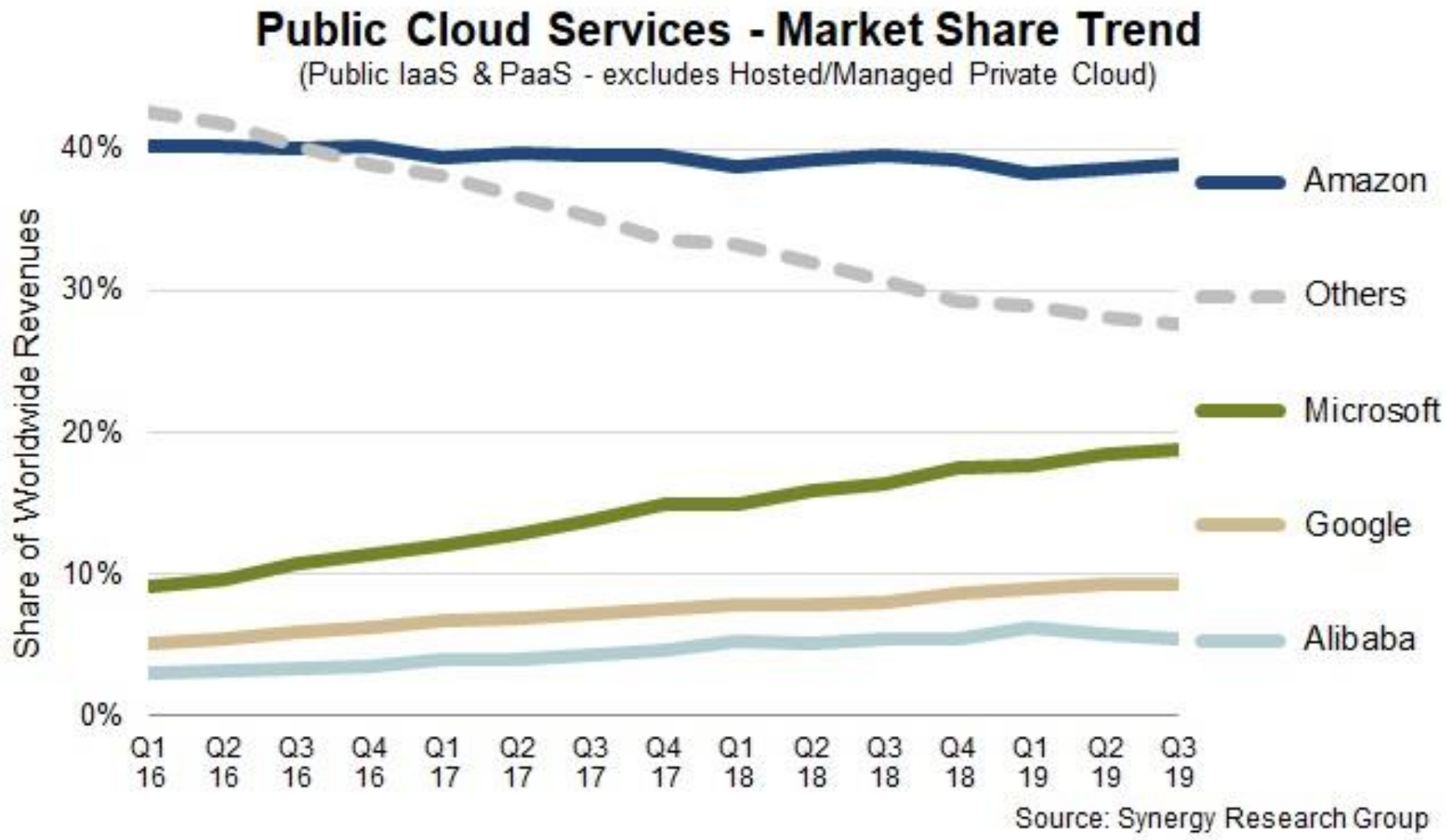
Market Data on the Growth of Public Cloud Computing



84% of Respondents have a Multi-Cloud Strategy!

Source: RightScale 2019 State of the Cloud Report from Flexera

IaaS + PaaS Market Shares



Cloud Service Providers in China

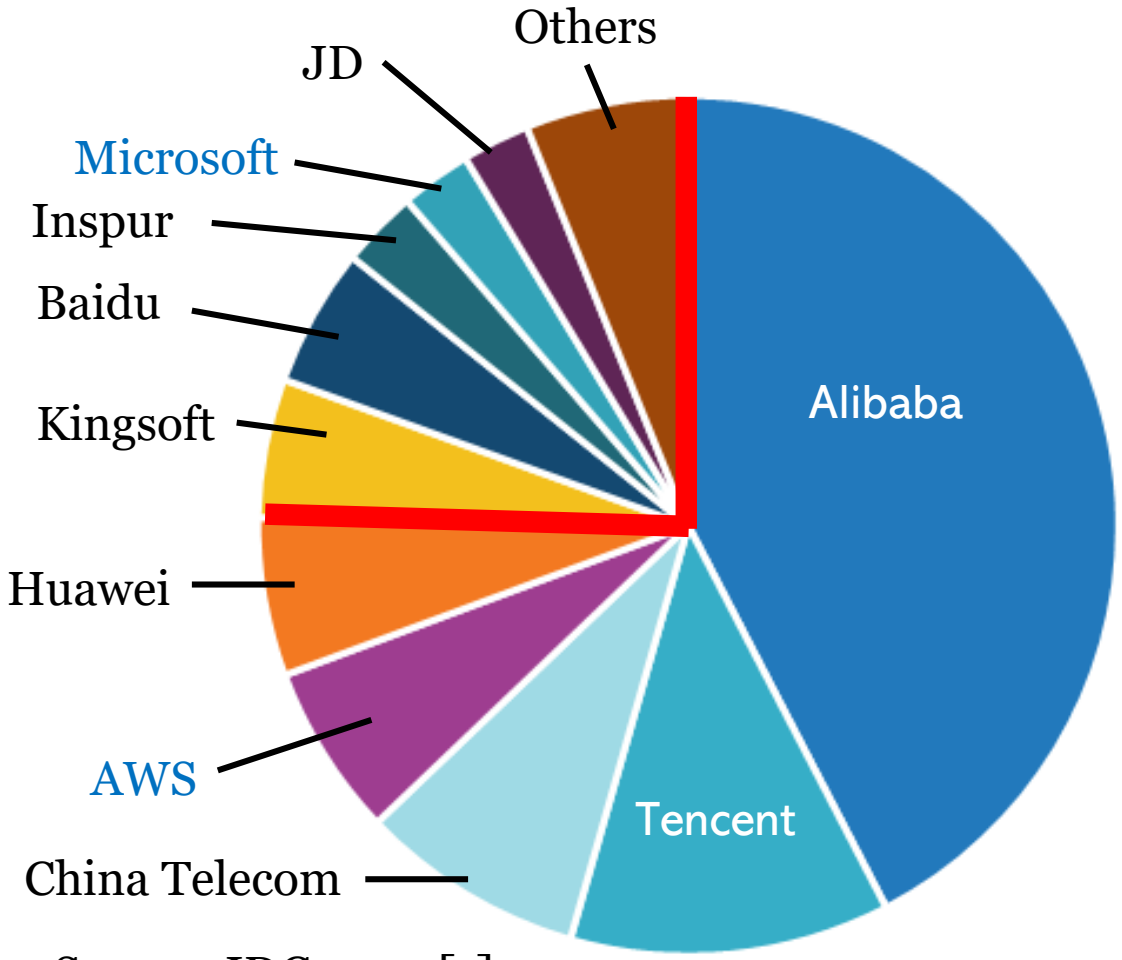
Local Providers

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

Foreign Providers

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

IaaS Vendors Market Share in China – 2019H1



Source: IDC 2019 [1]

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

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

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.

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 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`

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

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

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

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

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

See you in SANS SEC488 Cloud Security Essentials!