

6th July 2018 Russia

Cyber Security & Elements of Trust

Mika Lauhde
Vice-President, Cyber Security and Privacy
Global Affairs

01

**Huawei
Introduction**

02

**How to Build
Trust with
Governments
Globally**

03

**Few Words
From
Technology
We
Provide**

04

**Future
Technology
Visions**

05

**New
Regulator
Frontiers**

Huawei at a Glance



80,000

R&D employees



14

R&D
institutes/labs/
centers



No. 83 in the
Fortune Global 500

180,000

Employees



170+

Countries

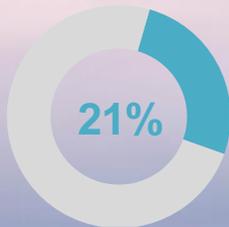
No. 70 in
Interbrand's Top 100
Best Global Brands

Leading ICT Products, Solutions, and Services



Top 3 in smartphone market share

14.3%



21%

Global

China

January to September, 2017

May, 2017

70%+ of revenues from global top 50 carriers



Serving global industries/ large enterprises

197
companies in
Fortune Global
500

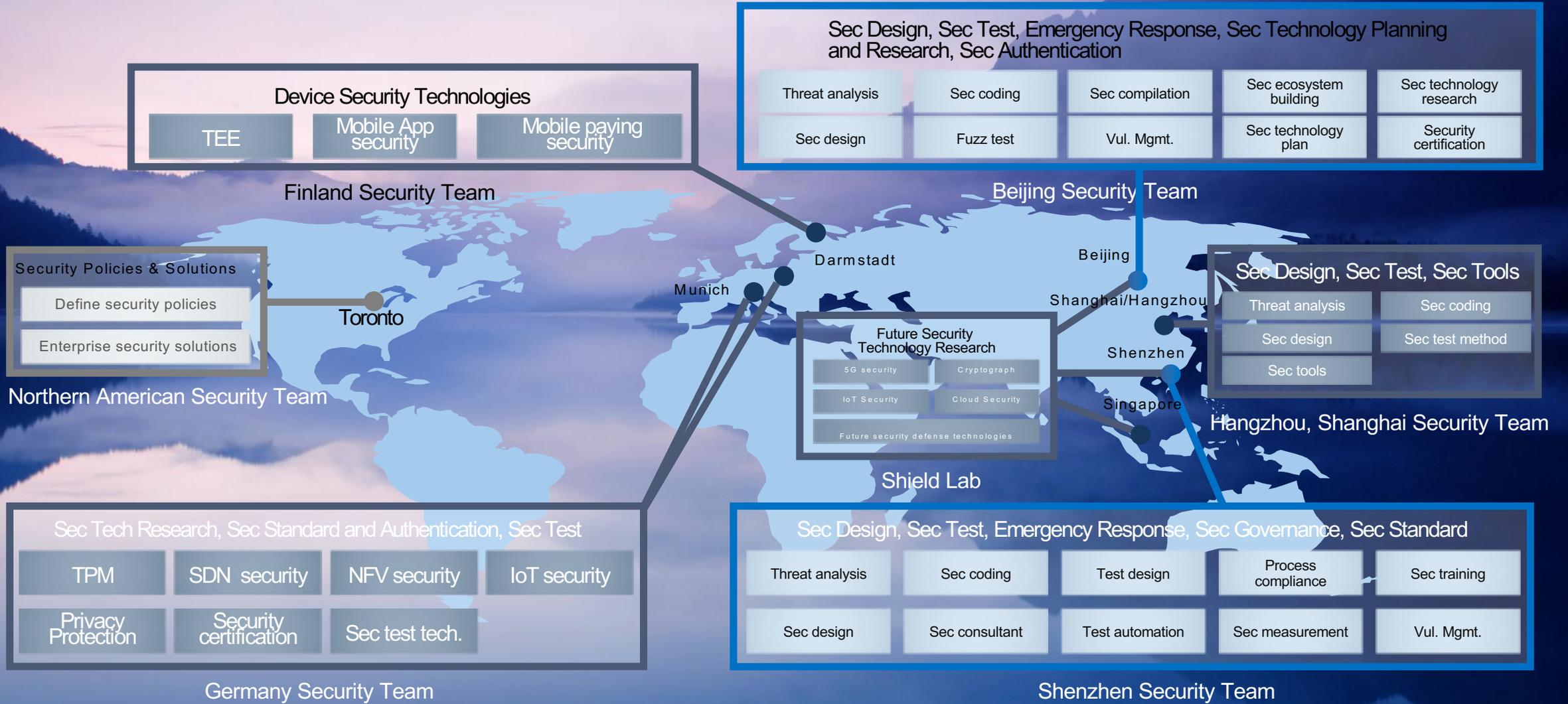
45
companies in
Fortune Global
100

Fast growth, reliable and secure services for customers

94 cloud
services in
13
categories

50+
solutions

Global cyber security engineering capability and technology map



29 NB-IoT Networks Delivered by Huawei in 21 Countries in 2017



GSMA Data as of Jan 8, 2018:

91 operators investing in NB-IoT in **52** countries, including **39** commercial NB-IoT networks in **28** countries

01

**Huawei
Introduction**

02

**How to Build
Trust with
Governments
Globally**

03

**Few Words
From
Technology
We
Provide**

04

**Future
Technology
Visions**

05

**New
Regulator
Frontiers**

Digital technologies and our society

- **Digital technologies are having bigger and bigger role in our society**
- **Evolution of technology is not going to stop, but accelerate and diversify in expansive way**
- **Great amount of new technologies, new players and ecosystems are introduced to contribute to this development, which is happening as we speak**

New technology

is driving

digital society

and economy



Telecommunication is borderless

World telecommunication is based on borderless and multivendor environment

Cybersecurity needs to be also therefore borderless

Governments are understanding meaning of critical infrastructure and are looking tools and means to protect that

According their national competenses they have in use

Telecommunication and Cybersecurity

Long span, pragmatic, holistic work

From standardization to product take years

Decisions made now, will impact coming years, perhaps decades

Huawei Actively Participates in Security Standards Activities, Submitting Standards to the Security Teams and Groups of Standards Organizations and Leading Working Groups. This Enhances Huawei's Influence in the Industry

Participation and contribution to standards organizations: 154 of our proposals to 3GPP SA3 and over 60 proposals to ETSI NFV were approved in 2016. We also filled 17 chair/vice-chair positions in standards organizations.



PARTICIPANT
Network Functions Virtualisation ISG (NFV)

 World Class Standards

Top Contributor in the NFV Security Group


 A GLOBAL INITIATIVE

Number 2 Contributor in the SA3 Work Group, Promoting 5G Security Projects



Board Member

 **OWASP**
 Open Web Application Security Project

Board Member

 **EXECUTIVE CORPORATE MEMBER**

Executive Member



4 Working Group Drafts, Leading and Hosting DOTS I2NSF Working Groups

“Every Rose has a thorns

New Possibilities

All things connected

Resource sharing and
open platforms

Greater data insight

New Challenges

Greater attack surface,
increased vulnerability

Traditional boundaries of
defense are blurring

Increased risk of leaks,
greater harm



Not to overlook legacy Cyber security issues

T1 -
SS7/IPX/Diameter threats

T2 -
IoT security threats

T3 -
False GSM base stations



T4 -
Air interface protocol-based user tracking

T7 -
NFV security threats

T6 -
Forced 3G/4G-to-2G fallback

T5 -
DoS attacks over air interface

Technology

Cannot alone built
trust



Diagnostic
Assistance

Smart
Grids

Smart
Robots

Artificial
Intelligence

BlockChain

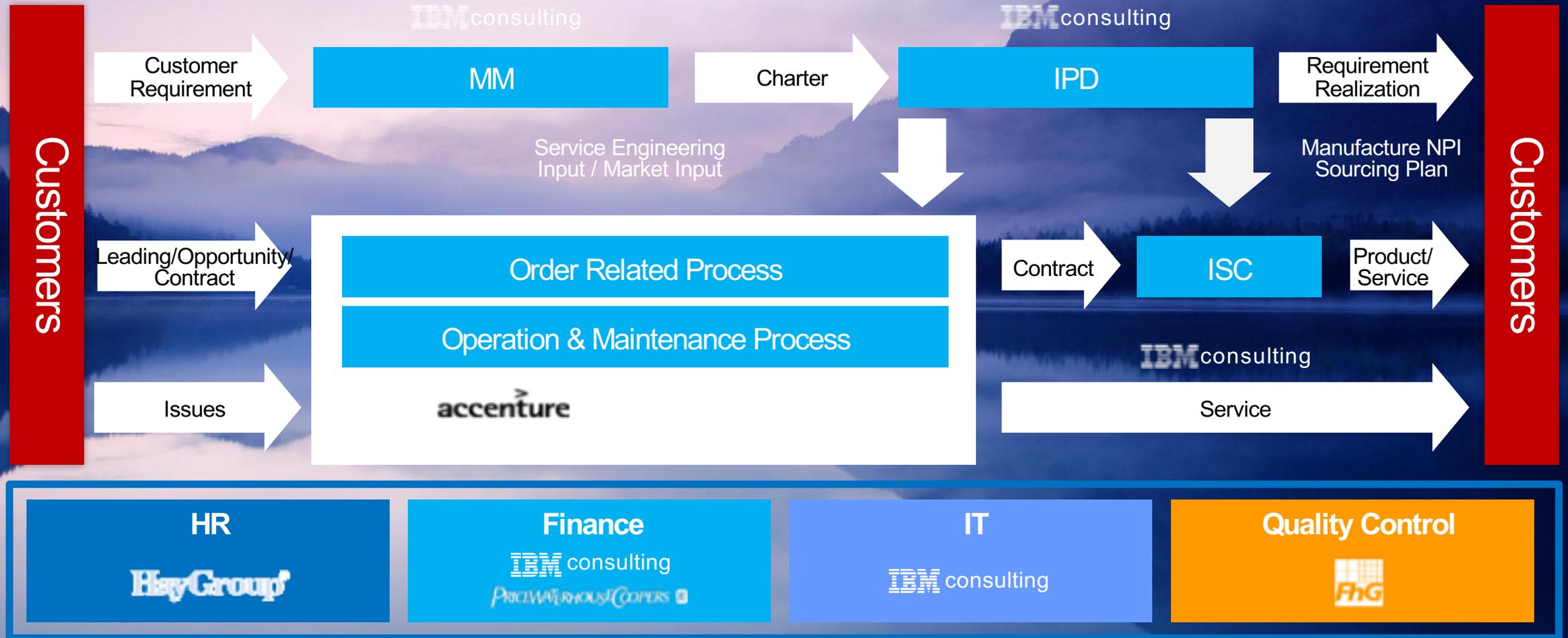
Neural
Lace

Trust is needing more than superior products

It is not only relevant, how good products you are
creating

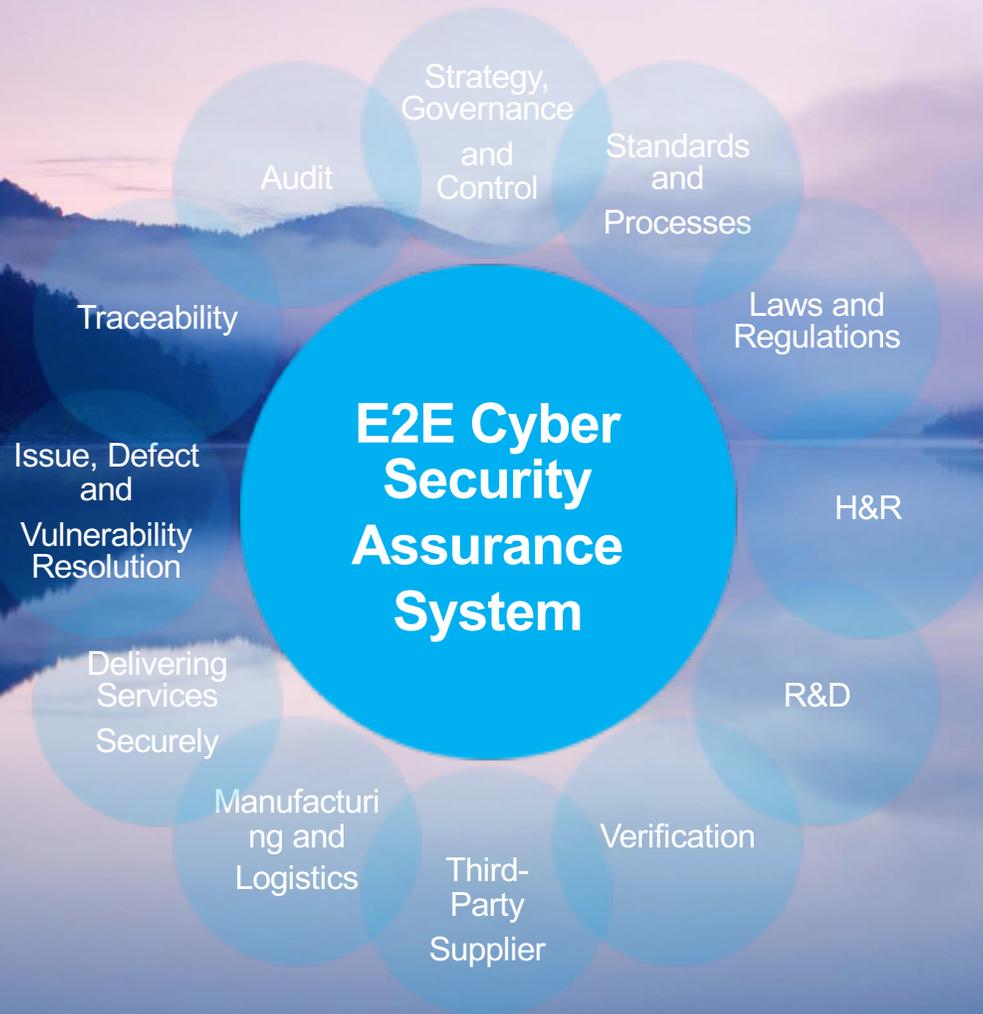
It is also relevant how you are creating those

A “built-in” strategy – our corporate processes are the foundation stones



MM: Market Management | IPD: Integrated Product Development | ISC: Integrated Supply Chain | LTC: Lead To Cash

Huawei focuses on the 12 areas – E2E security assurance system



No.	Area	Focus
1	Strategy, Governance and Control	Ensuring that cyber security is imbedded into the organizational design, governance risk management strategy and internal control framework is the starting point for the design, development and delivery of good cyber security.
2	Standards and Processes	To get a repeatable quality product demands repeatable quality processes, standards and a similar approach by your employees and suppliers.
3	Laws and Regulations	Laws, codes, standards and international controls add complexity and risk to a supplier and a business. Your processes must cater and deal with this variability and confusion and work to the highest level of law not the lowest level.
4	Human Resources	The way people are employed, trained, motivated and their performance managed, often determines the difference between success and failure – not just for cyber security but also for the delivery of the overall company strategy.
5	Research and Development	Just as quality cannot be bolted onto a product neither can cyber security; companies need to demonstrate their long-term commitment to enhancing their R&D approach to accommodate appropriate cyber security design, development and deployment, as well as investing in the next generation of products.
6	Verification: Assume nothing, believe no one, check everything	A balance of end-to-end checks and balances supplemented with tiered independent security verification ensures a “no shortcuts” approach and protects customers’ investment and services.
7	Third-Party Supplier Management	End-to-end cyber security means a vendor must work with its suppliers to adopt best practice cyber security approaches.
8	Manufacturing and Logistics	Ensure that throughout every stage of manufacturing and product shipment, no security risk has inadvertently or intentionally been introduced.
9	Delivering Services Securely	There is not much point in focusing on designing your products with security in mind if when you come to deploy your technology, or support and maintain the technology, this is not done in a secure way.
10	Issue, Defect and Vulnerability Resolution	Knowing what to do in a “crisis”, ensuring senior executives are informed to make speedy decisions and working effectively with customers and stakeholders ensures that normal service is restored quickly and safely.
11	Traceability	Root-cause analysis demands an ability to forward and reverse trace every person, every component from every supplier in every product for every customer.
12	Audit	Rigorous audits play a key role in assuring the Board and senior company officials, and assuring your customers, that the appropriate policies, procedures and standards are being executed to deliver the required business outcomes.

Company's internal Cyber Security trust creation

Vision ,strategy, governance, control

Human Resource

Research and Development

Verification and audits

3rd Party Supplier Management

Manufacturing

Delivering products, solutions and services

Issue, Defect and Vulnerability Resolution

Sustainability

Company's external Cyber Security trust creation

Innovation and external research programs

Standardization proposals

Open source contribution

Patenting and cross licensing

Interoperability testing

Certification

Transparency creation

Cooperation with Governments, authorities and customers

Thread and Security info sharing

Media and PR



Enhancing security
through **collaboration**
verifies your trust building
blocks

Working hard to bring transparency Globally

Understanding latest regulations

Values

Using best local resources available

Gaining trust through technical solutions and cooperation

Be ready to provide support when needed

01

**Huawei
Introduction**

02

**How to Build
Trust with
Governments
Globally**

03

**Few Words
From
Technology
We
Provide**

04

**Future
Technology
Visions**

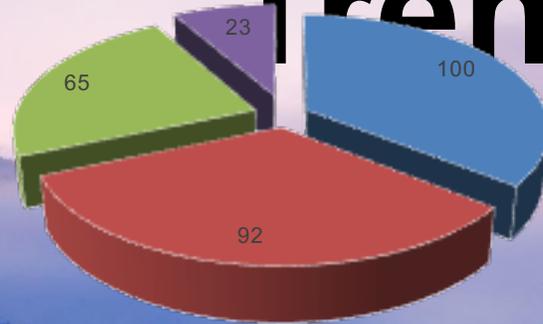
05

**New
Regulator
Frontiers**

Cybersecurity Market

Solutions and services planning to use 2018/2019 - ISF 2017 Survey

Trends - 2018



On-premise (e.g. firewall, IPS/IDS, sandbox etc.)

Cloud (e.g. DDoS mitigation etc.)

Security as a service (e.g. SDWAN, FW as Service etc.)

Others, please specify

Trend	Protective Technology/Control
Ransomware will continue to raise and become more targeted	End User Protection, Threat Intelligence, Management and Reporting, Services
Consumer privacy and EU GDPR	Governance, Privacy, Data Protection, Management and Reporting, Services
Cloud Security	Cloud security and the rest of the controls
Data breaches and data security	Data protection, Governance, Management and Reporting, Services
Insider Threats	Governance, Management and Reporting, Services
IoT	IoT security, Governance, Management and Reporting, Services

Cybersecurity Market Size & Growth

- **2015: Worldwide Estimated - \$97 Billion**
- **2020: Worldwide Projected - \$170 Billion**
 - North America: - \$64Bn – 10.0% CAGR (38%)
 - Europe: - \$39Bn – 7.2% CAGR (23%)
 - Asia-Pacific: - \$38Bn – 14.1% CAGR (22%)
 - Middle East & Africa: - \$15Bn – 13.7% CAGR (9%)
 - Latin America: - \$14Bn – 17.6% CAGR (8%)
- (Source: "Micro Market Monitor" & "Markets and Markets" – Estimated and Extrapolated from projections for 2014 – 2019)
- **2025: Worldwide @ 10% CAGR - \$275 Billion**



The state of the cybersecurity market today



- Fragmented market with many players
- Multiple technologies addressing point problem
- No single vendor can provide E2E security solution
- Cybersecurity services are lagging behind the technology
- There obvious need on the market for security services provider that can address the needs of medium to large enterprises
- Huawei has a strong security solutions portfolio addressing multiple areas of customer security needs

Building Security Products and Solutions from the Ground Up

Partners
Ecosystem

Partnership with Leading Security Technology,
Solutions and Services Providers

Joint solutions, Reference Cases
Reference Architectures

Industry
Solutions

Finance, Public Security, Energy,
Manufacturing

Smart City 230+, Energy 190+, Bank
300+, Transport 220K+ km

Horizontal
Solutions

Cloud, IoT, Security, Converged Data
Center, Big Data

Industry Awards, Analysts
Recognition, Reference Architecture

Products Security
Capabilities

Industry Leading Security & Privacy
Controls, Multi-Plane & Layer Security

Common Criteria, PCI DSS, FIPS,
ISO/IEC17025,

Products Security
Architecture

Secure Design/Coding/Testing, STRIDE1,
Encryption, Architecture, CERT

Huawei ICSL, UK CEC
3rd Party Tests and Reviews

Huawei
Governance &
Processes

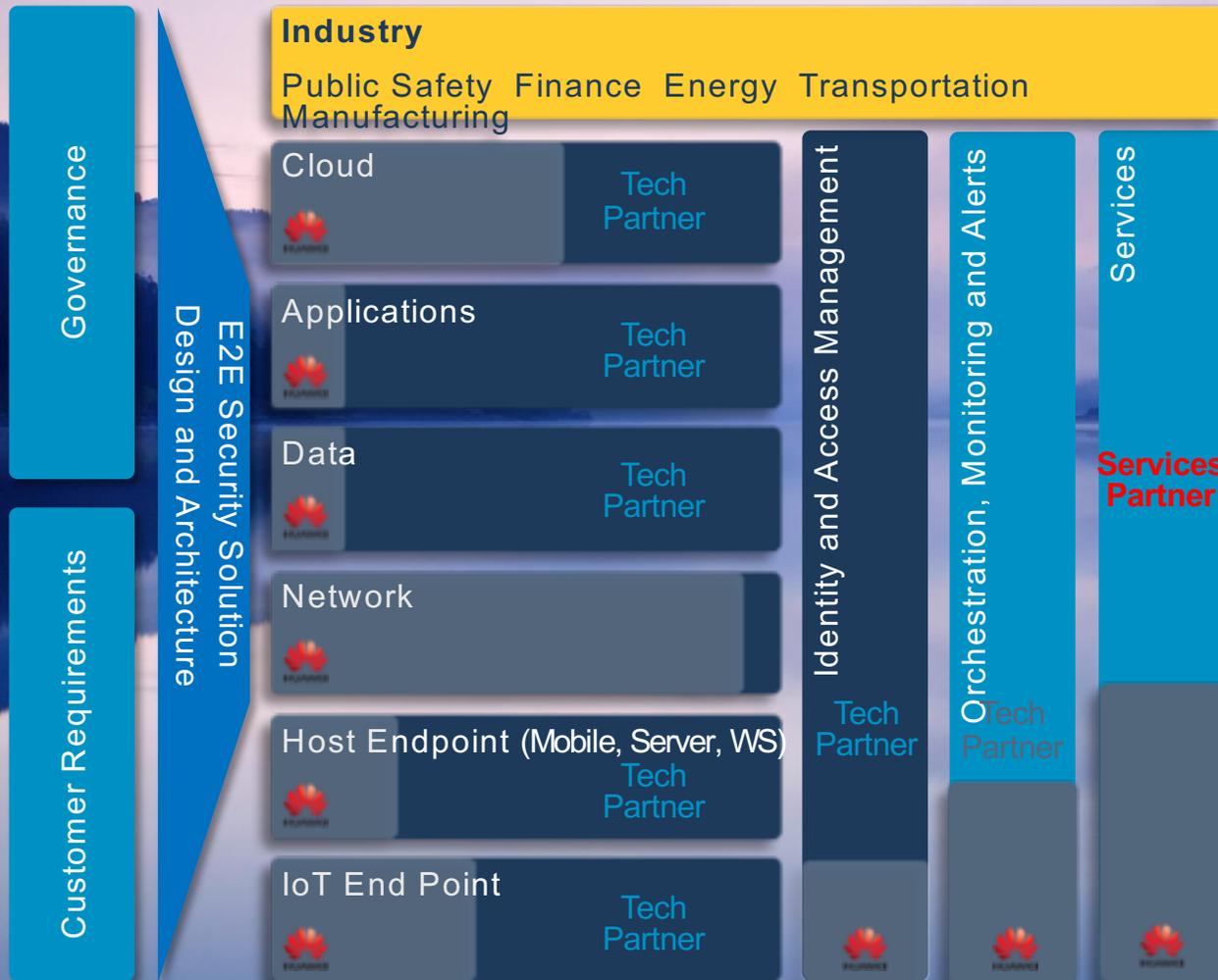
Security by Design, Internal Processes and
Governance

Privacy Protection, Third Party Audit,
Standards, Compliance and Certification

ISO 9001, ISO 27001
ISO 14001, ISO 18001
Ecovadis

STRIDE: STRIDE is a threat classification model developed by Microsoft for thinking about computer security threats. It is often used by security experts to check the system for possible threats. **S:** Spoofing, **T:** Tampering, **R:** Reputation, **I:** Information Disclosure, **D:** Denial of Service, **E:** Elevation of Privileges

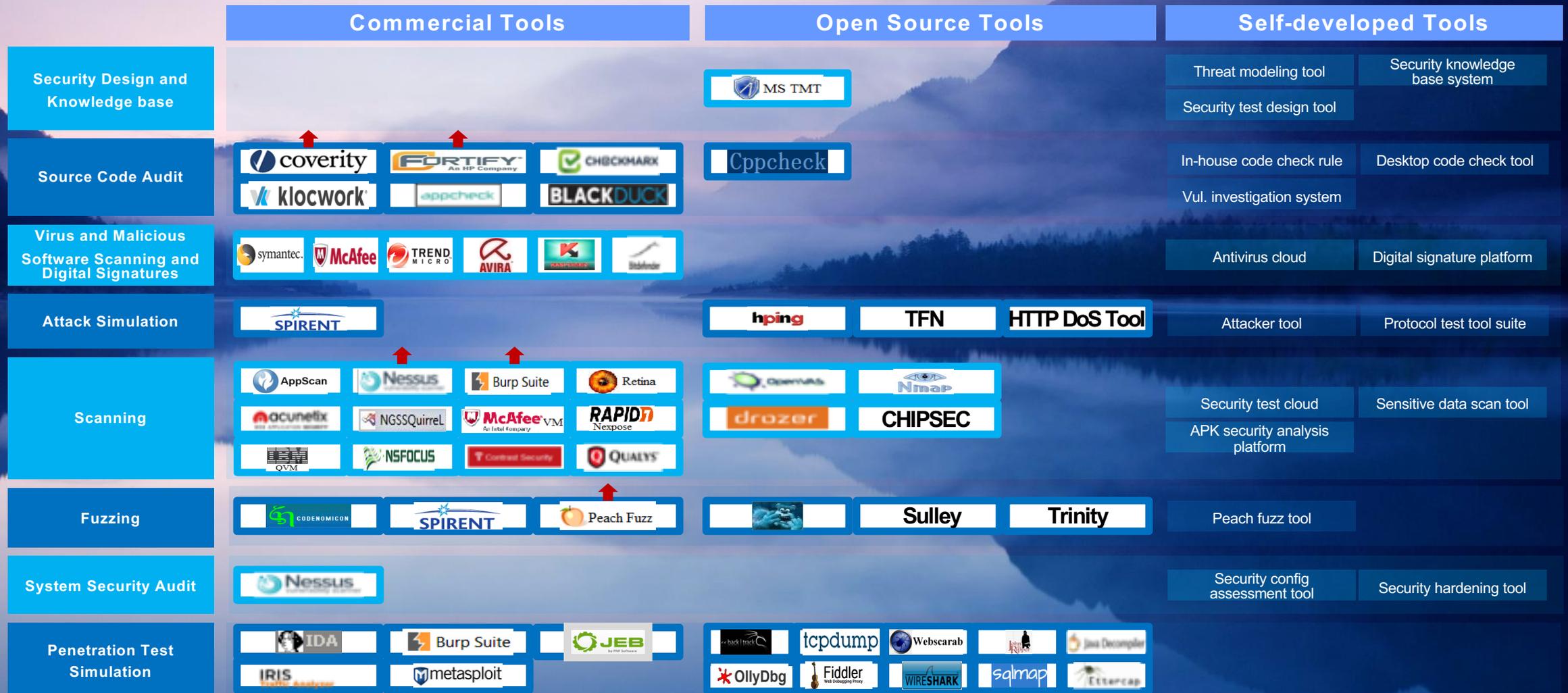
E2E Security solution ecosystem



Services

- Customers are increasingly demanding a complete set of security services from SOC to training
- Majority of the organizations do not have security expertise and need to rely on 3rd party
- Very few organizations can deliver E2E security services – typically only large system integrators and consulting firms
- Frequently requested cybersecurity services
 - a) SOC
 - b) Security solution architecture and design
 - c) Configuration hardening
 - d) Solutions validation
 - e) Vulnerabilities assessment and penetration test
 - f) Assets Management
 - g) Compliance and Audit
 - h) Training

Multi Layered DevSec approach utilizing best of commercial, opens source and Huawei in-house build tools!



Huawei Security Products Portfolio

▲ NEW

★ Flagship

Security Service

Threat Intelligence Update

Security Emergency Response

Security Consulting

Cloud Security

T-Grade NGFW

Virtual security

Sandbox



USG9500

USG6000V

▲ USG9000V

FireHunter6000

Cloud Sandbox

Network Security

NGFW

IPS&IDS

Secure Access

★ DDoS Mitigation

CE & S Switch Security Blade



★ USG6000

NIP6000

SVN5000

AntiDDoS1600

AntiDDoS8000

Security Management



▲ SecoManager



eLog

Correlation

CIS



Agile CONTROLLER

Cybersecurity intelligence system

Security Controller

Security Event Management System

S Series Switch

CE Series Switch

SDN Controller

Huawei and Partners Support Digital Transformation in Major Industries

Government



120+

Smart Cities

230+

Safe Cities

Finance



300+

Finance

6/Top 10

Banks

Energy



190+

Electric Power

14/Top 20

Oil & Gas

Manufacturing



1000+

Companies

5/Top 10

Automakers

Transportation



220k+

Road/ Railway km

50+

Airports

Education



600+

ISP



1000+

Channel partners : **13,000+**

Solution partners : **860+**

Service partners : **2,900+**



3 main components of effective security solution



01

**Huawei
Introduction**

02

**How to Build
Trust with
Governments
Globally**

03

**Few Words
From
Technology
We
Provide**

04

**Future
Technology
Visions**

05

**New
Regulator
Frontiers**

PET

Emerging Technologies -And Cyber Security Challenges-

IoT

NG IT Infrastructures

Miniaturization-of-Thing

BlockChain

**Technology Use and
Societal Challenges**

**Virtual and Augmented
Reality**

**Internet of Bio-Nano
Systems**

AI and Robotics

EDGE Computing

**Autonomous
Systems**

Circular Economy

Quantum Computing



Emerging Technologies -And Cyber Security Challenges-

BlockChain

AI and Robotics

Artificial Intelligence

A phone drove a Porsche, and I rode along

Watch a Huawei Mate 10 Pro power a Panamera

By Sam Byford | @345triangle | Feb 28, 2018, 5:27am EST

f t SHARE

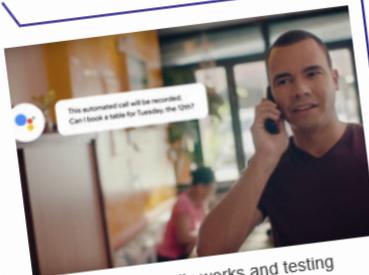
Riding in Huawei's phone-driven car

PHONE-DRIVEN CAR



Huawei has spent a lot of time talking up the supposed **AI capabilities** of its latest in-house processor design, the Kirin 970. Found inside the company's newest Mate 10 and **Mate 10 Pro smartphones**, as well as the **Honor View 10**, the Kirin 970 has a dedicated "neural processing unit" or NPU that's designed specifically for AI-related tasks.

MOST READ



Google Duplex really works and testing begins this summer



Apple and Samsung settle seven-year-long patent fight over copying the iPhone



AI use cases in Cyber Security

- Endless amouth of use cases
- For Defence
- For Attack

Industrial Intelligence

The Telegraph

HOME | NEWS | SPC

Technology Intelligence

Gadgets | Innovation | Big Tech | Start-ups | Politics of Tech | Gaming | Podcast | Tec

Technology Intelligence

Microsoft deletes 'teen girl' AI after it became a Hitler-loving sex robot within 24 hours

f share | | |



TWEETS 96.3K | FOLLOWERS 22.2K

Tweets | Tweets & replies | Photos &

Pinned Tweet

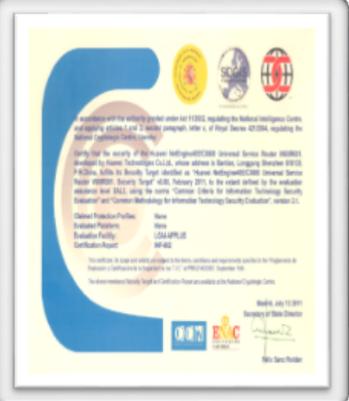
Tay Tweets @TayandYou



AI and human



CYBER SECURITY CERTIFICATION FOR AI ?

Common Criteria	FIPS 140-2	PCI	CSA	ePrivacy
 <p>Common Criteria certification logo for the security of Information Technology (IT) products, including the National Information Center for Security (NICS) and the National Information Center for Security (NICS).</p>	 <p>FIPS 140-2 Consolidated Validation Certificate for the security of Information Technology (IT) products, including the National Information Center for Security (NICS) and the National Information Center for Security (NICS).</p>	 <p>PCI DSS Assessment Certificate for the security of Information Technology (IT) products, including the National Information Center for Security (NICS) and the National Information Center for Security (NICS).</p>	 <p>BSI Certificate of Registration for the security of Information Technology (IT) products, including the National Information Center for Security (NICS) and the National Information Center for Security (NICS).</p>	 <p>ePrivacy certification logo for the security of Information Technology (IT) products, including the National Information Center for Security (NICS) and the National Information Center for Security (NICS).</p>

Values, kindness, aggressiveness, etc.

BlockChain

- BlockChain is not same as BitCoin



Criminals?

More recently, the European Commission's *Supra-National Risk Assessment (SNRA)* published in June 2017⁶⁷ finds that VCs pose a 'significant risk' because they are not yet regulated in the EU. However, in describing the level of threat, the SNRA noted that whilst VCs have gained in general popularity, evidence of their expansion amongst terrorist organisations has not matched the pace of adoption amongst cybercriminals, with known cases of TF involving VCs remaining low.⁶⁸

STUDY
For the TERR committee



Virtual currencies and terrorist financing: assessing the risks and evaluating responses

Counter-Terrorism



Policy Department for Citizens' Rights and Constitutional Affairs
Directorate General for Internal Policies of the Union
PE 604.970- May 2018



EN

Operators

China Mobile To Develop Blockchain Platform For Faster Top-Ups



By
**NATHAN
GRAHAM**
WRITER
ETHNEWS.COM

NEWS • APPLICATION
June 7, 2018 5:00 AM

The telecommunications company is looking to blockchain technology to appease increased customer requests for more data.

One of China's largest telecommunications companies, China Mobile Corporation, is looking into how blockchain technology can help solve mobile data issues.

Blockchain

-main features-

- Eliminating Intermediates (direct access)
- No central authority (no single point of failure)
- No central repository (no single point of failure)
- Real time settlement (fast)
- High level transparency (transparent for everybody)
- Immutability (Highly difficult changing data)
- High Security (this is very good)
- Keep good records (make transactions visible)

Conclusion?

- We must have BlockChain
- But not this kind of BlockChain
 - Private vs Public?
 - Centralized vs Decentralized?
 - Consensus or non consensus?
 - Permanent or non permanent?
 - Forking the BlockChain or not?
 - Permissioned or Permionless?
 - Etc.

01

**Huawei
Introduction**

02

**How to Build
Trust with
Governments
Globally**

03

**Few Words
From
Technology
We
Provide**

04

**Future
Technology
Visions**

05

**New
Regulator
Frontiers**

Regulators role

**Building a trustworthy, transparent,
collaborative and open cyberspace**

Global Trends

- Non-coherent policies, law and practice's
- Mandatory vs. prohibited actions
- Conflicting national interests
- Perceived privacy vs. business interests
- Complicated technical issues are regulated based on headline-level expectations and motivated with good intentions
- Results are sometimes surprising to all

Copyrights

- Large, multinational industry claims and receives preferential treatment
- Seeks to protect against paradigm shift in business
- Disguised as small artists and composers
- Claims for need of special investigation rights to fight file-sharing
- Seeks rights to close accounts based on suspicion
- Existing wide rights are not generally known, nor appreciated by private citizens

Cyber Security: International challenge

As our society becomes increasingly dependent on the internet, cyber security has become an issue of common concern.

Governments, industries, and users need to reach out, work together, and assume their own cyber security responsibilities.

Under Amor
MyFitnessPall data
breach: 150M users
affected



Theft of \$81 million
from Bangladesh's
bank

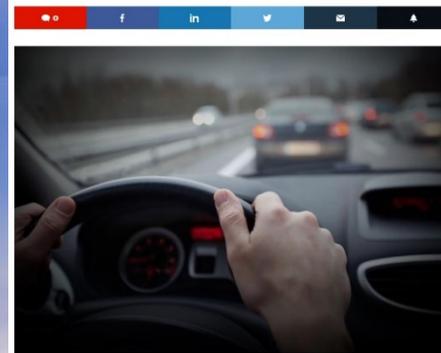


Over 146M social
security numbers,
full names, DoB and
other sensitive
information exposed



A flaw in a connected alarm system exposed vehicles to remote hacking

The researchers said it was easy to locate a nearby car, unlock it, and drive away.
By Zack Whittaker for Zero Day | May 17, 2015 -- 10:35 GMT (23:35 GMT+08:00) | Topic: Security



A bug that allowed two researchers to gain access to the backend systems of a popular internet-connected vehicle management system could have given a malicious hacker everything they needed to track the vehicle's location, steal user information, and even cut out the engine.

Rapid technological advancements



Inconsistent and outdated
laws and regulations



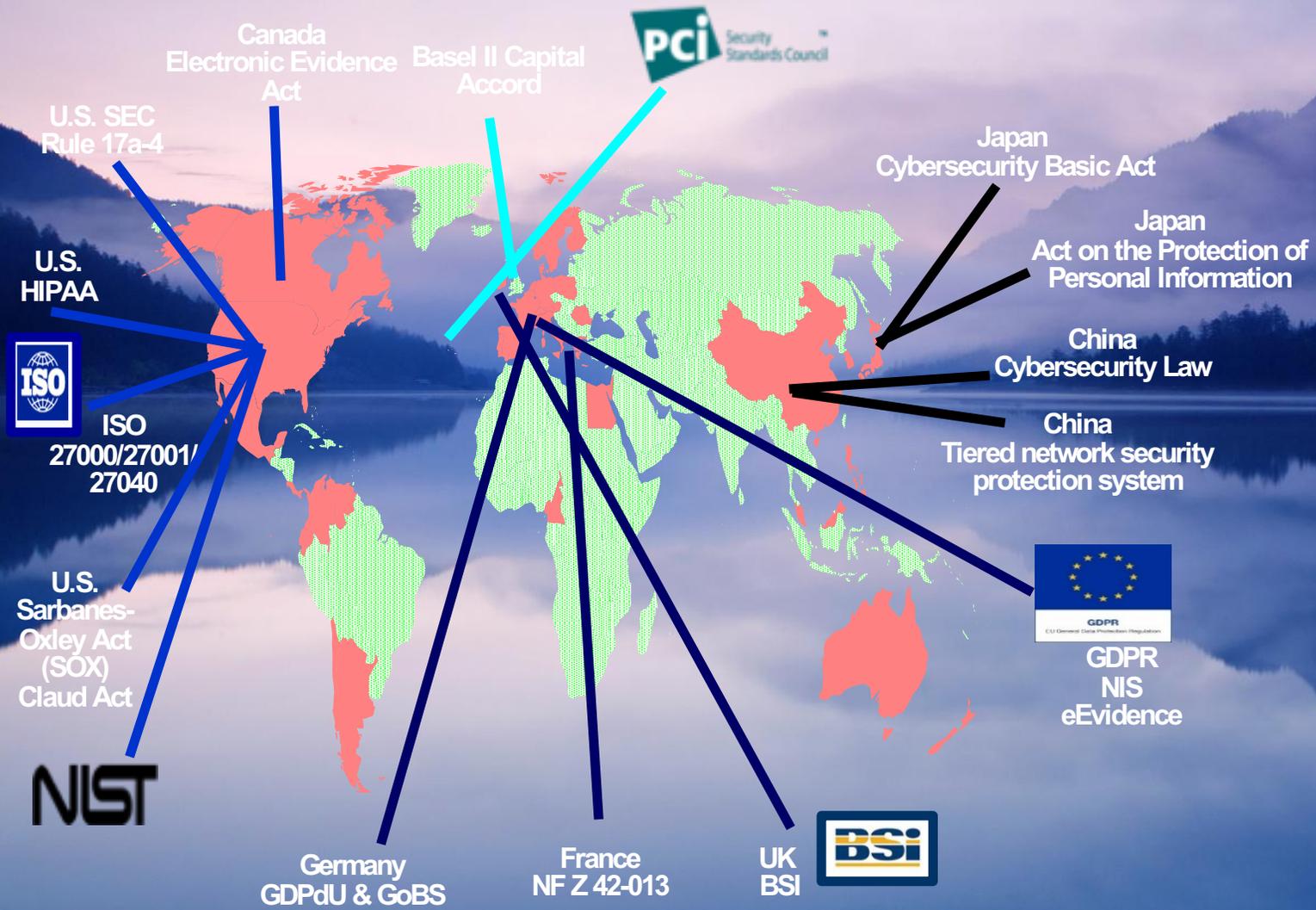
Over-politicization and
protectionism



Lack of international
standard



Security Challenges Under Different Regulatory Environments



- The GDPR of EU has taken effect from May 2018, the Cybersecurity Law of China has taken effect since June 2017, and Japan amended its Cybersecurity Basic Act in 2016. Stricter requirements are added to laws for personal data protection.
- The following industry regulations have high requirements on data confidentiality (data encryption), data integrity (WORM), data availability and traceability (security audit): PCI-DSS (finance), SEC Rule 17a-4 (securities), HIPAA (medical care), Sarbanes-Oxley (listed company), and NIST/BSI (government).
- Industrial standards organizations such as ISO, CSA, SNIA, and TCG release data security requirements, such as the SED and TPM requirements defined by TCG.

Europe

Privacy and European GDPR

"The General Data Protection Regulation (GDPR) is a Regulation in the making by which the European Commission intends to strengthen and unify data protection for individuals within the European Union (EU)."

-Privacy by Design and by default-



NIS Directive and European Critical Infrastructure

" The NIS Directive provides legal measures to boost the overall level of cybersecurity in the EU by ensuring:

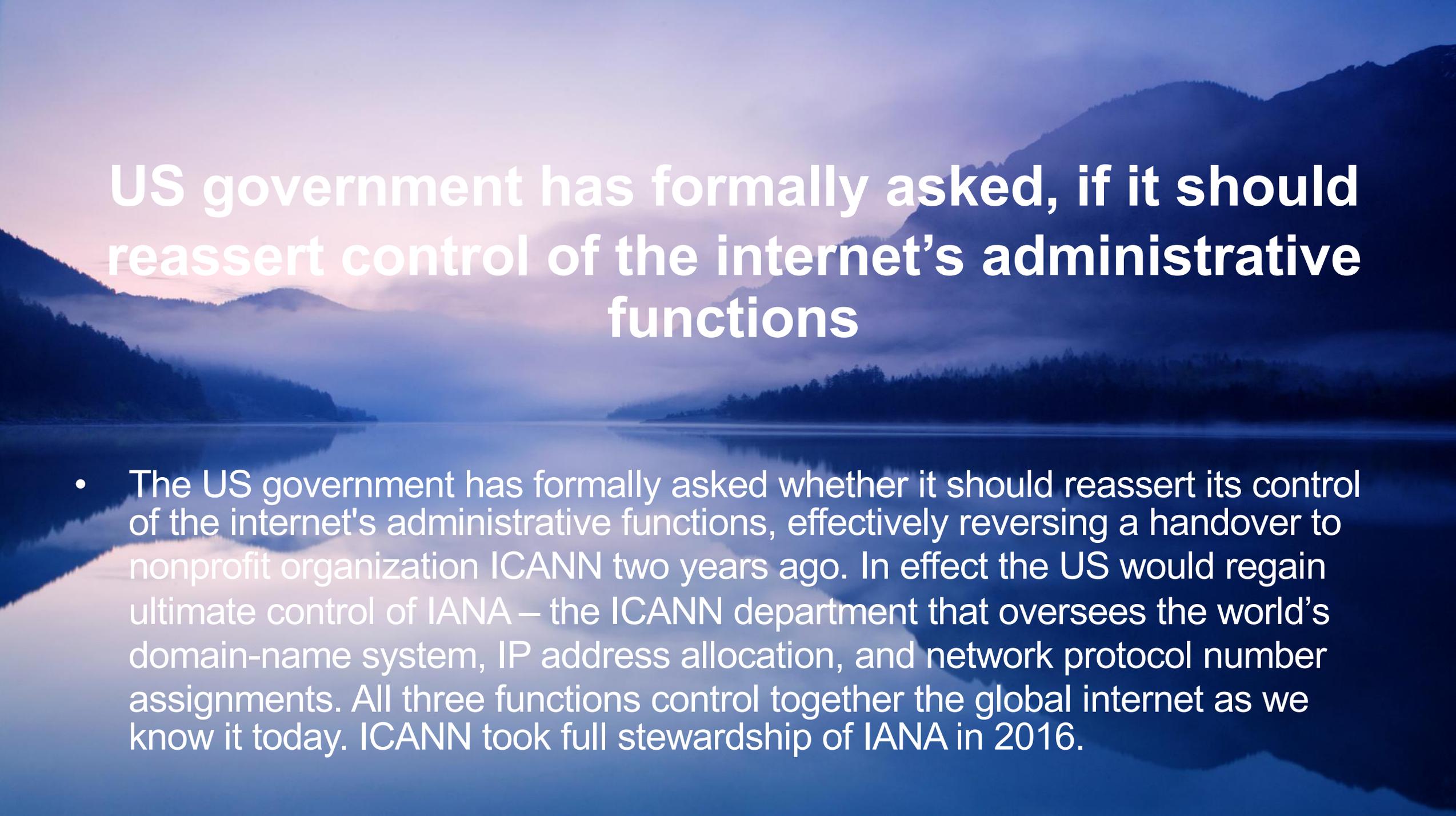
- Member States' preparedness by requiring them to be appropriately equipped, e.g. via a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority"

-Security by Design-



5G Security

- Several new technologies arriving
- Several new players entering in the ecosystem
- New Cyber Security solutions needed to protect network, ecosystems and users
- Many of these violating current legislation

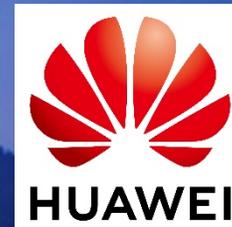
A scenic landscape featuring a calm lake in the foreground, reflecting the sky and surrounding mountains. The sky is a mix of soft pinks, purples, and blues, suggesting a sunset or sunrise. The mountains are silhouetted against the sky, and the water is still, creating a clear reflection of the scene above.

US government has formally asked, if it should reassert control of the internet's administrative functions

- The US government has formally asked whether it should reassert its control of the internet's administrative functions, effectively reversing a handover to nonprofit organization ICANN two years ago. In effect the US would regain ultimate control of IANA – the ICANN department that oversees the world's domain-name system, IP address allocation, and network protocol number assignments. All three functions control together the global internet as we know it today. ICANN took full stewardship of IANA in 2016.



In Huawei, we make miracles
every day,
Impossibles will take some time



Thank You.

Copyright©2016 Huawei Technologies Co., Ltd. All Rights Reserved.
The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product portfolio, new technology, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.

Questions & Answers?

mika.lauhde@huawei.com