Security Level:

16/ 09/ 2018

# Cybersecurity & Privacy
# A Huawei Perspective

Andy Purdy

Chief Security Officer, Huawei Technologies USA

# Huawei at a Glance

**180,000**

Employees

**80,000**

R&D employees

**170+**

Countries

**14**

R&D institutes/labs/ centers

**No. 70** in

Interbrand's Top 100

Best Global Brands

**No. 83** in the

Fortune Global 500

# Our Business Units

Hundreds of millions of consumers

Global carriers

Global enterprises, governments, and industries

**Consumer**
Products & Services

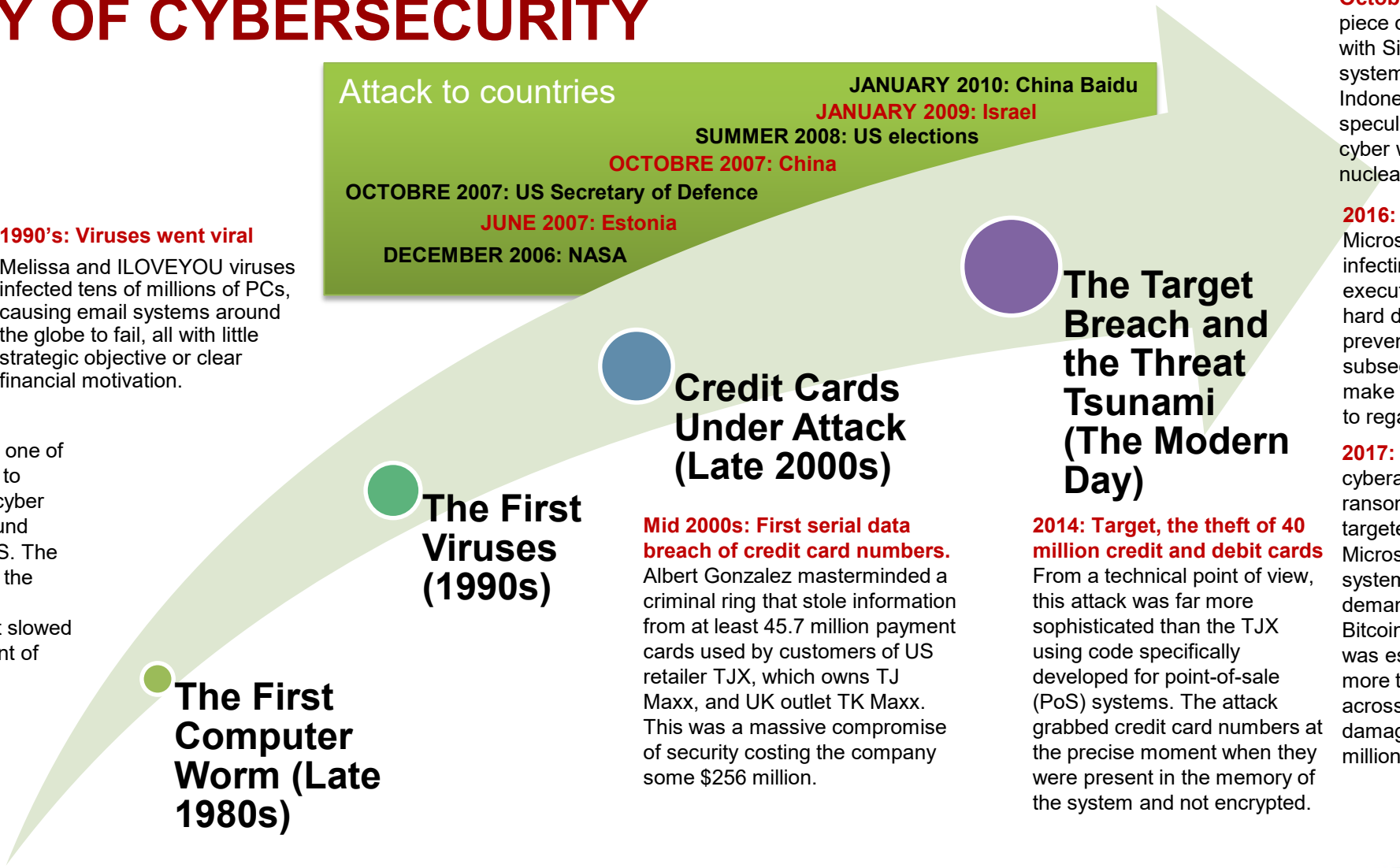
**Carrier**
Products & Services

**Enterprise**
Products & Services

**Cloud**
Products & Services


HUAWEI CLOUD
华为云

# HISTORY OF CYBERSECURITY




**1988 - The Morris worm** - one of the first recognised worms to affect the world's nascent cyber infrastructure - spread around computers largely in the US. The worm used weaknesses in the UNIX system Noun 1 and replicated itself regularly. It slowed down computers to the point of being unusable.

**1990's: Viruses went viral**

Melissa and ILOVEYOU viruses infected tens of millions of PCs, causing email systems around the globe to fail, all with little strategic objective or clear financial motivation.

**Mid 2000s: First serial data breach of credit card numbers.** Albert Gonzalez masterminded a criminal ring that stole information from at least 45.7 million payment cards used by customers of US retailer TJX, which owns TJ Maxx, and UK outlet TK Maxx. This was a massive compromise of security costing the company some $256 million.

**2014: Target, the theft of 40 million credit and debit cards** From a technical point of view, this attack was far more sophisticated than the TJX using code specifically developed for point-of-sale (PoS) systems. The attack grabbed credit card numbers at the precise moment when they were present in the memory of the system and not encrypted.

**October 2010: Stuxnet**, a complex piece of malware designed to interfere with Siemens industrial control systems, was discovered in Iran, Indonesia, and elsewhere, leading to speculation that it was a government cyber weapon aimed at the Iranian nuclear programme.

**2016: PETYA** The malware targets Microsoft Windows-based systems, infecting the master boot record to execute a payload that encrypts a hard drive's file system table and prevents Windows from booting. It subsequently demands that the user make a payment in Bitcoin in order to regain access to the system.

**2017: WANNACRY** Worldwide cyberattack by the WannaCry ransomware cryptoworm, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency . The attack was estimated to have affected more than 200,000 computers across 150 countries, with total damages ranging from hundreds of millions to billions of dollars

Evolution of the Cyber Security Response

**Creation of the first CERT**

**Development of antivirus technology**

**Development of more sophisticated security systems specifically designed to cope with threats on specific industries**

**Companies can no longer take an ad hoc approach to response. All levels of the organization must understand the risk of cybercrime and have committed all the appropriate resources to preventing breaches, detecting them when they do occur, and responding in the appropriate fashion**

# CYBERSECURITY HAS BECOME A TOP PRIORITY FOR THE EU

## European citizens and businesses rely on digital services and technologies:

Europeans believe that digital technologies have a positive[1] impact on:

**75%** our economy

**64%** our society

**67%** our quality of life

**86%** of Europeans believe that the risk of becoming a victim of cybercrime is increasing.[2]

Sectors like **transport**, **energy**, **health** and **finance** have become increasingly dependent on network and information systems to run their core businesses.

The **Internet of Things (IoT)** is already a reality. There will be **tens of billions** of connected digital devices in the EU by 2020.[3]

## Cyber incidents and attacks are on the rise:

**+4,000** ransomware attacks per day in 2016.

In some Member States **50%** of all crimes committed are cybercrimes.


Security incidents across all industries rose by **38%** in 2015 – the biggest increase in the past 12 years.

**80%** of European companies experienced at least one cybersecurity incident last year.[4]

**+150** countries and **+230,000** systems across sectors and countries were affected with a substantial impact on essential services connected to the internet, including

**hospitals and ambulance services.**

# Huawei's Approach to Trust

- Understand real cyber security risk in the global ecosystem and supply chain: sophisticated cyber actors can exploit systems and products virtually.
- Comprehensive cyber risk management – assessment, mitigation, and proof
- Agreed-upon security architecture
- Internationally recognized standards and best practices
- Risk-informed procurement requirements: recommended or required
  - NIST Cybersecurity Framework (CSF) – risk analytic tool
  - Strong supply chain risk management approach for suppliers of products and services (new version of NIST CSF released soon)
  - Testing of hardware and software for vulnerabilities or hidden functionality
- Conformance Programs to demonstrate trustworthiness of all providers

# Assurance -- “Transformation” of a Great Company

***Goal: to strengthen -- and promote transparency about – Huawei global and US assurance programs among customers and stakeholders.***

Huawei has released four global cyber security white papers:

- *21st century technology and security – a difficult marriage* (September 2012)
- *Making cyber security a part of a company’s DNA - A set of integrated processes, policies and standards (October 2013)*
- *Top100 cyber security requirements* – important to inform ICT buyers (Dec. 2014)
- *The Global Cyber Security Challenge – It is time for real progress n addressing supply* chain risk (June 2016).

http://www.huawei.com/en/about-huawei/cyber-security

# IMPLICATIONS FOR HUAWEI

**Technical Issue:** Attacks have grown in complexity and intensity, Cyber Security has become a priority for Governments

- Objective for Huawei: Huawei must comply with evolving national security laws and customers' technical requirements (NIS, Cybersecurity Act: « Certification »)

**Political Issue:** Cyber Attacks have become a Weapon more and more used by both State and Non-State Actors against Governments

- Objective for Huawei: As potential vector of an attack, Telecom Networks are the subject of concern for all the governments around the Globe. **Huawei, as a company originating from China, must make extra efforts to demonstrate that the company is a trusted partner.**

**Trade-related Issue:** Because it is a national prerogative, Cyber Security is instrumentalised to create a competitive disadvantage for Huawei compared to US or EU competitors

- Objective for Huawei: Although no proof has ever been found, **Huawei must answer to accusations of implementing backdoors, spyware etc. in its equipment to spy on foreign governments on behalf of the Chinese Government**

# HOW TO REACT?

## To political accusations

- Huawei is a **private company**, 100% owned by its employees
- **The Cyber Security, Counter espionnage and Intelligence Laws of China** have no impact on Huawei compliance to other countries' laws and regulations related to Cyber Security and Privacy, as stated in the « **Declaration of Jihong Chen and Jianwei Fang"**

## To trade-related issues

- Huawei has enjoyed the **trust from its customers** globally for 30 years
- Huawei has adopted an **open and transparent approach** and invites all customers and governments to test the equipment in Shenzhen (and soon in Brussels)
- Huawei has worked on **solutions with individual governments** when required (UK, Germany, Canada)
- Huawei is probably **the most poked and prodded ICT Manufacturer in the world**

## To Technically/process-related issues

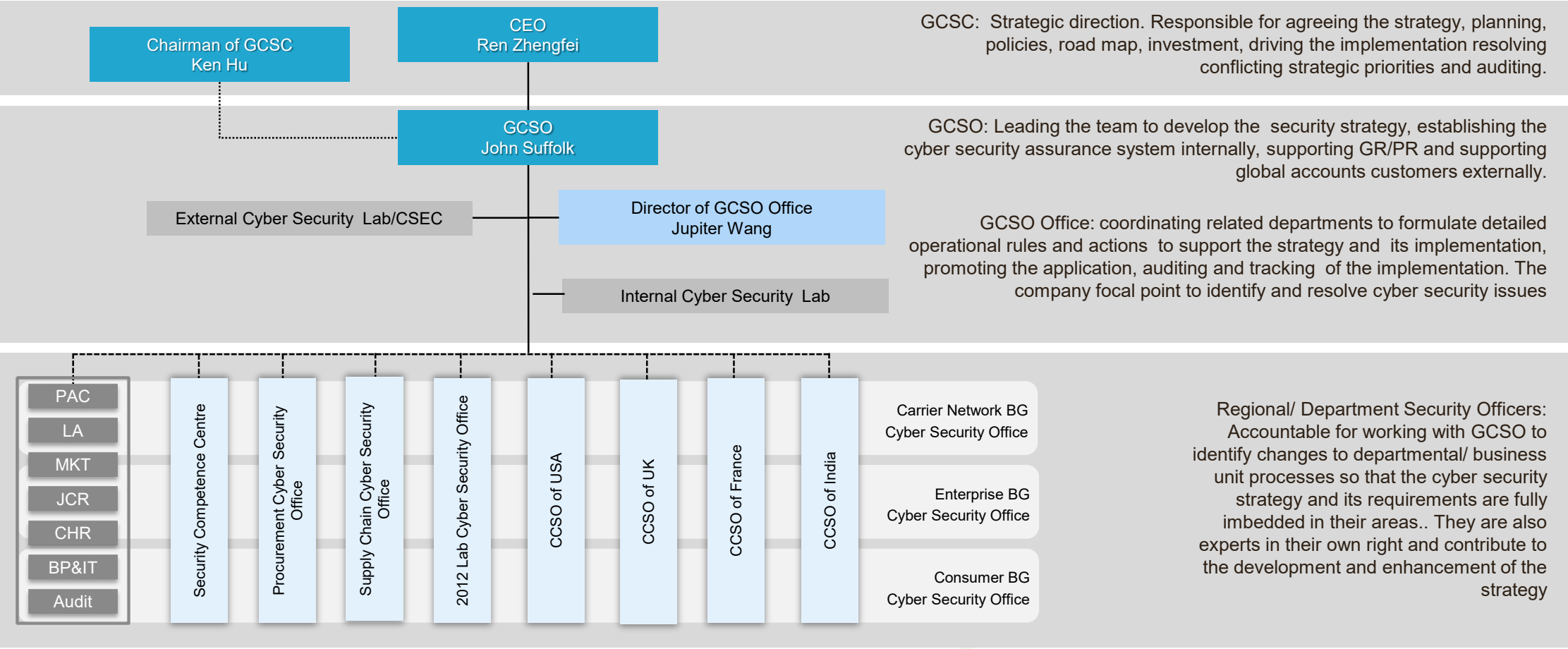
- Huawei over the years has built its own **Cyber Security Framework,** in which Security Assurance is built-in

# HUAWEI BUILT-IN CYBER SECURITY ASSURANCE

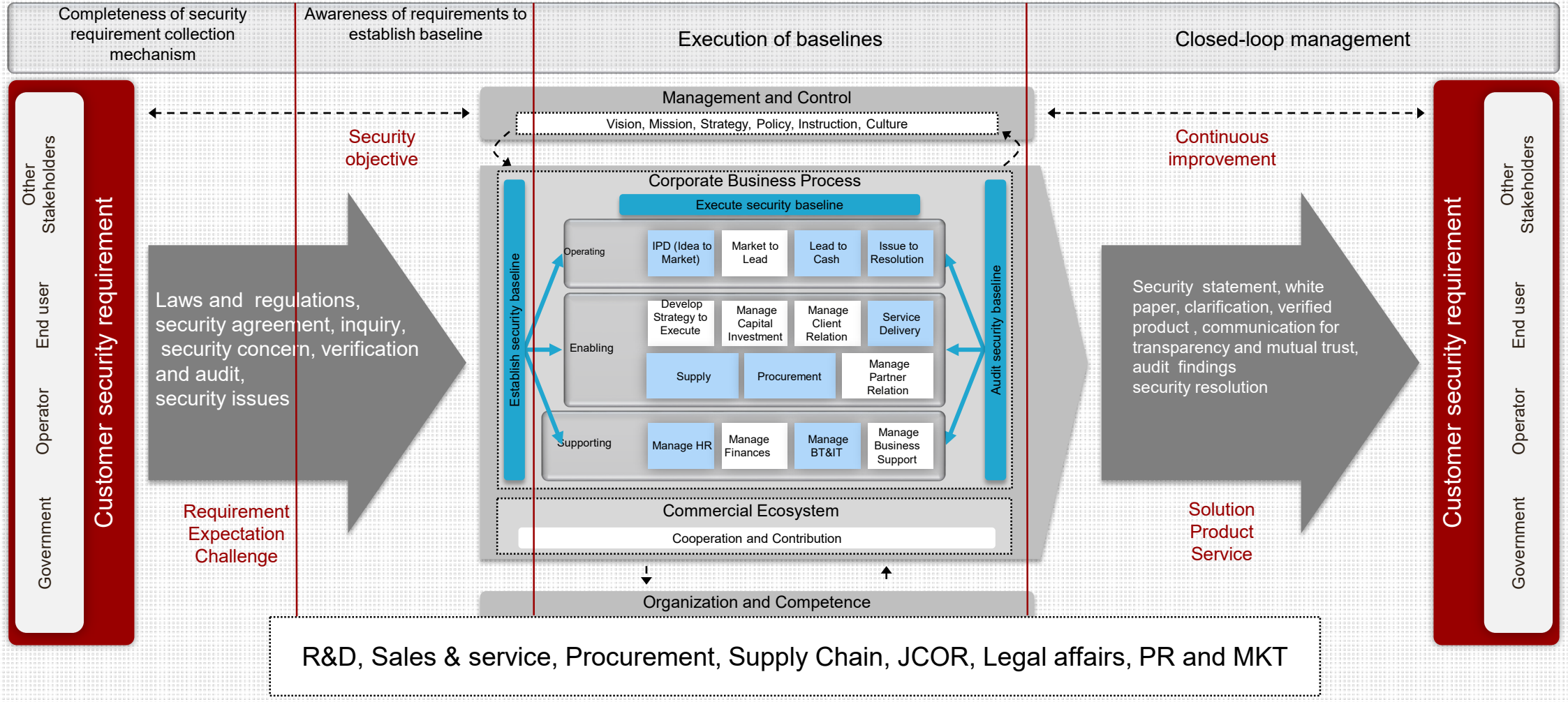

| Area | Focus |
|---|---|
| Strategy, Governance and Control | Having an overall strategy and the accountability to make it happen |
| Standards and Processes | Using the best standards and approaches to protect against threats and risks |
| Laws and Regulations | Making your products and operations legally compliant in every country you operate in |
| Human Resources | Getting the right people, in the right roles with the right behaviour to limit insider issues |
| Research and Development | Designing, building, testing products in a secure way that builds on the above building blocks |
| Verification: Assume nothing, believe no one, check everything | Many eyes, many hands many checks. Tiered independent approach to security verification |
| Third-Party Supplier Management | Getting your suppliers to take security seriously – 70% in the box is not Huawei's |
| Manufacturing | Manufacturing products that secure each step along the way – right through to delivery |
| Delivering Services Securely | Ensuring installation, service and support is secured. No tampering, fully auditable |
| Issue, Defect and Vulnerability Resolution | As issues arise, solving them quickly and ensuring customers technology is secured |
| Audit | Using rigorous audit mechanisms to ensure every part of Huawei conform to the strategy |

# GOVERNANCE

To deliver our strategy across the whole company we are led by a Board security committee, but ALL Huawei employees must “own” cyber security

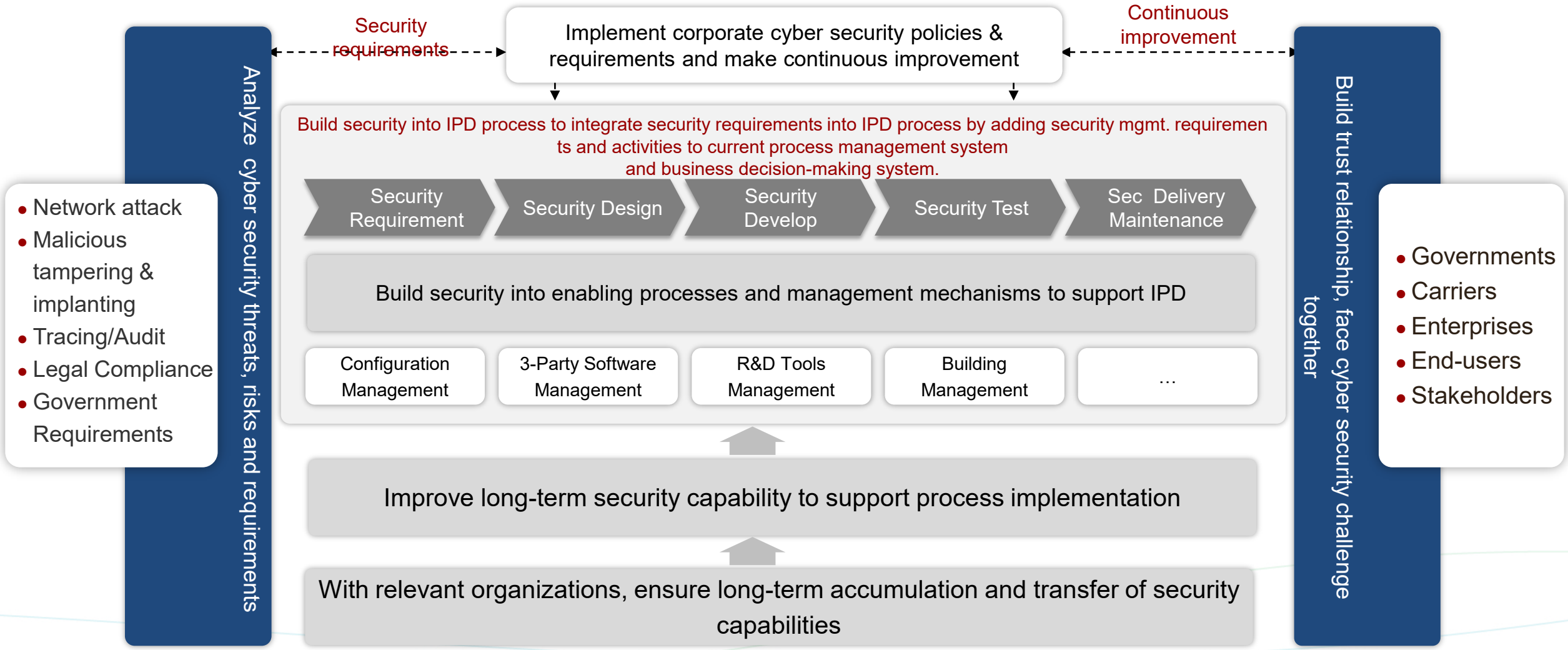


# Huawei Cyber Security Assurance
## End-to-End Cyber Security Management

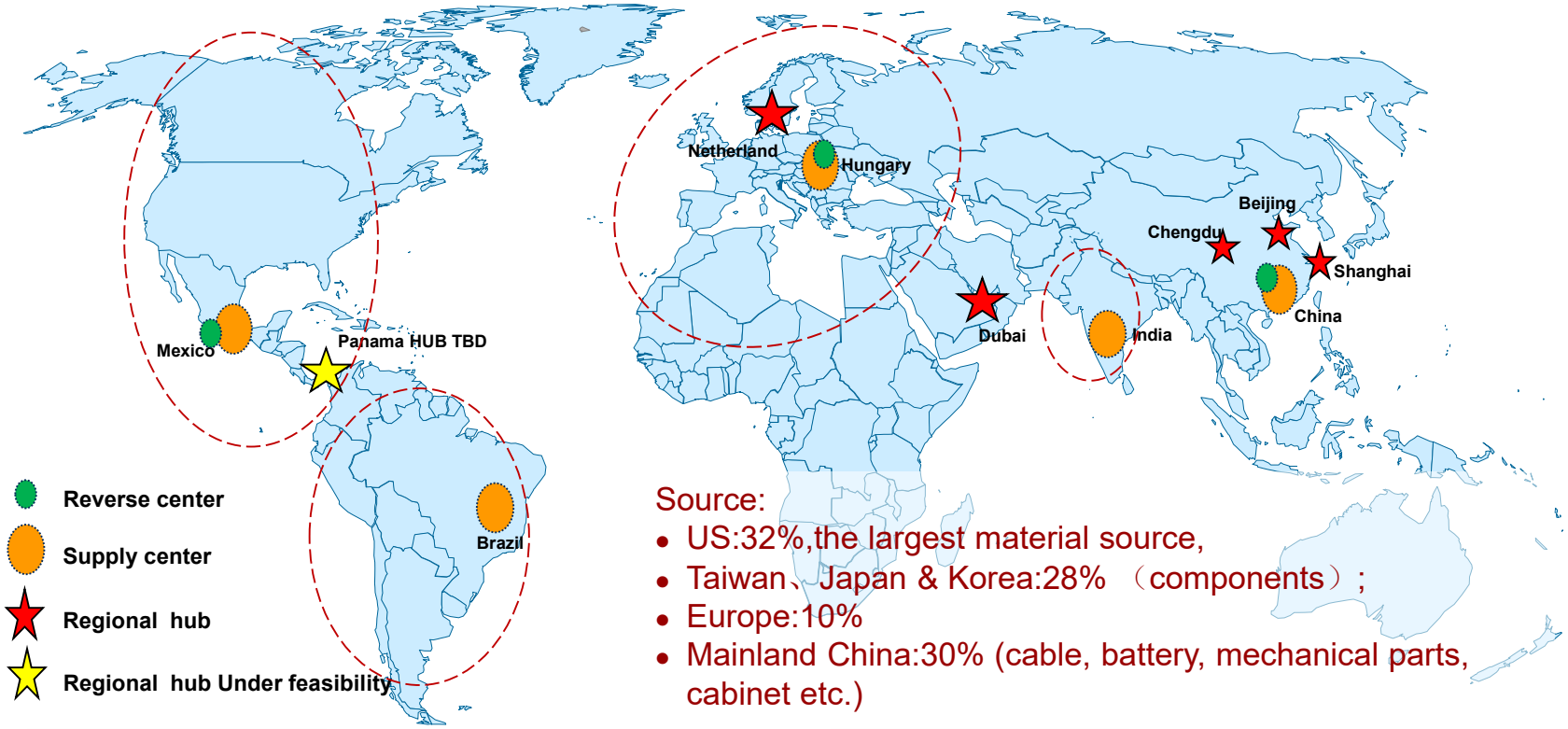


# Huawei R&D Cyber Security Assurance System

Philosophy: Enhance product security based on the main R&D process with enabling processes, capability building and organization establishment to support implementation



# Huawei Global Supply Network



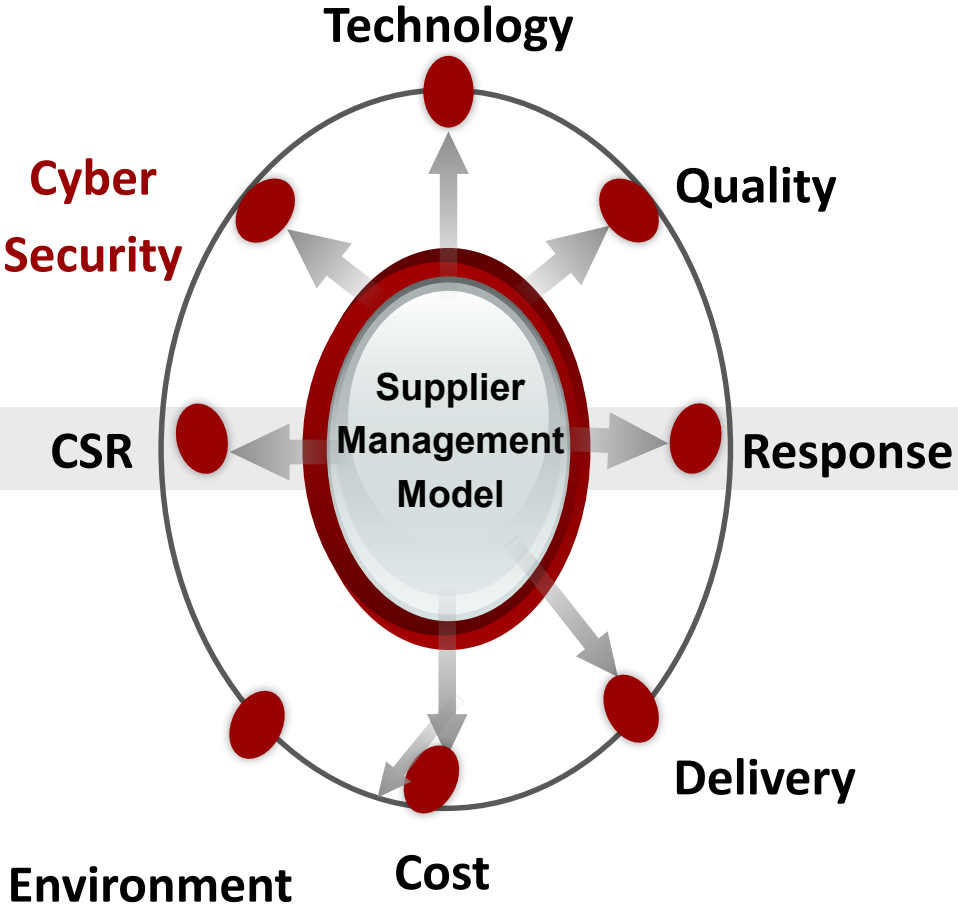

Source:

- US:32%,the largest material source,
- Taiwan、Japan & Korea:28% （components）;
- Europe:10%
- Mainland China:30% (cable, battery, mechanical parts, cabinet etc.)

| Supply Center | Regional Hub | Reverse Center | Local EMS |
|---|---|---|---|
| • China (Delivery for the globe)<br>• Europe (Delivery for West Europe &North Africa)<br>• Mexico (Delivery for North America & Latin America)<br>• Brazil (Delivery for South Latin America )<br>• India (Delivery for India) | • Dubai (United Arab Emirates )<br>• Netherlands | • China<br>• Mexico<br>• Europe | • Brazil , Mexico, India and Hungary supply centers work with local partners to do manufacturing and make delivery |

# Huawei's Approach

## 8 Elements of Supplier Management: TQRDCESS




CSR: customer satisfaction representative

TCO: total cost of ownership

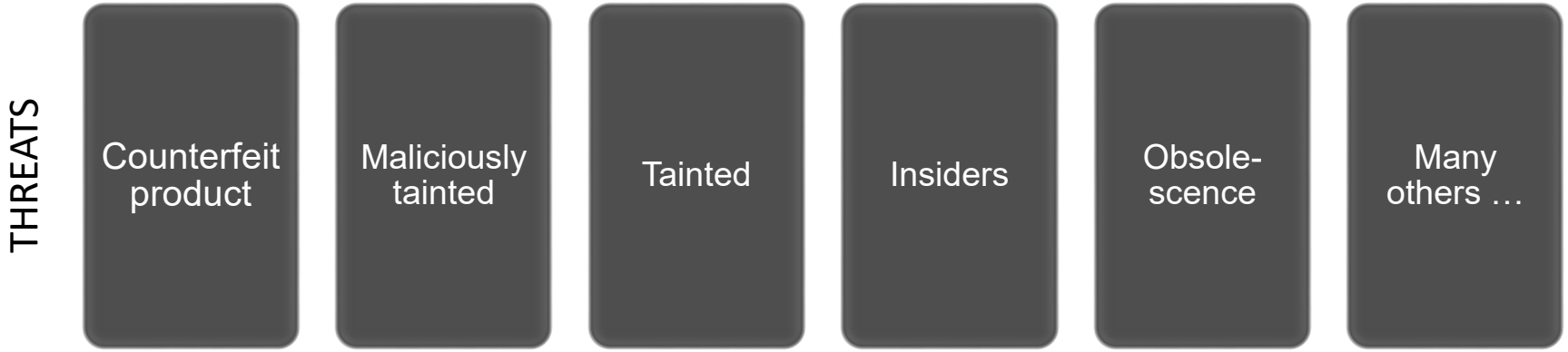
### Supplier Management Model

- Supplier management includes eight elements: Technology, Quality, Response, Delivery, Cost, Environment, CSR, and **Cyber Security**.
- **Security** has been integrated into the procurement business processes, including cyber security policies, baseline, and process criteria.

# Supply Chain Risk - A Threat-Based Problem

Global supply chain security for COTS products

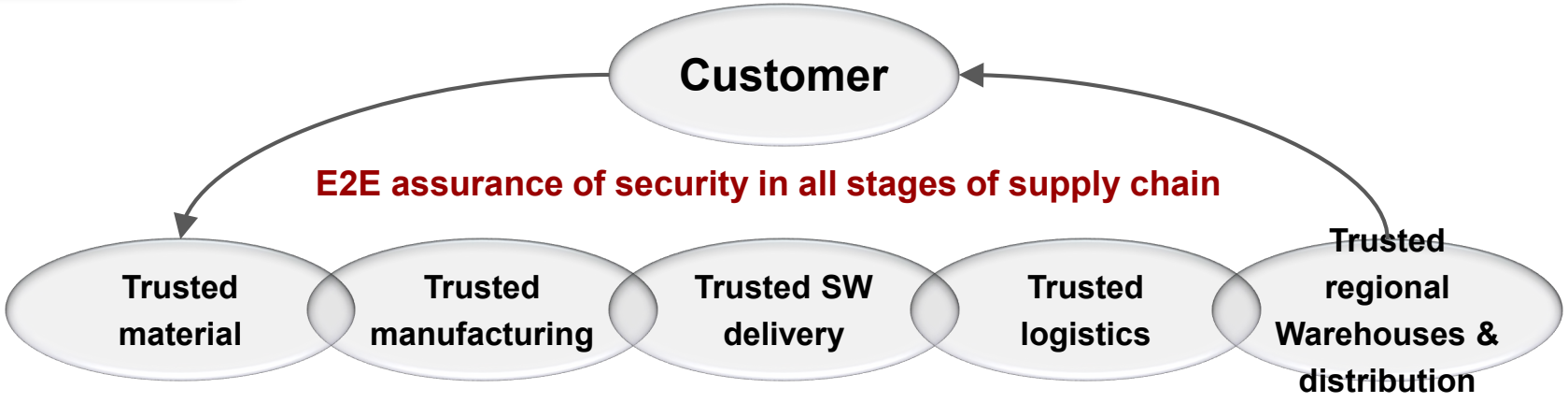
- Commercial Off the Shelf Products are developed and used globally
- COTS products rely on components that are often globally sourced
- COTS products are integrated into Critical Infrastructure, Government systems and Commercial solutions



# Supply Chain Security Strategy

Based on the overall corporate security strategy, Huawei is committed to establishing a supply chain with the following DNA:

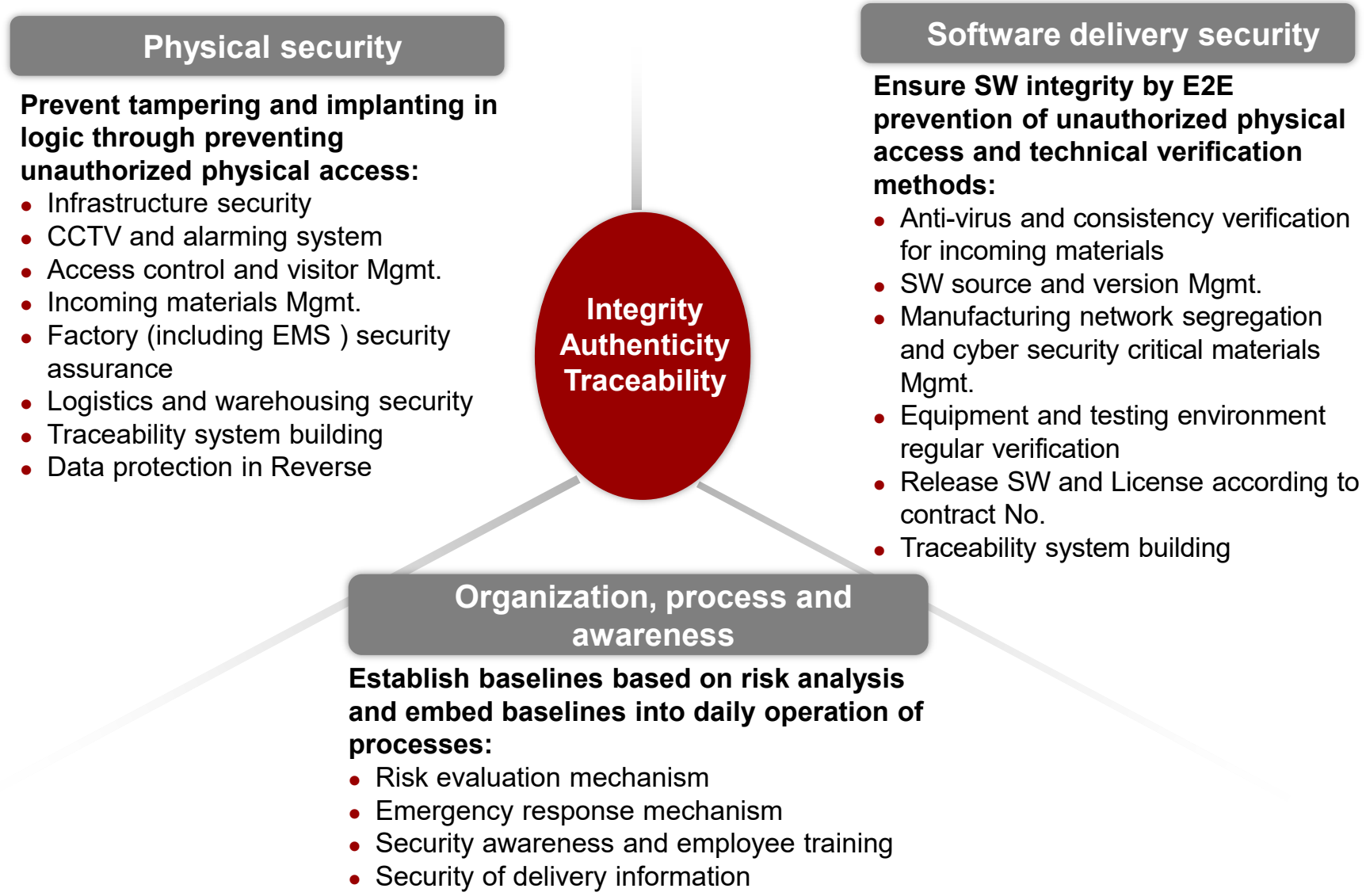
| | |
|---|---|
| **Efficiency** | Promote timely and efficient flow of products and services in the supply chain, protect the supply chain from exploitation and reduce the risks of supply chain interruption. |
| **Security** | Ensure products and services integrity in global supply chain. Identify and resolve threats early in the process and strengthen the security of supply chain infrastructure, logistics and information assets; establish a sustainable supply chain security management system. |
| **Resilience** | Identify supply chain risks and work out improvement plans to ensure the supply chain can quickly recover from disruption due to changing threats and risks. We will also establish an accurate and effective traceability system to identify and mark problems at the first time and recover and improve the supply chain quickly and pointedly. |



# Supply Chain Cyber Security Baseline Management


- Based on risks to the supply chain and customer & government requirements, we develop cyber **security baselines** aiming to protect product integrity, traceability, and authenticity and take a built-in approach to integrate the baselines into processes.
- **We have developed 93 baselines around 10 security elements** and developed or optimized 67 documents of L3/L4 processes.

# Framework of SCM Cyber Security Baselines



# Integrity and Traceability

## Integrated processes and technology required along supply chain

- ISO28000 supply chain security system operating and 3rd certification.
- Global multi-supply centres to provide efficient and resilient supply to customers.
- Set up barcode system to support multi-ways of tracing.

| S-NPI | Plan | Make | Order Fulfillment | Return | Manage Supply Operation |
|---|---|---|---|---|---|

### Security of incoming materials

- Identity verification of deliveryman
- Inspection of goods packing
- Review & inspection of goods
- Performance test
- SW integrity check
- Product distribution & pre-production inspection

### Security of Factory (EMS)

- Employee security training
- Control of sensitive area
- Separated & controlled production network
- Control of SW & documentation
- SW download verification & QC inspection
- Digital certificate loading & check
- Product 100% anti-virus inspection
- Regular equipment verification
- control of personal account & system authority

### Security of logistics & warehousing

- Realize electronic customs declaration, transportation route design & monitoring of logistics process through IT system
- Set up dedicated documents to check & monitor the integrity of containers, shipment &loading
- Seal mgmt & correct sealing

Infrastructure & entry control：7*24 security guard and CCTV monitoring, Electronic entry control & identify identification system

**ISO28000 certificate**


**C-TPAT 3rd party audit report**

# INTERNATIONAL COOPERATION IS KEY FOR OUR SUCCESS

We also believe that international standards should be adopted and promoted and we make a major contribution to international bodies and standards groups in relation to security – we adopt all recognized standards

# COMING NEXT: THE EUROPEAN CYBERSECURITY CENTRE

## Experience Center

**Demonstrate security competitiveness of Huawei solutions and Huawei's cyber security engineering capabilities that can be experienced and perceived.**

- Huawei's overall security solution philosophy and six major security solutions (SoftCom, Big Data, public cloud, 5G, IoT, and cloud-based network)
- Huawei's E2E cyber security assurance practices and engineering capabilities, as well as cyber security engineering capabilities
- Huawei's transparent and open test methods


## Evaluation Center

**Provide standardized white box cyber security test and evaluation services externally.**

Open test environments to governments and customers, and allow them to assess Huawei products and solutions.

## Knowledge Hub

**Construct a one-stop knowledge platform that can be used for external voicing, and build Huawei's position as a thought leader; Carry out communication and cooperation to enhance mutual trust and present value.**

- Hold cyber security conferences and events (such as launch events, workshops, lectures, and industry conferences) to promote research achievements of the industry/Huawei.
- Perform external communication in a professional, continuous, and consistent way, positioning Huawei as a thought leader.
- Provide customers with cyber security training services, such as cyber security management practices, cyber security awareness improvement, and supplier cyber security management.

# Thank You.