

Cyber Security Strategy and Approach

www.huawei.com

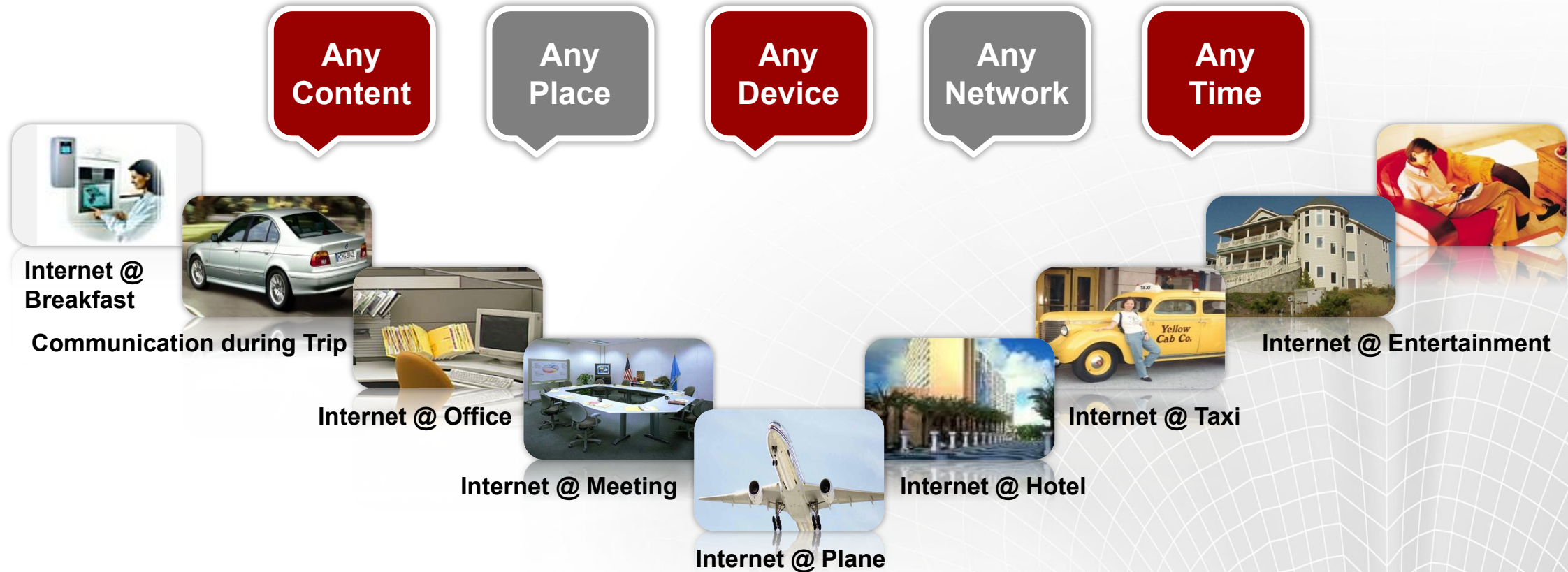
Huawei Confidential



The contents of this information pack are as follows:


- **The positive difference that technology brings to the world and every citizen**
- **Cyber Security Challenges that we all face**
- **Huawei's Strategy**
- **Closing Thoughts**

The positive difference that technology brings to the world and every citizen



Future = Ubiquitous + Omnipotent

Open networks connect the world, facilitate economic exchanges across regions, and promote global trade

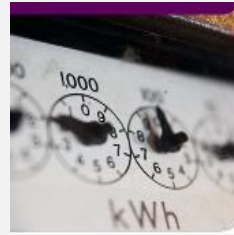
7 Billion People  **50 Billion Machine**

In-vehicle Communication & Smart Traffic



Vehicle communication, navigation, tracing, security and maintenance

Auto Meter Reading



Remote meter reading is safer and easier. Benefit for Green City construction

Merchandise Distribution



RFID is used for merchandise trade and garbage sorting mgmt

Remote monitoring & Healthy



Remote Home-caring, Healthy, Safety mgmt

Vending



Vending, cargos magt, E-wallet mgmt

Electronic Consumer



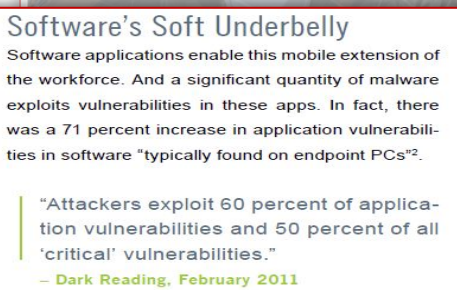
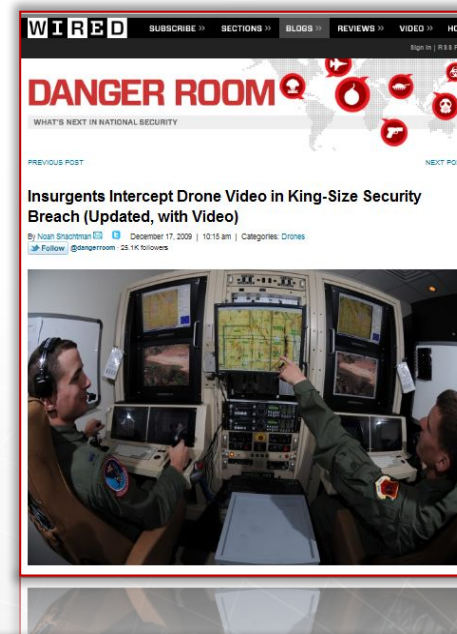
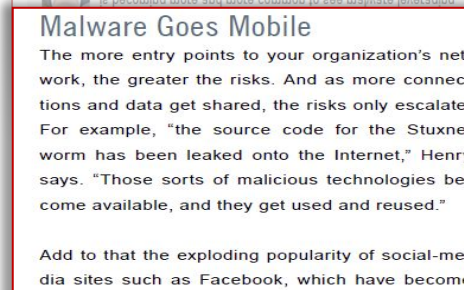
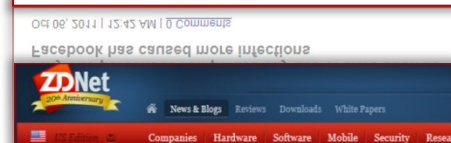
Info Sharing, on-line game, media download, communication and etc.

CONTENTS: However just as in other walks of life, there are Governments, business and individuals who wish to use technology for negative purposes

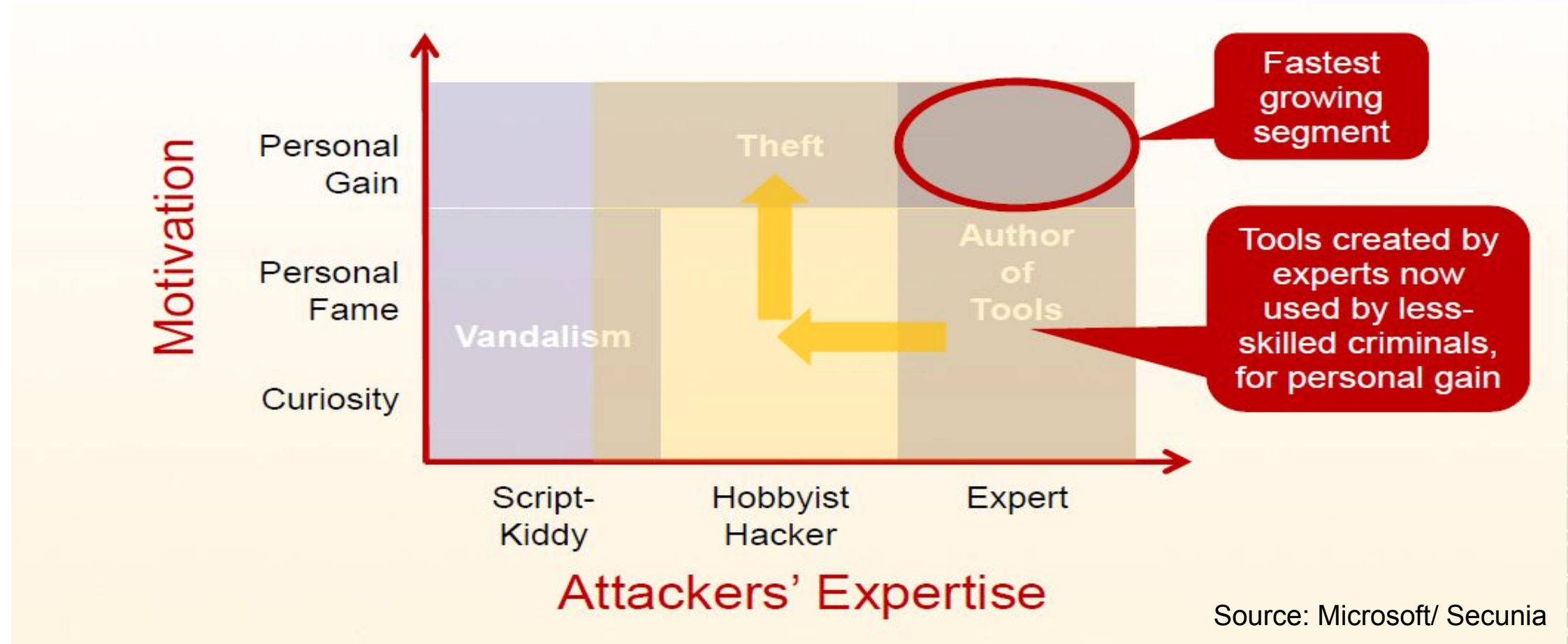
- The positive difference that technology brings to the world and every citizen
- **Cyber Security Challenges that we all face**
- Huawei's Strategy
- Closing Thoughts

Technology and its use is advancing at an amazing rate and brings substantial benefits to all, but so are the threats to the users of technology advancing

- It is hard to stop the tide of progress and technology innovation. Threats are increasing every day.
- The bad guys are getting significantly more sophisticated.
- And international law provides its own security twists and turns.
- And finally it is impacting on almost all hardware and software – even air-gaped systems are being breached.



Cyber Security – The threat is changing, roles are changing and the purpose of the attack is changing – politics, protectionism, money and hacktivism



Cyber space is a new competitive field. Achieving an effective, global, industry-wide solution is going to demand sober and fact-based dialogue

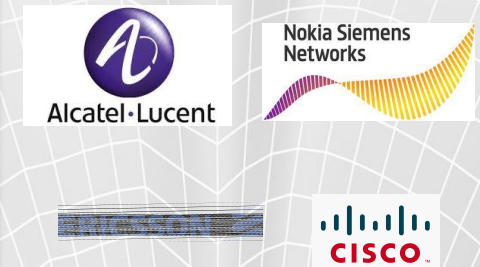
- Our world has become truly connected, cyberspace has gradually become the “nervous system” through which society operates.
 - As reported by the World Bank, for every 10% increase in broadband penetration, the GDP in developing countries will increase 1.38%.
 - In our world, over 87% of the planet’s population are mobile users, global smartphone users reached 3.9 billion by 2021, up 6.1 percent.
- Network technologies have turned out to be remarkable innovations. Open networks have made it easier to obtain and share information and have created untold opportunities for people to invent. There also has been a dramatic increase in the use of technology by governments, enterprises and consumers.
 - The costs of innovation are lowered which means that consumer, small and medium-sized enterprises and micro-enterprises have the opportunity to innovate on the same platform as large enterprises.
 - In the past 10 years, carriers' investments in network infrastructure have reduced the coverage gap from 1/3 to 6% globally. That is, only 6% of the global population live in areas without network coverage.
 - Global total 5G connections to reach 1 billion by 2022
- Now nearly everyone is connected and there are many ways to use cyberspace , so the means and the opportunity have therefore greatly increased.
 - The wave of telecommuting and cloud migration caused by COVID-19 opens up new avenues for cybercriminals. In 2021, cyber-attacks around the world are on the rise due to remote working conditions, data breaches caused by ransomware, phishing, and human misoperations are increasing, and cyber-threats remain on a global scale. In particular, ransomware is highly rampant. In the first half of the year, the number of attacks has reached 304.7 million, increase of 151%, far exceeding the total number of attacks in 2020, and has affected multiple countries, industries, and domains to varying degrees.

Cyber security is not a single country or specific company issue, because the world is global, innovation is global, the supply chain is global, we are also global– consider this...

The Chinese city of Chengdu has 16,000 companies registered and 820 of them are foreign-invested companies. Of these, 189 are Fortune 500 companies. Household brand names such as Intel, Microsoft, SAP, Cisco, Oracle, BAE, Ericsson, Nokia, SAP, Boeing, IBM and Alcatel-Lucent are all located there to name but a few.



Every major telecommunications equipment provider has a substantial base in China. Alcatel-Lucent has its biggest manufacturing base globally in China; Ericsson's joint-venture Nanjing Ericsson Panda Communications Co. has become the biggest supply centre of Ericsson in the world; Nokia-Siemens has 14 wholly owned or joint ventures in China, and its factory in Suzhou manufactures a third of its global production of wireless network products.

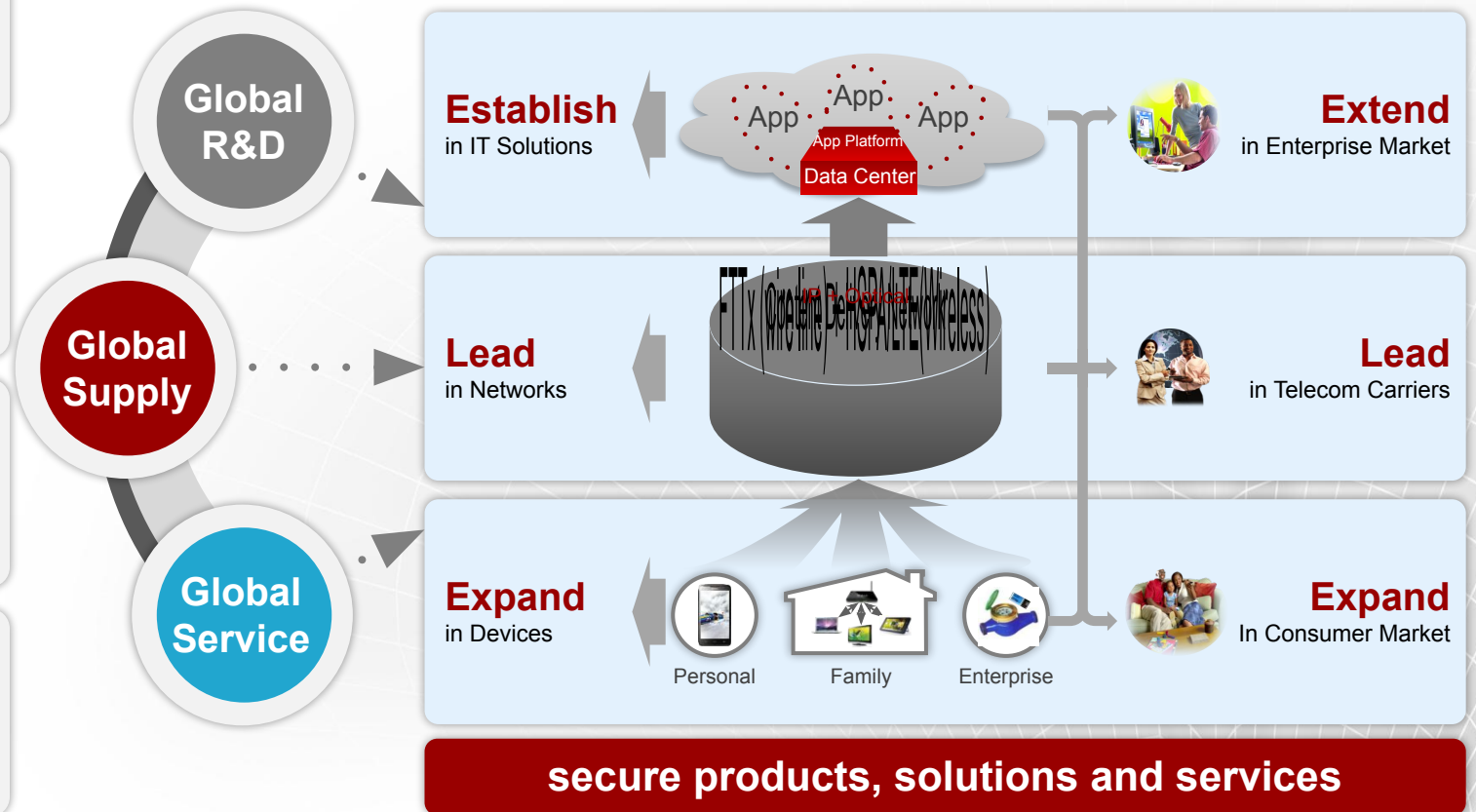


CONTENTS: To continue to maximise the benefits of the technology to mankind we must address the strategic and operational requirements of cyber protection

- The positive difference that technology brings to the world and every citizen
- Cyber Security Challenges that we all face
- **Huawei's Strategy**
- Closing Thoughts

Huawei is a global organization serving over a third of the planets population

- A leading global **ICT** solutions provider
 - A **private** company established in 1987
 - A **Fortune Global 500** company
-
- 14 Regional Headquarters, operations in 170+ countries
 - 190,000+ employees with 150+ nationalities worldwide, 73% recruited locally
-
- 70,000+ engaged in R&D
 - 15 R&D centers located in 29 cities
 - 25 Joint Innovation Centers
 - 26,539 patents
-
- \$99.8 B revenue in 2021
 - Serving 45 of the world's top 50 operators
 - Serving over 1/3 of the world's population



In considering our strategy, we position ourselves for a never ending company transformation that seeks to promote the use of ICT but mitigate the threats

THREAT ASSUMPTIONS

Cyber crime is a global clear and present danger and in the LONG term will continue to increase rapidly.

As globally more technology is designed and used as part of everyday life our globally interconnected technology world becomes even more attractive to attack from cyber criminals.

Cyber criminals are increasingly adept at gaining undetected access and maintaining a persistent, low-profile, long-term presence in IT environments.

The cumulative cost of attack and penetration techniques by cyber criminals are outstripping investment in remedial and defensive solutions.

All parts of an organisation are potentially weak-spots and must be given adequate attention when it comes to protective measures.

SO WE BELIEVE:

- We will be attacked and we will be breached.
- We will find some attacks but not others.
- We must plan for the worst outcome.

THEREFORE:

- We will adopt the “many eyes and hands” approach to design, development and testing of our technology.
- Tracking, tracing effective communication and remediation must become core skills across the whole Huawei value chain.

WE WILL:

- Adopt a “built-in” approach and implement, or develop, global best practice & processes on cyber security system.
- Significantly raise the awareness and understanding of cyber security with all Huawei people.
- Collaborate globally to mitigate threats and raise standards.

Cyber security is a Huawei crucial company strategy



Mr. Ren
Huawei CEO

“Huawei hereby undertakes that as a **crucial company strategy**... Taking on an **open, transparent and sincere** attitude, Huawei is willing to work with all governments, customers and partners to jointly cope with cyber security threats and challenges ... Our **commitment to cyber security** will never be outweighed by the consideration of commercial interests.”

Our Cyber security vision and mission focusing on the needs of our customers

Vision

To provide secure, easy and equal access to information services.

Mission

Working internationally to develop the most effective approach to cyber security, establishing and implement an end-to-end customer-oriented cyber security assurance system within Huawei, which is transparent and mutually-trusted, so that we ensure customer's long-term security trust.

To be successful in minimizing our ongoing threat, our cyber security strategy is a whole of company transformation – it isn't just a technology challenge

Critical Success Factors

- 1. Total commitment from the CEO, Board and Global Executives to develop and deliver a holistic cyber security strategy**
- 2. A strategy based on addressing future challenges, not just today's or yesterday's threat**
- 3. Clear governance, roles and responsibilities**
- 4. Consistently understood, globally rolled-out repeatable processes on which to imbed the change – it is not a “bolt-on” strategy but a “built-in” strategy**
- 5. Openness and transparency on our progress, our successes and our failures**
- 6. Many “eyes and hands” from around the world to improve and enhance our thinking and our actions on cyber security – Plan, Do Check, Act**
- 7. It is not a “Programme” so it never ends. We loop back to number 1**

Our current focus is on designing and implementing security activities

EXTERNALLY FOCUSED

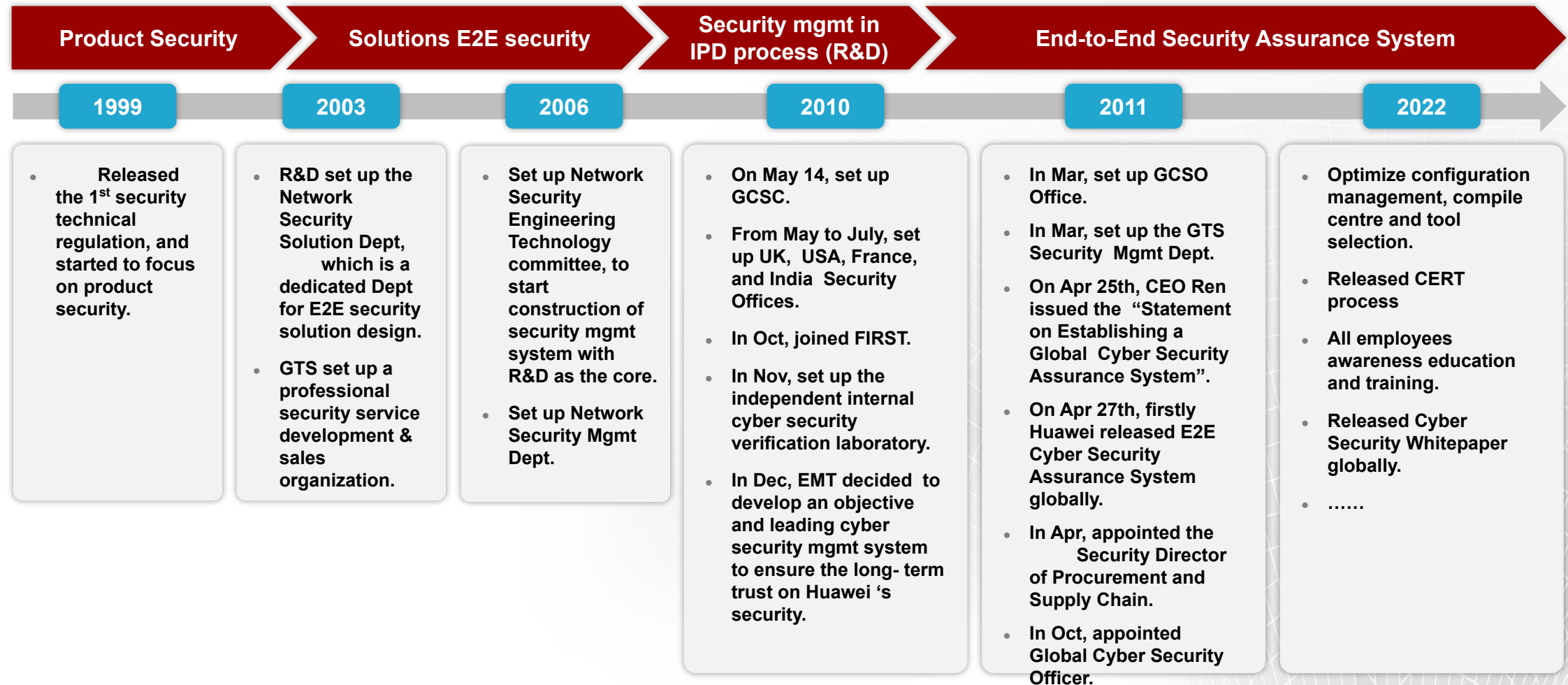
- **OPENESS, TRANSPARENCY AND COOPERATION:** We will actively work with stakeholders in an open and transparent manner to meet and resolve the security challenges and concerns of our customers and Governments.
- **PROACTIVE COMMUNICATIONS:** We will proactively communicate the global nature of ICT and cyber security to as wide an audience as possible encouraging mature debate with a recognition that we must all positively work together and champion international fair, reasonable and non discriminatory standards, policies and regulation.
- **COMPLIANCE WITH LAWS AND REGULATIONS:** We aim to comply with security and privacy protection standards and laws of relevant countries or regions, by analysing these laws and regulations and imbedding these requirements into our products and services and the way we do business. We will ensure the delivered products and services can withstand legal investigations and the result of investigation will prove positive to Huawei.
- **VERIFIED BY INDEPENDENT THIRD-PARTIES:** We will construct and develop a global capability to support independent testing, verification and certification of our products using approved third-parties, so that our customers receive internationally recognized security assurance.
- **EMERGENCY RESPONSE:** We aim to monitor threats on our own technology, national, international and company security vulnerabilities so as to be in a position to responsibly report or pre-warn our customers, respond quickly to threats and apply appropriate security patches to protect our customers.

Our current focus is on designing and implementing security activities

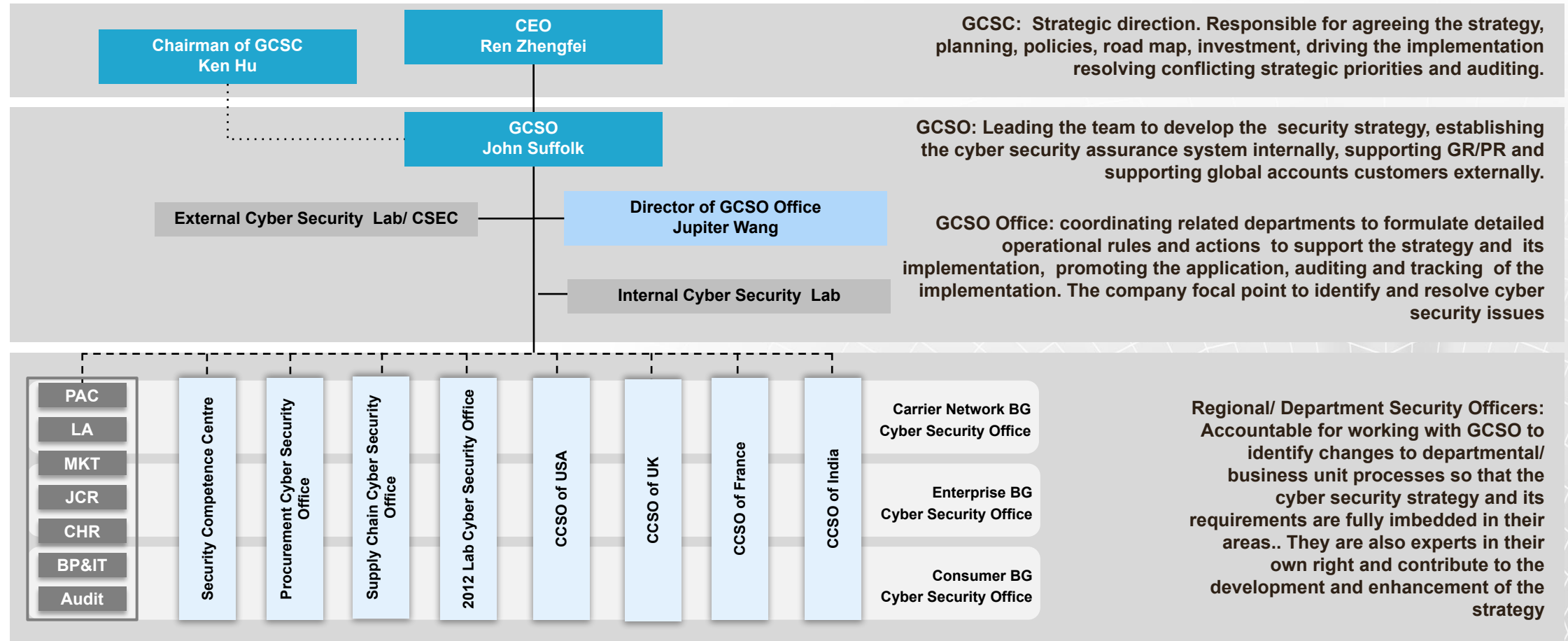
INTERNALLY FOCUSED

- **EMPLOYEE AWARENESS AND RESPONSIBILITIES:** We will raise employees' cyber security awareness based on law to make them understand they need to bear the liability for their behaviours even without malicious intention. For all critical positions appropriate security qualifications must be obtained and we will take measures to deter employees with malicious intention and prevent the occurrence of malicious acts.
- **SECURE BY DESIGN, DEVELOPMENT AND DELIVERY:** From the continuous analysis of emerging and actual technology threats across our complete product and service portfolio, we will build security into our processes, designs, development & delivery. We will separate out Huawei software from Huawei hardware thus enabling our competitor's software to execute on our hardware avoiding the claim that Huawei technology has hidden capability. We will also split our software so that our base software, country specific software (only allowed to be sold in certain countries) and engineering support tools are all individually approved and under the total control of our customers.
- **NO "BACK DOOR" AND TAMPER PROOF:** We will never knowingly allow a "back door" to be implemented and we will protect the integrity of software by implementing processes to protect against unauthorized tampering and potential breach using technologies such as digital signatures. We will legally manage remote access in case of trouble shooting from our several Global Technical Assist Centres, and never transfer data from customers' network to other country without the customer's permission.
- **TRACEABILITY:** We aim to make relevant products, solutions, services and components traceable through the complete product lifecycle using professional management tools and integrated systems.

We make no claims about our approach or comprehensiveness to cyber security, like all companies, we know we have much to do, but this is not the start of our journey



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

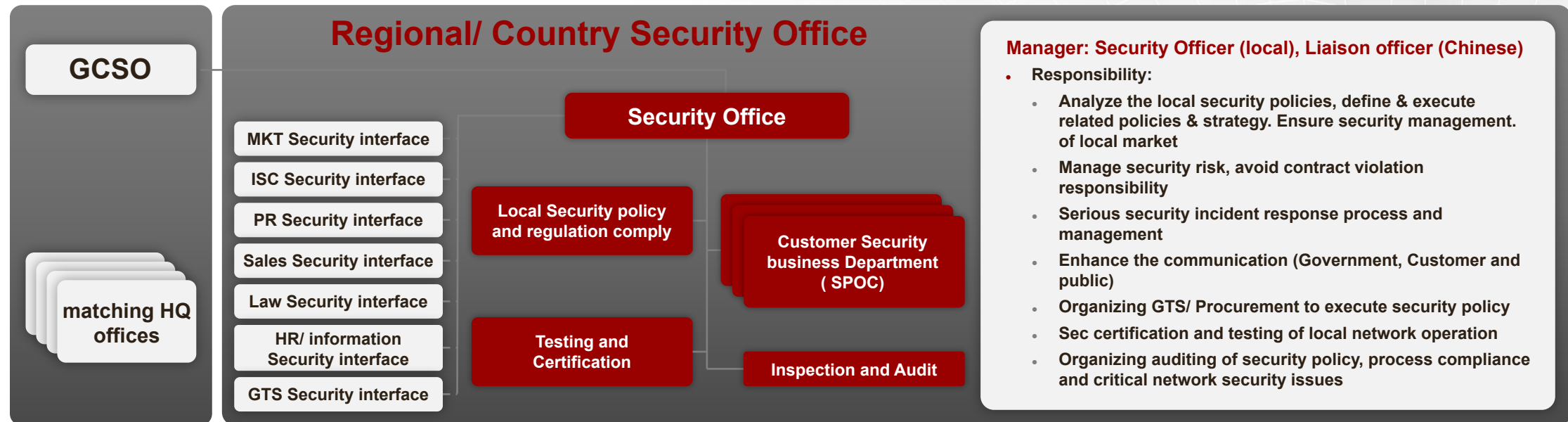


But not everything can be done from the centre, it is important that local country requirements and resources play a big role in making our strategy a success

The reality is the law cannot cope with the pace of the fast evolving new technologies, Internet cross-borders and many national legislations are in conflict. The concept of privacy has a large cultural component. American privacy is not German privacy, neither Arab privacy – A local view therefore is critically important.

THEREFORE:

The local Security office is in charge of the local security policy ensuring compliance with local laws and requirements. The focus is on local government and customer security requests, issues and concerns.



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

security groups in standard organizations



security product and solution providers



security certificating and auditing organizations



CERT(Computer Emergency Response Team) coordination organizations



CONTENTS: Huawei still emphasize that threat will never stop, we will continue to work hard, and cooperate with the government, operators and consumers together to management the global security conundrum

- The positive difference that technology brings to the world and every citizen
- Cyber Security Challenges that we all face
- Huawei's Strategy
- **Closing Thoughts**

Closing Thoughts: Threat will never stop, we never stop

- The development of networks has helped to advance social progress. Open networks have encouraged information flow and sharing, provided more opportunities for innovations, lowered the costs of innovation, and has helped improve the world's health, wealth and prosperity.
- Cyber security is not a single country or specific company issue. All stakeholders – governments and industry alike – need to recognize that cyber security is a shared global problem requiring risk-based approaches, best practices and international cooperation to address the challenge.
- As a crucial company strategy, Huawei has established and will constantly optimize an end-to-end cyber security assurance system.
- This is a continual effort, and Huawei is committed to providing best-in-class products and services to meet the needs of our customers. We take cyber security seriously and have invested substantial resources into our efforts to promote and improve the ability of our company, our peers and others to provide the best-possible security assurance and ensure a safer and more secure cyber world for all.



Thank you

www.huawei.com

Copyright©2012 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.