

Huawei's Position Paper on Cyber Security

November 2019



Contents

I. Executive Summary	03
II. Introduction	07
1. Huawei's white papers on cyber security	07
2. Purpose of this position paper	09
III. ICT Offers Enormous Potential for Global Development	11
IV. Rational Approach to Risk Management	15
1. Cyber security involves many elements	16
2. Supplier country of origin is not an element for security risk	18
3. Rational, objective, and evidence-based assessment of cyber security risks	20
V. Systematic Governance of Cyber Security	22
1. Unified cyber security standards	22
2. Independent cyber security verification	25
VI. Huawei Delivers Trustworthy and High-Quality Products	28
1. Huawei's Global Cyber Security and User Privacy Protection Committee (GSPC) led by Deputy Chair of the Board	28
2. Embedding cyber security elements into end-to-end processes ---	31
3. Huawei's Cyber Security 2.0	33
4. Launching transformation programs to drive innovation on security technology	35

5.	Providing secure products and solutions -----	37
a)	HiSec security architecture -----	37
b)	Huawei's 5G solution security architecture -----	39
c)	Huawei's IoT solution security architecture -----	49
d)	Huawei Cloud security architecture -----	55
e)	EMUI security architecture -----	57
VII.	Business Independence -----	61
1.	Huawei is a private company wholly owned by its employees ----	61
2.	The Chinese government does not interfere with our business or the security of our products -----	61
3.	Huawei exists to serve its customers -----	63
VIII.	Open and Transparent Collaboration -----	64
1.	Working more closely with security scholars through the Security Advisory Board -----	64
2.	HCSEC offers world-class security expertise and technical assurance -----	66
3.	Huawei's Security Innovation Lab in Bonn explores security standardization and verification for new technologies -----	68
4.	Huawei's Cyber Security Transparency Centre in Brussels: commitment to building trust in a digital world -----	69
IX.	Huawei cyber security manifesto -----	71
X.	About Huawei -----	74

I. Executive Summary

Information and communications technology (ICT) unlocks the enormous potential of the digital economy. The world's digital economy has grown 2.5 times faster than global GDP over the past 15 years. The digital economy will produce US\$23 trillion in new economic potential by 2025 (from US\$12.9 trillion in 2017). In other words, by 2025, the digital economy will represent 24.3% of global GDP, up from 17.1% in 2017.

The rapid development of digital technologies also brings new security challenges. All industries are undergoing digital transformation. New technologies like cloud, the Internet of Things (IoT), and artificial intelligence (AI) are spreading. All of these mean that cyber security risks are rising. If we want to benefit from the expansionary economic impact of ICT, maintaining secure ICT environment is key. As a global technology provider, Huawei is acutely aware of just how important cyber security is for ensuring trust in the digital world we all share.

Today, cyber security is increasingly intertwined with political

suspicious and trade barriers and falling trust between nations. Political suspicions have done nothing to solve the issues of cyber security. Frequently, cyber security is used simply as an excuse to erect trade barriers, and this has further obscured the real issues.

An effective solution must be firmly based in facts. Huawei encourages all stakeholders in the digital ecosystem to evaluate risks in a rational, objective, and evidence-based way. If we focus our attention on irrelevant factors like vendors' country of origin, it will only delay the resolution of security issues. If our approach to risk is based in emotion or bias, then our outcomes will be uncontrollable and we will be unable to achieve our security goals.

Cyber security involves many elements and stakeholders. An all-industry, full-society approach to collaboration is essential to enhancing systematic cyber security governance for everyone.

Governments and industry organizations should work together on unified cyber security standards. These standards should be technology-neutral and apply equally to all companies and

networks. Over many years, the telecom industry has made great strides in delivering continuity, reliability, and compatibility across telecom networks by developing shared, unified standards. As MIT Media Lab cofounder Nicholas Negroponte wrote in an article on *Fast Company*, "Telecommunications policy should be based on objective standards, not geopolitical issues."¹

Once clear, unified cyber security standards are developed, we need independent, comprehensive verification processes that apply these standards. As a global community, we need to establish third-party cyber security verification mechanisms for all industries and companies so that trust and distrust are based on facts, not feelings. Verifiable facts and unified verification standards will in turn lead to objective results enabling organizations to compare and choose products based on their security requirements.

Cyber security is the top priority at Huawei. We are committed

¹ Nicholas Negroponte (May 9, 2019), "Don't ban Huawei. Do this instead", <https://www.fastcompany.com/90344450/dont-ban-huawei-do-this-instead>

to supporting the secure and stable operations of customer networks. For the past three decades, Huawei has operated in more than 170 countries and regions, serving over three billion people around the world. Our equipment has never caused a large-scale network breakdown, and we have never experienced any serious cyber security breach. Huawei has never done anything to jeopardize the security of our customers' networks or devices, and thus no evidence of such actions exists.



II. Introduction

1. Huawei's white papers on cyber security

In September 2012, Huawei released its first cyber security white paper: *Cyber Security Perspectives: 21st century technology and security – a difficult marriage*.² This paper describes Huawei's perspectives on cyber security, including how Huawei maintains its independence on issues of cyber security.

In October 2013, Huawei released its second cyber security white paper: *Cyber Security Perspectives: Making cyber security a part of a company's DNA – A set of integrated processes, policies and standards*.³ This paper describes Huawei's end-to-end cyber security processes and practices,

² Huawei's first cyber security white paper – Cyber Security Perspectives: 21st century technology and security – a difficult marriage,

<https://www.huawei.com/en/about-huawei/cyber-security/whitepaper/white-paper-2012>

³ Huawei's second cyber security white paper – Cyber Security Perspectives: Making cyber security a part of a company's DNA – A set of integrated processes, policies and standards,

https://www.huawei.com/en/about-huawei/cyber-security/whitepaper/hw_310548

including how Huawei applies a systematic and open approach to cyber security.

In December 2014, Huawei released its third cyber security white paper: *Cyber Security Perspectives: 100 requirements when considering end-to-end cyber security with your technology vendors*.⁴ This paper describes Huawei's contributions to cyber security standards, including the concrete steps that Huawei has taken to ensure cyber security.

In June 2016, Huawei released its fourth cyber security white paper: *The Global Cyber Security Challenge: It is time for real progress in addressing supply chain risks*.⁵ This paper describes the methods and tools that Huawei uses to address supply chain risks.

⁴ Huawei's third cyber security white paper – Cyber Security Perspectives: 100 requirements when considering end-to-end cyber security with your technology vendor,

https://www.huawei.com/en/about-huawei/cyber-security/whitepaper/hw_401493

⁵ Huawei's fourth cyber security white paper – The Global Cyber Security Challenge: It is time for real progress in addressing supply chain risks,

<https://www.huawei.com/en/about-huawei/cyber-security/whitepaper/huawei-cyber-security-white-paper-2016>

2. Purpose of this position paper

The rapid development of digital technologies brings new security challenges. All industries are undergoing digital transformation. New technologies like cloud, IoT, and AI are spreading. All of these mean that cyber security risks are rising.

The rising number of mobile connections is creating a larger attack surface for every network. The increasing adoption of cloud platforms means that the geographical and legal boundaries are being blurred for cyber security. AI and big data help us to create and deliver much more value than ever before, but the risk of data breaches is also rising.

How can we resolve cyber security issues? We have found that discussions of security tend to revolve around two types of question:

The first type is analyzing the issues. Is cyber security a political or technical issue? Is an equipment vendor's country of origin a relevant risk factor? Are 5G networks less secure than 4G? Can equipment vendors control the data flowing through telecom networks? Could an equipment vendor

disable a carrier's network with a "kill switch"?

The second type is related to solutions. How should we solve cyber security issues in a global supply chain? Do we conduct security verification using unified standards or, should we exclude certain vendors from entering a market? How can we develop unified standards for cyber security and verification? How can we avoid or reduce timewasting and inefficiency resulting from political imperatives?

As a global technology provider, Huawei always tries to present a clear position on both of these sets of questions, so that governments, the industry, and other stakeholders can correctly analyze the issues and find effective solutions.



III. ICT Offers Enormous Potential for Global Development

ICT is a powerful driver of social and economic development. ICT has become a ubiquitous and positive stimulus in every society and every economy, and will continue to play that role.

According to Huawei's 2018 Global Connectivity Index (GCI), the global digital economy has been growing at a rate 2.5 times faster than global GDP over the past 15 years.

Frontrunners – the cluster of advanced economies on the GCI S-curve – are using intelligent connectivity to accelerate digital economy growth and unearth new opportunities. Powered by intelligent connectivity, industries across the board can tap into unprecedented growth opportunities. On average, if all countries increase their investment in ICT infrastructure by 8% every year (CAGR), it will produce US\$23 trillion in new economic potential by 2025 (from US\$12.9 trillion in 2017), breathing new life into the S-curve for all economies. In other words, by 2025, the percentage of digital economy will increase from 17.1% to 24.3% of global GDP.⁶

⁶ Global Connectivity Index, Huawei, <https://www.huawei.com/minisite/gci/en/>

The integration of AI with five enabling technologies – broadband, data center, cloud, big data, and IoT – is redefining the concept of connectivity. AI, when applied with practical focus, enhances the inherent value of ICT infrastructure with greater automation and intelligence. The result is intelligent connectivity. The true value of the digital economy lies in the positive impact that investments in ICT infrastructure and AI have on productivity and the optimization of economic structures. Long-term return on investment in digital technologies is 6.7 times that of non-digital investments.

Manufacturing is expected to be one of the main beneficiaries of intelligent connectivity. In terms of digital economy, the addition of intelligent connectivity to traditional manufacturing industries is forecast to produce an additional market value of US\$6.4 trillion by 2025. By leveraging intelligent technologies, traditional industries will be well-positioned to maximize their digital spillover and contribute more to the overall digital economy.

Other industries with tremendous growth projections include those that are typically more data-driven, and therefore more

likely to be early adopters of AI. Sectors like ICT, professional services, and finance are expected to prosper in the digital economy. They will see additional market growth of US\$5 trillion, US\$3 trillion, and US\$1.7 trillion, respectively.

Industries such as social and personal services, retail, transportation, and utilities are also on track to achieve digital transformation on a timeline now accelerated by intelligent connectivity.

According to the latest report published by the GSMA at MWC Barcelona 2019, by 2025, the number of 5G connections will reach 1.4 billion by 2025 – 15% of the global total. The number of global IoT connections will triple to 25 billion by 2025, while global IoT revenue will quadruple to US\$1.1 trillion. 5G will contribute US\$2.2 trillion to the global economy over the next 15 years, with sectors such as manufacturing, utilities, and professional and financial services benefiting the most from the new technology.⁷

⁷ New GSMA Study: "5G to Account for 15% of Global Mobile Industry by 2025 as 5G Network Launches Accelerate", February 25, 2019,

<https://www.gsma.com/newsroom/press-release/new-gsma-study-5g-to-account-for-15-of-global-mobile-industry-by-2025/>

The fourth industrial revolution is coming. We must embrace the moment and ride the tide of history, or we risk missing out on this remarkable opportunity for development.



IV. Rational Approach to Risk Management

Today, ICT is driving tremendous socioeconomic development. Meanwhile, cyber attacks are increasing rapidly. According to T-Systems, there were about 4 million security attacks on Deutsche Telekom infrastructure per day in April 2017, but by April 2018, that number had tripled. By April 2019, they were seeing 31 million attacks a day.

Cyber attacks have become a kind of service that can be leased and purchased by attackers. Every day, there are three to eight new attack vectors. Distributed denial of service (DDoS), advanced persistent threats (APTs), and dark nets are emerging in an endless stream. Ransomware encrypts the files of its victims and doesn't release them until a ransom is paid. Scenes from *The Matrix* have become reality on the Internet, step by step. Companies and individuals suffer losses, reducing people's trust in the Internet and spreading panic. Some AI technologies can be also exploited by attackers. This means different kinds of AI technologies will soon come into conflict with each other.

How should we assess and respond to all these challenges? Should we panic and keep vendors out of the market simply due to security concerns? Or should we adopt a rational, objective, and evidence-based approach to risk management?

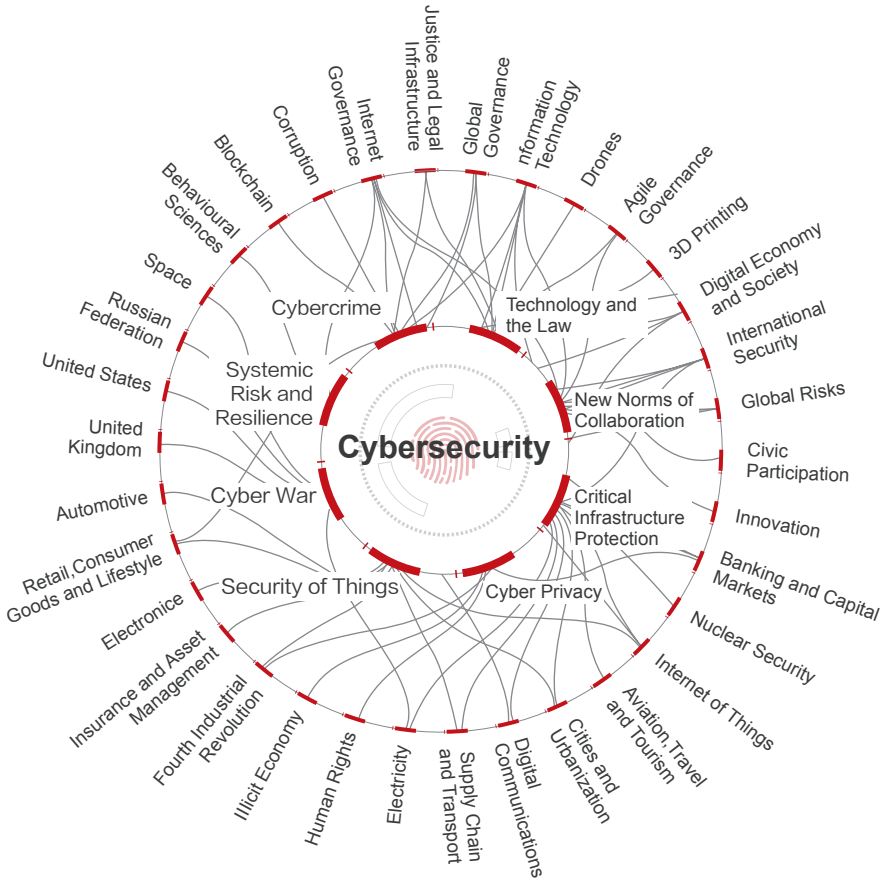
1. Cyber security involves many elements

As a variety of industries go digital, cyber security risks are increasing. The rising number of mobile connections is creating a larger attack surface for every network. The increasing adoption of cloud platforms means that the geographical and legal boundaries are being expanded for cyber security. AI and big data help us to create and deliver much more value than ever before, but the risk of data breaches is also rising.

Cyber security involves many elements, stakeholders, laws, and governance mechanisms. The World Economic Forum's Centre for Cybersecurity has identified eight key issues⁸ that we have to address as a global community. These include technology and the law, security of things, cyber privacy, new norms of collaboration, systemic risk and resilience, cyber war,

⁸ Centre for Cybersecurity, <https://www.weforum.org/centre-for-cybersecurity>

critical infrastructure protection, and cybercrime.



© World Economic Forum

The cyber security challenge is complex. We can't solve it by focusing on one vulnerability at a time, and no single person, company, or country can do it alone. We need to work together.

2. Supplier country of origin is not an element for security risk

Today, cyber security is increasingly intertwined with political suspicions and trade barriers and falling trust between nations. Political suspicions have done nothing to solve the issues of cyber security. Frequently, cyber security is used simply as an excuse to erect trade barriers, and this has further obscured the real issues.

Facts speak for themselves. In August 2018, the European Union Agency for Network and Information Security (ENISA) analyzed all 169 security incidents encountered by European telecom carriers in 2017. In their analysis, they found the following⁹:

- 62.1% of incidents were caused by system failures, with each incident affecting an average of 1.1 million user connections

⁹ 169 telecom incidents reported, extreme weather major factor. Retrieved on August 31, 2018, from

<https://www.enisa.europa.eu/news/enisa-news/169-telecom-incidents-reported-extreme-weather-major-factor>

- 18.3% of incidents were caused by human errors, with each incident affecting an average of 1.2 million user connections
- 17.2% of incidents were caused by natural phenomena, with each incident affecting an average of 600,000 user connections
- 2.5% of incidents were caused by malicious actions, with each incident affecting an average of 300,000 user connections

As the UK's National Cyber Security Centre (NCSC) recently noted, "In the 1,200 or so significant cyber security incidents the NCSC has managed since we were set up, the country of origin of suppliers has not featured among the main causes for concern in how these attacks are carried out... The techniques [...] were looking for weaknesses in how networks were architected and how they were run."¹⁰

From these findings, a few things are immediately clear.

¹⁰ Ciaran Martin's CyberSec speech in Brussels,

<https://www.ncsc.gov.uk/speech/ciaran-martins-cybersec-speech-brussels>

First, it's clear that system failure and human error constitute the greatest risk, and should be the focus of risk evaluation.

Second, and by extension, the potential risks inherent in any given product should be evaluated based on factors that have a material effect on security, such as the product's security architecture, security mechanisms, and security features.

By focusing on unrelated factors, such as country of origin, we do ourselves a disservice – both as purveyors of digital products and services, and as the joint custodians of cyber security. This will only hurt us and do no good to risk prevention.

3. Rational, objective, and evidence-based assessment of cyber security risks

As a global technology provider, Huawei is acutely aware of the importance of a secure and trustworthy digital environment. We fully support all efforts to build a more secure environment for our customers, and are committed to enhancing our own ability to do so. At the same time, we believe it's important that all stakeholders evaluate cyber security risks in a more rational, objective, and evidence-based

way. This is critical to better understanding cyber security challenges, and it gives each stakeholder a roadmap for enhancing their own cyber security capabilities.

If our approach to risk is based in emotion or bias, then our outcomes will be uncontrollable and we will be unable to achieve our security goals. If we hope to truly address the challenges of cyber security, we need to evaluate risks in a rational, objective, and evidence-based way. We need an all-industry, full-society approach. This will help us significantly reduce our collective exposure to cyber security risks and increase the return on our investment in cyber security.

V. Systematic Governance of Cyber Security

1. Unified cyber security standards

Governments and industry organizations should work together on unified cyber security standards. These standards should be technology-neutral and apply equally to all companies and networks.

Nicholas Negroponte, the cofounder of the MIT Media Lab, said it best in a recent article for Fast Company:

"Telecommunications policy should be based on objective standards, not geopolitical issues."¹¹

The telecom industry has a long history of developing shared standards to promote the continuity, reliability, and interoperability of telecom networks. This same approach can and should be adopted to create benchmarks against which we can evaluate the security of equipment.

¹¹ Nicholas Negroponte (May 9, 2019), "Don't ban Huawei. Do this instead", <https://www.fastcompany.com/90344450/dont-ban-huawei-do-this-instead>

For example, 3GPP SA3 has done incredible work driving unified 5G security standards. In terms of security architecture, 5G builds on 4G and expands its potential with more advanced security mechanisms.

- To more effectively protect user privacy, 5G uses the Subscriber Permanent Identifier (SUPI) to encrypt the transmission of user identity data.
- To secure communications, 5G uses integrity protection to prevent interception and modification of data during transmission.
- To ensure inter-operator security, 5G employs an end-to-end security channel between different carrier networks to prevent attackers from exploiting SS7 vulnerabilities.
- The 5G core also provides more enhanced authentication mechanisms for accessing network functions.

At the moment, some concerns about 5G security seem to have arisen from an inaccurate understanding of how 5G works at the core and on the edge. They say in 5G there is no

difference between core and edge. Ciaran Martin, CEO of UK NCSC (National Cyber Security Centre), has clearly described this: "Technical precision matters in getting 5G security right. 5G is an important innovation. But it's not magic. It doesn't change the laws of science or immutable concepts of security. It is an extremely complicated set of engineering and technological capabilities and architectures. Standards bodies' analyses of it run to hundreds of pages of dense tech-speak. That's why oversimplifying it into sweeping statements like there being no difference between core and edge, without substantiating or evidencing what you mean by there being no difference between core and edge, or even what you mean by core and edge, isn't the right way to consider the issue."¹²

Other concern also is raised such as central unit (CU) and distributed unit (DU) are not split, this has been directly addressed in an article coauthored by 3GPP SA3 Chairman, Anand R. Prasad. He writes: "In 5G the base-station is logically split in CU and DU with an interface between them.

¹² Ciaran Martin at Cyber 2019, Chatham House,

<https://www.ncsc.gov.uk/speech/ciaran-at-chatham-house>

Security is provided for the CU-DU interface. This split was also possible in 4G, but in 5G it is part of the architecture that can support a number of deployment options (e.g. co-located CU-DU deployment is also possible). The DUs, which are deployed at the very edge of the network, don't have access to any user data when confidentiality protection is enabled. Even with the CU-DU split, the air interface security point in 5G remains the same as in 4G, namely in the radio access network." ¹³

When it comes to evaluating the security of a specific product or solution, we can avoid misunderstandings like this by adopting unified standards. We are a major contributor to the security and privacy standards of 3GPP systems. In 2018, we submitted 464 contributions on 5G security to 3GPP's SA3, and 227 were approved.

2. Independent cyber security verification

Once we have a unified and clear set of cyber security

¹³ More examples of 5G security enhancements can be found here:

https://www.3gpp.org/news-events/1975-sec_5g

standards, we need to embrace independent verification across the board.

As supply chains become more global, if we are truly serious about the security of all systems and all infrastructure, we need to assess all suppliers and components in the same way. We can't just evaluate one part of a connected system, because bad actors will target the parts that haven't been tested for security.

Security verification is important for telecom carriers, governments and individuals alike, even if it is not perfect. Arguably, automotive crash tests are not able to emulate each and every possible accident scenario -and yet, there's no denying that crash test programs have vastly contributed to the development of safer cars. As a global community, we need to establish third-party cyber security verification mechanisms for all industries and companies so that trust and distrust are based on facts, not feelings. Verifiable facts and unified verification standards will in turn lead to objective results enabling organizations to compare and choose products based on their security requirements.

This systematic approach is already used in the telecom industry. Right now, GSMA and 3GPP are also making great progress with their Network Equipment Security Assurance Scheme (NESAS). This scheme will be useful for evaluating the security of wireless communications equipment. To help NESAS hit the ground running, GSMA will review the qualifications of third-party verification labs. Only qualified labs can be trusted to test and evaluate the security of network equipment.

We are a strong proponent of independent security verification. We support open, transparent, fair, reasonable, and non-discriminatory security verification. Huawei products have passed multiple independent third-party certifications. In total, we have been granted 39 Common Criteria or CC certificates, and 20 US Federal Information Processing Standards (FIPS) certificates.

According to the US firm CFI Group's survey of 177 carriers and 12,300 customers, Huawei products scored above industry average in terms of customer satisfaction, system stability, and reliability for three years in a row.

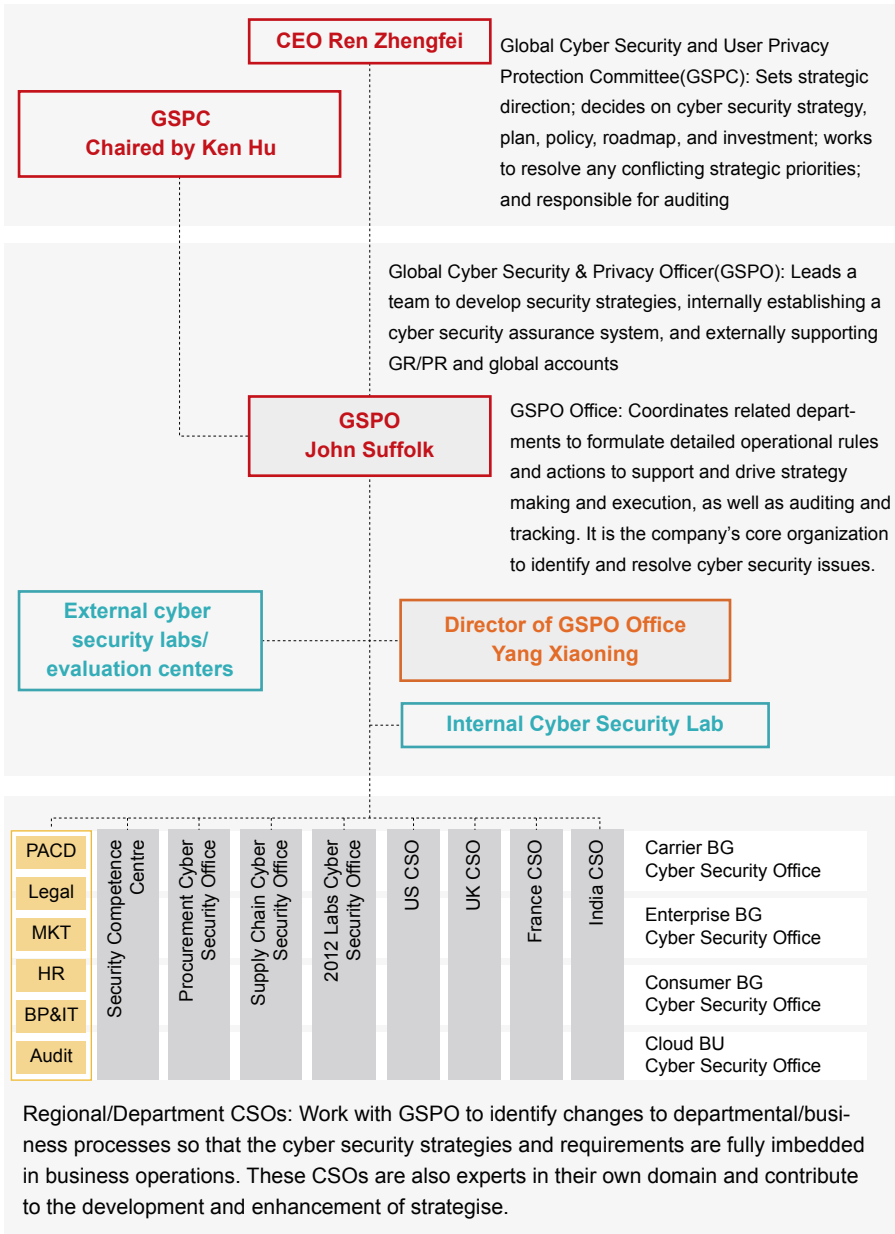
VI. Huawei Delivers Trustworthy and High-Quality Products

1. Huawei's Global Cyber Security and User Privacy Protection Committee (GSPC) led by Deputy Chair of the Board

As quoted in the third edition of Huawei's cyber security whitepaper, *Cyber Security Perspectives: 100 requirements when considering end-to-end cyber security with your technology vendors*¹⁴, "If cyber security isn't seen as a priority by the Board and senior officials, it won't be seen as a priority by the organization's staff. Ensuring that cyber security is embedded into the organizational design, governance and internal control framework of any organization is the starting point for the design, development and delivery of good cyber security."

¹⁴ Huawei's third cyber security white paper – *Cyber Security Perspectives: 100 requirements when considering end-to-end cyber security with your technology vendors*, https://www.huawei.com/mx/about-huawei/cyber-security/whitepaper/hw_401493

Since 2010, Huawei has assigned a deputy chair, several board members, and multiple business department presidents to serve in the GSPC and to manage the development and execution of cyber security and privacy protection strategies. This gives board members and senior managers a crystal clear understanding of security and privacy issues as well as their responsibilities, and allows them to step up to the plate to tackle the issues. They make sure sufficient resources are provided to embed cyber security and privacy requirements into Huawei's strategic design and governance structure.



2. Embedding cyber security elements into end-to-end processes

In the first edition of our cyber security whitepaper¹⁵, we stated, "In addressing the requirements of cyber security, we have built into all of our standard processes, baselines, policies, and standards the best practice that is required. In this way, cyber security is not something that is an afterthought. Instead, it becomes a standard part of the way we do our daily business – it has become part of our DNA."

Cyber security is already an integral part of our Integrated Product Development (IPD) process which we have developed in collaboration with leading US consultants. The work never stops here. We have launched the IPD 2.0 transformation to further integrate security into all stages of our process, from requirement analysis, design, and coding to testing and lifecycle management. With this transformation, we aim to deliver both trustworthy processes and trustworthy results.

¹⁵ Huawei's first cyber security white paper – Cyber Security Perspectives: 21st century technology and security – a difficult marriage

<https://www.huawei.com/en/about-huawei/cyber-security/whitepaper/white-paper-2012>

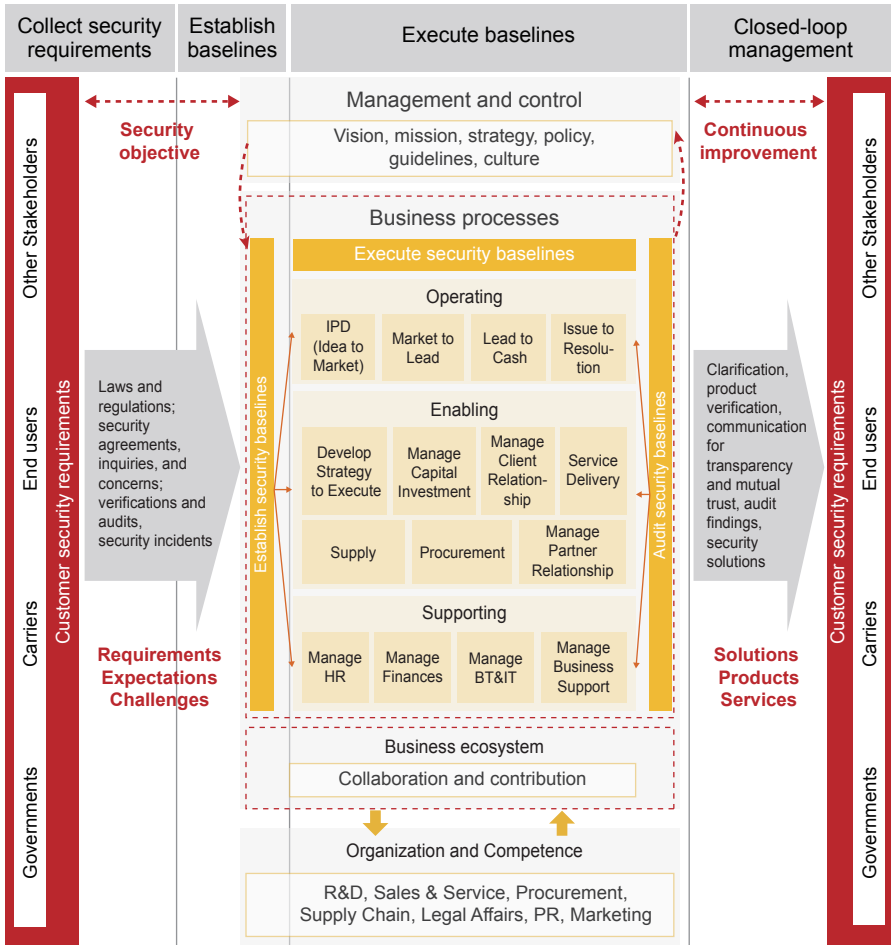
Huawei has established an end-to-end cyber security framework where:

(1) Security requirements come from customers as well as laws and regulations. Huawei summarizes and extracts these requirements, and turns them into security baselines.

(2) We embed all baselines into business processes, ensuring they can be executed repeatedly rather than randomly.

(3) Closed-loop management of security requirements is conducted. Our Internal Audit Department checks whether business departments have carried out cyber security activities as required.

(4) We invite senior managers to share their thoughts on cyber security, and integrate them into the cyber security management system. Business department presidents participate in GSPC discussions and decision making. Their decisions are extracted into resolutions, strategies, and policies, steering business departments in a correct direction for ensuring cyber security.



3. Huawei's Cyber Security 2.0

Moving forward, new technologies such as cloud computing, IoT, and AI will reshape the ICT industry and create significant opportunities and challenges in cyber security. To address this

new landscape, Huawei has launched the Cyber Security 2.0 initiative based on the assumptions that cyberspace is insecure and that cyber attacks are pervasive. With this new initiative, Huawei aims to turn cyber security into a core competency of our products, services, and solutions, to help our customers build more resilient networks.

Specifically, Huawei is committed to do the following:

- Develop insights into network environments, identify and resolve threats, and align our approaches with industry-leading practices;
- Improve compliance with applicable standards, laws, and regulations;
- Build a culture that emphasizes quality and security and attaches equal importance to security and business value;
- Constantly develop skills of our security experts and leaders;
- Move security governance closer to business operations. Change our governance model from being control-focused to capability-focused, and reinforce results-focused

evaluation and supervision to ensure strategies are executed as intended.

Our approach centers on technology and business success, and we are making every effort to continuously improve product quality, critical security technologies, and engineering capabilities. Network resilience is our key target as we work to make our products more secure and competitive. Huawei has been and will always be open and transparent in terms of cyber security. Cyber security is not a one-person job. We are engaging with our customers, governments, the media, and other stakeholders to create a robust ecosystem for cyber security.

4. Launching transformation programs to drive innovation on security technology

Huawei considers cyber security and privacy protection our top priorities throughout the produce lifecycle, from design, development, to delivery. We will not compromise security for any reason, be it cost, schedule, or functionality. Right now, the quality and performance of our network products is top in the industry. Moving forward, we will invest US\$20 billion every year to develop even more secure and trustworthy products.

We actively invest in security innovation. The cyber environment is becoming more and more complex, which raises the bar for product security. In response to this, we have allocated an initial budget of US\$2 billion to fully enhance our software engineering capabilities.

Huawei has become a process-based organization – one that is fundamentally driven by repeatable processes, which deliver a consistent quality of products and service. We adopt a "Built-In" approach, which means incorporating security into all stages of our process so that we can deliver trustworthy, high-quality products.

We aren't just looking back to see what we can improve; we are actively looking forward. We are working with the industry to predict new threats and prepare our technology for challenges society will face in the decades to come.

Huawei focuses on research and innovation in security technologies like trusted computing, data security, application passwords, privacy protection, and the security of connected cars, and we are working closely with academia and industry partners in these areas.

5. Providing secure products and solutions

a) HiSec security architecture

HiSec provides common security products and components that can be integrated into Huawei's 5G, IoT, and cloud solutions to build resilient networks. HiSec offers the following four advanced features to protect network borders, defend against threats and attacks, enable real-time awareness of the security situation, and promptly address security risks.

Security risk identification: HiSec's vulnerability detection system rapidly identifies vulnerabilities in existing products on live networks, analyses vulnerability exploitation, assesses vulnerability risk levels, and determines which vulnerabilities to handle first. This makes the identification and resolution of vulnerabilities more prompt and proactive, lowering the risk of vulnerabilities being exploited. The system provides a vulnerability management tool.

Security situation awareness: By employing Huawei's extensive data sources and advantages in big data and AI technologies, the security situation awareness (SSA) system – as part of HiSec – can collect network data to detect threats in

real time, automatically address threats, display and track the sources of attack chains, and enable comprehensive, visualized risk management and alerts. A big data-based security awareness product is provided as part of the system.

Security risk prevention: Huawei's security portfolio includes cloud, network, and device products, as well as common components customized for different sectors. First, Huawei provides security products – such as next-generation firewall (NGFW), intrusion prevention system (IPS), web application firewall (WAF), and Anti-DDoS – to keep network borders secure and shield business systems from external attacks. Huawei also provides security components that third parties can integrate into their own products for enhanced security. Each Huawei product is supported by a multi-layer security mechanism, with integrity protection at the bottom layer, security assurance at the operating system layer, anti-attack features at the host layer, and web protection at the app layer.

Security ecosystem: In partnership with security companies, Huawei has built a robust ecosystem that revolves around HiSec. These partnerships have produced many highly effective and reliable security products that now lead the industry.



b) Huawei's 5G solution security architecture

5G builds on and extends 4G in terms of security architecture. Huawei outlined the security architecture of its 5G solutions in its *5G Security White Paper*¹⁶ released on May 29, 2019.

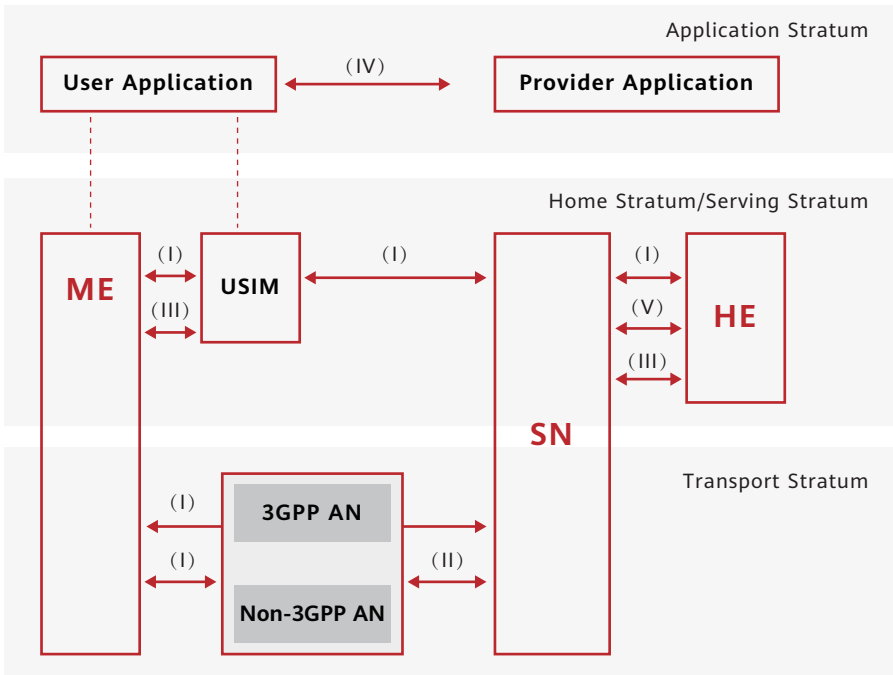
¹⁶ *5G Security White Paper*:

<http://www-file.huawei.com/-/media/CORPORATE/PDF/white%20paper/2019/huawei-5g-security-white-paper-4th-en.pdf>

Currently, 3GPP SA3 has developed 5G R15 security standards and is in the process of developing 5G R16 security standards. To ensure that 5G standards move ahead consistently at all technical levels, the 3GPP is developing security standards at the same pace as that of architecture and wireless standards. 5G R15 standards have defined security architectures and security standards for eMBB scenarios, covering Standalone (SA) and Non-Standalone (NSA) architectures. Based on the 5G R15 security architecture, 5G R16 and R17 standards will cover security optimization for mMTC and URLLC scenarios.

The security architecture of mobile networks is hierarchical and classified by domain in design. The 5G security architecture contains the following security domains:





Network access security (I), Network domain security (II), User domain security (III), Application domain security (IV), SBA domain security (V)

- Network access security (I): the set of security features that enable a UE to authenticate and access services via the network securely, including the 3GPP access and Non-3GPP access, and in particular, to protect against attacks on the (radio) interfaces. In addition, it includes the security context delivery from serving network (SN) to

access network (AN) for the access security. Specific security mechanisms include bidirectional authentication, transmission encryption, and integrity protection.

- Network domain security (II): the set of security features that enable network nodes to securely exchange signaling data and user plane data. Network domain security defines security features for interfaces between access and core networks and between home and serving networks. The separation between access and core networks in 5G is as clear as that in 4G. For the interfaces between RAN and Core, specific security mechanisms, such as IPsec, can be used to provide security separation and protection.
- User domain security (III): the set of security features that secure user access to mobile equipment. Mobile equipment uses internal security mechanisms, such as a PIN code, to ensure security between the mobile equipment and universal subscriber identity module (USIM).
- Application domain security (IV): the set of security

features that enable applications in the user domain and in the provider domain to exchange messages securely. Security mechanisms of the application domain are transparent to the entire mobile network and are provided by application providers.

- SBA domain security (V): the set of security features that enable network functions of the SBA architecture to securely communicate within the serving network domain and with other network domains. These features include network function registration, discovery, and authorization security, as well as protection for service-based interfaces. SBA domain security is a new security feature in 5G. An SBA forms the basis of the 5G core network. To ensure security between UEs in the SBA, security mechanisms such as Transport Layer Security (TLS) and Open Authorization (OAuth) are needed.
- Visibility and configurability of security (VI): the set of features that enable the user to be informed whether a security feature is in operation or not. (Note: The visibility and configurability of security is not shown in the figure.)

Like the 4G security architecture, 5G security architecture consists of the transport stratum, serving stratum, home stratum, and application stratum, which are securely isolated from each other.

- Transport stratum: Located at the bottom of the architecture, the transport stratum has low security sensitivity. It includes some UE functions, all gNodeB functions, and some core network functions, such as the User Plane Function (UPF). These functions, excluding the UE functions, do not involve sensitive data, such as subscription permanent identifiers (SUPIs) and user root keys. They manage only low-level keys in the key hierarchy, for example, user access keys. Low-level keys can be derived, replaced, or updated by a high-level key at the home/serving stratum. However, a low-level key cannot induce a high-level key.
- Serving stratum: It has relatively high security sensitivity and includes such core network functions of the operator's home network as the Access and Mobility Management Function (AMF), Network Repository Function (NRF), Security Edge Protection Proxy (SEPP), and Network

Exposure Function (NEF). The core network functions of this stratum manage only mid-level derived keys (such as AMF keys) in the key hierarchy. A mid-level key can be derived, replaced, or updated by a high-level key at the home stratum. However, a mid-level key cannot induce a high-level key. This stratum does not involve gNodeBs.

- Home stratum: It has high security sensitivity and includes the Authentication Server Function (AUSF) and Unified Data Management (UDM) of the operator's home network, as well as the USIM in the UE, and therefore it contains sensitive data such as the SUPIs, user root keys, and high-level keys. This stratum does not involve gNodeBs or other functions of the core network.
- Application stratum: It is closely related to service providers, but hardly related to operator networks. The application stratum involves 5G applications that, similar to 4G applications, need end-to-end security assurance for services that require high security in addition to transport security. For example, mobile payment requires end-to-end security assurance at this stratum, even if transport security is guaranteed on the 4G network, to

ensure the security and correctness of transactions.

The 5G network inherits the 4G network security architecture with different strata and domains. The 5G access and core networks have clear boundaries, interconnect through standard protocols, support inter-vendor interoperability, and have standards-based security protection mechanisms. In terms of cyber security risks, regulators need to monitor all four strata, service providers need to monitor the application stratum, operators need to monitor the transport, serving, and home strata, and equipment vendors need to focus on the underlying network equipment. All industries shall work together to tackle the security challenges brought by services, architectures, and technologies under the standard architecture.

In Ovum's paper entitled The Facts on 5G¹⁷, it has been described that concerns have been raised that the architectural separation between core and RAN might be weakened in the future. This would mean that the clarity and stability of the interface between core and RAN would be lost.

¹⁷ The Facts on 5G: <https://huaweihub.com.au/the-facts-on-5g/>

However, there are strong reasons to believe this will not happen.

- The first reason is technical. Core/RAN separation is fundamental to the architecture of 5G standards, as it is for previous generations of mobile technology. If core/RAN is not separated, standards development would become much more complex and difficult, slowing down innovation. Weakening this separation would be a major U-turn that has no support in either the vendor or the operator community. And because 5G standards in fact implement core/RAN separation, any mobile technology that broke with this separation would not be 5G and would not be compatible with 5G networks (or any earlier generation of network technology).
- The second and more powerful reason is that both operators and vendors would suffer if this separation were to be relaxed.
 - i. Mobile operators that tried to implement networks without a clear core/RAN separation it would be difficult to adopt multi-vendor solutions, because it would no longer

be possible to guarantee that different core and RAN equipment could be connected in a simple, modular way. Operators would be forced to adopt a single vendor and stick with them indefinitely. This would ease competitive pressure on vendors, and push up operator costs.

ii. While it might seem that vendors would welcome this, they would still be competing with other vendors offering the standard 5G solution that maintained a clear core/RAN separation. A technology offer that failed to maintain the advantages of core/RAN separation would not be competitive, and not achieve any economy of scale. Even if an operator were to demand such a bespoke and non-standard solution, the additional costs of implementing could not be amortized over the rest of the industry so it would be expensive. No rational vendor would put themselves in this position.

- The third reason is because security within a network that has been built to be resilient to attack, such that no single action could disable the system, can be best achieved by diversifying suppliers. The arguments for this are two-fold:

- i. Reducing over-dependence and increasing competition. First, the network should not be dependent on just one vendor, as this would render it less resilient.
- ii. Secondly, using equipment from more than one vendor increases competition between those vendors. This will force them to improve their security standards. And it is this raising of the bar on cyber security standards across the board that is needed - together with a requirement for more stringent regulation and enforcement of those standards.

c) Huawei's IoT solution security architecture

Huawei uses a "3T+1M" security architecture for its IoT solutions, which is explained in depth in the *Huawei IoT Security White Paper*¹⁸ released on October 23, 2018, at the fourth IoT Solutions World Congress.

There are many different IoT use cases: low power wide area (LPWA), connected cars, industrial IoT, wearables, etc. In an

¹⁸ *Huawei IoT Security White Paper*:

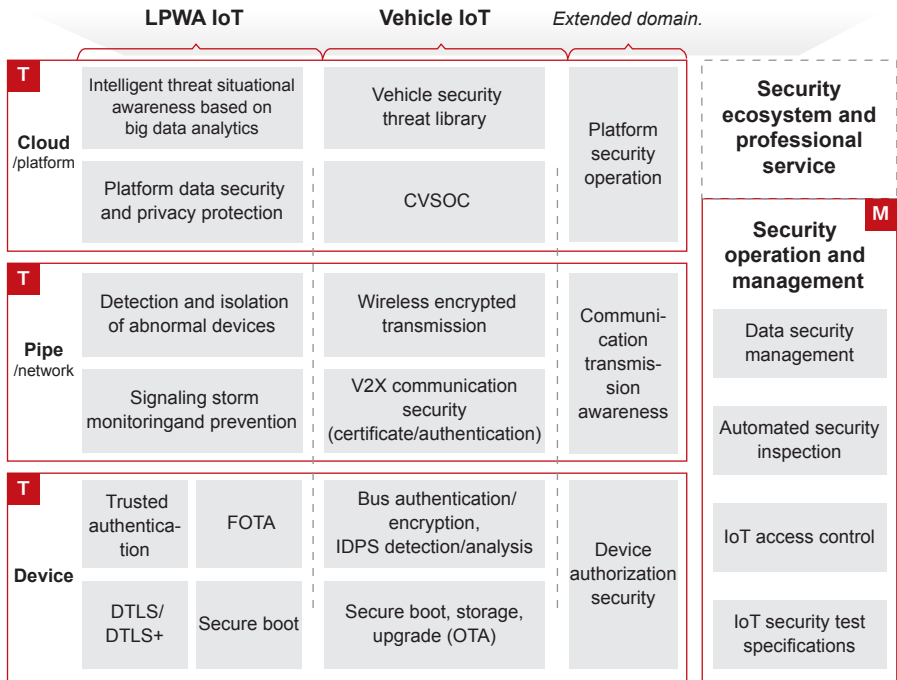
<https://www.huawei.com/en/press-events/news/2018/10/huawei-iot-security-whitepaper-2018>

IoT ecosystem, numerous connected devices generate and use massive amounts of data; networks provide security assurances for highly parallel communications; and the cloud and IoT platform supports a wide range of IoT applications. All these supporting systems and applications may be subject to potential malicious attacks.

The 3T+1M architecture focuses on the security features at device, network, cloud, and platform levels, all coordinated with each other. These will counter security threats at sensor, network, and application levels in an IoT network. Building on platform and cloud security, Huawei leverages its extensive experience in providing assurances of telecom network security to offer security situational awareness, analysis, and detection for IoT. Working with partners, Huawei uses this architecture to effectively respond to the challenges of IoT security. We keep refining the 3T+1M architecture to better adapt to the security needs of different industry applications, particularly industry-specific security needs. Huawei builds security through innovation, and responds to diverse customer needs through evolution.

IoT Security 3T+1M Framework

Threats	Weak password	Device hijacking	Signaling storm	Privacy disclosure	Near field attack	Industrial control vulnerability	Others
----------------	---------------	------------------	-----------------	--------------------	-------------------	----------------------------------	--------



Compliance and certification

Compliance with key laws/regulations in countries/regions	Industry security standards (3GPP/ISO-JTC1/IEEE1609/OWASP...)	Security standards/specifications of major enterprises
---	---	--

T : Security technology
 M: Security operation and management

The 3T+1M security solution for IoT focuses on the security of IoT scenarios (e.g., connected cars, LPWA, and industrial IoT) that integrate three technologies (3T) and one management approach (1M) to deliver assured protection for IoT networks. "3T" refers to IoT device defense, network security assurance, and cloud protection technologies, and "1M" refers to security operation and management. The architecture aims to ensure compliance with local and international law and industry standards, and deliver end-to-end protection against online threats. The architecture is shown below:

1. IoT device defense technology family (1T): Delivers matching security capabilities and device-cloud synergy for IoT devices in different application scenarios. Basic security capabilities, such as DTLS/DLTS+, trusted DICE, FOTA, and secure boot must be provided for weak devices (e.g., LPWA smart meters and shared bike locks). For strong devices (e.g., vehicle-mounted T-Box and OBU) require security certificate management, intrusion detection, encryption authentication, and trusted platform module (TPM).
2. IoT network assurance technology family (1T): Detects

malicious behavior and implements isolation, especially for abnormal behavior of IoT devices (e.g., vehicle-mounted T-Box and LPWA smart street lamps). Abnormal behavior includes abnormal traffic and abnormal reporting frequencies. Different IoT pipe security capabilities are enhanced for different scenarios. For example, anti-DDoS and signaling storm prevention capabilities are improved for NB-IoT devices. For Cooperative Intelligent Transport Systems (C-ITS) of connected vehicles, the trusted capability of V2X communication needs to be improved.

3. IoT platform protection technology family (1T): Focuses on how to build IoT platforms and clouds to provide security situational awareness based on big data analytics, security analysis and awareness of connected vehicles, and IoT data security and privacy protection. It also provides configurable cloud security assurance capabilities for customers.

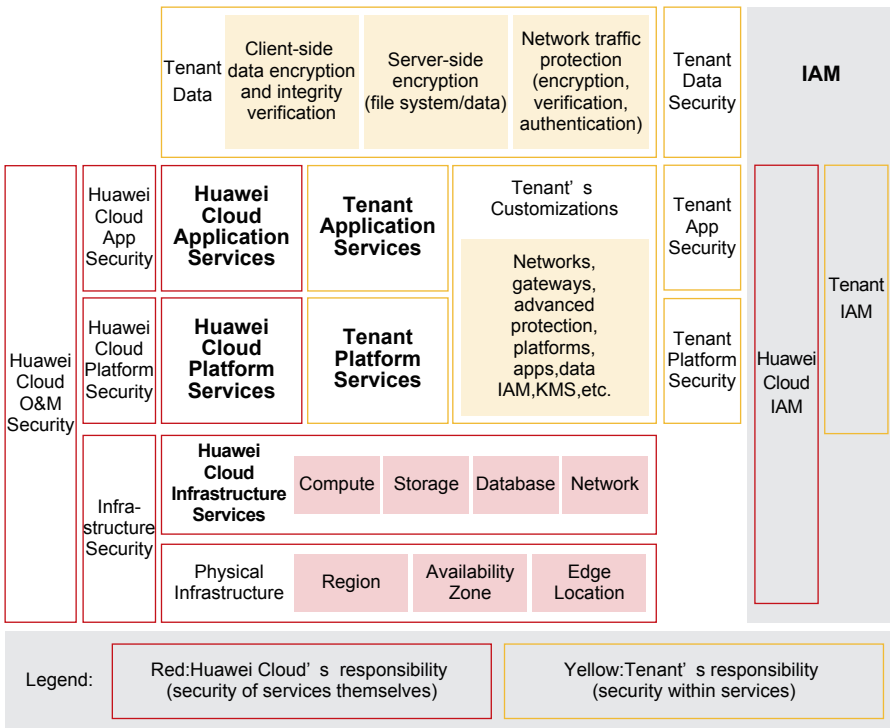
4. IoT security operation and management (1M): Focuses on how to build E2E security maintenance tools and develop security operation and management

specifications and procedures to improve operation and testing efficiency. It also focuses on improving the IoT security system in terms of threat prevention, detection and analysis, and response. This includes improving security inspection tools, periodic IoT security evaluations, automated device and application security detection tools, and threat intelligence libraries.

With the 3T+1M security architecture, different key IoT security technologies are used in different areas. Some focus on the security of devices, some on security of networks, and others on security of cloud. None of these technologies are isolated; they are synergic and combine to form a comprehensive security assurance system. Coordination of security technologies at the device, network, cloud, and O&M layers is a must. For example, IoT devices usually need to support a variety of apps with a limited amount of resources, so the security capabilities of devices (e.g., trusted devices, malicious device detection, and DTLS+) must be linked with those of cloud and networks, in order to maximize security at the edge.

d) Huawei Cloud security architecture

The *Huawei Cloud Security White Paper*¹⁹, released in September 2017, describes the shared responsibility model that has been developed for Huawei Cloud based on industry practices.



¹⁹ Huawei Cloud Security White Paper:

https://intl.huaweicloud.com/content/dam/cloudbu-site/archive/hk/en-us/securecenter/security_doc/Security_en_201709.pdf?1539874232718

As shown in the above figure, the primary responsibilities of Huawei Cloud are developing and operating the physical infrastructure of Huawei Cloud data centers; the IaaS, PaaS, and SaaS services provided by Huawei Cloud; and the built-in security functions of a variety of services. Huawei Cloud is also responsible for the secure design, implementation, and O&M of the multi-layered defense-in-depth, which spans the physical, infrastructure, platform, application, and data layers, in addition to the identity and access management (IAM) cross-layer function.

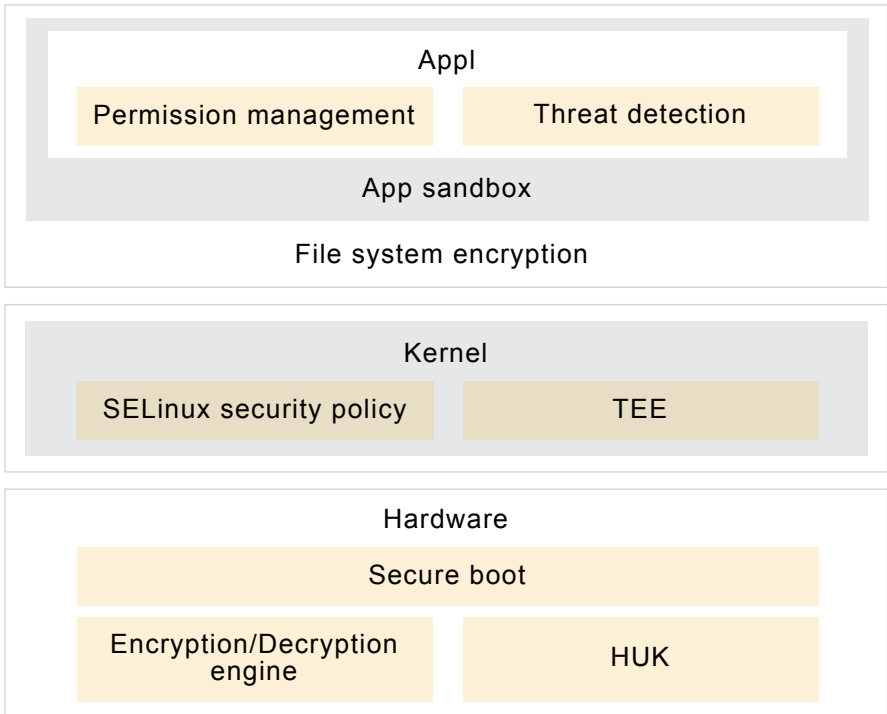
The primary responsibilities of the tenant are customizing the configuration and operating the virtual network, platform, application, data, management, security, and other cloud services to which a tenant subscribes on Huawei Cloud, including its customization of Huawei Cloud services according to its needs as well as the O&M of any platform, application, and IAM services that the tenant deploys on Huawei Cloud. The tenant is also responsible for the customization of the security settings at the virtual network layer, platform layer, application layer, data layer, and cross-layer IAM function, as well as the tenant's own in-cloud O&M security and the

effective management of its users and identities.

e) EMUI security architecture

Huawei takes the security of mobile devices seriously. On November 30, 2018, Huawei released the *EMUI 9.0 Security Technology White Paper* to systematically explain the security protection mechanisms of EMUI (Emotion UI) that is used on Huawei devices.

Security is a systematic project. EMUI provides end-to-end security protection that stretches from hardware, to systems, to apps, and to the cloud (as shown below), including security and privacy protection for the management of hardware chips, system kernels, data, apps, networks, payment, cloud services, and devices.



EMUI provides a secure boot mechanism in the underlying hardware chip to prevent the EMUI read-only memory (ROM) image from being tampered with. The ROM image can run on a device normally only after passing signature verification, which ensures secure boot for the boot loader, recovery, and kernel image. The Android native system provides verified boot to ensure the secure boot of the Android system and prevent tampering and malicious code implantation, thereby

ensuring system security from the hardware chip to the Android boot.

To ensure data security, the system encrypts user data using a hardware-based hardware unique key (HUK) and user lock screen passcode. Data files of different apps are stored in the directories of the corresponding apps, so that the files of one app cannot be accessed by other apps. The data erasure function is provided for permanently erasing data during device recycling or factory default restoration to prevent unauthorized data restoration. EMUI also allows cloud services to help users back up and synchronize data to ensure data security.

For app security, in addition to the Android security sandbox and permission management mechanisms, EMUI pre-installs the Phone Manager to provide virus scanning, block and filter, traffic management, notification management, and other functions. With these functions, the system can automatically detect viruses and Trojan horses in apps and provide fine-grained permission, traffic, and notification management functions.

Let's summarize the secure products and solutions. Since

2013, Cigital, a US company, has conducted annual BSIMM assessments on how Huawei manages the security, design, engineering, and testing of its products. A total of 12 security practices are tested, including security governance, security design, security coding, and security testing. Huawei has ranked above the industry average in all of the 12 security practices, and ranked among the industry's best in 9 of them.

US futurist George Gilder said, "I can contribute to a re-construction of Internet architecture to address the terrible security collapse across the Internet that is making everybody paranoid and preventing everybody from trusting anybody else. This is really a technical problem that Huawei can address and not a political problem" during a forum discussion²⁰ with Huawei founder Ren Zhengfei and Nicholas Negroponte, a co-founder of the MIT media lab. Cyber security is a technical issue that must be addressed through technical means.

²⁰ Transcript of A Coffee with Ren (June 17, 2019),

<https://www.huawei.com/en/facts/voices-of-huawei/a-coffee-with-ren>

VII. Business Independence

Huawei is an independent company, committed to supporting the secure operations of our customers' networks and services.

1. Huawei is a private company wholly owned by its employees

No government or any third party holds shares in our company, intervenes in our operations, or influences our decision-making. Although we are not a public company, we abide by many established standards and norms for public companies, including the publication of an Annual Report, which contains financial statements audited by KPMG, an independent third-party organization. We do this to provide people outside the company with additional assurance of our business integrity, our independence, and the transparency of our finances.

2. The Chinese government does not interfere with our business or the security of our products

These days, there is much debate about Chinese intelligence law. Some groups of politicians claim that Chinese law allows the government to force companies to collect intelligence on its behalf. This is simply not true. The Chinese government has been explicitly clear about this, as have multiple independent legal professors and a well-known international law firm: Government requests for company assistance must be in accordance with the law. There is no Chinese law authorizing the state intelligence agency to require a telecommunications equipment manufacturer to collect intelligence information, implant backdoors or disable customer networks. The Chinese government does not interfere with our business or the security of our products. And if any attempt were made to force our hand – from any country or organization – we would reject it outright.

We have been very clear on this point: If we are ever put in a position that jeopardizes our independence, the security of our products, customer networks, or security of foreign nation states, we would sooner shut down the company than violate our principles. We are happy to sign any "no-spy" and "no-backdoor" agreements if that would provide further comfort

to our customers and governments around the world.

3. Huawei exists to serve its customers

We support stable, reliable, and secure network operations no matter the circumstance, whether it be a natural disaster, social conflict, or cyber-attack. During Wenchuan earthquake and Fukushima nuclear leakage, Huawei people did their utmost to repair communication networks and maintain the availability of network services.

Over the past three decades, Huawei has operated in more than 170 countries and regions, serving over three billion people around the world. Our equipment has never caused a large-scale network breakdown, and we have never experienced any serious cyber security breach. Huawei has never done anything to jeopardize the security of our customers' networks or devices, and thus no evidence of such actions exists.

VIII. Open and Transparent Collaboration

1. Working more closely with security scholars through the Security Advisory Board

As an effort to work more closely with security scholars, we established our Security Advisory Board (SAB) in August 2014. Since then, we have been inviting roughly 10 global top security and cryptographic experts every year to provide consultation to us, guiding us to better engage in security research and security engineering. Every year in late summer or early autumn, Huawei convenes a SAB Workshop in Europe, inviting security advisors and other renowned scholars and industry experts in cyber security research or work to give presentations. These experts meet with Huawei's internal security experts and technical managers for in-depth discussions on security trends, popular security technologies, and security technology challenges facing Huawei. The discussions mainly revolve around security in 5G, IoT, AI, cloud, blockchain, hardware, and future networks, along with post-quantum cryptography. Building on these discussions,

Huawei and these security advisors and experts have collaborated extensively on security technologies.

Huawei also refers to articles these security advisors have written to help the industry better understand cyber security. For example, Mark Ryan, member of the SAB and professor at the University of Birmingham, published an article titled *Interoperability is the solution to the Huawei dilemma* in the Birmingham Brief. In this article, he emphasized that open and consistent standards are key to addressing security issues. In particular, he said, "The way to avoid technology lock-ins and monopolies is to have open international standards, and encourage lots of organizations and individuals to develop hardware and software that matches them. By making the standards open and unambiguous, we can ensure that products are interoperable, so that nobody is forced to buy equipment from any particular manufacturer, and can swap devices made by different manufacturers with no loss of compatibility. The 3GPP is the organization that coordinates 5G standards, and its technical specifications are available for anyone to view and implement. Patents exist on some technologies, but 3GPP mandates licensing on fair,

reasonable and non-discriminatory (FRAND) terms."²¹

2. HCSEC offers world-class security expertise and technical assurance

On November 24, 2010, the Huawei Cyber Security Evaluation Centre (HCSEC) was established under a set of arrangements between Huawei and the UK government. The centre independently evaluates the security of Huawei products used in live networks in the UK, and the UK government provides ideas and suggestions for improvement.

The UK's National Cyber Security Centre (NCSC) appoints Ernst & Young to audit HCSEC's independent operations every year, and the HCSEC Oversight Board (OB) oversees the independence, competence, and overall effectiveness of HCSEC. HCSEC is free to run tests using any tools, environments, methods, processes, and amount of time without informing other Huawei organizations and personnel.

²¹ Mark Ryan, "Interoperability is the solution to the Huawei dilemma", May 20, 2019
<https://www.birmingham.ac.uk/news/thebirminghambrief/items/2019/05/interoperability-is-the-solution-to-the-huawei-dilemma.aspx>

The UK's regime is arguably the toughest and most rigorous oversight regime in the world for Huawei. NCSC continues to believe that the UK mitigation strategy (HCSEC performing technical work and OB providing assurance) is the best way to manage the risk of Huawei's involvement in the UK telecommunications sector. In the 2018 HCSEC Oversight Board Annual Report, the OB noted, "It is evident that HCSEC continues to provide unique, world-class cyber security expertise and technical assurance of sufficient scope and quality as to be appropriate for the current stage in the assurance framework around Huawei in the UK."²²

Huawei is also the first major telecom equipment supplier that has proactively and voluntarily accepted the toughest supervision and review of its source code, which demonstrates our efforts in remaining open and transparent. Huawei hopes that policy makers encourage more vendors to cooperate with regulators in an open and transparent manner to identify and mitigate risks, and voluntarily disclose their weaknesses and

²² Huawei Cyber Security Evaluation Centre Oversight Board: Annual report 2018 (July 2018), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/727415/20180717_HCSEC_Oversight_Board_Report_2018_-_FINAL.pdf

improvement plans.

3. Huawei's Security Innovation Lab in Bonn explores security standardization and verification for new technologies

On November 16, 2018, Huawei opened its Security Innovation Lab in Bonn, Germany. The opening ceremony was attended by Arne Schönbohm, President of the German Federal Office for Information Security (BSI), and Ken Hu, Huawei's Deputy Chairman. The Lab was established to serve as a platform for strengthening today's technology security, discussing innovative security concepts for future technologies, and contributing to ICT security certifications and global standardization. This Lab works closely with regulators, customers, and research partners and institutes across three aspects:

- Discussions on new technologies and security challenges: continuously communicating with each other to better understand new technologies and cyber security risks, and carrying out forward-looking and innovative cooperation

- Exploration and implementation of trust and verification mechanisms: verifying the results from cooperation on existing products or new technologies
- Collaboration on security standards and certification: discussing and pushing for unified security standards and regulations, and improving security management across the industry

4.Huawei's Cyber Security Transparency Centre in Brussels: commitment to building trust in a digital world

On March 5, 2019, Huawei opened its Cyber Security Transparency Centre in Brussels, which has three major functions:

- Showcasing Huawei's end-to-end cyber security practices, from strategies and supply chain to R&D and products and solutions. This allows visitors to experience cyber security with Huawei's products and solutions, in areas including 5G, IoT, and cloud.
- Facilitating communication between Huawei and key

stakeholders on cyber security strategies and end-to-end cyber security and privacy protection practices. Huawei is working with industry partners to explore and promote the development of security standards and verification mechanisms, to facilitate technological innovation in cyber security across the industry.

- Providing a product security testing and verification platform and related services to Huawei customers.

We welcome regulators, standards bodies, and Huawei customers to work more closely on security standards, verifications, and innovation through this platform. Together, we can improve the security of the entire value chain and help build trust based on verifiable facts.



IX. Huawei cyber security manifesto

Security. We do more.

That's because security is more than what most see it to be.

At Huawei, security starts with our values and beliefs.

The world today is digitally connected, so people can benefit from technology. We will go to the ends of the earth to achieve this – from the hottest to the coldest places on the planet.

We believe security is about keeping networks running, regardless of what Mother Nature throws at it. We stand by our customers in hurricanes, earthquakes, tsunamis, and even wars.

Security isn't just about bits and bytes, it's about human life. It's about being with you through good times, and bad. It's about ensuring we don't put making money ahead of securing the networks we build.

Technology is a wondrous thing, but it's also a complex thing. Technology is not something you can do on your own. It takes

partnerships, global supply chains, industries and governments working together to benefit the world.

We're fully committed to security in every way. We welcome input, ideas and suggestions to improve everything we do, so we can benefit our customers, and their customers. Today, we're probably the most open, most evaluated and transparent company in the world.

We will always prioritize security over costs, schedules and functions. We imbue security processes into product lifecycles: from design, to development, to delivery.

If there is a security standard or security certification that needs to be achieved, we will achieve it.

We believe you cannot have good privacy without good security, nor good security without good privacy.

We would never do anything illegal. We will never harm any country or any individual, and never accept any request to use Huawei products for malicious purposes. If we are ever put such a position, we would rather close the business.

We're here to help our customers maximize the value of their

assets. Nothing matters more to us than being customer-centric. It's why we do more to build trust, to enhance our capabilities, to be transparent, and advocate collaboration.

Security isn't just something we invest in constantly, but a value that serves as the foundation of our existence.

When we do more for security, you can expect more from us.

X. About Huawei

Huawei products and solutions have been deployed in over 170 countries and regions, serving more than three billion people around the world. We have more than 188,000 employees, and more than 80,000 of them are R&D employees, accounting for 45% of the total Huawei workforce.

Huawei is an industry leader in both 5G technology and commercial deployment, and we are the only equipment vendor in the industry that can provide a full set of end-to-end 5G systems. As of August 2019, we had signed 50 commercial contracts for 5G, and had signed 5G cooperation agreements with more than 50 business partners worldwide. We had shipped over 200,000 5G commercial base stations to our customers around the world – far more than any of our peers in the industry. In the first half of 2019, we launched our first 5G smartphone powered by in-house 5G chips, and it will be widely available in the second half of the year.

Huawei maintains its leadership in the industry through continuous innovation, and has one of the most valuable

intellectual property (IP) portfolios in the telecom industry. We respect and protect the IP of others. Every year, we invest at least 10% of our revenue in R&D. In 2018 alone, Huawei invested about US\$14.8 billion in R&D, about 14.1% of our annual revenue. Our R&D investment over the past decade exceeded US\$70 billion. Moving forward, Huawei will be increasing its R&D investment progressively to between US\$15 billion and US\$20 billion per year.

As of the end of 2018, Huawei has held 87,805 patents worldwide. The United Nations World Intellectual Property Organization (WIPO) reported having received 5,405 patent applications from Huawei in 2018 – more than any other company in the world. Huawei began researching 5G more than ten years ago and has declared 2,570 5G standard-essential patent families to ETSI. We advocate for IP protection because it is critical to our ongoing success.

We worked with 25 leading customers through our NetCity joint innovation program, and fully upgraded our Intent-Driven Network Solution. About 46.4% of our revenue comes from overseas markets. 70% of the materials used by Huawei are from suppliers outside China's mainland. In 2018, we

evaluated 2,778 of our mainstream suppliers for cyber security risks, and verified the progress of related corrective action plans. We signed a Data Protection Agreement with 582 suppliers for privacy protection, and performed due diligence on these suppliers.

In 2019, we shipped 100 million units of smartphones within just 149 days – nearly two months ahead of 2018.

Huawei is passionate about supporting mainstream international standards and actively contributes to the formulation of such standards. Huawei is an active member of more than 400 standards organizations, industry alliances, and open source communities, where we hold more than 400 key positions. We are a member of the board or executive committee in organizations like the 3GPP, IIC, IEEE-SA, BBF, ETSI, TMF, WFA, WWRF, CNCF, OpenStack, LFN, LFDL, Linaro, IFAA, CCSA, AII, CUVA, and VRIF. In 2018, Huawei submitted more than 5,000 standards contributions, bringing the company's total number of standards contributions to nearly 60,000.

Huawei continues to invest in its Developer Enablement

Program. In 2018, the number of registered developers worldwide reached nearly 300,000 – a 150% increase over the previous year. We also launched around 600 new certified joint solutions, and were joined by over 1,700 new developers in 2018.

More than 4,700 students from 108 countries and regions have studied at Huawei as part of the Seeds for the Future program, which has just celebrated its 10th anniversary. Huawei's ICT academy covers 557 colleges across more than 60 countries and regions.

As of December 31, 2018, the company has 96,768 employees participating in the Employee Stock Ownership Plan (ESOP). This plan effectively aligns employee contributions with the company's long-term development, fostering Huawei's continued success. This gives us the ability to take a long-term view; it also ensures balance among risks, incentives, and strategies. Employees know if they do not serve their customers well or if they engage in inappropriate activities, their shares and bonuses may be affected.

Huawei Technologies Co., Ltd.



Huawei Industrial Base, Bantian, Longgang

Shenzhen, China

Tel:+86 755 28780808

Zip code:518129

www.huawei.com

 **HUAWEI**, **HUAWEI**  are trademarks or registered trademarks of Huawei Technologies Co.,Ltd
Other Trademarks,product,service and company names mentioned are the property of thier respective owners

Copyright © 2019 HUAWEI INVESTMENT & HOLDING CO., LTD. All Rights Reserved.

GENERAL DISCLAIMER

THE INFORMATION IN THIS DOCUMENT MAY CONTAIN PREDICTIVE STATEMENT, INCLUDING BUT NOT LIMITED TO, STATEMENTS REGARDING FUTURE FINANCIAL RESULTS, OPERATING RESULTS, FUTURE PRODUCT PORTFOLIOS, AND NEW TECHNOLOGIES. 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 PURPOSES ONLY, AND CONSTITUTES NEITHER AN OFFER NOR A COMMITMENT. HUAWEI MAY CHANGE THE INFORMATION AT ANY TIME WITHOUT NOTICE, AND IS NOT RESPONSIBLE FOR ANY LIABILITIES ARISING FROM YOUR USE OF ANY OF THE INFORMATION PROVIDED HEREIN.