Cyber Security Perspectives

21st century technology and security – a difficult marriage

John Suffolk

SVP | Global Cyber Security Officer
Huawei Technologies

HUAWEI

TABLE OF CONTENTS

September 2012

1 Introduction

This document provides an open and frank perspective of Huawei's viewpoints regarding cyber security and the overall ramifications and impact it has on technology, society and our daily life.

Within this document we provide an overview of the current state of cyber security in terms of historical context, the players, and the unique challenges that the ever-expanding global supply chain poses for all of us.

Included is an overview of the Huawei approach to the cyber security and global supply chain challenge and suggestions for how to address these concerns in a proactive and pragmatic way across our industry. Without a doubt, the need for ongoing transparency and an even-handed partnering approach across our industry to proactively manage cyber security and global supply chain risk mitigation is required between both the public and private sectors.

As a global company, Huawei is dedicated to closely collaborating, innovating and establishing international standards with other global organisations to ensure that the integrity and security of the networked solutions and services we provide meets or exceeds the needs of our customers and provides the assurance confidence required by their own customers. This document represents one step to improve industry awareness of our own global efforts to ensure a secure and better cyber future for all of us and to present our view on actions companies and governments need to carry out to manage the global cyber security challenge.

2 Executive Summary

Our world has become truly connected.

During the past twenty years, we have witnessed the blossoming of the commercial Internet, which planted the seed of an interconnected and global digital network that has made such things from email to telemedicine to browsing and social networks to online banking and retailing ubiquitous and affordable.

Cyberspace is a new strategic domain, but it is unlike the physical territory of which we are used to. It has gradually become the "nervous system" through which society operates. Countries now attach significant importance to the development of cyberspace technologies. 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.

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. As technologies become more pervasive, 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.

The development of interconnected networks has encouraged investment and has enabled new consumption models that has driven global economic growth and has fueled the global economy. Open networks connect the world, facilitate economic exchanges across regions, and promote global trade. Information technology has become a key driver behind economic growth. As reported by the World Bank, for every 10% increase in broadband penetration, the GDP in developing countries will increase 1.38%.[1]

With the substantial growth in data and the use of technology we must adopt a positive attitude towards "data floods" and technology – not merely looking at the ills or complexities that they create. We must utilise information to bridge the digital divide, provide more people with access to communications and information systems, and allocate information resources more appropriately, so that everyone on the planet can benefit from the use of technology. The openness of networks makes it possible for people to have equal access to information, improve social justice, and balance development across regions. The openness of networks has promoted cultural exchanges and helped to soften many of the misunderstandings, acts of discrimination, and cultural conflicts that exist between people with different cultural backgrounds.

Yet, notwithstanding the monumental personal, social and enterprise-oriented benefits that we have realised as a result of the digital and broadband revolutions, age-old real-world evils ranging from vandalism, theft and disruption to espionage and wilful destruction have naturally gravitated to the new digital environment.

Huawei, a global organisation doing business in over 140 countries and connecting almost one-third of the planet's population, is actively engaged in meeting these challenges head-on. As one of the world's leading ICT solution

[1] http://www.broadbandcommission.org/Reports/Report_2_Executive_Summary.pdf

providers, Huawei has deep technical understanding of how networks operate, and how technology fundamentally underpins and drives the health, wealth, safety and prosperity of citizens around the world.

Yet not a day goes by that we do not read or hear politically - or competitor-inspired negative commentary about cyber security. While worry about breaches of cyber security is understandable and legitimate, the rhetoric risks distracting from the wide range of challenges our industry faces. Achieving an effective, global, industry-wide solution is going to demand sober and fact-based dialogue, not commercial or political jousting.

In a world where over 87% of the planet's population are mobile users, where the Apple App Store has seen over 25 billion downloads, and where the downloads of Google Play Application Store have exceeded 20 billion, the stark reality is that cyber security is a growing global challenge demanding rational and universal solutions.[2, 3, 4]

No longer is technology designed, developed and deployed only in one country; no longer can any country or large company claim to rely on a single sourcing model; and no longer is it possible with today's complex technology ecosystem and architecture that we can stop all threats from all threat actors.

As governments, enterprises and consumers have become increasingly reliant on ICT solutions that integrate inputs designed, developed, coded and manufactured by multiple suppliers around the world, the scale of the cyber security challenge has grown exponentially.

Cyber security is not a single country or specific company issue. All stakeholders – governments and industry alike – need to recognise that cyber security is a shared global problem requiring risk-based approaches, best practices and international cooperation to address the challenge.

With the recent publications of threats such as Stuxnet and Flame, the world has reached a decision point: does it continue on its current path whereby any misguided actor, regardless of motive, can operate freely in an unregulated world and develop malware for any purpose? If we accept this route, then we must stop complaining and accept the consequences of the cyber race to the bottom of the pit and the return of the Wild West. Or should we collectively step back from the precipice, as we have done in other forms of warfare, and establish laws, norms, standards and protocols – accepting that trust has to be earned and continually validated and also accepting that a lack of trust exists between some stakeholders when it comes to cyber security. In this scenario we must be realistic but determined.

This paper favours and supports international collaboration, openness and verifiable trust as the foundation for a world where technology can continue to drive economic and social improvement for the majority of the 7 billion citizens on the planet.

We hope you support this option too.

At Huawei we make this commitment: We will support and adopt any internationally agreed standard or best practice for cyber security in its broadest sense; we will support any research effort to improve cyber defences; we will continue to improve and adopt an open and transparent approach enabling governments to review Huawei's security capabilities, and finally, as we have done to date, we warmly welcome the assistance from our customers in enhancing our processes, our technology, and our approach to cyber security so that we can provide even greater benefits to them and their customers.

---

[2] http://www.itu.int/ITU-D/ict/facts/2011/material/ICTFactsFigures2011.pdf

[3] http://www.apple.com/pr/library/2012/03/05Apples-App-Store-Downloads-Top-25-Billion.html

[4] https://sites.google.com/a/pressatgoogle.com/google-i-o-press-2012/android

3 Communications and our 21st Century Society

It's about keeping faith…in a global ecosystem

Much of the world today tends to take the ability to communicate by voice and data for granted. In this respect, we expect and desire it to always be accessible and always be on. The way communications technology has woven itself into the interactions of our society is itself a marvel to behold; the availability and capability of the systems and applications we use every day has come to be relied upon to make our lives easier.

There has been a dramatic increase in the use of technology by governments, enterprises and consumers. By the end of 2011, global mobile users reached 5.96 billion people accounting for 86% of the global population, an increase of 12.3% from 2010.[5]

Increasingly rich telecommunications and Internet applications have become widely available. The market share of smartphones is increasing year by year. Take the United States as an example: the market share of smartphones in March 2012 reached 50.4%, up from 47.8% in December 2011.[6] Smartphones integrate more and more functions and applications, among which are applications involving personal data such as contacts, location data, personal photos and mobile banking. The number of applications for smartphones is surging. For example, the number of applications in Apple's App Store has reached the 25 billion downloads milestone; an average of 79 downloads for every iPhone, iPod Touch and iPad owner.[7]

Malicious collection of personal data and unintended design errors all potentially cause damage to the network and to its users.

The global growth in social networks has created personal security challenges with one survey claiming that in England and Wales, a Facebook crime occurred every 40 minutes, with some 12,300 cases linked to the site.[8] This is not an indication of the cyber security provided by the social network, but of how innocent social media technology can be misused or abused.

As the usage of smartphones has increased, so too have the motives and methods of attacking them. Between 2004 and 2011, the prevalence of malware in smartphones increased by 600%.[9]

With the enrichment of business capabilities and improvements in user experience, the complexity and scale of ICT-related software is rapidly expanding. As the scale and complexity of software has increased, so too has the number of security vulnerabilities. [10]

In the past, the telecommunications network infrastructure was closed and dedicated. However, nowadays with

[5] http://www.itu.int/ITU-D/ict/statistics/

[6] http://techcrunch.com/2012/05/07/nielsen-smartphones-used-by-50-4-of-u-s-consumers-android-48-5-of-them/

[7] http://www.guardian.co.uk/technology/appsblog/2011/jul/07/apple-iphone-app-store-downloads

[8] http://www.dailymail.co.uk/news/article-2154624/A-Facebook-crime-40-minutes-12-300-cases-linked-site.html

[9] F-Secure Mobile Threat Report Q4 2011

[10] Alhazmi OH et al., Measuring, analyzing and predicting security vulnerabilities in software systems, Computers & Security (2006), doi:10.1016/j.cose.2006.10.002

the development of new services such as VOIP IMS, the network infrastructure also provides interfaces to third-party service providers and IP-based open protocols are applied more frequently. In the past, telecommunications equipment was usually run on special hardware, whereas today, more and more equipment is based on common infrastructure components and operating systems. The shipment of Advanced Telecommunications Computing Architecture (ATCA) platforms, which are based on common infrastructure and operating systems, increased by 10 times from 2008 to 2011, and more than 100 companies participate in the ATCA ecosystem today.[11]

Uncertainty about being able to securely communicate and access online data and applications can create disorder and confusion and shake the faith of users. As stewards of communications technology, we need to ensure that trust is maintained and relationships, processes and approaches continually evolve to meet the digital challenges of the 21st century and beyond.

3.1 The Growing Cyber Security Challenge

Approaches to cyber security were originally developed to protect networks and data, evolving in recent decades to the fight against cybercrime and other online malicious activity. Cybercrime is the same as any other kind of crime – there is a culprit and a victim. For a cybercrime to be successful, like any other crime, it needs the motive, the opportunity and the means. As technology has become more widespread and more intertwined into the fabric of everyday government, business and personal use, so too have the potential rewards for cybercrime. As accessibility and connectivity have increased, the means and the opportunity have also increased for cyber incidents. Prior to the Internet age, only a few people knew how to use computers and there was little reason to "assault" them. Today, the Internet can be easily accessed from a mobile device in your pocket, so the means and the opportunity have therefore greatly increased. Now nearly everyone is connected and there are many ways to use cyberspace both for private and commercial use – for good motives and for bad.

In a presentation to the RSA Conference, Dr Stefan Frei, the Research Analyst Director at Secunia, a Danish computer security service provider, articulated how the threat environment is changing from script-kiddies undertaking hacking for curiosity to experts developing a means for others to implement for personal gain. Where there is money or advantage to be gained, there will be crime – technology is no different; in some instances it just makes it easier.[12]

Global technology companies have to protect their technology from a range of malicious uses, these include:

Use in sabotage: Control, paralysis, interruption or take-down of networks or infrastructures

Use in espionage: Enabling a third-party to illegally spy on another person or entity through their technology

Becoming the extension of another group/state: The Company's global reach and capability being directed by another government/group to act against another state/sub-state, group or individual

Lack of precaution and competence: Lack of best practice, end-to-end cyber security capability renders the technology an easy attack vector – used by any of the threat actors to use the company's technology or capability for an illegal or inappropriate purpose

All companies that develop and support technology must build in risk-informed mechanisms, counter-measures, policies and procedures that limit the likelihood of perceived or actual threats from being successful. These include,

[11] http://www.heavyreading.com/details.asp?sku_id=2228&skuitem_itemid=1111

[12] http://secunia.com/resources/reports/?action=fetch&filename=Secunia_Moving Target_presentation_RSA2012.pdf

but are not limited to:

- Hardware/software "kill switch" (fixed or remotely controlled)
- Control via backdoors, Trojans, viruses and software logic bombs
- The company (individuals or groups) is instructed to close down networks, undertake espionage or sabotage or assist a third party in illegal activities
- Enabling access to data (including technological intelligence, national security information, commercial security information, private data)
- Built in "call home"/ wiretap capability to transfer data or control to another country/group
- Weakness in R&D process – inject person or software threat
- Weakness in supply chain – inject component (pre or post build)
- Weakness in person – bribe
- Weakness in onsite support capability – inject person/bribe or install illegal software

As can be seen by the range of ways and methods technology vendor's hardware and software could be maliciously used requires continuous assessment of the techniques and potential weaknesses to be undertaken. At Huawei we assess all of these items and ask ourselves the question "what would someone need to do to execute one of these attack mechanisms?" We then ask "what would be a cheaper, lower risk, higher probability of success mechanism?" and from these answers we work out how best to mitigate any such event. Our current model is, we assume nothing, we believe no one, and we check everything.

3.2 Devices, Data, Drama

Given the intense media attention being given to cyber security, you would think that "data/IPR loss" was something new, something that didn't happen in the non-digital or paper world. But of course it did, and it continues to this day.

Just remember all of those people who left their company and took client lists with them, or the future product portfolio, or the product pricing model or even the designs and technical drawings of the next product. It just so happens that technology has helped people who are so inclined to do it faster and cheaper, while accruing vast amounts of data – they can even do it remotely. A recent survey discovered that 51% of European office workers take information from their current employer when they switch jobs and are helping themselves to confidential customer databases, despite data protection laws forbidding them to do so.[13]

The cost of this data leakage, at its kindest or industrial espionage at its most aggressive, is claimed to run into the billions, although actually getting an accurate assessment of losses appears impossible. One thing is for certain, any search for a company whose asset value has been reduced due to alleged cyber espionage is impossible to find. Nor has it been possible to find an external audit on such a potential loss or a declaration to any stock exchange for listed

[13] http://www.businesscomputingworld.co.uk/when-employees-leave-your-company-so-does-your-data/

companies by Board Directors as part of their fiduciary duties. Unless we are honest with what is happening we cannot assess where to invest, and importantly might end up over regulating and reduce the untold benefits technology brings.

Other things have changed too. We are almost totally reliant on technology to store data, process transactions and run our businesses, and, to some extent, our lives. The data that we store continues to increase at dramatic rates.

We own more and more devices and we are connecting more and more of them together. In developed countries it is not uncommon to find mobile penetration rates that exceed the number of citizens – each one of these devices gives us yet another place to store, and perhaps lose, data. Crucially, these devices also act as a potential entry point for people who wish to steal your data from your infrastructure, corrupt it in total, or, even worse, corrupt small elements of your data, thereby significantly reducing your confidence in the data that is held.

Just imagine the horror of stored blood types being changed in some random way, or some of your banking transactions being changed infrequently by random amounts – it is hard to spot, hard to trace and therefore hard to fix. Imagine the negative impact on the confidence of the public in institutions affected by such a scenario.

Of course the threat is not limited to random manipulation. It could be someone hacking into your car's technology and manipulating your engine to turn it on or off via a text message,[14] although there are companies working hard to prevent this.[15] Or, indeed, it could be cyber terrorists hacking into the electricity grid, a scenario detailed in the RUSI Journal article "Cyber-Weapons" by Rid and McBurney, which clearly showed how critical infrastructure often has remote access and can therefore be exploited.[16]

A less dramatic scenario involves that small smartphone application you downloaded – the one that asked for "trusted status" and access to your stored phone data. If malicious software was downloaded inadvertently, suddenly your calendar, your contacts, emails and texts have been uploaded (probably unencrypted) onto some distant server for purposes you may never know, and you may never know that it happened.

3.3 Identifying the Players

It is important to recognise the wide range of adversaries in the cyber world we live in. They include:

- Individuals, who engage in a range of activities, including harassment, intimidation, bullying and grooming children for sexual exploitation
- Hacktivists, who are individuals or groups (lose or tightly linked) that have a particular point to make and use hacking to promote their cause(s)
- Criminals, organised (and disorganised) who run various scams, from illicit trade and counterfeiting to industrial espionage
- Terrorists, however defined, who set out to cause harm
- Government-sponsored agents who use technology as they use other intelligence methods: to gather data and information on items of interest to them
- Commercial espionage undertaken by a range of parties to obtain advanced information from a country or competitor for their own advantage

---

[14] http://www.securityweek.com/car-hacking-researchers-highlight-emerging-risks-and-lack-security-automobiles

[15] http://www.reuters.com/article/2012/08/20/us-autos-hackers-idUSBRE87J03X20120820

[16] http://dx.doi.org/10.1080/03071847.2012.664354

Without a doubt, there is a need for everyone to consider the issue of technology security, as part of the larger risk environment in which we live and work. As the world has become increasingly interconnected and as governments, enterprises and consumers have become more reliant on technology, the scale of the challenge has become significantly greater.

The world has probably lost more confidential records than there are people on the planet, and it is easy to get the impression that there are more breaches of security each year than there are drops of rain in a storm. Barely a day goes by without a report of a potential critical infrastructure in some part of the world being attacked (or having the potential for attack) by cyber criminals.

As we deploy more technology, connect more technology, use more technology and share more technology, we are becoming more blasé about personal and corporate data and the technology we use. This naivety represents a dangerous disrespect for the importance of data to our daily lives, which in itself fuels an increase in security risks.

Consider this: International protection software vendors now claim that there are 12 new unique malware technology threats being created every second of every day[17] and if you knew where to look, each of us could go and purchase unique malware offered for $249 with a service level agreement and replacement warranty if the purchased malware is detected by any anti-virus software within nine months.

While the inclusion of governments on the list of cyber world adversaries seems incorrect given the outspoken nature of governments that vehemently decry those hacking their country, it is important to keep in mind that throughout history, spying and espionage have continually played a role in diplomacy, for better or for worse. In two recent Forbes articles – "Meet The Hackers Who Sell Spies the Tools to Crack Your PC (And Get Paid Six-Figure Fees)" and "Shopping For Zero-Days: A Price List for Hackers' Secret Software Exploits" – Forbes detailed that there is a vibrant industry in identifying and selling zero-day exploits, which are defined as attacks on security vulnerabilities as soon as those vulnerabilities are discovered. In fact, the articles indicated that governments around the world are frequently the purchasers of zero-day exploits and that large defence contractors also buy and sell zero-day exploits. If Governments are indeed involved in the acquisition of zero-day exploits or are developing or "weaponising" attack software, such as Flame and Stuxnet, the phrase "what we sow we reap" springs to mind.[18, 19, 20, 21]

---

[17] http://www.symantec.com/threatreport/topic.jsp?id=threatreport&aid=2011_in_numbers&om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2012Apr_worldwide_ISTR17

[18] http://news.cnet.com/8301-1009_3-57445975-83/flame-a-glimpse-into-the-future-of-war/

[19] http://www.bbc.co.uk/news/technology-12633240

[20] http://www.europeaninstitute.org/EA-November-2011/main-cyber-threats-now-coming-from-governments-as-state-actors.html

[21] http://www.smithsonianmag.com/history-archaeology/Richard-Clarke-on-Who-Was-Behind-the-Stuxnet-Attack.html

3.4 Understanding the Impact of the Global Supply Chain

Open up any smartphone, tablet, personal computer, television or even consumer white good and you will see within the device the work of a global supply chain. Taiwan for instance, produces a notebook computer every 0.35 of a second, a PDA every 8.54 seconds, and a desktop computer every 0.68 seconds.[22]

In the United States, a Government Accountability Office (GAO) report published in March 2012 warned that the global supply chain of IT products could be putting national security at risk:

> *"Federal agencies rely extensively on computerized information systems and electronic data to carry out their operations. The exploitation of information technology (IT) products and services through the global supply chain is an emerging threat that could degrade the confidentiality, integrity and availability of critical and sensitive agency networks and data."* [23]

The report said officials at the Departments of Energy, Homeland Security, Justice and Defence told investigators from the GAO that they did not know the extent to which their telecommunications networks contained foreign-developed equipment, software or services. According to the report, the Departments of Energy and Homeland Security had not defined supply chain protection measures. The Justice Department had defined protection measures, but had not implemented them or developed procedures for monitoring compliance with the measures.

There appears to be no definition of what is meant by "foreign-developed" and whilst the report may have focused on telecommunications networks, it really needs to consider all technology from all vendors.

The reality is a single piece of equipment, such as a laptop, can include components from all over the world, from Canada, Ireland, Poland, Italy, the Czech Republic, the Slovak Republic all the way to China, Israel, Japan, Malaysia, the Philippines, Singapore, South Korea, Taiwan, Thailand, Vietnam and many others.

Consider this: The Chinese city of Chengdu has 16,000 companies registered and 820 of them are foreign-invested companies.[24] Of these, 189 are Fortune 500 companies. Household brand names such as Intel, Microsoft, SAP, Cisco, Oracle, BAE, Ericsson, Nokia, Boeing, IBM and Alcatel-Lucent are all located there to name but a few. Should what these companies do be considered "foreign developed"?

Cisco has a huge presence in China, with R&D centres in six major cities. Over 25% of all Cisco products are produced by Chinese partners, and the company announced a US$16 billion investment in China that includes training 100,000 network engineers and the opening of 300 centres at vocational colleges to train students in networking technologies.[25] Cisco CEO John Chambers stated, "What we are trying to do is outline an entire strategy of becoming a Chinese company."[26, 27] - does this constitute "foreign developed"?

According to company reports, every major telecommunications equipment provider has a substantial base in China.

---

[22] http://www.taiwan-technology.com/edit/p/epaper/200902180.htm
[23] http://www.gao.gov/assets/590/589568.pdf
[24] http://www.chengduhitech.co.uk/Default.asp
[25] http://www.usatoday.com/tech/products/2007-11-01-425344141_x.htm
[26] http://www.epi.org/publications/trade_policy_and_the_american_worker/
[27] http://news.xinhuanet.com/english/2005-06/17/content_3096764.htm

Alcatel-Lucent has one third of its global manufacturing done by Shanghai Bell; [28] Ericsson's joint-venture Nanjing Ericsson Panda Communications Co. has become the largest supply centre of Ericsson in the world; [29] at the end of 2011, Nokia Siemens Networks had 10 manufacturing facilities worldwide: 5 in China (Beijing, Shanghai, Tianjin, Hanghzou and Suzhou), and 2 in India [30] – is what they do "foreign developed"?

If we look at India, a mature professional set of international companies and support services has been created over the last 20 years, providing technology on-shoring and off-shoring for the global enterprise community. In purely financial terms, total exports from the Indian IT sector were at US$59 billion during FY11. The industry has seen strong growth at a CAGR of 16.4% during FY07-11 despite weak global economic growth,[31] and India has generated world-class IT players, such as TATA, Wipro, Infosys and HCL Technologies. World-class companies, such as many of those mentioned above, plus the likes of Siemens, HP, Philips, ABB, Flextronics and AT&T, have all established operations there. Cisco has over 8000 employees in India including R&D, sales and business support staff. There is extensive support system for customers with 18 logistics centres. The Cisco Global Development Centre is in Bangalore and is the largest outside of the US. Cisco also established joint development centres with Wipro Technologies and Infosys Technologies in Bangalore; HCL Technologies in Chennai and Zensar Technologies in Pune.[32]

In summary, the concept of "foreign developed" in today's globally intertwined world is meaningless just as the notion that companies or products from one part of the globe can be trusted more than companies or products from another part of the globe. You have to wonder whether this thinking is any more than trade protectionism masquerading as national security. In today's globalized world, any policy toward cyber security that is based solely upon the nationality of the provider or upon where the provider's headquarters is located is bound to be ineffective. Any approach to cyber security that simply singles out companies on the basis of their national origin is not logical. Such an approach moreover is inherently discriminatory and violates most-favoured-nation treatment.

A Microsoft paper entitled, "Cyber Supply Chain Risk Management: Towards a Global Vision of Transparency and Trust", which we fully endorse, includes the following:

> *"First, vendors have a significant economic incentive to resist the efforts of national governments to taint the supply chain for a very simple reason: there is a significant risk that back doors or other intentional defects will be discovered and made public, and such a revelation will lead to loss of public trust, and, ultimately, market share. Indeed, it is likely that a company engaging deliberately in such activities may be forced out of business, especially if one appreciates that the loss of trust would be global; that is, even people in the vendor's home country are likely to reject a product with secret backdoors, even if they were inserted primarily so that the local government could obtain advantage against foreign adversaries. In many countries, there is concern not just about foreign surveillance, but domestic surveillance as well."*

And their conclusion:

> ***"While government concerns are understandable, it is important that government responses do not threaten the vitality of the global ICT sector, stifling both innovation and competition."*** [33]

The fact is that when you connect devices from multiple suppliers into your technology infrastructure, the equipment and software are likely to be designed, developed and manufactured via tens, if not hundreds, of companies from around the world.

---

[28] http://www.alcatel-sbell.com.cn/Default.aspx?tabid=262&ArticleID=1173

[29] http://www.ericsson.com/cn/thecompany/ericsson-china/background-china

[30] http://i.nokia.com/blob/view/-/1015984/data/3/-/form20-f-11-pdf.pdf

[31] http://www.ibef.org/industry/IT-ITeS.aspx

[32] http://www.cisco.com/web/IN/about/company_overview.html

[33] http://www.microsoft.com/en-us/download/details.aspx?id=26826

The global ICT supply chain issue was summed up by Richard Clarke, who served as Chair of the Counter-terrorism Security Group and as a Member of the National Security Council under President George H.W. Bush, and who also served under President Clinton. In 2002-2003 Clarke served as a Special Advisor to President Bush on cyber security and chaired the President's Critical Infrastructure Protection Board that helped draft the United States National Strategy to Secure Cyberspace that was released by President Bush in February 2003. Clarke said, "My attitude is, whether it comes from New York state or Shanghai, it probably has the same risk in software. There are people in the United States who can be bribed, too." [34]

3.5 Analogue Law in a Digital World

Cyber security is a global issue. The transfer and process of data is a global activity and data flow does not respect national boundaries or the territorial jurisdictions of governments or courts; an Internet search in the US could be processed by a server in the US, or a server in Europe or even in Asia. However, legal and regulatory systems are based on such boundaries and jurisdictions, which pose a major problem to all multi-national businesses engaged in the processing and transferring of data.

Taking data protection and privacy laws as a measure for laws in general that impact the ICT industry, Europe has a more consolidated approach to data protection law. But even so, while there is a uniform approach to data protection law provided for in the EU Data Protection Directive, the implementation of the Directive through each of the 27 Member States varies significantly. In the United States, privacy laws are fragmented between the federal and state levels. Federal legislation is sector specific, where laws addressing privacy in the financial, health and other select industries exist but there is no comprehensive federal law addressing privacy. States also have privacy laws, but such laws are not consistent among the various states. For example, virtually every state has enacted its own data security breach notification law. Obligations related to the content of breach notification notices, as well as whether the company has to notify regulators, state attorneys general or credit bureaus vary significantly.

Many countries and regions (e.g., Australia, India, China, Argentina, Malaysia, Hong Kong, etc.) differ greatly in obligations imposed by laws and in enforcement. Even in a single country, different regions may be inconsistent in enforcement and interpretation of relevant law. Companies are confronted by additional challenges in countries that may not have formal laws, but instead define standards and codes that are not enshrined into law.

In summary, this demonstrates that all companies, including equipment vendors such as Huawei and its corporate customers, face a patchwork of laws and regulations where obligations vary not just based on geography but also on subject matter. The legal and regulatory environment imposes obligations with respect to surveillance and interception that impacts industry standards. Thus, equipment manufacturers must produce equipment that will comply with numerous industry standards and laws. Further, equipment manufacturers face additional challenges given that laws are by no means static. As laws change, hardware and software must be modified to reflect the new legal requirements.

Huawei would welcome a coordinated international approach to principles of data protection and cyber security. We believe that such an approach would foster better overall standards of data protection on a global basis, rather than having vendors, service providers and corporations struggle to apply inconsistent standards and approaches across various countries. As illustrated by this White Paper, equipment manufacturers such as Huawei operate in a complex legal and regulatory environment. Huawei is committed to complying with all of the applicable laws and regulations in every jurisdiction in which it operates and will restrict its operations as necessary to comply with international sanctions and local law.

---

[34] http://www.networkworld.com/news/2011/091911-clarke-cybersecurity-251014.html

4 The Huawei Approach

In cyber security…it's a marathon, not a sprint

Huawei is proud of its heritage and proud to have an entrepreneurial founder who, by an act of fate, just so happens to have been born in China. We would be equally proud if our heritage was American, Indian, German or of any other country.

The complexity of communications infrastructure, diversity of suppliers, technical vulnerabilities created by rapid development and difficulties in complying with changing legislative and regulatory mandates, make managing supply chain risk challenging, but in our experience, the problem is not insurmountable. One of Huawei's commercial values is maintaining its business and political independence. As a global company headquartered in China, Huawei knows that it needs to be committed to going the extra mile in cyber security assurance. Huawei does not, and would not, support, condone or conduct activities intended to acquire sensitive information related to any country, company or individual, nor do we knowingly allow our technology to be used for illegal purposes.

This is a continual effort, and Huawei is committed to providing best-in-class (as defined by our customers and government stakeholders) 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.

4.1 Cyber Security as a Corporate Global Policy

Huawei has always understood that to provide the level of confidence required in a small number of markets by customers who have been "challenged" by their local or regional political or commercial environments to "buy local" or "buy Western" may require us to provide independent assessments of our products and processes along with dedicated localisation to ensure that the integrity of the supply and support flow is maintained to a high degree of security assurance.

We have established and implemented an end-to-end global cyber security assurance system. We emphasize that our commitment to cyber security will never be outweighed by the consideration of commercial interests. It is our primary responsibility and guiding principle to ensure the stable and secure operation of our customers' network and business (especially in times of natural disasters such as earthquakes and tsunamis and other emergencies); we understand that cyber security concerns of the industry and society are increasing.

For reasons detailed in the Microsoft paper referenced earlier, for our survival, we have never damaged any nation or had the intent to steal any national intelligence, enterprise secrets or breach personal privacy and we will never support or tolerate such activities, nor will we support any entity from any country who may wish us to undertake an activity that would be deemed illegal in any country. In this context, with the eyes of the world always upon us, with

us positively encouraging audits and inspections of our capabilities, those that wish a vendor to undertake such an activity is more likely to select a company that is under less scrutiny.

We understand the sensitivity of the industry we are engaged in and the vulnerability of advanced technology. The end-to-end cyber security assurance system has been established and implemented in terms of policy, organization, process, management, technology and specifications. Huawei started its cyber security journey in 1999 when it published its first set of security technical regulations to enhance the security of products and solutions. In 2011, our founder and CEO Ren Zhengfei fully endorsed the strategy and issued the following Cyber Security Assurance policy that further reinforced and enhanced our commitment:

> *"As a global leading telecom solutions provider, Huawei Technologies Co. Ltd. ("Huawei") is fully aware of the importance of cyber security and understands the concerns of various governments and customers about security. With the constant evolution and development of the telecom industry and information technology, security threats and challenges are increasing, which intensify our concerns about cyber security. Huawei will therefore pay a great deal more attention to this issue and has long been dedicated to adopting feasible and effective measures to improve the security of its products and services, thus helping customers to reduce and avoid security risks and building trust and confidence in Huawei's business. Huawei believes that the establishment of an open, transparent and visible security assurance framework will be conducive to the sound and sustainable development of industry chains and technological innovation; it will also facilitate smooth and secure communications among people.*
>
> *In light of the foregoing, Huawei hereby undertakes that as a crucial company strategy, based on compliance with the applicable laws, regulations, standards of relevant countries and regions, and by reference to the industry best practice, it has established and will constantly optimize an end-to-end cyber security assurance system. Such a system will incorporate aspects from corporate policies, organizational structure, business processes, technology and standard practice. Huawei has been actively tackling the challenges of cyber security through partnerships with governments, customers, and partners in an open and transparent manner. In addition, Huawei guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests.*
>
> *From an organizational perspective, the Global Cyber Security Committee (GCSC), as the top-level cyber security management body of Huawei, is responsible for ratifying the strategy of cyber security assurance. The Global Cyber Security Officer (GCSO) is a significantly important member of GCSC, in charge of developing this strategy and managing and supervising its implementation. The system will be adopted globally by all departments within Huawei to ensure consistency of implementation. The GCSO shall also endeavor to facilitate effective communication between Huawei and all stakeholders, including governments, customers, partners and employees. The GCSO reports directly to the CEO of Huawei.*
>
> *In terms of business processes, security assurance shall be integrated into all business processes relating to R&D, the supply chain, sales and marketing, delivery, and technical services. Such integration, as the fundamental requirement of the quality management system, will be implemented under the guidance of management regulations and technical specifications. In addition, Huawei will reinforce the implementation of the cyber security assurance system by conducting internal auditing and receiving external certification and auditing from security authorities or independent third-party agencies. Furthermore, Huawei has already been certified to BS7799-2/ISO27001 accreditation since 2004.*
>
> *In connection with personnel management, our employees, partners and consultants are required to comply with cyber security policies and requirements made by Huawei and receive appropriate training so that the concept of security is deeply rooted throughout Huawei. To promote cyber security, Huawei will reward employees who take an active part in cyber security assurance and will take appropriate action against those who violate cyber assurance policies. Employees may also incur personal legal liability for violation of relevant laws and regulations.*

Taking on an open, transparent and sincere attitude, Huawei is willing to work with all governments, customers and partners through various channels to jointly cope with cyber security threats and challenges from cyber security. Huawei will set up regional security certification centers if necessary. These certification centers will be made highly transparent to local governments and customers, and Huawei will allow its products to be inspected by people authorized by local governments to ensure the security of Huawei's products and delivery service. Meanwhile, Huawei has been proactively involved in the telecom cyber security standardization activities led by ITU-T, 3GPP, and IETF etc., and has joined security organizations such as FIRST and partnered with mainstream security companies to ensure the cyber security of its customers and promote the healthy development of industries.

This cyber security assurance system applies to Shenzhen Huawei Investment Holding Co., Ltd., and all subsidiaries and affiliates which are under its direct or indirect control. This statement is made on behalf of all the above entities.

This statement should comply with local laws and regulations. In the event of any conflict between this statement and local laws and regulations, the latter shall prevail. Huawei will review this statement on an annual basis, and shall keep it in line with laws and regulations.

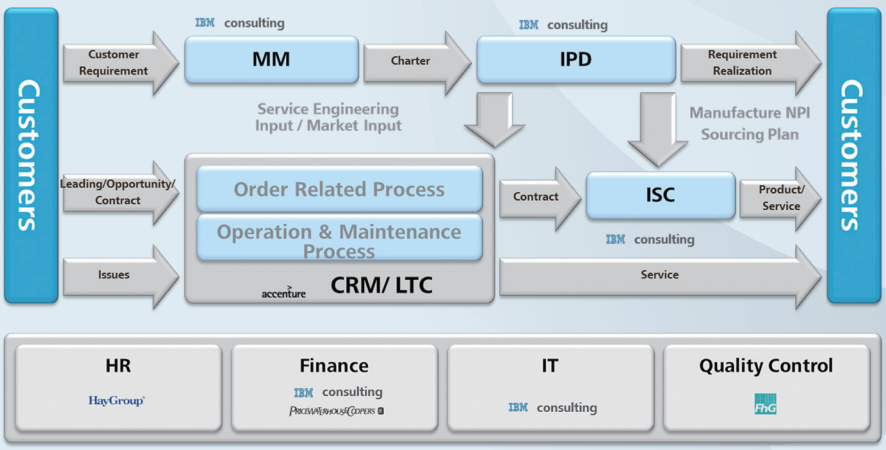
Huawei Technologies Co., Ltd.

CEO Ren Zhengfei"

4.2 Designing Security from within – "Built-in" not "bolted on"

Many companies will talk about quality and innovation; yet delivering sustained, innovative quality products and services requires consistent, repeatable, globally rolled-out processes that deliver on those objectives. Without this level of commitment, each event, each product and each customer interaction becomes a random event – sometimes the experience and product quality is good, and sometimes the experience or product quality is bad. Huawei has employed IBM since 1997 to develop, train and support Huawei in becoming a process-based organisation – one that is fundamentally driven by repeatable processes, which deliver a consistent quality of products and service.

Our high-level process map is detailed below. As you can see, we use some of the world's most innovative and professional organisations to support us: IBM on processes and technology, Accenture on our customer relationship management, the Hay Group on our HR processes, PricewaterhouseCoopers on finance and (not shown on the chart) we use KPMG as our global external auditor.



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

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.

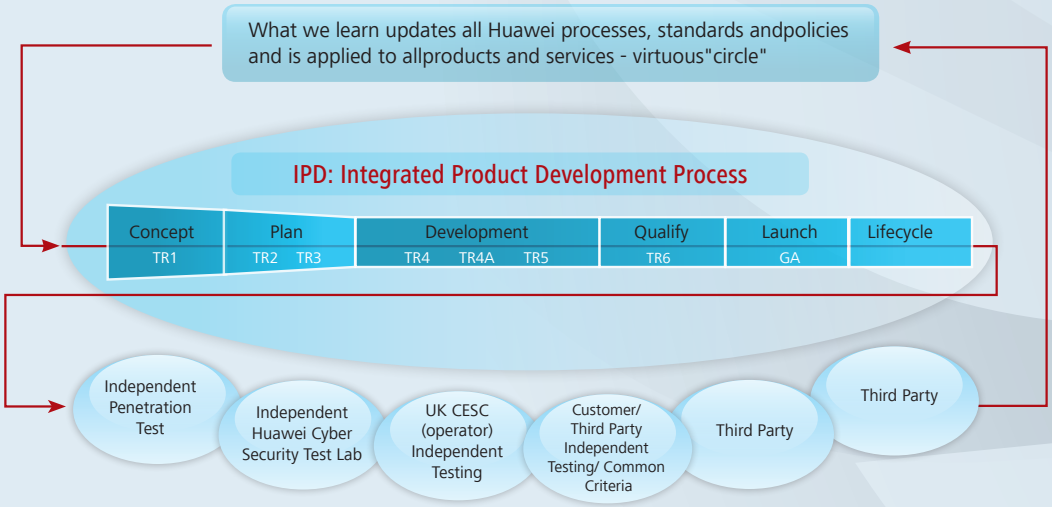
However, we accept that just because you have a process that does not mean that it is a good process, or that anyone actually executes the process. To address these issues, we have taken the following actions:

- Huawei has established standardised business processes globally and has identified Global Process Owners (GPOs) for each process and Key Control Points (KCPs). In addition, Huawei has established a Global Process Control Manual and a Segregation of Duties Matrix that are applicable to all subsidiaries and business units. The GPOs are responsible for ensuring the overall internal control effectiveness, in light of changes in operational environment and risk exposures.

- From a governance perspective, there is a standing Board Committee dedicated to cyber security chaired by a Deputy Chairman. On this Board sits the main Board Members and Global Process Owners who have a role in ensuring that cyber security requirements are imbedded in processes, policies and standards and that they are executed effectively. If there is any conflict, or resource issue in cyber security, this committee has the power, remit and seniority to make decisions and change the business without reference to anyone else.

- Huawei Auditors use the Key Control Points and the Global Process Control manual to ensure processes are executed and that they are effective. Audits, external inspections and third-party reviews all validate what is happening against what should happen. Individual personal accountability and liability (the rules and regulations) are built into Huawei's Business Conduct Guidelines and business processes that specify how we must behave in our daily operations. Knowledge is updated through online exams every year to keep knowledge current and this forms part of our Internal Compliance Programme.

However, there is nothing more important than allowing your processes and internal systems to be opened up to audit and scrutiny from your customers and from governments. It is this ability to use real customers and experts from many fields and governments to inspect, vet and validate our approach that truly enables us to develop world-class processes and integrated systems. Huawei operates in over 140 countries because it is trusted by customers in over 140 countries. Once again, it is a repeatable process that is also a virtuous circle: we develop – we test – we validate – we learn – we update – we develop. It is depicted in this model:



In practice what does this mean? Let us give you an example. Many global technology vendors such as Huawei licence and use software components from many third parties, and this is included within our own developed computer code. Our own software may be developed by multiple teams in multiple countries. Yet when there is a security issue, or vulnerability is found, it is crucial that our internal processes and systems give us the ability to forward and reverse-trace the software components that have been developed and pinpoint what products they are in.

At Huawei, we are continuously enhancing our internal systems and processes to enable us to trace-forward from a raw customer requirement all the way through to the computer code that was produced, and also to reverse-trace from the computer code (or patch/modification) all the way back to the raw requirement that required that computer code to be developed.

Within this, we ensure segregation of duties in the R&D process. Software developers cannot approve the final test results or final release. No software developers can authorise the implementation of their own software as there is an independent rigorous review and sign-off process – once signed off, software is automatically uploaded onto support websites, ready for downloading into manufacturing or customer sites.

However, cyber security is not just about technology. It is also about people, laws, incentives and disincentives. Whilst there is undoubtedly a focus on the design, development and deployment of technology, there is an equal focus on all other processes – human resources, legal, sales, finance, marketing, and supplier management. For instance, in terms of supply chain diversity, 70% of the components used by Huawei come from suppliers outside of Mainland China, with the United States serving as the largest provider at 32% and the majority are high technology components, and Taiwan and Europe combining to provide 32%. In terms of people diversity, the average localisation rate in the more than 140 countries in which we operate is 72%.

At Huawei, because we have built cyber security requirements into our processes, each executive, manager and individual has personal accountability and ownership of their responsibilities. This level of responsibility implies several underlying factors, including continuous training, getting the balance right between incentive and personal liability, and continuous loop-back processes to enhance our capabilities and validate our assurance level. This is the Huawei way of meeting the challenges of cyber security.

At Huawei, we adopt the “many eyes” and “many hands” approach to provide openness and transparency on what we do. We positively encourage audits, reviews and inspections on all technology vendors, including Huawei, in a fair and non-discriminatory manner, as each audit or review enables companies to challenge their thinking, their policies and their procedures, in turn enhancing their capability, product quality and product security. At Huawei, we already provide our customers and governments with the ability to undertake comprehensive validation and verification of our products.

With the growth of mobile and cloud computing, Huawei closely follows the increased demands of network capability brought about by this explosive growth. We actively participate and undertake cloud computing research and we develop some of the industry leading technologies and products in virtual platform security, virtual network defence and the security of cloud computing data to build comprehensive security capabilities in terms of cloud computing. Huawei has become one of the core members of the International Standard Council (ISC) of the influential cloud computing security standard organization (CSA). The ISC of CSA has enabled Huawei, as the liaison officer of CSA, to promote and communicate CSA cloud security standards with Chinese Japanese and Korean Security workshops and CCSA (China Communications Standards Association) on behalf of CSA.

To address cyber security threats, Huawei is proactively communicating with governments, operators and industry experts to discuss establishing a global Cyber Security Advisory Committee to guide the capability building of Huawei cyber security. Huawei has also established the Cyber Security Verification Lab, which is independent from the business, to conduct independent security testing on Huawei products and provide verification reports that fully detail the quality and security capability of the products that have been verified to our customers. In addition, this Lab is also open to Huawei customers and governments for them to validate the security of Huawei products.

Huawei has established deep cooperative relationships with many organizations focused on key cyber security areas, such as threat modelling, malware detection and attack behaviour analysis, to effectively share security capabilities. These include: APWG (Anti-Phishing Work Group), CNCERT/CC (China CERT), OPERA, CNNIC (China Internet Network Information Centre), APAC (Anti-Phishing Alliance of China), anti-virus provider AVG, InterPol (International Criminal Police Organization) and IWF (Internet Watch Foundation).

Huawei has sponsored and participates in numerous cyber security forums and conferences so that we can share and learn from each other. For instance, in EWI (East West Institute) Cyber Security Conference, Huawei participated in workshops about how to reach global cyber security consensus and supply chain security; Huawei also sponsored and presented at the GIIC (Global Information Infrastructure Commission). Huawei sits on the GIIC board, as a Chair, and has also joined the Quest Forum.

Huawei is a substantial contributor to global security standards. For instance, Huawei submits numerous security proposals to 3GPP (The Third Generation Partnership Project) each year. Huawei also takes the lead in developing the H(e)NB security standard and pushes the security research on M2M (Machine to Machine) and PWS (Public Warning System) system together with the main operators and vendors in the industry. Huawei positively encourages its people to be very active in many IETF (Internet Engineering Task Force) work groups such as IPsec, Karp, syslog, OSPF, MPLS, Hokey and IPv6 to discuss IP related security issues with industry experts and because of this active involvement many improvements to proposed standards have been released. Huawei contributes to the security of virtual networks and the standard of anti-junk information. Huawei is a member of the Open Group whose preliminary criteria for development for supply chain standard has been adopted by Huawei. Furthermore, Huawei has participated in the security standard activities of organizations such as IEEE (Institute of Electrical and Electronic Engineers), OMA (Open Mobile Alliance), UPnP Forum (Universal Plug and Play Forum) and WiFi-Alliance.

In summary at Huawei we believe that the resolution of cyber security challenges is a shared challenge. We must come together in an open and transparent way and all of us must make a positive contribution to improving our own knowledge, processes and products as well as actively supporting the development and implementation of international laws, standards, policies and best practice.

5 Managing the Global Security Conundrum - It's about collaboration

We should not assume there is nothing that can be done to meet the cyber security challenge. Verizon's 2012 Data Breach Investigations Report (DBIR) affirms for the fourth year in a row that the majority of data breaches (97%) could have been avoided with the implementation of simple countermeasures.[35]

In Australia, the Defence Signals Directorate (DSD), an intelligence agency in the Australian Department of Defence, produced the Top 35 Mitigation Strategies, a document first published in February 2010 and periodically revised based on the DSD's analysis of incidents across the Australian government. The DSD claims that by implementing its top four strategies, at least 70% of the intrusions that DSD responded to in 2009, and at least 85% of the intrusions responded to in 2010, could have been prevented.[36] The Australian government, as well as other governments, can significantly reduce their concerns over cyber security risks by implementing mitigating actions.

There is much we can do if we show collective will, determination, openness and transparency.

The technology landscape is complex, and is getting more so, given the growing role of smartphones and cloud computing and the extensive use of application stores that contain software developed around the world to differing quality and security standards.

Cyber security issues add to this complexity as cyber security itself incorporates policies, technologies, behaviours, standards, guidelines and laws that cut across multiple sectors and levels of society. In order to adequately address cyber security issues, the private and public sectors must align their goals and responsibilities and collaborate to ensure the integrity and security of data and information systems within a risk-based framework.

Collaboration on cyber security should not be limited by geographical, political or competitive differences. While some may view it as a competitive advantage, the reality is the impact of not collaborating provides the bad actors with many opportunities to exploit the weak links in the global cyber security chain. There are multiple forums available for collaboration, yet even these are the equivalent of loose cooperation and do not fulfil a true comprehensive united front.

In this context governments must take the lead to establish united and integrated governance to drive forward comprehensive and collaborative approaches to cyber security – Huawei commits itself to supporting such an endeavour.

[35] http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

[36] http://www.dsd.gov.au/infosec/top-mitigations/top35mitigationstrategies-list.htm

6 Going Forward - Together

Looking back and reflecting on the current state of the cyber security landscape, we observed that a general lack of cooperation and trust amongst stakeholders has thus far stymied efforts to address these issues in a comprehensive manner. All technology users and vendors have an equally large stake in finding a solution to address these challenges and we must set a better example. Industry and governments must work together to develop the right policy framework to enhance cyber security. Our collective work should be guided by a set of principles to provide a framework for coordination of action to drive progress on an aligned set of strategic priorities and goals, and time-based milestones. We should be prepared to accept that the commitment from some parties may initially not be as strong as we would wish it to be due to the inherent lack of trust between some parties, the issue of local politics and geopolitics, trade protectionism and competitor misinformation – having said that, we should not allow any of these issues to be used as an excuse for not taking action.

Guiding Principles

1. IT'S GLOBAL: Efforts to improve cyber security must properly reflect the borderless, interconnected and global nature of today's cyber environment in terms of governance, laws, standards and sanctions
2. IT'S THE LAW: Efforts to harmonise and align international laws, standards, definitions and norms must be undertaken, accepting the challenges of cultural differences
3. IT'S COLLABORATIVE: Efforts to improve cyber security must leverage public-private partnerships to maximise our chances of increasing our collective ability to thwart attacks
4. IT'S STANDARDS-BASED: Efforts to design, agree on and implement international standards and benchmarks of ICT vendors should set the standard based on the perceived risk level – there has to be a balance between security and risk
5. ITS VERIFICATION-BASED: Efforts to design, develop and implement global independent verification methodologies that ensure products conform to the agreed standards and benchmarks should be agreed and adopted
6. IT'S EVIDENCE-BASED: Efforts to improve cyber security must be based on evidence of risk, evidence of the attacker and evidence of loss or impact – we should focus on facts, not fiction
7. IT'S DOING THE BASICS: Efforts to improve basic cyber security "hygiene" must be collectively prioritised to drive the entry point of successful attack to a much higher point

This paper favours and supports international collaboration, openness and trust as the foundation for a world where technology can continue to drive economic and social improvement for the majority of the seven billion citizens on the planet. We hope you will also support this option.

7 About Huawei

Huawei is a global information and communications technology (ICT) solutions provider that operates in over 140 countries. Our products and solutions serve more than one-third of the world's population and we employ 140,000 people. On average, 72% of our people are locally employed in countries in which we operate, and the average age of our employees is 28. We serve 45 of the world's top 50 telecommunications operators, and, as of 2011, Huawei's wireless networks products and solutions had been deployed by more than 500 carriers worldwide. Huawei has shipped over two million base transceiver stations, serving more than 1.5 billion mobile subscribers.

We are a science and engineering-based private company engaged in research, development and deployment of new commercial technology. Huawei keeps a leading role in the industry through continuous innovation and has one of the most significant IPR portfolios in the telecommunications industry. Huawei respects and protects the IPR of others. Huawei invests 10% of its annual revenues into R&D, with $3.76 billion invested in R&D in 2011 and total investment of over $15 billion in R&D in the last decade.

Huawei has reached patent licensing or cross-licensing agreements with companies such as: Ericsson, Sony Ericsson, Nokia, Nokia-Siemens, Sisvel, Qualcomm, Alcatel-Lucent, Nortel, Dolby, Rovi, BT and KPN etc. In 2011, we paid more than $300 million for patent licenses and the accumulated total payment reached $1.2 billion. Our internal innovation comes from our 1,265 world-class PhDs, 44,690 masters, 62,000 R&D employees, and as of the end of 2011, Huawei had filed 36,344 patent applications in China, 10,650 under the Patent Cooperation Treaty (PCT), and 10,978 patent applications overseas. We have been awarded 23,522 patent licenses. The protection of IPR is therefore critical to the ongoing success of Huawei, and because of this, Huawei is a champion of IPR protection.

We have 23 R&D centres around the world, 34 joint innovation centres with some of our key customers, and 45 training centres. Overall, 68% of our revenue is generated outside of Mainland China, and we source 70% of our materials from non-Chinese companies. The United States is the largest provider of components at 32% (some $6.5 billion of purchases from United States companies in 2011) through 185 suppliers; Taiwan provides 22% of components, and Europe 10%; Mainland China provides 30% of components.

We provide managed services for 115 networks in 60 countries to help customers achieve operational excellence. Huawei has built cloud-based IT solutions and collaborated with over 300 partners to accelerate the commercial application of cloud computing technologies across various industries. By the end of 2011, we had helped customers around the world set up 210 data centres, including 20 cloud computing data centres

In 2011, Huawei's consumer business shipments totalled nearly 150 million units, including 55 million mobile phones. In 2011, Huawei shipped over 60 million mobile broadband devices globally; Huawei also shipped over 30 million home devices, including fixed access and fixed wireless terminals.

Huawei is passionate about supporting mainstream international standards and contributes to the formulation of such standards. By the end of 2011, Huawei had joined 130 industry standards organizations, such as the 3GPP, IETF, ITU (International Telecommunication Union), OMA, ETSI (European Telecommunications Standards Institute), IEEE, the Open Group and 3GPP2. In total, Huawei submitted more than 28,000 proposals to these standards organizations and has served as a board member for OMA (Open Mobile Alliance), CCSA (China Communications Standards Association), ETSI, ATIS (Alliance of Telecommunications Industry Solutions), and numerous other authoritative organisations in which we hold more than 180 positions.

It is written by some that Huawei is different and that we play by different rules. In one sense this is true: we are wholly owned by 65,596 of our employees, who have purchased an equity stake in the company by 31st December, 2011. This gives us the ability to take a long-term view; it also ensures we balance risk with reward and strategy. Employees know if we do not excel at serving our customers, or if we undertake inappropriate activities, their equity and pensions may be destroyed. We also grow significant talent by taking the best scientists and engineers from the best universities around the world, nurturing them and quickly giving them global experience.

Finally, we are an innovation-based organisation: We were ranked fifth behind Facebook, Amazon, Apple and Google by Fast Company magazine in 2010, and we were also awarded the "2010 Corporate Use of Innovation Award" by The Economist.

During the creation of this document, my excellent team provided wonderful assistance and constructive suggestions which are reflected in the lines of the document. Their professionalism and cooperation affirmed my impression of Huawei that we employ some of the best people in the world. Here, I would like to express my gratitude to those who have given me valuable suggestions: Nan Jianfeng, Wang Weijian, Peng Liwei, Yu Zhilin, Paul Michael Litherland, Liu Chenxi, Andy Purdy, Andy Hopkins, Yang Guanglei, John Koshy, Peter Rossi, Didier Blanchard and other people who contributed to this paper directly or indirectly. Please accept my apologies if I have missed your name.