The Economist Intelligence Unit

Politics, cyber-security, trade and the future of ICT supply chains

A custom research report by The Economist Intelligence Unit for Huawei Technologies, Inc

February 2014

www.eiu.com

Table of contents

Foreword

In early 2013, The Economist Intelligence Unit produced a report for Huawei, titled *A brave new world: What it means for Huawei*. It examined major global trends in politics, trade and cyber-security and drew out their implications for Huawei, both as a leading technology firm and as a pioneer among Chinese companies going global. At the time, Huawei was in the spotlight of the global cyber-security debate, following the publication of the controversial report by the US House of Representatives Intelligence Committee (hereafter, "the US House Report"), which accused Huawei and another China-based information and communications technology (ICT) firm, ZTE, of aiding and abetting Chinese state espionage—although the report was widely suspected of protectionist motivations. Placing the US's action in the context of wider political and economic trends, we analysed the challenges facing emerging-market multinationals, particularly those in sensitive industries. The conclusions emphasised the importance to Huawei of increasing transparency and building trust, for instance through stepping up collaboration with non-Chinese companies and governments, or by taking a more active stance in shaping international trade agreements and cyber-security standards.

Over the course of a year, a great deal has changed in the global cyber-security debate. US whistle-blower, Edward Snowden's revelations about US interception activities conducted by the National Security Agency (NSA) and its "Five Eyes" counterparts (in Australia, Canada, New Zealand and the UK)—often in collusion with private-sector companies—have turned the issue on its head, moving the focus from Chinese to US companies. Cyber-security has become more prominent in the public consciousness, and consumer mistrust of technology providers and governments has deepened.

Many countries are currently seeking to frame responses to the new knowledge about US interception laws and capabilities, and this is one of the topics that we address in this year's report. Data privacy and rules on cross-border data flows, in particular, have become hot topics in both domestic politics and international trade negotiations. Legislative and practical solutions to the current trust deficit will vary by country, with a higher risk of protectionist reactions in certain regions. In the EU, for instance, Huawei faces possible future discrimination as a result of new rules, which, while aimed at US companies, would eventually affect all non-EU companies. The following report takes a closer look at how ICT supply chains generally, and Huawei's in particular, may be impacted by ongoing negotiations over cyber-security and trade.

Executive Summary

Chapter One: Cyber-security and the evolution of global ICT supply chains

From national champions to globalisation

In the second half of the 20th century, governments in developed and emerging economies increasingly recognised the national-security and economic value of encouraging the development of an advanced domestic ICT sector. The US led the way, providing supportive measures for research and development (R&D). Meanwhile, Japan adopted a more clearly defined, government-led approach, with policies identifying specific technologies for support and protection from foreign competition. The Japanese model of close co-operation in R&D and commercialisation between the state, national telecommunication carriers and large domestic companies was emulated, with some variations, by other countries, including South Korea and, later, China.

China's large population has been at once a blessing and a curse for its ICT sector: since China joined the WTO in 2003, foreign manufacturers have been attracted en masse by the low-cost operating environment, as well as the prospect of being close to the world's largest emerging consumer market. Yet, the low cost of labour has also meant that there has been little incentive to move up the value chain, and this has been compounded by a perception of China as a poor cyber-security environment, with the result that China has yet to develop a significant capacity in semiconductor and micro-processor manufacturing. Nonetheless, China has come to play a crucial role in the supply chains of all leading ICT manufacturers.

The cold war ended around the same time that the US was realising that high-speed micro-processors, once jealously guarded for their role in weapons development, had been commoditised to such an extent that there was no point in continuing with the majority of export controls. Furthermore, in the first years of the new millennium, policies to ensure the cyber-security of core networks tended to focus on domestic ownership and operation of networks, rather than provenance of hardware. These factors enabled the acceleration of ICT-sector globalisation in the 1990s and 2000s, while shrinking margins in the sector fuelled the same trend. It was only with the US House Report of late 2012 (and, later, the Snowden revelations) that hardware security came back into the spotlight.

Hardware security in fragmented global supply chains

The piece of hardware most vulnerable to cyber-malfeasance is the micro-processor or "chip". In this sense, the top chip manufacturing locations (the US, South Korea and Taiwan) are the most sensitive links in global supply chains. China's ICT sector, by contrast, predominantly comprises lower-value parts of the chain. Yet, vulnerabilities can be introduced elsewhere, for example during the manufacture of chip sub-components. At present, chip manufacturers are neither keen to be transparent about where each part of their production process sits, nor, with slim margins, can they afford to "re-shore" the entire process to their home countries. Localisation of all hardware production

© The Economist Intelligence Unit Limited 2014

is, therefore, highly unlikely. This leads to the conclusion that more research is needed into defences against hardware-based risk, while the sector continues to employ supply-chain diversification and other security measures.

The future of ICT supply chains

The value distribution along ICT supply chains is changing. In the future, even less value will come from hardware, which will be further commoditised with the advent of software-defined networks, and more value will come from software and services. Competition to lead in emerging technologies, such as cloud computing, is fierce; and, at the same time, these advances bring with them new complications in terms of trade rules and national-security considerations. In particular, the information supplied by Mr Snowden about the NSA's access to foreign data hosted by US service providers has given momentum to "sovereign-cloud" initiatives. Trust will be a major issue going forward, and will need to be addressed by cloud service providers and governments.

Similarly, in a software-defined future, in which networks are controlled and altered remotely, including across international boundaries, new norms and international agreements will be needed in order to build trust.

Conclusions

While ICT-sector globalisation has been rapid in the last 20 years, it would be much more difficult, and economically unsound, to unpick the diverse production networks that have emerged. Understanding this, although the US government has restricted procurement of network gear from China, it has made no wider attempt to force US hardware manufacturers to cut China out of its supply chains. Policy transmission of the anti-Chinese-company measures have been limited and that is likely to continue, given the US's recent loss of the moral high ground with regard to cyber-security.

On the other hand, Mr Snowden's revelations have diminished trust in the ICT sector at a time when the trend is towards remotely administered services and networks, introducing new security concerns. Going forward, trust will be a key asset for any company that hopes to be a leading provider of equipment or software-management services for ICT infrastructure.

Chapter Two: The politics of cyber-security

Categorising cyber-threats

Cyber-security has risen rapidly up policy agendas around the world in the past few years. Among economically motivated cyber-attacks, cyber-crime is the main concern. Geopolitically motivated attacks range from an overlap with the economically motivated, in the case of intellectual-property (IP) theft by governments, to online espionage and cyber-warfare.

Generally speaking, the more developed a country is, the more likely it is to be a target of cyber-attacks. This is in large part due to the correlation between economic development and cyber-dependency. The more dependent a country's population is on the Internet, the more opportunities there are for cyber-fraud; likewise, the more a state relies on the Internet for the operation of

© The Economist Intelligence Unit Limited 2014

government and core physical infrastructure, the more political targets can be found. Among cyber-dependent countries, a cyber-arms race easily develops.

As cyber-dependency is an accelerating global trend, cyber-attacks are becoming more frequent. Criminals often target emerging economies, in which cyber-security awareness is low. Meanwhile, the security agencies of more advanced economies have apparently become giddy with the monitoring opportunities offered in an online world where policy struggles to keep pace with technology, and in which international agreements on physical cross-border incursions are not applied.

Politically motivated cyber-threats

Mr Snowden's revelations pertaining to collaboration between the public and private sectors in intelligence gathering has led to a widespread loss of trust. In the absence of international agreements regulating data and communications security, politicians may take unilateral measures to protect their constituents' interests, as Huawei and ZTE discovered in the US. Alternatively, consumers may make their own choices to avoid untrusted companies, as a US firm, Cisco, recently experienced in China.

To mitigate any fall in revenue in the wake of the Snowden leaks, a number of leading US ICT companies are pushing for government reform, in order to exonerate themselves. Some firms have begun taking their own measures to restore trust, for instance by publishing the number of government requests they receive in order to increase transparency. This may help, but solid regulatory responses would do more to restore trust at home and abroad. However, commercial arguments are unlikely completely to overtake national-security concerns, particularly in the absence of international agreements.

International agreements (or the lack thereof)

Nearly all current cross-national agreements focus on the economic category of cyber-threats. Given that a weakness in one country can enable attacks against another, many international initiatives aim to build developing countries' cyber-security capacity.

International agreements are, however, harder to achieve when political motives are a factor. Decisions on cyber-espionage and warfare remain firmly under the auspices of individual nation states. This situation is unlikely to change in the near term and any cross-national agreements will be regional or otherwise limited in scope. The most organised and motivated region at present appears to be Europe. The Council of Europe's Convention on Cybercrime (or the "Budapest Convention"), as the title suggests, deals with crime, rather than national security, yet it appears to have codified norms of extra-territorial data seizure, which have been applied for political purposes by national-security organisations. Such norms have left private Internet service providers in a predicament, subject to conflicting national laws. The Budapest Convention's committee is now looking at renegotiating its terms on cross-border data flows for a binding international treaty.

Any such international agreements will be slow in coming, particularly with countries such as the US and UK reluctant to give up their extensive powers of interception. Until clear rules emerge among a significant number of countries on key issues, such as extra-territorial data requests, private-sector

© The Economist Intelligence Unit Limited 2014

Internet service providers remain in a difficult legal situation and can only resort to introducing their own confidence-building measures.

Overview of policies and politics across regions

Generally speaking, the more economically developed and cyber-dependent a country, the more elaborate cyber-policies it has. Some regional trends in policy approaches are discussed below.

Europe has primarily been concerned with privacy of personal data and data protection, especially after Mr Snowden revealed that the NSA monitored the phones of some European politicians, and that data stored by US companies for European customers had been subject to US interception activities. In response to the loss of political trust in the US, new rules on cross-border data flows are being considered under the Budapest Convention, as well as under the European Commission, which will affect all international companies doing business in Europe. Non-EU companies hoping to provide cloud-computing services will face particular problems. Microsoft has already taken the unilateral measure of allowing customers to choose in which jurisdiction their cloud data are stored.

The risk of protectionism is higher here than in less-developed ICT markets, as the EU has the technical resources to develop its own sovereign cloud. Motivated not only by security concerns, but also by a desire to boost the economy, the region is likely to focus on EU-wide standards and interoperability going forward. Huawei should anticipate some challenges ahead, and ensure it can demonstrate support for local R&D, as well as compliance with EU data-privacy standards.

Cyber-security has featured prominently in **US** politics for decades and is centrally co-ordinated. Homeland security has been a key factor in motivating the expansion of its global intelligence gathering, for instance in the USA PATRIOT Act of 2001. As a result of Mr Snowden's revelations, US Internet service providers and equipment vendors have seen their international reputations and businesses suffer.

There is likely to be some give and take between the interests of industry—which is pushing for more transparency—and government, resulting in some watered-down policies to restore the reputation of US technology firms through limited restrictions on governments' interception powers. This will likely only increase the impetus of US officials to restrict foreign access to domestic networks, as they feel their national-security capacity has been reduced. Huawei should continue to focus on consumer products, rather than network infrastructure in the US.

In **developed Asia**, Snowden's revelations have shown the depth of the security relationship between the US and certain developed Asian countries, such as Australia and Japan. US pressure for its allies in the region to restrict Chinese companies' access to core ICT infrastructure is likely to continue, although South Korea's refusal to do so shows that not everyone shares the US's view on this. A common factor among developed Asian countries is concern about the cyber-security threat posed by China to both IP and national security, and, with a volatile geopolitical situation in East Asia, policies towards Chinese ICT companies are likely to fluctuate. For Huawei, proactive trust-building efforts will be key.

© The Economist Intelligence Unit Limited 2014

Among **emerging markets**, depending on their political alliances, either the Snowden revelations or geopolitical friction with China will add impetus to national efforts to improve cyber-security. In general, efforts focus on securing ICT infrastructure as economies become more cyber-dependent, although Russia and China are also likely to continue to work towards developing domestic software and Internet services to reduce the reliance on foreign providers.

Huawei would benefit from targeting emerging markets that have good relations with China. Huawei should continue to focus on its overall image abroad, building on recent moves towards greater transparency and support for international cyber-security initiatives. One particular area of interest might be the current lack of IP protection in software, in which Huawei could emerge as a leader by establishing international co-operation.

Conclusions

Given the global increase in cyber-dependency, combined with a lack of comprehensive international agreements on cyber-security to build trust and establish norms, it is likely that cyber-threats will continue to affect international politics, the global economy and individual businesses.

The Snowden case has hurt long-term US interests, particularly in countries that have the ability to develop domestic ICT products and services. Many governments see advantages to promoting domestic capacity in emerging technologies, such as cloud computing. The example of cloud computing not only brings with it complex issues, such as extra-territorial data-seizure powers, but can also simplify the process of localisation, making regionally focused policies both more appealing and easier to implement. The US already has its own cloud, Europe is building one and other countries are certainly considering it. This is likely to impact Huawei’s global cloud-computing business more in the future, if trust in international service providers cannot be restored.

Chapter Three: Trade and the ICT sector

Global ICT trade and trust

Over the past 15 years, cross-border trade in ICT has increased faster even than global trade as a whole. Underpinning this has been the reduction in global-trade barriers that resulted from two multilateral trade agreements: the Uruguay Round of 1995 and the Information Technology Agreement (ITA) of 1997, under the WTO.

Multilateral trade deals are no longer possible on the scale they once were, and the WTO now preserves the status quo, rather than achieving greater liberalisation. An updated ITA is an important exception, but its completion is far from assured. Meanwhile, countries have opted to pursue trade liberalisation through other means, namely in the form of bilateral and regional free-trade agreements (FTAs). Efforts are now underway to complete a series of “mega-regionals”, such as the US-led Trans-Pacific Partnership (TPP), the US-EU Trans-Atlantic Trade and Investment Partnership (TTIP), and the China-led Regional Comprehensive Economic Partnership (RCEP). These could incentivise or even compel ICT firms to restructure their supply chains.

© The Economist Intelligence Unit Limited 2014

The overriding problem confronting global ICT trade sits at the intersection of cyber-security, geopolitics and trust. Cyber-security is seeing unprecedented prominence and trust is at a low. As a result, there are now seeing increasing attempts by governments to restrict cross-border data flows, to create national clouds, and to inhibit e-commerce. If trust is eroded, then trade can be diminished along with it. This is especially true in sensitive sectors, such as ICT.

The WTO and cyber-security

When it comes to cyber-security and global ICT supply chains, the WTO has a particularly thorny rule to guard: the National Security Exception (NSE) contained in General Agreement on Tariffs and Trade (GATT) Article 21. This gives states the right to take any actions they deem necessary in the interest of national security. The rule is seen by some as a "ticking time-bomb", as it relies on good faith. Chances are slim that there will ever be a serious challenge to the NSE, as any challenge that makes it to adjudication will likely result in the defendant simply ignoring an unfavourable ruling. That would thoroughly undermine the WTO as a rules-based institution.

Information Technology Agreement: Past, Present and Future?

Most momentum for the first ITA came from the private sector. With such slim margins in the sector, even slight tariff reductions had a big impact and prompted rapid globalisation. However, despite serving a rapidly evolving sector, the scope of products covered has not been updated since 1997, making the ITA less and less relevant. Negotiations are underway for an ITA 2, which neared completion in late 2013, before being delayed after China requested a new list of exclusions. This was reported to include a number of low-value Chinese export products, for which China is keen to limit competition. Most people still expect that China will compromise, because China has gained the most from the current ITA and stands to lose the most if a new ITA does not go forward. As it is not party to the TPP or TTIP, if the ITA did fail, new and improved market access for Chinese firms would be limited to countries in the RCEP mega-regional.

The mega-regionals: TPP, TTIP and RCEP

As the ITA takes precedence over any other FTAs (as will an ITA 2, if concluded), when it comes to the ICT sector, other agreements therefore concentrate on issues that are not well covered by the ITA or WTO, such as cross-border data flows, data localisation and e-commerce. In the absence of an ITA 2, the way these are handled in the mega-regionals is likely to be influential. So far, little is known about the TTIP's and RCEP's approaches to the issues, but a forward-looking analysis can be attempted on what is known or assumed about the TPP's stance.

On e-commerce, the US is pushing for as much liberalisation as possible and, above all, for goods and services delivered electronically to be given the same treatment as those that are delivered physically—including being subject to the agreement's dispute-settlement provisions, a stipulation that faces considerable opposition. We believe that most countries will be brought around to the US stance on this through compromise in other areas, and/or coercion.

When it comes to cross-border data flows, the US is hoping for more stringent guarantees of

© The Economist Intelligence Unit Limited 2014

openness than were included in its bilateral agreement with South Korea, KORUS. Some countries are pushing back against US efforts in this area, voicing concerns about how this would affect domestic privacy and national-cyber-security concerns, and the US has lost the moral authority to negotiate hard on this point.

Finally, there is a chance that the mega-regionals, and particularly the TPP, may introduce new rules of origin (ROO), which will affect ICT supply chains in future.

Conclusions

To the extent that any of the above-mentioned agreements will affect ICT supply chains, there is still time—probably years, in most cases—before they come into effect. Therefore, Huawei can prepare for various possible outcomes.

The best-case scenario for Huawei is that an ITA 2 is successfully concluded, given that the ITA has benefited China more than any other country, and that many countries prefer to deal with China in the context of the WTO. The worst-case scenario is that there is no new ITA, and, meanwhile, all three mega-regionals are completed. The TPP would be the most aggressive of these, and would spread rules and standards unfavourable to Chinese companies, limiting their new market access. The middle-case scenario, and also the most likely outcome, is that all three mega-regionals and an ITA 2 are concluded. For Huawei, on the plus side, the ITA 2 would provide it with improved access to nearly all of the world's key ICT markets.

Conclusions and implications for Huawei

Huawei will need to follow closely the responses of key nations, international groupings and even individual firms to the current deep concern over cyber-security and data privacy, and formulate its own responses in anticipation of future norms and laws. It will also need to be sure of how its domestic legal obligations as a Chinese company affect its ability to comply with more stringent requirements in future. Whether Huawei proceeds with unilateral measures or through a new cyber-security forum, it should keep in mind that trust is the key to successful trade, especially in sensitive industries. With geopolitical headwinds in East Asia, strong anti-China lobbies in the US and deep-rooted concerns over privacy and security in the EU, Huawei does not face an easy road ahead. Its current proactive efforts to become not just a trusted partner, but an industry leader in cyber-security, are the right approach, but will be more effective if it can pursue this agenda in a co-operative international forum.

© The Economist Intelligence Unit Limited 2014

Chapter One: Cyber-security and global ICT supply chains

Overview

The purpose of this chapter is, firstly, to trace how and why global information and communications technology (ICT) supply chains, specifically for the manufacture and operation of network infrastructure, have evolved to their present structure—considering political, economic, technological and cyber-security-related trends shaping the sector. Secondly, the report will discuss how and why these supply chains are likely to change in the future. Finally, the implications for Huawei are examined.

Evolution of supply chains: From national champions to globalisation

Introduction

In the second half of the 20th century, the world's most dynamic economies—notably the US, Japan, South Korea, Taiwan and much of the EU—advanced policy agendas to establish competitive ICT sectors. Early policies focused on promoting, protecting and sustaining a sophisticated domestic manufacturing industry for telecommunications-network gear and components. Many other countries, including China, as well as emerging economies in South and South-East Asia, Eastern Europe and Latin America, have attempted to emulate these strategies. The key motivations of such policies are as follows:

1. Military application of ICTs: particularly until the 1990s, a country's level of computing technology was seen as closely connected to its weapons-development capacity.
2. National-communications security: the desire to protect domestic communications from foreign interception or disruption—the latter becoming more relevant with the increasing dependence of vital infrastructure on ICT, and the growing sophistication of cyber-attacks.
3. Economic growth: over time, the spill-over effects of a strong ICT sector on other parts of the economy have become increasingly evident.

To elaborate on the third point, if a country has an advanced ICT sector, this can bring multiple economic advantages. Within the ICT sector, innovation can lead to the creation of patents and royalty rights, which generate scalable income and allow for "swaps" with other providers of technology. Beyond the ICT sector, it enables other sectors, at a minimum, to run more efficiently, and, in the best-case scenario, to move up the value chain and enhance competitiveness—with the added benefit of creating more skilled jobs. Later in this chapter, this study will examine why, especially since the 1990s, this economic consideration has grown in importance as a factor influencing government ICT policies and also supply chains. Firstly, it will examine how some key markets built up their ICT sectors. This sets the scene for understanding how global ICT supply chains evolved.

The technology of champions: Case studies of ICT-sector development

The earliest examples of government-driven ICT-sector development were either direct—where government bodies invested in and directed the development of national ICT manufacturing and services—or indirect, where government agencies supported ICT-sector development indirectly, through research and development (R&D) spending, often via national science and defence agencies or universities. In the most successful cases, such as those of the US, Japan, South Korea and Taiwan, government leadership has helped to define the ICT sector and has provided support for national champions. Yet, in other cases, such as those of India and Brazil, government protectionism has had a negative impact on the competitiveness of the local ICT sector.

The ICT development trajectory of the **US** is the most successful example of indirect government cultivation of the sector. Government, including defence-agency sponsorship of R&D initiatives, such as microwave-radio technology and micro-processing, served as the catalyst for the development of the industrial cluster that is Silicon Valley. Most R&D work was carried out at academic facilities and laboratories in and around the San Francisco Bay area, and similar clusters later developed in Southern California and around Boston, all building up expertise in computing technology. Government tolerance of a monopoly on national-telecoms services, under AT&T until the mid-1980s allowed Bell Labs, AT&T's R&D wing, the breathing room to develop such seminal innovations as data networking and cellular telephony.

There were also some instances of direct government involvement in R&D. ARPANET—the world's first packet-switched network, recognised as the cornerstone of the global Internet—was a US Department of Defense initiative. While US-style state-sponsored innovation lacked the central planning and focus on critical technology outputs of the Japanese model (discussed below), government investment and support undeniably kick-started the world's largest and most innovative ICT sector.

Until the 1990s, there was a particular focus in government policy on advancing and protecting the US's capabilities in terms of computer-processing speed: weapons development relied on what were considered at the time to be "super-computers". As well as supporting domestic R&D in this area, the government banned exports to non-allies of high-speed processors until the end of the 20th century.

Japan's Ministry of International Trade and Industry (MITI) is perhaps the archetype of a government agency successfully driving the ICT sector. Beginning in the 1950s, MITI organised government resources and regulatory frameworks to promote the creation of a domestic electronics industry, with telecoms equipment as a mainstay of that industry. The government provided protection from foreign competition in the form of measures such as tariffs, subsidised credit for domestic companies, R&D incentives and government-initiated R&D co-operative programmes.[1] The close collaboration between the state, national telecoms operators and domestic industrial conglomerates was a working model for rapid catch-up and development of self-sufficiency in telecoms manufacturing, which many emerging economies have tried to emulate. However, like the US (and

[1] M. Fransman. Japan's computer and communications industry: The evolution of industrial giants and global competitiveness (Oxford University Press), p.199, 1990.

unlike most of the emerging economies seeking to follow its approach), Japan already had a relatively advanced ICT-research scene, having begun research into key technologies such as fibre-optics, even before the second world war.[2] This helps to explain the apparent ease with which it kept up with, and, in some areas, surpassed, US technological achievements in key areas, including micro-processing; as well as the very varied degrees of success achieved by other countries, who often had a great deal more catching up to do, in adopting the same approach.

South Korea pursued an ICT-development model in many respects similar to that of Japan, focused on core network infrastructure, including public switches and integrated circuits. Having started to build its technical-skills base from the late 1960s, Korea began to encourage imports and assembly of key technologies through laws such as the Foreign Capital Inducement Act (1966) and Technology Development Act (1972). This allowed it to pursue imitative innovation, and, by the 1970s, domestic pioneers such as Korea Semiconductor (later acquired by Samsung) began to spring up.[3]

A critical difference between the Korean and Japanese national ICT-development projects was that Korea chose to encourage collaboration with foreign infrastructure vendors to produce local versions of their products. Korea's first comprehensive network infrastructure R&D initiative began in 1986, co-ordinated by the country's Electronics and Telecommunications Research Institute (ETRI), and saw licensing agreements and joint-ventures pairing local telecoms giants (such as Samsung and LG) with established vendors from North America, Japan or Europe. Each such pairing co-developed a version of a domestic switch known as the TDX,[4] which, within a decade, was both the dominant switching platform in the country's own telecoms network and was being exported globally, chiefly to emerging markets. Over time, the active participation of the foreign partners was reduced, as Korean firms strengthened their own R&D capabilities.

The TDX's success was followed by local production of other network elements to support the Korea Information Infrastructure initiative, the country's high-speed-data-network project, such as optical transmission and asynchronous transfer mode (ATM) switch equipment. Korea's localisation policy successfully laid the groundwork for a competitive position in the global production of telecoms infrastructure, and created a particular competency in semiconductors (of which South Korean firms, Samsung and SK Hynix, remain among the world's ten largest producers).

However, the country's approach to national ICT development has since broadened, and the focus is now on securing best-in-class solutions for the nation's Internet infrastructure (with a view to the knock-on benefits to other industries), regardless of provenance. Eschewing Internet protocol switches made by Cisco simply because they are not Korean, for instance, is incompatible with the country's wider ICT goals. While Korean technology policy is still supported by domestic champions, there is recognition that being plugged into global supply chains is the best way forward, and the government has effectively dismantled its protectionist policies as a result.

From 1984 on, **India** tried to develop its own native telecoms equipment from scratch, although with much less success than Japan. This was done through India's Centre for Development of Telematics (C-DOT), a government-owned R&D and production centre. Largely focused on rural telecoms infrastructure, C-DOT produced telephony exchanges, which state-owned network operators

[2] Ibid., p.209.

[3] K. Lee. 'How can Korea be a role model for catch-up development?' in United Nations University—World Institute for Development Economics Research (UNU-WIDER), Research Paper No. 2009/34, 2009. http://www.wider.unu.edu/stc/repec/pdfs/rp2009/RP2009-34.pdf.

[4] K. Lee, The political economy of networked mobility: The historical development of the Korean information infrastructure, 1995-2005. PhD dissertation presented to the University of Texas at Austin, August 2008).

© The Economist Intelligence Unit Limited 2014

were compelled to procure. While, today, half of India's fixed-line installed base is supplied by C-DOT, its fixed-line telephony projects have largely been abandoned, in part because the domestic products were not price or performance-competitive compared with global offers, and in part because technology has moved on. While C-DOT has some ongoing R&D efforts in wireless (including the supposed development of 4G capabilities) and next-generation "softswitches", it is no longer operating in a policy environment that guarantees it preferential treatment in the domestic market; India's carriers—now largely mobile-centric, privately owned and in fierce competition with one another—are no longer compelled to procure locally developed technology.

China has already attained leadership in some areas of technology, yet certain key elements—particularly semiconductors—still elude its researchers. What is clear is that, since the era of opening up and reform began, China's ICT sector has rapidly grown to the point where it has become essential to the success of ICT sectors in many other countries. This dependence has altered the global state of play in the sector, and a side-effect of this has been to reignite the concerns of some governments, particularly that of the US, about cyber-security and military application of ICTs.

The development of China's ICT sector has become a model for other emerging markets looking to enhance their ICT competitiveness through localisation, technology transfer and the development of native capabilities. Similar to the Japanese, Korean and Taiwanese models, China's ICT sector was built through tight co-ordination between government industrial promotion bodies, leading technology manufacturers, state-controlled R&D organisations and national telecoms carriers. A period of local innovation and product development was supported by a captive domestic market, where telecoms-service operators favoured domestic champions (or joint-ventures involving domestic manufacturers) when purchasing network infrastructure. The effective way in which China has marshalled its national resources to create a competitive ICT sector has certainly served as a reference point for other emerging markets looking to develop localisation policies, particularly India and Brazil.

China is, therefore, the latest heir to an East Asian ICT-policy tradition: intense support for a domestic manufacturing sector in order to foster a globally competitive ICT export sector. However, in stark contrast to its East Asian forebears, China has, to date, not been able to develop a globally competitive semiconductor and micro-processor segment. As semiconductor production is capital- and skills-intensive, rather than labour-intensive, fewer fabrication plants have been outsourced to lower-cost destinations by major producers.[5] There is also the consideration of intellectual-property protection, which leads chip manufacturers to fragment their supply chains to limit risk. China's competitive advantages in most of the network-infrastructure supply chain, therefore, have not been as relevant to the production of chips. In addition, it has simply been more cost-effective for Chinese manufacturers to purchase semiconductors, rather than to invest in local R&D and production.

China's rise on the technology landscape has been a key impetus for the growing global concern over security risk in network-infrastructure supply chains—although revelations in 2013 about the cyber-espionage activities of the US and its allies have brought this issue to even greater prominence and have balanced the discourse somewhat. Nonetheless, most global suppliers source components and processes either from their own China-based production facilities, or from second- or third-tier component manufacturers based in China.

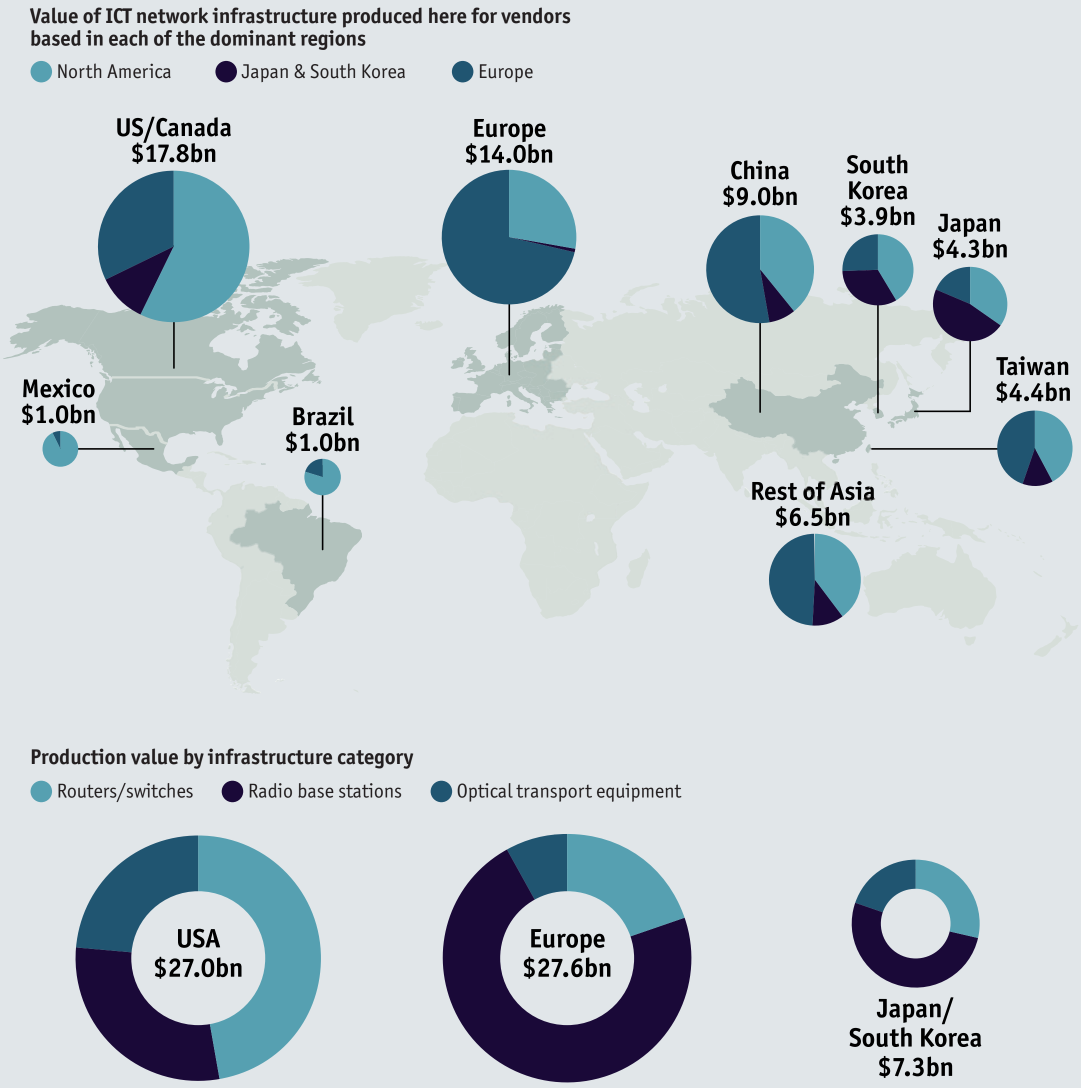
[5] Nonetheless, the escalating volume of semiconductor production, fuelled by their increasingly pervasive use, has meant that some of the more scale-intensive manufacturing processes—particularly testing and assembly—have compelled chip manufacturers to locate facilities in lower-cost markets. Intel's largest testing and assembly facility globally, for instance, is in Vietnam.

Global network infrastructure production ecosystem

The pie charts in Figure 1 shows where the world's largest clusters of network infrastructure vendors—North America, Europe, and Japan and South Korea—manufacture their infrastructure products. The doughnut charts below the map show the proportion of manufacturing by region for three product groups: routers and switches, radio base stations for cellular networks, and optical transport systems for transmission networks. Production levels in each group are represented by an estimate of their book value.[1]

Figure 1: Global ICT network infrastructure production - by value

(By component; 2012 estimates in US$ bn)

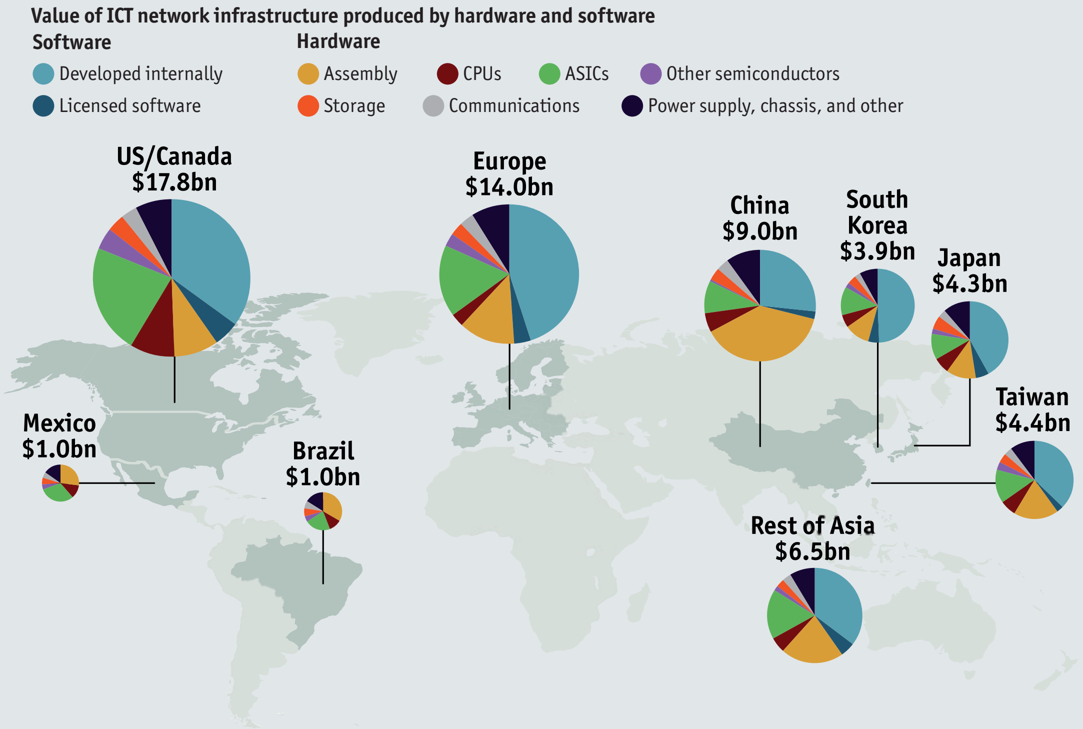


[1] The book value constitutes an estimate of the vendor's inventory of finished goods in the category before it is priced into the market, and disregards any margins made through third-party channels.

© The Economist Intelligence Unit Limited 2014

While not comprehensive, these three product categories not only comprise the majority of the value of the telecommunications infrastructure market, they collectively represent the three foundational processes of the world's telecoms networks today—signal switching, backhaul transport and mobile connectivity.

Figure 2: Global ICT network infrastructure production - by value
(By component; 2012 estimates in US$ bn)



In Figure 2, the product categories are broken down by their major components, which represent the vast majority of each product's value. These are broadly divided between the components for which intellectual property is key—mainly semiconductor chipsets (including CPUs, ASICs and other semiconductors) and software—and the more commoditised components, such as chassis assembly and wiring. Custom chips and other electronic components are assigned a larger proportion of R&D expenditure, while commodity component value is more derived from prevailing market prices. The value of custom chips and software has been increasing as a proportion of value in telecommunication infrastructure, a metamorphosis driven by the higher level of programmability required. This stems from the more complex network demands as the number of smart devices (notably smartphones and tablets) has increased over the last three years or so, with an associated increase in the capacity and network density of microprocessors. This isn't exactly a software-defined network, but a software-centric one.

Some of the trends revealed by the production ecosystem map are as follows:

- Production is globally dispersed: The three major clusters of ICT vendors produce over $60bn worth of network equipment annually, but less than two-thirds of this within the borders of their own countries.

© The Economist Intelligence Unit Limited 2014

- Although North American vendors produce the lion’s share of key components, especially switches, only about two-thirds of this value is produced in the region.
- North American and European vendors produce more infrastructure in China than any other single market besides their own and each other’s. 13% of North American vendors’ production value is sourced from China (the case is 24% for European vendors).
- The bulk of China’s ICT production for foreign vendors is in less valuable, less IPR-intensive, and thus, arguably, less ‘cyber-sensitive’ areas.
- The preceding two points demonstrate the very heavy reliance of North American and European vendors on China to keep costs down and margins acceptable.
- The locations most heavily represented in the manufacture of semiconductors and ASICs—arguably the most ‘cyber-sensitive’ products—are Taiwan and North America: this creates a quarter of Taiwanese production value; the percentage is over 30% in North America, but less than half that in China.

Liberalisation and supply-chain fragmentation

Deregulation and globalisation

Towards the end of the 20th century, some profound shifts took place, which combined to precipitate ICT-industry deregulation and the global spread of ICT supply chains. In addition to the changing geopolitical and economic landscape, technological developments affected governments’ security considerations and industry players’ economic considerations.

As discussed above, in the first decades of the development of a world-leading computing industry in the US, the key capability that the government wished to protect was processing speed, in the form of increasingly powerful microprocessor chips. By the end of the 20th century, processing speed had become largely irrelevant to weapons development, due to the commoditisation and global spread of high-speed computers. Experience and knowledge of how to apply technology had become the key competitive advantage (in both military and commercial contexts).[6] From around 2000, the US progressively relaxed its export controls on high-speed computers, and the Wassenaar Arrangement raised the speed limit to an updated definition of military-grade computers in 2005. This paved the way for a security climate in which it was more acceptable to outsource micro-processor assembly or the production of components. As for remaining security measures, restrictions on foreign involvement in the US and elsewhere now tend to be limited to who can own and operate key ICT infrastructure—not whose technology they can procure for its development, or where that technology is produced.[7]

Meanwhile, globalisation of industry took off at a rapid pace following the end of the cold war. More developing economies opened their doors to international trade, notably China. Security considerations took a back seat as the world raced to take advantage of the new trading opportunities presented. The WTO, its membership growing fast, worked to reduce trade barriers and introduce more international industry standards. As part of this trend, the Information Technology Agreement

[6] J. Lewis, “Computer exports and national security in a global era,” Centre for Strategic and International Studies, 2001. See csis.org/files/media/csis/pubs/010601_computerexports.pdf.

[7] See, for instance, the OECD summary of individual country restrictions, at http://www.oecd.org/sti/broadband/2-5.pdf, accessed December 15th 2013.

© The Economist Intelligence Unit Limited 2014

(ITA) of 1996—discussed further in Chapter Three—was a particularly important development for the ICT sector. The Asian financial crisis of 1997-98 and subsequent conditions of the distribution of recovery aid from international financial institutions accelerated deregulation in East Asia. Shortly thereafter, the "dotcom bubble" burst at the turn of the century, providing an economic imperative for ICT companies to consolidate and reduce costs in order to compete and survive. By the early 2000s, ICT companies were highly motivated to shift production to low-cost locations, while the relaxed security environment and trend of economic liberalisation—as well as specific rules emerging under the WTO—provided the necessary conditions to expand geographically.

With the rapid economic development of emerging markets in Asia, Latin America and Eastern Europe, proximity to markets beyond the US and EU also took on more importance in deciding manufacturing and assembly locations. China, seen as the most exciting growth market for many industries, naturally found it easier to attract investment than many other markets of a comparable level of development.

Nowadays, fostering a domestic ICT sector through protection of local-content manufacturing regimes is largely a thing of the past. Most emerging economies have few explicit requirements around local production, although echoes of localisation programmes exist today, particularly in Brazil. In opposition to trends elsewhere in the world, the Brazilian government is stepping up local-content requirements: last year, spectrum auctions for the country's 4G mobile-data-service licences stipulated local network infrastructure content requirements of 60%, rising to 70% in 2017. This caused trade bodies from the US and Europe to launch (unsuccessful) trade-agreement-infringement complaints against Brazil.[8]

This type of economically driven protectionism is now relatively rare, with most governments prioritising the provision to their populations of cheap, good-quality ICT services over the protection of domestic industry. However, in light of the US's recent accusations against Chinese ICT companies, as well as the revelations by Edward Snowden, the former National Security Agency (NSA) and Central Intelligence Agency (CIA) contractor who has leaked information regarding vast US technology-surveillance programmes, the question remains of whether security concerns (perhaps in addition to, or acting as cover for, economic concerns) will lead to a revival of government-protectionist measures.

Law of diminishing returns

The economic necessity to globalise ICT supply chains has been driven not just by increased competition, but also by rapid changes in the technology itself and the associated changes in service-provision models.

ICT market participants and pundits are given to boiling down the dynamics of their sector into pseudo-scientific maxims. Moore's Law, for instance, is named after the co-founder of Intel, Gordon Moore, who observed in 1965 that the capacity of an integrated circuit (IC) roughly doubles every two years, in direct proportion to a halving in its production costs. Moore's Law has remained roughly true ever since, meaning that the last half-century has seen the rapid commoditisation of these core components of ICT-network infrastructure—even as their processing power has expanded exponentially.

[8] For more details, see http://www.linhadefensiva.com/2012/05/brazil-questioned-by-us-over-national-tech-requirements-for-4g/

Another observation relates to the development of telecoms networks themselves. Metcalfe's Law, based on a concept first noted by Robert Metcalfe, co-inventor of Ethernet computer-networking technology, and updated by George Gilder in 1993, states that the value of a communications network is proportional to the square of the number of connected users of the system. Metcalfe's Law has had negative implications for telecoms operators, however, in that the exponential value created by these expanding networks has disproportionally accrued to their end users, rather than to their owners and operators. This is in large part because deregulation of fixed, mobile and data-communications service markets, which began in mature economies in the 1980s and rippled through the world's communications markets in the decades after, has made the provision of network services extremely competitive.

To compete successfully for customers, carriers have used two weapons: lowering service prices, and increasing bandwidth access. The second weapon continues to be deployed for competitive advantage; with every passing technology generation, as Moore's Law observes, processing power and data-transmission speeds increase inexorably, while the costs of the associated technology are drastically reduced. The benefits of this dynamic were recently felt by US carrier, Verizon Communications, which saw profitability in the third quarter of 2013 improve by 40%, in large part due to its aggressive roll-out of a 4G mobile service. By contrast, the negative impact of the principles of Metcalfe's Law has seen the benefits accruing to carriers from service provision squeezed lower and lower.

This conundrum has had a significant knock-on effect on the network-technology-purchasing strategies of telecoms and data-service operators: in short, it has resulted in a massive scaling back of global capital expenditure. This has been achieved by developing leaner manufacturing models and by outsourcing.

A secondary impact has been that network operators—particularly those that have successfully leveraged next-generation technology—still have to invest significantly in network infrastructure to keep pace with end-user demand. Moreover, these increases in bandwidth and speed require increasingly disproportionate investment in base-station coverage; sector analysts estimate that, in some markets, the transition from 3G to 4G services can require up to a 25-fold increase in mobile base stations in densely populated areas.[9] This secondary effect not only places additional pressure on infrastructure vendors and their supply chains, but also creates the need for a different approach to managing these networks.

Value shift: From equipment to services

Network operators and other procurers of telecoms equipment tend to see security-risk management as a standard, self-imposed procedure that is part of the procurement process (and hope to keep it that way), but do not see the provenance (country of origin) as the primary security threat.[10] One explanation for this is the highly fragmented nature of many supply chains. From a commercial perspective, fragmentation of supply chains across multiple locations helps to reduce risk (primarily the risk of IP theft, and, to a lesser extent, the risk of government or criminal tampering with key components).

[9] Arguably an unfair comparison, as 4G mobile carriers have to install many more smaller base stations to ensure service quality at these higher speeds. Yet, while a 25-fold increase in cell sites will not result in a 25-fold increase in capital expenditure, it does create an escalation of costs, and of network-management resources required.

[10] This is a much-simplified summary of findings from the US Government Accountability Office's testimony before the Subcommittee on Communications and Technology: "Telecommunications Networks: Addressing Potential Security Risks of Foreign Manufactured Equipment", released May 2013 and available here: http://www.gao.gov/assets/660/654763.pdf.

However, another explanation could be that companies do not want to acknowledge the risks of overseas procurement or manufacturing, as they simply rely too heavily on this business model. While not a unique phenomenon in manufacturing, producers of ICT-network infrastructure have come to rely heavily on outsourcing to component manufacturers, software and hardware developers and, increasingly, full-service contract manufacturers.

Most major "national-champion" integrated vendors have, over the last 25 years or so, compartmentalised their production processes into the manufacture of commodity components (like printed circuit boards—PCBs—housing and cabling) and the more processing-intensive—and therefore higher-value-added—software and hardware elements. Commodity components have increasingly been outsourced to second- and third-tier manufacturers, while value-added elements have generally stayed in-house.

The need to increase efficiency and scale has been compounded by the fact that most of the value in ICT supply chains is now derived from services, rather than production of physical components. Telecoms-sector dynamics since the mid-1980s have steadily trended away from nationally owned and/or monopolistic provision of voice and data services, to extremely deregulated and competitive markets, in which multiple service providers compete on the basis of comprehensive—and inexpensive—voice and data services.

This has had an impact on how the value of network equipment has been delivered: rather than simply building network infrastructure and installing it for carriers, vendors have had to adjust their business models to offer the physical infrastructure as cheaply as possible, while their added value now comes from providing engineering and management services to carrier clients. In many countries, major telecoms-network service providers themselves receive managed network services from their infrastructure vendors; sector analysts estimate that perhaps as much as half of what carriers spend globally on "infrastructure" is actually spent on network-management services—running, upgrading and optimising networks on their behalf—and not physical installations.

Moreover, many telecoms carriers themselves have shifted to a non-proprietary network-infrastructure model. Networks are often leased from other providers (sometimes the vendors themselves; Indian mobile operators pioneered this approach), and, increasingly, networks are built co-operatively by otherwise competitive carriers and the capacity is shared by all.[11] This also serves to manage the cyber-security risk, as a potential threat would need to navigate multiple layers of different companies' technologies within a network.

With most value to be gained from services, rather than network equipment, there has been more and more pressure to squeeze costs further down the supply chain. It is neither in the interests of the procurers of network equipment, nor of policymakers in charge of national economies, which now depend on affordable ICT services, to argue for re-shoring of production unless low costs can be maintained. It is unsurprising, then, that, until high-profile political spats over cyber-espionage broke out in 2012-13, the issue of network-gear provenance had been largely pushed to one side.

The result of these growing economic pressures, along with the above-mentioned relaxation in

[11] A significant recent example was seen in March 2013, when Brazil's four major carriers announced a management agreement to share cell sites and backhaul traffic transport infrastructure across all their 4G LTE mobile-network operations nationwide.

© The Economist Intelligence Unit Limited 2014

the security environment and of controls over processing capabilities, was that the fragmentation of global ICT supply chains came to extend even to the most geographically stable of components—semiconductors.

Let the chips fall where they may

Network-security professionals point to one component—the micro-processor—as being any physical network's root vulnerability to cyber-malfeasance. Micro-processors are deployed within all pieces of network infrastructure, and are the "brain" of any telecoms switching, storage, routing and transmitting process. Any gathering and transmitting of information, legitimate or otherwise, within a telecoms network must be done at the level of the chip.

This implies that, if geography were to be used as a factor in assessing cyber-vulnerability, the provenance of micro-processors would be an essential part of that investigation. This assumption both simplifies the discussion and complicates it. It simplifies it, in that the number of market participants is small; while their market share in different applications varies, more than 90% of the world's micro-processor market in 2012 was controlled by just five companies: three from the US (Intel, Qualcomm, Freescale and AMD), and one Korean (Samsung). The argument is more complicated, in that these companies, like those higher up the network-equipment supply chain, are also under margin pressure—compelling them to outsource production. Electronic-chip-development processes are now distributed among many countries. Intel's largest global facility for testing and assembly processes, for instance, is in Ho Chi Minh City, Vietnam. While many chips are produced in China, most of the world's top chip manufacturers currently do not have their final-testing and quality-control processes physically within China, in part due to commercial and political-security concerns.

While the global leaders in chip production still tend to retain ultimate control over chip design and manufacturing at home, they have come to outsource more and more parts of the production process. This includes production of the PCBs on which the chips are mounted; manufacturing of the chips according to a given design; and even the design of some modules. Not only are many steps in the production process outsourced, but the process is fragmented across multiple companies and locations. From a commercial perspective, this is seen as improving security: no single company in the chain has too much sight of the process, making it harder to replicate. The mother companies are highly protective about the details of their supply chains. This implies that the onus falls on the final vendor to ensure security, through a rigorous checking process throughout their supply chains and especially at the final point of production, assembly or testing.

Hardware security in fragmented global supply chains

From a national-security perspective, those governments that wish to limit the use of foreign technology in their critical ICT infrastructure (and military equipment) have tended to design legislation to prevent the procurement of foreign technology for sensitive applications, or to prevent foreign ownership of infrastructure owners/operators. Less attention has been paid to the routing of supply chains of their domestic ICT manufacturers.

Cyber-security efforts, until recently, focused largely on software-based vulnerabilities and attacks. However, as awareness of hardware-based cyber-attacks has grown, new concerns about chips have

© The Economist Intelligence Unit Limited 2014

arisen; if fitted with malicious hardware, and then used in strategic contexts, such as in military equipment, communications or other critical infrastructure, they can pose a severe threat, which is much harder to detect than a software threat. More attention was brought to this vulnerability when researchers at Cambridge University in 2012 discovered and broke into a "backdoor" in "an American military chip that is highly secure, with sophisticated encryption standard, manufactured in China".[12] This was an Actel chip, widely used in US military applications. The researchers noted that 99% of all chips are manufactured in China, and there was no sure way of ascertaining whether the vulnerability was part of the original design or introduced during fabrication—although they later found evidence to suggest it was a part of the original design. The fact remains that experts believe chips could be deliberately altered at various points in the fabrication process.

A 2011 Brookings Institution report noted that, with the advent of fragmented global supply chains, there were now "multiple potential vectors for the insertion of malicious hardware" throughout the supply chain,[13] a view supported by the Computing Community Consortium (CCC) and the Semiconductor Research Corporation (SRC), both US-based ICT-sector organisations.[14] Academics tend to concur that it would be easiest for a hard-to-detect vulnerability to be inserted by those in charge of hardware design, but this is not limited to the overall chip design; it also extends to the design of modules, which is often outsourced. Moreover, tampering at other points in the production process would also be possible. Research into detection of and defence against hardware-based threats is currently lagging that into software-based threats, which adds to government concerns about using hardware produced, or partially produced, overseas.

The future of ICT supply chains: PRISM, the cloud- and software-defined networks

The post-PRISM world

Cyber-security has moved to centre stage in public debate over the last two years, firstly owing to the accusations by the US against Huawei and ZTE, and then Mr Snowden's revelations of the cyber-espionage activities of the US and its allies, including the now notorious PRISM data-gathering programme. This comes at a time when public views on Internet privacy are rapidly evolving and government policies are struggling to keep up. Many individuals are fed up of their personal data being collected and used without consent, whether for sale to advertising companies or for purposes of national security.

In light of the concerns Mr Snowden has raised over data privacy and network security, one might expect a knee-jerk reaction of protectionism and localisation. Some countries are indeed considering more localised ICT initiatives, an initiative discussed in Chapter Two. Europe's response has focused on privacy issues, for example considering how to arrange the ownership and location of data centres in such a way as to make it illegal (under US law) for the US to mine their data. So far, the calls of some in the US to avoid procuring network gear from Chinese manufacturers has not been made into law, even in the US, and the policy impact of this elsewhere has so far been limited to those who are party to intelligence-sharing agreements with the US, such as Australia, or who host US military bases (and

[12] See http://www.cl.cam.ac.uk/~sps32/sec_news.html.

[13] See http://www.brookings.edu/research/papers/2011/05/hardware-cybersecurity.

[14] See http://www.src.org/calendar/e004965/sa-ts-workshop-report-final.pdf.

© The Economist Intelligence Unit Limited 2014

hence secure communications networks), such as South Korea—which has been under pressure from the US to avoid procuring from Huawei, albeit to no effect. Even the US's close security ally, the UK, has not tried to prevent its private sector from procuring Huawei network equipment.

Notably, there is no legislation on the horizon that would limit the countries to which manufacturers of key hardware can outsource their production processes. It is worth discussing why this is the case. As detailed above, the world has changed since the cold war. Network owners and operators are unwilling to take the economic risk of withdrawing their well-established supply chains from convenient low-cost locations, and so are unsupportive of any moves to re-shore production.[15] Meanwhile, governments understand the need to support their domestic ICT industries, and are not keen to introduce harmful legislation pushing up the cost of Internet services. In any case, there is recognition that, in a globalised society with constant cross-border flows of people and data, keeping production at home does not necessarily eliminate risk.

As a result, there is a strong argument for government and private-sector efforts to focus instead on supporting research and introducing processes better to detect and defend against both software- and hardware-based vulnerabilities and attacks—and this is already happening. At present, it seems unlikely that there will be a significant trend of re-routing hardware supply chains out of countries perceived as presenting a security risk.

There is, of course, one inevitable location in most of the world's ICT supply chains, and that is China. One US-based technology company CEO expresses it simply: "I think we are all fully aware of the industry's collective over-reliance on China's productive capacity"—but he/she also notes that most technology companies are bound to continue to route production through the country's ICT clusters, as "There is no practical, or compelling, way to engineer processes around China."

The cloud

Cloud computing has developed rapidly in recent years, becoming an important feature of ICT supply chains. It involves the remote provision of services to replace certain hardware elements to which users previously needed physical access, including extra data storage and processing power. It can also encompass software as a service.

Sensitivities have already arisen around the location and protection of data centres for cloud storage, particularly in light of Mr Snowden's revelations. In addition to pre-existing concerns about the protection of personal data from cyber-criminals (and aggressive advertising firms), individuals are now aware that data-storage-service companies may be obliged to allow access to their home governments' security agencies. As with other ICT infrastructure, the possibility of hardware-based threats from criminals or governments exists, but is not currently central to the public debate around security, focused as it is on privacy and integrity of data.

Many countries see the provision of cloud-computing services as a key growth area, and are vying for investment by service providers. The Snowden leaks show that being political allies does not necessarily remove potential insecurity of cross-border provision of cloud services. Trust will be a major issue going forward, and will need to be addressed by cloud-service providers (in terms of ensuring

[15] See, for example, the following report by EU and Japanese industry organisations: home.jeita.or.jp/iad/pdf/20120621_e2.pdf.

security against software- and hardware-based attacks) and governments (in terms of domestic regulations and international agreements limiting private- and public-sector abuses of privacy).

However, it is important also to bear in mind that security and economic considerations will not be the only factors affecting the location of data centres. There are practical considerations, such as the need for adequate, low-cost and reliable power supplies. Some countries will, therefore, have much more impetus to avoid localisation policies than others.

Preparing for a software-defined world

The promise of software-defined networks (SDNs) is usually expressed in similar terms to most innovations in network technology: that is, they will allow network operators to improve speed and efficiency.[16] In traditional networks, switches and routers are pre-set with instructions on how to forward data traffic, and must be manually altered or upgraded; in SDNs; by contrast, the instructions controlling traffic can be altered through software administered from a remote location.

A parallel to the SDN is the software-defined radio (SDR), which performs a similar function for radio transceivers; remotely delivered software instructions can set, or alter, its operations, including its frequency range or power output. SDN and SDR are considered critical to any future network-infrastructure generation, such as the discussions around 5G broadband mobile technology. The performance of a communications network in years to come will be determined not just during the physical construction of its infrastructure, but will be managed throughout its operational lifecycle by an ongoing connectivity to software instructions.

The potential benefits of the SDN stem from its increased levels of automation and flexibility, which will allow networks to cope much more easily with fluctuations in traffic volumes, increasing bandwidth as and when required. It is considered a disruptive technological advance, and the main potential economic risk is to those companies that manufacture proprietary network gear, such as Cisco and Huawei. Many industry commentators now expect the commoditisation of network gear and increased use of generic, standardised hardware, while value increasingly accrues to software and service providers. As well as amplifying the existing need to suppress hardware costs, this will force many vendors of network infrastructure to move into software development. Little wonder, then, that Huawei showcased its own SDN technology in October 2013: Net Matrix, part of the SoftCom network architecture. Meanwhile, Cisco has announced its Open Network Environment (ONE) SDN strategy. The industry has not yet developed a full set of standardised protocols, so proprietary protocols are still in use in these SDN trial runs. However, it is very likely that such standards will be developed over the next few years, representing a significant shift in the telecoms sector.

The advent of software-defined networks will bring new cyber-security challenges. There are advantages, including the possibility of responding faster and more flexibly to software-based attacks. Yet, the standardisation of network gear will also make it easier for malware, such as worms, to navigate across multiple networks, facing fewer barriers like those currently posed by the differing specifications of proprietary gear. Just as legitimate alterations to routers and switches can be remotely administered, so can an attack be managed from any location. Much work will need to be

[16] http://www.economist.com/news/business/21568435-software-defined-networking-inspiring-hope-and-hype-network-effect

© The Economist Intelligence Unit Limited 2014

done to guarantee network security so that organisations and individuals feel comfortable adopting SDN technology, and this will require co-ordination among industry and government stakeholders. In terms of hardware-based threats, SDNs will not fundamentally change the risks: hardware could be compromised during design or at various points in the manufacturing process, and those in charge of final testing, as well as procurement of gear, will need to improve their ability to detect vulnerabilities and defend against attacks.

Policy responses to SDNs are likely to focus on similar issues faced in cloud computing: data and communications privacy, standards and interoperability, and rules on cross-border data flows. As in cloud computing, there will be sensitivities around cross-border remote management through software, and how this relates to different countries' legal intelligence activities.

The tremendous potential of SDN technology has begun to reawaken the interest of national technology promotion and development agencies. Korea's ETRI, in particular, has been increasingly active in funding R&D around both SDN and SDR, and intends for this next-generation network capability to be a key component of Korea's domestic ICT supply chain.

Conclusions

In the short term, it does not look like supply chains for key network gear will be re-routed out of China, or any other locations viewed as risky by governments of key markets. This is not even being discussed in terms of solid legislation or international agreements—although the US is recommending that network operators do not procure equipment from Huawei, they are not asking local equipment vendors to cut China out of their production processes. The key reasons for the lack of will to do so are as follows:

- The economic imperative: with fierce competition, and less and less value accruing to production of hardware, network-equipment producers cannot afford to move to higher-cost manufacturing locations. This will be even more the case as hardware is commoditised, with the introduction of software-defined networks. Most governments appreciate the need to maintain low-cost ICT services to support their domestic economies, so are unlikely to demand re-shoring or to raise local-content requirements, except where they are pursuing an economically left-wing agenda, as in Brazil.

- More sensible alternatives exist: governments and network operators can focus instead on improving their capacity to detect and defend against hardware-based risks, in addition to the current approach of risk management through supplier diversification.

- Mr Snowden's revelations about the surveillance activities of the US and its allies have detracted attention from concerns about Chinese espionage, with the result that the public and governments around the world are more concerned about developing legislation that protects against (and allows prosecution for) any excessive abuse of privacy, regardless of provenance.

- Related to the preceding point, the US has lost the moral high ground when it comes to matters of cyber-security, and this significantly reduces the likelihood of other countries following its lead in limiting private-sector procurement of network gear from Huawei or ZTE.

© The Economist Intelligence Unit Limited 2014

As top vendors of network equipment adapt to the software-managed world of SDNs and cloud computing, and find new ways to add value through software development and services, the main challenges they will face in market expansion will relate to trust. Individuals and organisations want reassurance that their data and communications will not be vulnerable to criminals, abused for marketing and advertising purposes, or indiscriminately gathered by government agencies—domestic or foreign. Trust will be a key asset for any company that hopes to be a leading provider of equipment or software-management services for ICT infrastructure.

Chapter Two: Cyber-security and politics

Overview

The purpose of this chapter is, firstly, to describe the rise in digital development and the threats that come with it. Secondly, the limited nature of current international agreements from a policy perspective, and the barriers to their development, will be discussed. Finally, the bulk of the chapter analyses current policies and politics across the US, Europe, "developed Asia" and emerging markets, in order to gain a better understanding of governments' efforts, particularly in the wake of the Snowden revelations, and what might be expected moving forward. For each region, any particular implications for Huawei are also examined.

Introduction to the politics of cyber-security

Cyber-security has risen rapidly up policy agendas around the world in the past few years and extends beyond ICT supply chains, especially among countries with a high reliance on ICT more broadly. The underlying reasons can be classified into two overarching categories: economic and geopolitical, both of which have an impact on governments, businesses and individuals alike. The current state of relations between the US and China is a particularly striking illustration of the stakes across these areas.

From an economic perspective, China accounts for about 80% of intellectual-property (IP) theft in the US, as a result of which the US loses around US$300bn in potential exports, according to a 2013 report from the Commission on the Theft of American Intellectual Property, a bipartisan government initiative. For instance, in February 2013 an American security firm concluded that an allegedly state-sponsored Chinese entity had targeted hundreds of companies around the world, including US ones, such as *The New York Times*.[17] A week later, China noted that its own websites are often attacked and that the US is the source of the largest number of assaults.[18] Chinese government websites constitute the majority of targets, but commercial actors, including banks and high-profile websites, such as Baidu, are also targeted.

The perception of collusion between the Chinese government and industry has been a particularly sore point in the relationship between China and the US and has affected the fortunes not only of Huawei, but also other international companies, such as Lenovo in the US and Google in China. Hence, when US president, Barack Obama, called to congratulate Xi Jinping on becoming China's president in March 2013, the topic of cyber-security was reportedly also high on the agenda.[19]

Shortly thereafter, the revelations by Edward Snowden completely changed the international discourse, shifting the focus of cyber-security concerns from China to the US and its allies. Western allies started to point fingers at each other, with potential political and trade implications. With each

[17] http://www.economist.com/blogs/analects/2013/02/chinese-cyber-attacks

[18] http://www.npr.org/blogs/thetwo-way/2013/02/28/173158072/china-accuses-u-s-of-hacking-military-sites

[19] http://www.nbcnews.com/technology/technolog/obama-chinas-xi-discuss-cyber-security-dispute-phone-call-1C8874180

new Snowden leak, the US continues to lose any perceived moral high ground it could once claim in respect of cyber-security.

In an effort to defend its massive surveillance programmes, the US emphasises national security and denies any government involvement in commercial espionage. Back in 2000, former Central Intelligence Agency (CIA) director, James Woolsey, responded to allegations of commercial espionage by acknowledging that the US does spy on foreign businesses, but only to investigate possible breaches of trade sanctions, flows of dual-use technology, and allegations of bribery—not to steal foreign technology.[20] Yet, allegations by Mr Snowden that the National Security Agency (NSA) has spied on certain oil companies in Brazil and Mexico, as well as on European political allies, have renewed speculation that the US, too, may use its intelligence services for more than proportionate national-security purposes. As one analyst put it, "They surely didn't spy on Germany to gain military insights," and The Economist called on the US to "reaffirm that for the NSA to pass secrets to American firms for commercial advantage is illegal".[21] This demonstrates a widespread loss of trust.

This is an issue that affects countries around the world and will only increase in importance as they become more dependent on ICT and hence more concerned with cyber security. Although the final outcome is yet to be seen as the Snowden leaks continue (and are likely to do so for some time, according to sources familiar with the situation), they have already raised fundamental questions about the possibility of international norms. In particular, it is still far from certain whether trust in the US and its allies in the 'Five Eyes' community (Australia, Canada, New Zealand and the UK) can be restored. Greater transparency is often cited as the best way to improve trust, but sometimes an open and transparent approach is not enough to convince doubters.

This chapter begins by illuminating the tie between cyber dependency and the rising importance of cyber security through a framework that combines the demand- and supply-side factors that underlie digital development.[22]

Global competitiveness, demand and supply

Although the extent to which a country is engaged in ICT supply chains is important, it does not necessarily correlate with the potential political ramifications at stake more broadly. For instance, a country such as Vietnam can have large-scale ICT production without the government and its citizens being cyber-dependent in everyday life; conversely, a country can have very low levels of production, but be heavily dependent on ICT. In Denmark, for example, the government has made online-service delivery legally mandatory by 2015, raising its dependence even further.

A basic framework to gauge levels of cyber-dependence across the world or in individual countries should include an assessment of a country's overall ICT competitiveness and how that links to socio-economic factors, such as GDP, as well as demand-side factors in terms of connectivity and usage.

The underlying assumption is simply that businesses and governments are both increasingly moving their processes online in an effort to improve productivity. Recent technological developments, such

[20] See http://cryptome.org/echelon-cia.htm.

[21] http://www.economist.com/news/leaders/21588861-america-will-not-and-should-not-stop-spying-clearer-focus-and-better-oversight-are-needed

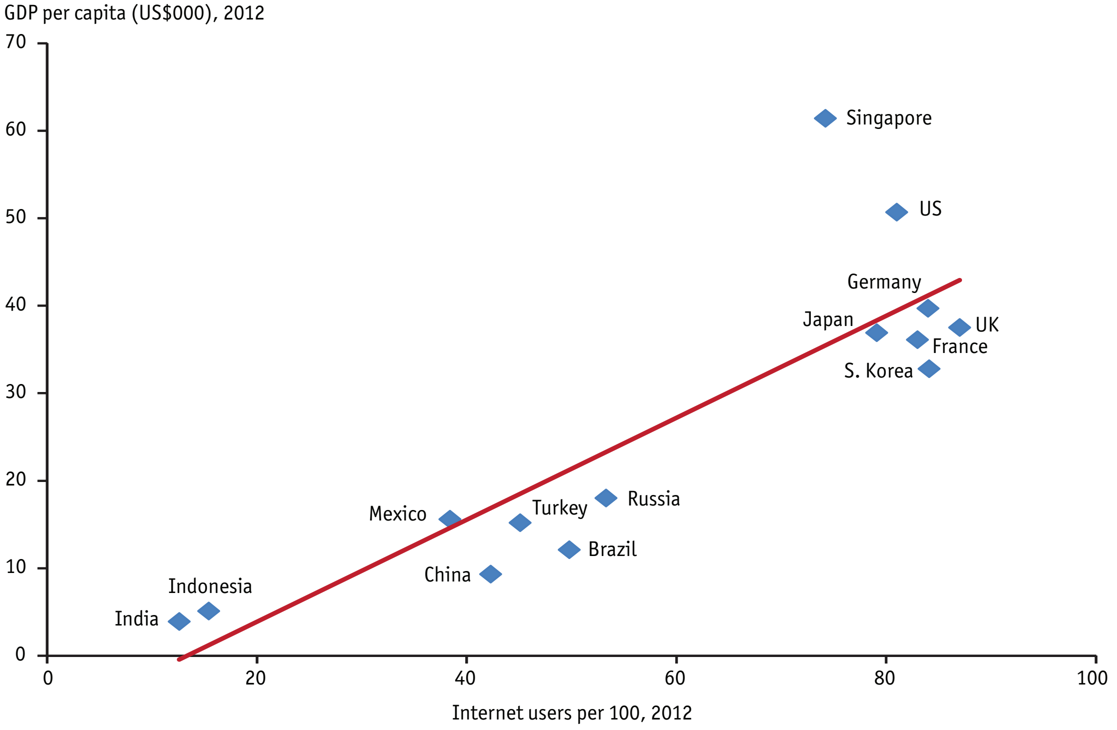
[22] Adapted from Kim Andreasson (ed.), Cybersecurity: Public sector threats and responses (CRC Press, 2011). http://www.crcpress.com/product/isbn/9781439846636

as software-mediated supply chains and cloud computing, offer new benefits in this regard and serve to expedite digital dependency across the world.

The greater use of ICT is tracked globally by a number of reports, including the annual *Global Information Technology Report* from the World Economic Forum (WEF).[23] In 2012, Sweden led the world in its Networked Readiness Index, which "measures the extent to which 142 economies take advantage of ICT and other new technologies to increase their growth and well-being". The primary source for tracking government efforts is the biennial E-Government Development Index in the UN E-Government Survey, which, in 2012, found that "Progress in online service delivery continues in most countries around the world," with the Republic of Korea leading the way.[24] Because of the socio-economic opportunities associated with usage, people around the world are also jumping at the opportunity to receive information online and conduct services on the Internet or over mobile phones.

Combining supply of ICTs and the ability of the population to take advantage of them (using GDP per capita as a proxy indicator) with the demand for them (using Internet usage as a proxy indicator), one can identify the development stages of cyber-dependency in individual countries (see Figure 3, below). It is possible not only to assess where a country currently stands in its cyber-development, but also to predict where it is heading next by looking at the potential threats facing those that are further ahead. For instance, a distributed denial of service (DDoS) attack shutting down Internet banking in India and Indonesia, which are less cyber-dependent than Western counterparts, would be of lesser concern than if this happened in the US or the UK. Similarly, countries with higher GDP are also more likely to

Figure 3: Matrix of cyber dependency (select countries)



Sources: *World Development Indicators, CIA World Factbook.*

[23] World Economic Forum, *Global Information Technology Report 2013*: http://www.weforum.org/issues/global-information-technology

[24] UN, *E-Government Survey*: http://unpan3.un.org/egovkb/

be targets of corporate espionage. Hence, rising cyber-dependency also means an increase in risk. The potential consequences vary, depending on the threat and the target's level of development.

Categorising cyber-threats

Different countries (and non-state actors) have various cyber-related motivations, from stealthy intelligence gathering and IP theft, to military sabotage and high-profile disruptions to both software and hardware components, all of which can affect business relationships and trade negotiations.

By categorising threats into the two overarching categories introduced earlier—economically motivated and politically motivated—it is apparent that (with few exceptions) cyber-dependent countries face far greater politically motivated threats than others, hence they are also more inclined to be part of cyber-espionage activities themselves compared with those who have a lower level of cyber-dependence, where challenges primarily concern financial crimes.

Cyber-crime and non-political threats

As organisations, their customers, and society at large went online, so too did criminals. ICT provided a new platform for fraud and various forms of illegal activity. Although there are other non-politically motivated cyber-threats, such as disruptive behaviour of employees, most threats within this category would fall under the general heading of cyber-crime. This is distinct from politically motivated threats, notably from state actors, which primarily target the confidentiality, integrity and availability of information (CIA model).

The cost of cyber-crime is staggering by any estimate. According to Norton, a security company, which surveyed thousands of people around the world, the global cost is about US$110bn annually.[25] Assumptions about indirect costs are hard to make and such estimates are, therefore, frequently questioned, but it is safe to assume that they are significant.[26] Beside the numbers, cyber-crime can also result in a loss of trust, which is a particular concern for e-commerce and financial institutions.

In a global study of cyber-crime in UN member states, the UN Office on Drugs and Crime (UNODC) found that, overall, countries were equally concerned about three broad categories of threat: attacks falling under the CIA model; financially driven threats, such as fraud, forgery and *phishing*; and, content-related crimes.[27] Although regional differences are small, there is one discernible trend: in less-developed countries, the law is enforced less frequently against the CIA model, whereas, in more developed countries, there appears to be an equal distribution among the three, supporting the theory that higher development leads to an increase in politically motivated threats.

Politically motivated threats

Different countries are said to have varying motivations with regard to their online espionage activities: China is often cited as trying to steal confidential commercial information; Russia is seen as primarily interested in financial information; leaks have shown the "Five Eyes" community to seek advantage in international negotiations through interception; and, in East Asia, given the history of tensions, South Korea and Japan wonder aloud about North Korean-supported online disruptions.

Whether the attacker is a nation-state, a group, or an individual, the common objective for

[25] http://www.symantec.com/about/news/release/article.jsp?prid=20120905_02

[26] http://www.economist.com/node/21557817

[27] UN Office on Drugs and Crime, Comprehensive Study on Cybercrime, 2013:

http://www.unodc.org/unodc/en/organised-crime/expert-group-to-conduct-study-cybercrime-feb-2013.html

© The Economist Intelligence Unit Limited 2014

politically motivated cyber-threats is generally that they seek to compromise the confidentiality, integrity and availability of information (the so-called CIA model), targeting either hardware or software, including Internet services.

In 2010, Stuxnet, a malicious software—or malware—became the first cyber-attack with physical consequences for critical infrastructure, by reportedly succeeding in disrupting Iran's nuclear-power reactors. Given the sophistication needed, attacks with such consequences are rare, yet are increasingly likely as countries invest in offensive cyber-attack capabilities and consider these to be an alternative to diplomacy or traditional military action. For instance, the US has officially labelled cyberspace as the fifth domain (after air, land, sea and space) and established offensive intelligence and military capabilities; others have joined in the cyber-arms race and more are likely to do so.

Cyber-espionage is similar to offline espionage, in essence aiming to eavesdrop or steal information without being detected. In a purely commercial setting, it would be labelled "corporate espionage" and considered a cyber-crime (see previous section). However, evidence has recently come to light that governments and the private sector collude in carrying out such attacks. As the Snowden documents illustrate, the US government has in the past often worked closely with domestic-technology companies to gain access to information from other countries through "backdoors".

It is obvious that intelligence agencies do what they can to gather information, but, when they are detected, it can affect trust (and cause loss of face), which in turn affects the prospects for greater international co-operation, particularly when corporate collusion is suspected or proven. This has become more important, as, today, trade agreements have global repercussions. Without international agreements regulating online behaviour and with a rise in politically motivated threats, it is likely that politicians will increasingly use legislative measures to protect domestic businesses and constituents in the name of national security. There are numerous such examples, including in China and the US, where companies have been coerced to withdraw from business opportunities or barred from competing on an equal basis.

Unlike Huawei, Lenovo was able to acquire its US target—IBM's personal computer (PC) business—only to find a tougher operating environment in government procurement, hence its focus on consumer business in the US. Although Chinese companies may be unfairly treated in the West, the argument goes both ways. Since 2002, China's Government Procurement Law and other policies supporting indigenous innovation in science and technology, have restricted foreign access to central and local-government procurement processes, with state-owned enterprises representing a grey area. Differences in political culture have also affected foreign companies' ability to operate in China; for instance, Google announced in January 2010 that it would stop censoring search results on its Chinese version, Google.cn, and had to relocate to Hong Kong, a Special Administrative Region, to avoid violating Chinese rules.

Cyber-security as a geopolitical issue, therefore, also affects individual organisations. In addition to ICT trade and investment patterns, which can be disrupted by political decisions (although, so far, mostly in an ad-hoc way, rather than through legislation with widespread effects on industry supply chains), this appears to be the case for online services as well. The rise of cloud computing, for

© The Economist Intelligence Unit Limited 2014

example, means that data fall under the jurisdiction where they are stored, not only where they are used. In the UK, for example, the government has pushed for greater use of cloud services, only to find that four of its suppliers store data in the US, which means the US authorities can tap into the data without a warrant if they concern US interests.[28] The likely implications are that US cloud providers may see international business drop, while domestic providers in some countries are likely to thrive in this increasingly localised market.

But, although the temptation is great to replace foreign hardware and software systems with domestic ones, most countries lack the capacity to do so, while others find it costly and ineffective. Both Russia and China have tried to develop their own computer-operating systems without commercial success (although both still continue this effort). The US also set different encryption standards for domestic use and export around ten years ago, only to find its companies complaining about a lack of advantage and the strategy was abandoned; more recently, Facebook cried foul over lack of transparency in US regulation, which it sees as hindering its international prospects.

To mitigate the Snowden revelations and any resulting fall in revenue, and in order to exonerate themselves, a number of leading US technology companies are pushing for government reform. With the proposed legislation they support facing stiff opposition, notably the “USA Freedom Act” proposed by a senator, Patrick Leahy, and a representative, Jim Sensenbrenner, some have begun taking their own measures to restore trust. In February 2014, Facebook, Microsoft, Google and Yahoo started publishing the number of government requests they had received in order to increase transparency, and, in the process, show the limited number of requests made.[29] This may help to improve their tarnished reputations, but solid legislative responses would do more to restore trust at home and abroad. However, commercial arguments are unlikely to overtake completely national-security concerns, particularly in the absence of international agreements.

International agreements (or the lack thereof)

Moving from an assessment of the key drivers behind digital development and the threats that come with them, international agreements are now used to illustrate current efforts to establish norms in cyberspace.

Recalling the classification of cyber-threats as either politically motivated or criminal and non-political in nature, one can see that cross-national initiatives focus on the latter. For instance, countries are generally in agreement that cyber-crime needs to be prevented, as most are also victims thereof. Developed countries are targeted because of their wealth, whereas less developed countries may be proportionally more vulnerable to such crimes, given a lack of awareness on the part of users. In Indonesia, for example, cyber-criminals prey on the many new Internet users who have limited cyber-security knowledge. As a consequence, Indonesia has emerged as the country from which the largest numbers of cyber-attacks emanate, not because of local crime groups, but, rather, because foreign groups have taken control of many computers there and use them for a variety of attacks elsewhere.[30] In situations like this, international initiatives can help in building up a country’s cyber-security awareness and responses, benefiting all parties.

[28] http://www.independent.co.uk/life-style/gadgets-and-tech/news/mps-call-for-government-to-consider-ending-use-of-cloud-amid-concerns-that-us-authorities-can-access-information-8473693.html

[29] http://www.reuters.com/article/2014/02/04/us-internet-nsa-idUSBREA121H920140204

[30] http://www.thejakartaglobe.com/news/hackers-paradise-or-host-nation-indonesian-officials-weigh-cyber-threat/

© The Economist Intelligence Unit Limited 2014

Table 1: Summary of current international initiatives for cooperation

	Political	Non-political (CBM or technical)	Scope
United Nations resolutions		✓	Global
ITU and UNODC		✓	Global
IMPACT		✓	Global
Council of Europe's Convention on Cybercrime		✓	Regional with global elements
CERT and CSIRT		✓	Global
FIRST		✓	Global
Wassenaar Arrangement		✓	Global but limited in scope
Internet Governance Forum	✓		Global
UK supported cyberspace security conferences	✓		Global
Regional (Arab League model law, Commonwealth model law, the ECOWAS Directive, Draft African Union Convention)		✓	Regional

International agreements are, however, harder to achieve when political motives are a factor, such as in the debate over the role of the Internet Corporation for Assigned Names and Numbers (ICANN) and, more broadly, how the Internet should be governed; or, equally, when it comes to trying to rein in a rapidly evolving cyber-arms race. According to multiple sources, the situation is particularly difficult when governments are suspected of involvement in corporate espionage, which further erodes trust.

Politically motivated attacks are primarily conducted by advanced economies against other developed countries, as they have entered a new dimension of ICT capabilities and dependency.[31] Exceptions to this basic premise include countries such as China, Iran and Russia, which have developed a particular military dependence on ICT and are, therefore, targets and issuers of politically motivated cyber-attacks as well.

Despite recent calls for agreement on international law or behavioural norms when it comes to political attacks via cyber-warfare and espionage, decisions regarding their use remain firmly within the auspices of individual nation-states. The following overview of prominent cross-national initiatives on cyber-security shows that this situation is unlikely to change in the near term and any agreements are likely to be regional or otherwise limited in scope and nature, among groups of like-minded and allied nations.

UN resolutions

The UN General Assembly (UNGA) has addressed cyber-crime primarily through resolutions 55/63 (2000) and 56/121 (2001) on Combating the Criminal Misuse of Information Technology, which, together with other relevant resolutions, urges member states to consider the multilateral dimensions of threats in the usage of ICT, as well as proposing measures to limit them. Because the UNGA does not have any authority to punish non-compliance, these resolutions are merely advisory. Despite being spied on itself, as first revealed by Bradley Manning, a US soldier who leaked thousands of documents

[31] In this regard, see also the arguments put forth by a former US Defense Secretary in William J. Lynn, “Defending a new domain: The Pentagon’s cyberstrategy”, *Foreign Affairs*, Sep/Oct 2010: : http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain

to WikiLeaks, the anti-secrecy organisation, the UNGA has not taken an active role when it comes to the political dimensions of cyber-security.[32] It has also delegated more detailed work to the International Telecommunications Union (ITU) and the Internet Governance Forum (IGF), as described below.

ITU and UNODC

As the UN agency for ICT, ITU is also the global lead for cyber-security.[33] Of particular note is the agency's development of the Global Cybersecurity Agenda (GCA), a framework to help countries take national measures and harmonise them at international level. The five pillars of the GCA are: legal measures; technical and procedural measures; organisational structures; capacity building; and international co-operation. It is designed, however, to help individual—and primarily developing—countries enhance cyber-security at basic level, rather than to promote international agreements per se. This is similar to the mandate of the International Multilateral Partnership Against Cyber Threats (IMPACT), which is the operational arm of the ITU. The UN Office on Drugs and Crime, meanwhile, leads the UN efforts against an "uncivil society", which includes organised crime and terrorism; hence, it is also tasked with combating cyber-crime, not creating international co-operation regarding politically motivated activities in cyberspace.

IMPACT

In 2011, IMPACT, headquartered in Kuala Lumpur, the Malaysian capital, officially became the operational cyber-security arm for the ITU and was tasked with providing access to expertise and information through the Global Response Centre (GRC), which helps realise the GCA through the Network Early Warning System (NEWS) and Electronically Secure Collaboration Application Platform for Experts (ESCAPE). With 147 member nations, it is the world's largest cyber-security alliance.[34] In addition to international collaboration through NEWS and ESCAPE, IMPACT also provides training in cyber-security around the world; however, like the ITU itself, the organisation is designed to help individual—and primarily developing—countries enhance cyber-security at a basic level, rather than promoting broad international agreements per se.

Computer Emergency Response Team (CERT) and Computer Security Incident Response Team (CSIRT)

CERT and CSIRT fulfil the same function, as they are both designated to handle computer-security incidents. The approach was established at Carnegie Mellon University in 1988 and, today, most countries have a CERT, sometimes affiliated with the government and sometimes not. Although international co-operation is an underlying feature between them, this is limited to technical measures with other CERTs/CSIRTs and, given the lack of government involvement in most countries, does not lend itself to any geopolitical considerations.

Forum for Incident Response and Security Teams (FIRST)

Founded in 1990, FIRST provides a platform for members to deal more effectively with security incidents by providing information on best practice and access to various tools.[35] The organisation consists of incident-response teams across the world from a wide variety of actors, including the public and private sectors, as well as academia. Similar to CERT/CSIRT, there is an underlying international

[32] http://www.theguardian.com/world/2010/nov/28/us-embassy-cables-spying-un; http://www.reuters.com/article/2013/10/29/us-usa-security-un-idUSBRE99S14E20131029

[33] "Building confidence and security in the use of ICTs," known as Action Line C5, was established at the second World Summit on the Information Society (WSIS) in Tunis, Tunisia, in November 2005.

[34] IMPACT: http://www.impact-alliance.org

[35] FIRST: http://www.first.org

© The Economist Intelligence Unit Limited 2014

co-operation, although it is also limited in nature to technical information, with a lack of direct government involvement in most countries.

Wassenaar Arrangement

The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies ("Wassenaar Arrangement") is a multi-national export-control agreement that has recently gained attention in respect of cyber-security, due to its continuing work in limiting dual-use export technologies (those that can be used for both civilian and military purposes).[36] For instance, The Financial Times reported in December 2013 that diplomats were expected to establish new export controls on complex surveillance, hacking and cryptography technologies in order to prevent certain states from using them to gain insight into—or block—Western intelligence capabilities.[37] The Wassenaar Arrangement is limited in both scope and geography—the 41 participating states are predominantly Western countries (Russia being one obvious exception) and do not include emerging markets such as Brazil, India and China.

Internet Governance Forum

The Internet Governance Forum (IGF) is a multi-stakeholder forum that brings together the public and private sectors, as well as civil society, to discuss Internet governance.[38] It was formally established by the then UN secretary-general, Kofi Annan, in July 2006 and has held annual meetings since, the most recent of which was in Bali, Indonesia, and was entitled Building bridges—Enhancing multi-stakeholder co-operation for growth and sustainable development. Although its mandate is international in scope, the discourse focuses on capacity building, rather than geopolitics.

UK-supported cyberspace-security conferences

In part due to the lack of international forums to discuss politically motivated threats and norms in cyberspace, the UK foreign secretary, William Hague, has explained the growing importance of the topic by pointing to three attacks against British interests, including one targeting his office. He subsequently announced a conference on the topic in 2011, "to lay the basis for a set of standards on how countries should act in cyberspace". The London Conference on Cyberspace to "build a secure, resilient and trusted global digital environment" was followed by events in Hungary and South Korea in 2012 and 2013, respectively.[39]

Although, at one point, this was perhaps the most promising of international initiatives, one European government official who has attended the series of events recently described them as "back to square one" and was of "two minds" as to whether they will now succeed in establishing norms. Specifically, there are baseline issues to be addressed, such as whether offline international legal obligations also apply online, and defining the rights and obligations various actors have in cyberspace. Given differences of opinion in this regard, the official said that expectations have been downgraded from creating a comprehensive agreement to establishing some basic international norms.

Regional responses

Regional frameworks for co-operation include the Arab League model law, Commonwealth model law, the Economic Community of West African States (ECOWAS) Directive,[40] and the Draft African Union Convention,[41] all of which focus primarily on financial crimes. However, the most wide-ranging and

[36] http://www.wassenaar.org

[37] http://www.ft.com/cms/s/0/2903d504-5c18-11e3-931e-00144feabdc0.html#axzz2mgQaiqXJ

[38] http://www.intgovforum.org/cms/

[39] https://www.gov.uk/government/news/london-conference-on-cyberspace-chairs-statement

[40] ECOWAS: http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/documents-ecowas.html

[41] African Union Convention background information available at: http://www.au.int/pages/infosoc/pages/cyber-security For the draft convention: http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/events/2011/WDOcs/CA_5/Draft%20Convention%20on%20Cyberlegislation%20in%20Africa%20Draft0.pdf

© The Economist Intelligence Unit Limited 2014

influential initiatives have sprung out of Europe. The EU has arguably established the first regional cyber-security strategy that encompasses political threats, as well as financial, in a document entitled An Open, Safe and Secure Cyberspace in July 2013, although the scope is limited to the EU itself.[42] Furthermore, the Council of Europe's Convention on Cybercrime has become an important forum and warrants more in-depth discussion.

Council of Europe's Convention on Cybercrime

Cyber-crime was defined by the 2001 Council of Europe's Convention on Cybercrime (informally known as the "Budapest Convention") as encompassing four categories: offences against the confidentiality, integrity and availability of computer data and systems; computer-related offences; content-related offences; and offences related to infringements of copyright and related rights.[43] This is commonly used as the standard definition of cyber-crime, and its substantive criminal-law section is used as a reference for creating national laws. As of February 2014, 41 countries, including the US, had ratified its use, although it remains a largely European undertaking.

Of particular relevance at present is Article 32b of the Convention, which deals with cross-border data flows for the purposes of investigating crimes. Essentially, it allows extra-territorial searches and seizure of data by law-enforcement authorities, without the obligation to notify the other state's authorities. It states:

[A] Party may, without the authorisation of another Party [..] access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the **person** who has the lawful authority to disclose the data to the Party through that computer system. (Emphasis added.)

The "person" referred to here could theoretically be a US company storing data on an EU-based cloud server, which could legally (under US law) be asked to provide data to the US authorities. Yet, this act may be illegal under the EU country's law. Even before the PRISM revelations, concerns had been raised about the problems this could cause for system operators and Internet service providers, as well as abuses of to which this could lead—so much so that an Ad-hoc Sub-group on Jurisdiction and Trans-border Access to Data had been formed under the Cybercrime Convention Committee to look at trans-border access to data. It pointed out in a report of December 2012 that private-sector third parties could be "put [...] in jeopardy, both legally and practically".[44]

Although the Budapest Convention, strictly speaking, deals only with crime and not national security, it has codified norms of seizure of extra-territorial data by states which, as Mr Snowden confirmed, have been applied for political purposes by national-security organisations. The sub-group's December 2013 report advised that it was worth the trouble of negotiating a binding international treaty, in the absence of which "risks to the procedural and privacy rights of individuals" would only increase.[45]

Analysis of international agreements

The overview of current international initiatives shows that they fall into one of the two categories established earlier: those concerned primarily with financial crimes and those that also encompass

[42] http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

[43] Council of Europe, Convention on Cybercrime: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

[44] Council of Europe, Cybercrime Convention Committee (T-CY), Ad-hoc Subgroup on Jurisdiction and Transborder Access to Data: "Transborder Access and Jurisdiction: What are the Options?" Report of the Transborder Group, adopted by the T-CY on December 6th 2012.

[45] Council of Europe, Cybercrime Convention Committee (T-CY), Ad-hoc Subgroup on Transborder Access and Jurisdiction, 'Report of the Subgroup for 2013' (2013).

© The Economist Intelligence Unit Limited 2014

politics (technical agreements, such as CERT/CSIRT/FIRST/Wassenaar Arrangement, arguably tackle both implicitly, but certainly are not focused on the political dimension).

Initiatives that cover technical issues or cyber-crimes, such as the Budapest Convention, are successful because most countries find common ground. When it comes to applying similar norms to threats of a political nature, however, there is no common ground, due to differing views on governance, fierce protection of domestic legislative autonomy with regard to national-security issues, and also a lack of trust.

Lack of trust was evident even before the Snowden leaks, as many countries started developing offensive intelligence and warfare-type capabilities in cyberspace without much transparency. The US, China, Israel and Russia are among those leading the way, but, as countries develop, so does their dependence on cyberspace and hence the need for defensive capabilities—which tends to lead to a desire for offensive capabilities. Indonesia, for instance, recently announced the formation of a military strategy for cyberspace. Experts disagree as to whether cyberspace will be an important battleground in case of war, but almost everyone seems in agreement that it is a scenario worth planning for. The inherent technical difficulty in tracing the source of a well-executed attack also increases suspicion when an event occurs and exacerbates the lack of trust. Countries cannot do much in this regard, which means they use the only tool available to them: to limit foreign investment and ownership in key ICT infrastructure.

Beyond a lack of trust, states also disagree on governance of cyberspace and, in particular, the extent of sovereignty. A remaining fundamental question is whether current international norms are applicable to cyberspace; some argue that they are, others that cyberspace remains a separate arena. The Budapest Convention, as discussed above, has codified a view that the Internet is an international dimension, with different rules to physical territory; although this concept is now being re-examined and, indeed, has always been anathema to some non-signatory countries. As noted above, until clear rules emerge among a significant number of countries on key issues, such as extra-territorial data requests, private-sector Internet service providers remain in a difficult legal situation and can only resort to introducing their own confidence-building measures.

Overview of policies and politics across regions

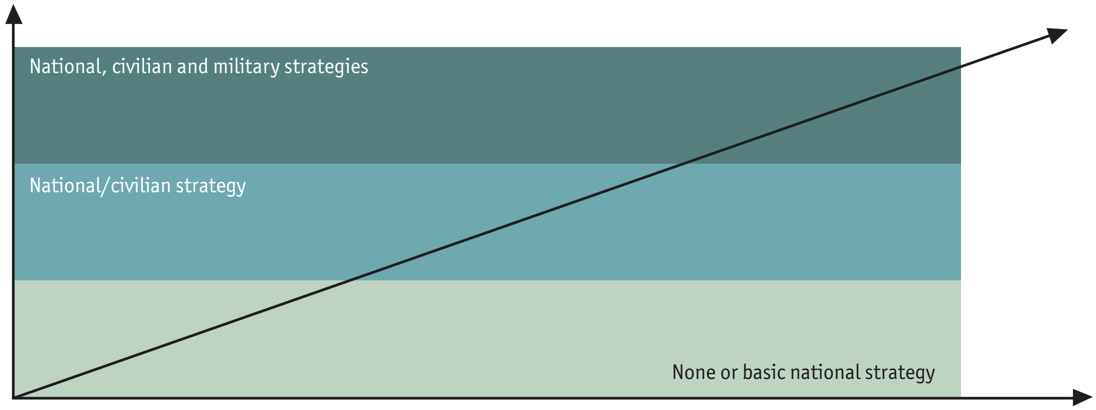
In part due to the lack of international agreements, countries tackle cyber-security individually, along three broad stages of development that largely mimic the cyber-dependency matrix introduced earlier. The first includes those that recognise the tie between ICT and socio-economic growth and make that explicit as part of the country's national strategy, development agenda or equivalent document. This often leads to a second effort to secure the civilian cyberspace in order to sustain those benefits, such as the National Security Strategy in the UK, which highlights cyber-attack by other states, terrorists or organised crime groups as one of the four highest risks to the nation.[46] Although there is some overlap, the third category consists of those that have built on the initial strategy expressly to establish military capabilities in cyberspace, such as the US.[47] In essence, then, enhanced cyber-

[46] UK Government, A strong Britain in an age of uncertainty, Oct 2010: http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191639.pdf

[47] The first US Cybercom commander was appointed in May 2010: http://www.defence.gov/releases/release.aspx?releaseid=13551

© The Economist Intelligence Unit Limited 2014

Figure 4: A rise in dependency often leads to more elaborate cyber strategies, including military ones


National, civilian and military strategies
National/civilian strategy
None or basic national strategy

dependency leads to greater awareness of cyber-security and the need to develop further in this area in order to stay ahead of international threats and competitors.

What follows is an overview of current trends in cyber security policies and the responses that come with them, with a particular focus on key actors such as the leading European countries, the US, developed Asia, and emerging markets, primarily China.

Europe

Since the second world war, Europe (in part through the EU) has primarily been concerned with the privacy of personal data and strong data protection. Indeed, the region has a history of anti-trust and privacy regulations that are sometimes at odds with the aims of international companies. For instance, the EU battled Microsoft's dominance for years, and, more recently, has turned to Google's various privacy violations.[48] In April, German regulators fined Google €145,000 over illegal collection of personal data during development of its Street View feature. In September, French officials said they would impose sanctions against Google after it missed a deadline to explain how it collects and uses personal data in the region.

Data-protection policies can affect individual businesses to a great extent and they are currently driven in part by the loss of political trust in the US, after the Snowden leaks revealed that the US had been spying on its European allies. According to one European official, Europeans were not surprised that the US collected sensitive information, as many countries undertake the same activities and this, in fact, is the objective of intelligence agencies. What surprised them, however, was the extent of the efforts and how easily they could access data. "It's not bringing the world together," said the European official. "It's about trust, and trust was breached in this instance, and it is hard to restore."

For instance, there was a European outcry after revelations that the NSA had monitored the phones of 35 world leaders, including German chancellor, Angela Merkel.[49] Ms Merkel and François Hollande, the French president, expressed alarm at the NSA's spying, while French EU commissioner, Michel Barnier, said, "enough is enough" .

[48] http://articles.washingtonpost.com/2013-09-27/business/42450023_1_cnil-google-s-data-protection-officials

[49] http://www.bbc.co.uk/news/world-europe-24647602

© The Economist Intelligence Unit Limited 2014

European concern over data protection is likely to continue and will affect all international companies doing business in Europe. On October 21st 2013, the European Parliament Committee voted to strengthen the Commission's proposal on data protection, to introduce stricter controls on how personal data are shared with non-EU countries. The committee recommended that the fine for non-compliance should be increased from 2% to 5% of worldwide annual company turnover (or at least €100m if the company's turnover is below €2bn).

Also in response to the Snowden revelations, many in the European Parliament sought to reintroduce the controversial Article 42 to the region's revised data-protection proposal. Largely seen as an "anti-FISA" regulation, it originally proposed to "prohibit third countries (such as the US and other non-EU Member States) from accessing personal data in the EU, where required by a non-EU court or administrative authority, without prior authorisation by an EU Data Protection Authority".[50] In other words, non-EU companies would have had to disclose to the EU when data are requested on an EU subject by a non-EU entity (such as the US government). This would have had complex implications for many international companies, including Huawei, but, as it stands, the European Parliament has only approved a watered-down version.[51] The new data-protection policies are also yet to be negotiated with the EC Council, and further revisions are likely. It is, therefore, too early to tell what the final outcome will be, but some member states do not seem keen on moving ahead with even the current watered-down version, due to the complexity of the implications for international business, notably the UK—presumably also because of its co-operation with US intelligence agencies.[52]

For Chinese companies such as Huawei, this is a good time to revisit their own data-protection policies. In 2012, the Chinese Ministry of Industry and Information Technology (MIIT) published guidelines on the protection of personal data, which, in essence, said that any data collected by Chinese companies must be in line with their intended purpose. The MIIT has also published the Regulation of Market Order Internet Information Services, an administrative law that subjects Internet service providers (ISPs) to limitations on personal-data collection and use, including restrictions on sharing information with third parties without user consent.

Adopting these as standard business practice, and publicising the fact that this is being done, not only makes domestic sense, but will also prepare an international organisation such as Huawei for compliance with potential future European data requirements.

In particular, cloud computing brings new cross-border challenges and further complicates the current geopolitical situation. This has particular ramifications for global companies that are heavily dependent on the ability to send data between jurisdictions and hence might become a key issue in future international-trade agreements, as will be discussed in the next section of this report. In 2013, Gartner estimated the value of the global cloud-services market at US$131bn, up from US$111bn a year earlier.[53] US providers account for an 85% market share, but that may dwindle as non-US service users discover that they may be subject to US data regulations and monitoring.[54] As opposed to the EU, the US does not have a single directive on data regulation, making the rules more complex for international businesses, although the important point is that all foreign data stored on US servers are subject to monitoring without court order in cases of national interest.

[50] http://www.sidley.com/European-Parliamentarians-Seek-Reinsertion-of-Onerous-Anti-FISA-Article-42-into-Proposed-EU-Data-Protection-Legislation-07-02-2013/

[51] http://www.wsgr.com/WSGR/Display.aspx?SectionName=publications/PDFSearch/wsgralert-compromise-amendments.htm

[52] http://www.ft.com/intl/cms/s/0/6930c9a6-5e8a-11e3-8621-00144feabdc0.html#axzz2sGPrvIVZ

[53] http://www.gartner.com/newsroom/id/2352816

[54] http://www.independent.co.uk/life-style/gadgets-and-tech/news/mps-call-for-government-to-consider-ending-use-of-cloud-amid-concerns-that-us-authorities-can-access-information-8473693.html

"If European cloud customers cannot trust the US government, then maybe they won't trust US cloud providers either," said Neelie Kroes, the EU's Digital Agenda commissioner, in a recent interview.[55] The EC also published an EU strategy paper on cloud computing in September 2012, which could be the basis for moving data from US clouds into Europe, in the process saving money for business, while generating new jobs for Europe. Such a localisation strategy—geographically storing data where it is used—is a global trend. Despite US advocacy of the free flow of information, this has always come with the usual national-security caveats: the US, too, has its own cloud for government functions. The trend towards data localisation has implications beyond US companies and affects anyone conducting cross-border business, as these are often designed to promote national (or, in the case of Europe, regional) providers for security purposes. International providers must, therefore, contemplate how to counterbalance this trend. Microsoft, for instance, recently announced that it would let its customers select where their data are stored, giving them the option to avoid jurisdictions with less stringent privacy regulations.[56] Whether such technical and legal manoeuvring will resolve the issue remains to be seen, as a lot of regulatory initiatives are still under way, but they do highlight the importance for an international company, such as Huawei, of actively considering alternative options regarding data usage, storage and movement. Meanwhile, the Snowden leaks also revealed disagreements within Europe itself, as Britain was "forced" to sign an EU statement expressing "deep concern" over the spying allegations.[57] Similarly, Sweden's prime minister, Fredrik Reinfeldt, remained unconcerned about the allegations when US president, Barack Obama, visited the country earlier this year; later, *The Guardian* newspaper revealed that Sweden had collaborated closely with both the US and the UK.[58] In fact, *The Guardian* later named Germany, France, Spain, Sweden and the Netherlands as countries where intelligence agencies had developed methods of co-operation with their counterparts, including Britain's GCHQ, begging the question of whether some heads of state had prematurely accused the US (and, to some extent, the UK) without accounting for their own actions. In essence, the US may have had the misfortune of being the first exposed—and to the greatest extent—as revelations concerning smaller actors, such as Sweden, whose intelligence gathering in Russia over the years were considered "unique" by the NSA, have largely gone unnoticed in the international press.

Meanwhile, the Snowden leaks also revealed disagreements within Europe itself as Britain was "forced" to sign an EU statement expressing "deep concern" over the spying allegations.[58] Similarly, Sweden's Prime Minister Fredrik Reinfeldt remained unconcerned about the allegations as President Obama visited the country earlier this year; later The Guardian newspaper revealed that Sweden had close collaboration with both the US and the UK.[59] In fact, The Guardian later named Germany, France, Spain, Sweden and the Netherlands as countries where intelligence agencies had developed methods of cooperation with their counterparts including Britain's GCHQ, begging the question whether some heads of state had prematurely accused the US (and to some extent the UK) without accounting for their own actions. In essence, the US may have had the misfortune of being the first exposed—and to the greatest extent—as revelations concerning smaller actors, such as Sweden, whose Russian intelligence gathering over the years were considered "unique" by the NSA, have largely gone unnoticed in the international press.

[55] http://www.euractiv.com/infosociety/prism-cloud-european-silver-lini-news-530004

[56] http://www.networkworld.com/news/2014/012314-microsoft-cloud-278034.html

[57] http://www.telegraph.co.uk/news/worldnews/northamerica/usa/10404436/US-spying-Britain-forced-to-sign-EU-statement-expressing-deep-concern.html

[58] http://www.thelocal.se/20131102/snowden-revelations-implicate-sweden-in-uk-spying

[59] http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191639.pdf; http://www.yhteiskunnanturvallisuus.fi/en/materials/doc_download/38-finlandas-cyber-security-strategy

© The Economist Intelligence Unit Limited 2014

European countries are proceeding with their individual cyber-security agendas, illustrated by the 2010 UK National Security Strategy and Finland's cyber-security strategy, published in January 2013, which explained that cyber-threats can have "increasingly serious repercussions for individuals, businesses and society in general" and noted that attacks can also have socio-economic consequences.[59]

The Snowden revelations have, to some extent, divided Europe between those who collaborated with the US intelligence activities and those that did not. However, the general consensus remains that the episode has hurt long-term US interests in Europe, particularly as the region has the capability of replacing US equipment (hardware and software) with its own. This is also evident in Europe's own strategy for cyber-security, in which one of the five strategic priorities is to "develop industrial and technological resources for cyber-security" and thereby create a "single market" for them at EU-level. It is designed as a response to security concerns, but, equally, to bring jobs and economic prosperity back to the region, partly at the expense of foreign companies. The region's technology systems are currently fragmented and European officials think this can help to integrate them.

Trust is seen as a key issue and the EU is looking inwards to restore it. For instance, one European official predicts that "interoperability" will be the catchword in the future as the continent consolidates its various platforms to improve cyber-security. Another strategic priority for the EU is the extension of an open, safe and secure Internet environment, a message it is likely to propagate internationally.[60] Specifically, one of the five strategic priorities is to "establish a coherent international cyberspace policy for the EU and promote EU core values". Although not designed to be at odds with US (or Chinese) efforts, it is likely further to regionalise the issue. In fact, several sources indicate that, because international agreement is unlikely, Europe is expected to build on its digital agenda, recent cyber-security strategy, and initiative for a European cloud, to enhance security and productivity within the region as a priority.

Summary of European policy responses

The surprises appear to have passed for Europe, as the continent is moving firmly ahead with an integrated cyber-security agenda, combining its focus on data protection with support for local ICT-sector development. Its solution involves increased localisation of data storage, along with improving and further standardising regional ICT offerings. Individual country strategies and legislation are likely to supplement the broader European agenda, rather than being at odds with it—the exception being the question of whether countries such as the UK and Sweden will continue their surveillance programmes in the face of EU protests against the US. Even such differences are unlikely to tilt the broader consensus. Given the clear direction in which the region is progressing in respect of cyber-security, Huawei should anticipate some challenges ahead, and ensure it can demonstrate support for local research and development (R&D), as well as compliance with EU data-privacy standards.

The United States

Cyber-security has featured prominently in US politics for decades and current federal initiatives stretch across multiple domains, including military, intelligence, homeland security, law enforcement and commerce.

[59] http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191639.pdf; http://www.yhteiskunnanturvallisuus.fi/en/materials/doc_download/38-finlandas-cyber-security-strategy

[60] http://www.eeas.europa.eu/policies/eu-cyber-security/

© The Economist Intelligence Unit Limited 2014

Over time, however, it has become clear that, while the motivations of different attackers may be not be the same, the means that they use to accomplish a cyber-attack are often identical. Since the tools, techniques and technologies to address threats are often similar, it makes sense to have a more co-ordinated federal response to improve cyber-security and, on December 22nd 2009, Mr Obama announced that Howard Schmidt would become the first-ever White House cyber-security co-ordinator, a decision that was soon followed by the introduction of various co-ordinated cyber-security strategies.

Homeland security has been a key component in domestic consolidation of cyber-security efforts and contributing to its global intelligence gathering. In the wake of the attacks of September 11th 2001, US politicians sought to improve intelligence gathering to combat terrorism. The resulting Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 made a number of changes to US law, including vast expansion of the Foreign Intelligence Surveillance Act (FISA). Of particular relevance to cyber-security are Titles II, V and IX, which cover surveillance procedures, removal of obstacles to the investigation of terrorism, and improved intelligence gathering. The expanding scope of electronic surveillance, combined with diminishing barriers (such as the removal of the need of warrants in some circumstances) led to a massive increase in data gathering. Although this was, in part, the purpose of the Act, the Snowden leaks surrounding the NSA and its PRISM programme illustrate that those efforts went beyond its intended purpose, as outlined in an op-ed in *The Guardian* by a Republican representative, Jim Sensenbrenner, one author of the Act itself.[61] What most surprised US officials in the information revealed in the Snowden leaks, therefore, was not the intention to gather information, but, rather, the scope of the surveillance.

Internationally, the US continues to focus on securing the Internet as a reliable global platform, as businesses rely on the free flow of information for commerce. In part because of their dominant global positions, US companies benefit immensely from an open Internet. Hence, their government supports them by officially advocating the free movement of data, while telling other countries to limit their censorship and stop cyber-attacks.

However, digging deeper, the US government is itself a significant perpetrator of censorship violations, according to sources that track blocked websites or requests for removal, such as the Google transparency report.[62] For example, following the leaking of sensitive government information to WikiLeaks, the US not only attempted to block access to the website, but the White House Office of Management and Budget also sent out a memorandum prohibiting unauthorised employees from accessing the website. The level and extent of online censorship that is deemed necessary for national-security reasons varies greatly between countries, of course, but the fact that everyone is doing it to some extent further illustrates the difficulties in establishing international norms in this area.

As outlined in the previous chapter, there has traditionally been a close R&D relationship between the US Department of Defense (DoD) on the one hand and the academic community and corporations on the other, which has formed the basis for the government's weapons-development and communications-interception programmes. Many of the companies that benefited from such

[61] http://www.theguardian.com/commentisfree/2013/jun/09/abuse-patriot-act-must-end

[62] http://www.csmonitor.com/USA/USA-Update/2013/1114/Google-transparency-report-curiously-opaque-thanks-to-FBI-gag-order

© The Economist Intelligence Unit Limited 2014

government investment have since been shown to introduce back-door vulnerabilities for NSA.

The US's greatest asset in intelligence gathering is its dominance in the manufacture of key IT hardware (primarily micro-processors) and software, such as productivity suits and online services, all of which one source calls "immensely valuable" to national-security capabilities.

In part due to this knowledge, one US official says the government is also extremely careful about using any type of foreign equipment. In fact, when looking at various service providers, the government views foreign actors as "weak links" and steers away from them. Given US dominance in the software market, officials are currently primarily worried about ICT supply chains, which are currently described as a "huge concern."

The primary issue from a political viewpoint, then, remains whether the US can sustain its current advantage and what will happen when the dominant ICT players are no longer from the US. The US has already lost its global market share in certain sectors, such as telecommunications equipment. In this particular area, the US response has been to invoke national security to bar certain companies, such as Huawei, from entering the market, following concerns voiced by the US Committee on Foreign Investment.[63] Although this could be a sign of an increasingly protectionist policy to shield domestic companies, it is also likely that the US is genuinely concerned about the involvement of certain countries in sensitive industries, and China is prominent among these, according to multiple sources.[64] In essence, the US is sacrificing economic openness in the name of national security and there appears to be little that affected companies can do. Another such example, albeit in a different industry, was when Dubai Ports World, a UAE-based company, attempted to take over six major US ports in 2006; facing a national-security response, the company was subsequently forced to walk away from the deal. Because there is little concern at the moment that other countries may switch hardware (micro-processor) or software providers, US academics and officials view the Snowden revelations primarily as an embarrassment to the US' reputation and the practical implications are seen as minor.

One source simply describes *The Guardian* stories as coming from a journalist "with an axe to grind", although he/she acknowledges the difficulty the stories pose for ICANN, headquartered in Los Angeles, California, in making its case internationally for continuing to maintain the Internet architecture. ICANN is specifically responsible for co-ordination of the Internet's unique identifiers, such as Internet Protocol addresses, and the management of top-level domains (TLDs). Because of the global nature of the Internet, many countries wonder why a US non-profit that reports to the US Commerce Department, should determine the world's TLDs. Debate has ensued regarding whether such responsibility should be transferred to the UN, for example, and the Snowden revelations may play a role in strengthening the case to put ICANN under global control. Almost everyone is in agreement that the Snowden leaks hurt long-term US interests, particularly in Europe and China, which have the capability of supplanting American equipment (hardware and software) with their own, or can import from other sources. As mentioned, Europe, for instance, is vowing to build its own cloud platform to ensure that data are stored securely within the continent.

[63] http://moneymorning.com/2008/02/21/china%E2%80%99s-involvement-helps-derail-3com-takeover-on-national-security-concerns/

[64] http://www.nytimes.com/2012/10/09/us/us-panel-calls-huawei-and-zte-national-security-threat.html?_r=0

© The Economist Intelligence Unit Limited 2014

US agencies have been keenly aware of the potential security implications of the cloud for some time. Hence, the country has developed a private government cloud that is entirely hosted within the US. Faced with the issue of massive electronic espionage or enhanced national security, Americans simply opt for the latter, says one source. Although that may be true in large segments of society, the recent Snowden leaks have added a further twist to the situation, as US companies, and some in government, are seeing the downside from a business perspective.

For instance, this poses a problem for US companies trying to do work internationally, with many executives, such as Mark Zuckerberg of Facebook, calling on the US government to increase transparency.[65] According to Reuters, "Zuckerberg said the revelations about US online surveillance had a much bigger impact on users' trust in Facebook than any criticisms related to the company's own privacy policies." Due to such concerns, six of the largest US technology firms—Google, Apple, Microsoft, Facebook, Yahoo and AOL—recently urged Congress to improve surveillance transparency and privacy protection.[66]

There are numerous judicial and political battles ongoing to limit the powers of the NSA. In December 2013, a presidential task force, in a 300-page report, recommended 46 changes to NSA operations, including FISA court reforms and restrictions on spying on foreign allies.[67] In light of this, Mr Obama introduced some limits to NSA spying in a January 17th speech, but he also stopped short of ending its controversial bulk-spying programme.[68] Meanwhile, as mentioned above, Mr Sensenbrenner and Mr Leahy introduced legislation entitled the Freedom Act to limit bulk data collection; Mr Sensenbrenner recently estimated the chances of passage as 50-50.[69] In light of the president's speech, some lawmakers believe the chances are increasing.[70] In a simultaneous effort, lawmakers also introduced a requirement for NSA to do unclassified reporting of how it collects and uses metadata, as a condition of a US$1.1trn spending bill to fund the federal government.[71] This effort should be resolved in February, but could drag on. In summary, efforts to limit NSA powers are ongoing and are likely to continue for some time. As opposed to many other issues in US politics, there is both strong bi-partisan support and opposition (as well as divisive court decisions), leaving the future of NSA legislative support rather unpredictable.

Summary of US policy responses

In stark contrast to Europe, the future direction of US policy is murky. In particular, the final outcome in the tussle between the economic interests of its international companies and the government's national-security interests remains unclear. Now that the battle is public, the stakes are raised and are becoming increasingly influenced by domestic politics. But it is also an issue that has been dealt with in the past. The Federal Bureau of Investigation (FBI) ran a controversial programme called Carnivore that tracked online data and the NSA developed the Clipper chip, which was a hardware-based tool intended to allow law-enforcement officers to be able to access communications. In prior instances, practices were reeled in after public outcry, only to reappear in new forms. It is likely the pattern will repeat itself. Expect new legal limitations, as well as concessions to industry, while the government looks for new ways to meet its security needs. For instance, at least some versions of the proposals outlined above to limit NSA powers should eventually succeed, in order to give the perception of

[65] http://www.reuters.com/article/2013/09/18/net-us-usa-facebook-washington-idUSBRE98H19P20130918

[66] http://www.google.com/hostednews/afp/article/ALeqM5ioRYwa1v8lk01L4N2lOFJZJeUYMA?docId=3a5dde73-fd21-4e56-b98b-c7937f9205a4&hl=en

[67] http://articles.latimes.com/2013/dec/18/nation/la-na-nsa-report-20131219

[68] http://www.theguardian.com/world/2014/jan/17/obama-nsa-reforms-end-storage-americans-call-data

[69] http://www.dw.de/sensenbrenner-freedom-act-ends-bulk-data-collection/a-17403111

[70] http://www.theguardian.com/world/2014/jan/18/nsa-congress-reform-barack-obama-speech

[71] http://www.bloomberg.com/news/2014-01-14/congress-spending-bill-demands-details-about-nsa-spying.html

© The Economist Intelligence Unit Limited 2014

curbing current practices, while retaining what the government sees as adequate intelligence-gathering capabilities.

This means the situation is unlikely to change materially for Huawei in the medium term. Given the probability of compromise in other areas, US officials will be only too keen to maintain control over foreign investment in key ICT infrastructure, and will face little domestic political opposition. To win support in this area will be difficult for Huawei. One potential avenue would be a bottom-up approach, aggressively promoting consumer products in order gradually to build greater brand awareness and acceptance. In respect of the network-infrastructure market, however, the current approach of not prioritising the US is still the best course of action for the time being.

Developed Asia

There is a growing concern in developed Asia that the primary cyber-security threat has shifted from financial motives, such as cyber-crime, to government espionage and infiltration. In particular, cyber-dependent Asian countries, such as Japan and South Korea, have both seen increases in the number of politically motivated threats, in part due to their uneasy relationships with China and North Korea. For instance, the July 2009 co-ordinated distributed denial of service (DDoS) attacks on the US and South Korea, widely believed to originate from North Korea, led Japan to publish its *Information Security Strategy to Protect the Nation* on May 11th 2010. It states:

> The large-scale cyber-attack in the US and South Korea particularly alerted Japan—where many aspects of economic activities and social life are increasingly dependent upon Information and Communication Technology (ICT)—to the fact that a threat to information security could be a threat to national security and require effective crisis management.[72]

Those aligned with US policy in the broader region (primarily Taiwan, South Korea, Japan and Australia) all have new cyber-security strategies under way to deal with emerging threats. Although this has yet to affect ICT trade, Huawei's inability to enter the Australian market, as well as recent US advice to South Korea to reject Huawei (which South Korea ignored), indicates that the US is pressuring its allies to follow its policies. If this is the case, expect more difficulties on the horizon, as the Snowden leaks have revealed Japan's reliance on US support in relation to cyber-security.

Japanese consumers tend to use US-based Internet services, including Facebook and Google. The country's lack of a domestic online service industry puts it at a disadvantage when sharing intelligence with allies. According to one source, who advises the Japanese government, the US and Japan have established a cyber-security working group to share intelligence, but Japan—in part owing to its lack of online services—does not have much to offer US officials, so the relationship is asymmetric. This leads to concern on the part of the US that secrets entrusted to Japan are at risk, making it likely that Japan is facing US pressure to keep Chinese ICT companies from participating in its core infrastructure.

The lack of intelligence-gathering capacity in Japan also stems from a strong belief that the military should not help the private sector gather information and vice versa. This is the primary complaint about China: it is not the number or extent of attacks perceived as originating within the country that is the problem; rather, Japanese officials are primarily concerned about collusion between the public and private sectors, particularly with regard to IP theft.

[72] http://www.nisc.go.jp/eng/pdf/New_Strategy_English.pdf

© The Economist Intelligence Unit Limited 2014

IP theft is a global problem, but is particularly relevant in an Asian context. This is reflected in current negotiations over the Trans-Pacific Partnership (TPP), a free-trade agreement (FTA) with 12 negotiating members. From a business perspective, IP theft in the form of counterfeit ICT products holds two immediate implications: 1) a potential loss of revenue and 2) increased exposure to cyber-threats, as pirated products cannot be properly secured. In part due to the importance of ICT trade, the Association of Southeast Asian Nations (ASEAN) has also called on its members to improve cyber-security, including regional co-operation with Japan and South Korea.[73] In addition, the region benefits from the work of the Asia-Pacific Economic Cooperation (APEC), whose Strategic Plan for 2010-2015 includes, as a priority area, the development of ICT to enhance socio-economic growth, while providing a safe digital environment and improving regional co-operation.[74]

Summary of policy responses in developed Asia

Compared to Europe and the US, cyber-security initiatives in Asia are more fragmented. The region benefits from strong ICT exports and, as a result, several initiatives are under way to improve international cyber-security relations. A common theme among developed countries, however, is a sceptical view of China's cyberspace intentions. Uncertainty persists over the extent to which this and US pressure will affect trade ties beyond Huawei's negative experience in Australia. While South Korea's refusal to bow to US pressure with regard to Huawei bodes well, the fact that the region lacks a clear and co-ordinated policy on cyber-security means that Chinese ICT companies may be subject to sudden changes of course, particularly given the volatile geopolitical situation in East Asia. It seems logical that Huawei should be very proactive in engaging developed Asian markets and building trust.

Emerging markets

From a manufacturing perspective, emerging markets such as China, Mexico, Malaysia and Hungary see massive opportunity to contribute to global ICT chains, as outlined in the previous chapter. For instance, the WTO's 1996 Information Technology Agreement (ITA), in which participating countries removed tariffs on many ICT products, led to a massive increase in trade for developing countries that have more than doubled their share of global exports. This had a huge impact on developing Asian markets in particular, as the continent is now home to almost two-thirds of the world's total exports of US$1.8trn.[75]

Many emerging markets are low on the cyber-dependency curve and are mostly interested in exporting ICT goods. As a result, cyber-security is often of less concern to them. In an ironic twist, stricter cyber-security controls on the goods they produce may also increase costs of production, causing companies to shift production elsewhere. This is said to have happened to Hungary when it improved standards and subsequently saw a loss of exports to competing manufacturing countries, such as Turkey.

However, as emerging markets strive to capture the benefits associated with the information society and move along the digital-development curve, they are also becoming more susceptible to cyber-threats.

The rapid rise in consumer and constituent demand is driven by underlying factors, such as a decreasing cost of access and the increasing availability of mobile digital-communication solutions.

[73] http://www.asean.org/news/asean-statement-communiques/item/joint-media-statement-of-the-12th-asean-telecommunications-and-it-ministers-meeting-and-its-related-meetings-with-dialogue-partners

[74] APEC, Strategic Plan for 2010-2015. http://www.apec.org/Home/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/Telecommunications-and-Information

[75] http://unctad.org/en/pages/InformationNoteDetails.aspx?OriginalVersionID=37&Sitemap_x0020_Taxonomy=1629

© The Economist Intelligence Unit Limited 2014

The ITU's ICT price basket, a measure of affordability, shows an 18% decrease in the price of access globally compared with the previous year, with the fastest price decline in developing countries.

Over the next three-to-five years, therefore, the potential socio-economic impact of cyber-attacks on emerging markets will grow, as these markets begin to catch up with developed countries. Because of rising threats and geopolitical friction, less developed economies in Asia are also looking to enhance their cyber-defences; these include Indonesia, which announced the formation of a unit dedicated to securing military systems and national IT infrastructure in 2012.[76] A recent paper highlighting the concerns of South-East Asian states showed that Chinese cyber-warfare capabilities are considered a significant threat to ASEAN countries, and that a cyber-arms race may be in the making in the region due to lack of political agreement.[77]

China is an exception to the digital-dependency matrix, because countries with similar levels of development are usually not quite so susceptible to politically motivated cyber-threats. There are two plausible explanations why China is different in this regard. Firstly, as opposed to most other countries at its level of digital development, China has already established cyber-espionage and offensive military cyber-capabilities. This leads directly to a cyber-arms race, with other countries, such as the US, seeking to find out more about China's programmes. Secondly, geopolitical friction is increasingly accompanied by cyber-attacks. In the case of China, there are numerous such instances; for example, disagreements with the US, friction with Taiwan, or territorial disputes with other Asian countries.[78]

China also frequently makes newspaper headlines when it comes to cyber-security, over its approach to monitoring and censoring its own population and online environment. For example, there was a media frenzy after Google announced in January 2010 that it would relocate its Chinese-based operations to Hong Kong, after it refused to comply with censorship regulations on its Chinese version, Google.cn.[79]

While China's central government may be very cyber-aware, China's online world at large is less well-prepared to face security challenges. One security analyst dubbed China a "glass dragon" because of its offensive intent, but woeful cyber-defence.[80] An independent assessment of cyber-preparedness around the world conducted by the Security and Defense Agenda, a European think-tank, rated China just 3 out of 5, where the most developed countries scored 4 or more, and India scored 2.5. In 2009, the government said 1m Chinese IP addresses were controlled by other countries.[81] In 2011, CNCERT/CC reported that 8.9m hosts are controlled from overseas, led by 23% from Japan, 20% from the US and 7% from South Korea. In 2012, the American Chamber of Commerce in China (AmCham China) and the US Information Technology Office (USITO) co-hosted a panel focusing on cyber-security as part of AmCham China's 2012 Business Climate Survey event series. The gathering noted China's increasing reliance on the Internet, in particular corporate usage of cloud-computing platforms for which information security is a must, leading to further concerns regarding the protection of data within the country.[82] The revelations of the NSA's HALLUXWATER and HEADWATER "backdoors" into Huawei hardware should further highlight fears in this area, not only within the country, but also for Huawei's foreign customers. Although the information is damaging to the US, it simultaneously exposes the potential vulnerabilities of Huawei's products.

[76] http://www.janes.com/products/janes/defence-security-report.aspx?id=1065973890

[77] http://icaps.nsysu.edu.tw/esfiles/122/1122/img/1421/40.pdf

[78] http://www.voanews.com/content/in-china-hacker-allegations-seen-as-omen-opportunity/1608173.html

[79] The Economist Intelligence Unit, *China Country Commerce 2013*.

[80] http://threatpost.com/en_us/blogs/glass-dragon-chinas-cyber-offense-obscures-woeful-defense-042711

[81] http://english.gov.cn/2010-06/08/content_1622956.htm

[82] http://www.amchamchina.org/article/9514

© The Economist Intelligence Unit Limited 2014

Besides new technology trends, a particular challenge in China also comes from a lack of IPR protection, such as counterfeit products and even entire fake stores purporting to be outlets for major brands.[83] According to estimates from the US International Trade Commission (ITC), counterfeit goods in China cost US businesses alone an estimated US$48bn in 2009.[84] This is more than the reported financial losses in China from cyber-crime, which, in 2012 were estimated at US$46bn, according to the Business Software Alliance (BSA) and International Data Corp.

This high volume of pirated software—which does not come with appropriate security updates—also makes China particularly vulnerable to cyber-crime. For example, according to the threat exposure rate (TER) in the Security Threat Report 2013 from Sophos, a security firm, 21% of Chinese PCs experienced a malware attack, whether successful or failed, over a three-month period, which is the second-highest rate in the world, trailing only Indonesia, at 24% (this can be compared with Norway and Sweden at 2% and 3%, respectively).[85]

As in many emerging markets, which tend to do technological leap-frogging, China is also particularly reliant on mobile devices and vulnerable to the threats that come with them. According to a report released in January 2013, 420m Chinese accessed the Internet through their mobile devices during 2012, up by 18% from a year earlier.[86] China has now overtaken the US as the largest market for smart phones. In 2011, CNCERT/CC reported 6,249 new malware designed specifically to target mobile devices, a doubling of the year-earlier figure.

China is particularly vulnerable to trade implications stemming from changes to other countries' cyber-security policies, because of its domestic reliance on ICT exports. In 2004, for example, China overtook the US as the world's largest exporter of ICT goods.[87] There is a growing risk that the allegations and evidence about cyber-espionage operations could affect US-China trade ties, a point also made by a Brookings Institution report from 2012.[88]

There are also stories beyond the headlines: China will in fact become less reliant on ICT exports to developed countries, in particular the US. Firstly, as a February 2013 trade forecast from HSBC notes, although China is gradually moving to higher-value-added sectors, industrial machinery is forecast to overtake ICT as the key export driver.[89] The contribution of ICT equipment to overall growth in merchandise exports will decrease from 25% in the near term, to 18% in the years 2021-30, according to this analysis. Secondly, most growth in export demand is expected to come from other emerging markets, primarily Asian countries such as Vietnam and India. Behind the dynamic intra-Asian trade, Chinese exports are also forecast to increase to the Middle East and North Africa, albeit from a low base, in large part due to friendly government relations and a lack of domestic alternatives in these places. Exports to the US, meanwhile, as a percentage share of the overall total, are currently estimated at 17.2% in 2012, down from its peak of 21.5% in 2002.[90]

Although China is frequently cited in the West as a particular concern, the picture is more nuanced globally. According to one report, for instance, Indonesia has overtaken China as the country from which most cyber-attacks emanate.[91] Perceptions of China also vary according to political alignment; according to a Russian source, from the perspective of Russia the US looms as a far bigger cyber-security concern than China.

[83] http://www.bbc.co.uk/news/technology-14503724

[84] http://www.reuters.com/article/2011/07/21/us-china-apple-fake-idUSTRE76K1SU20110721

[85] http://www.sophos.com/medialibrary/PDFs/other/SophosSecurityThreatReport2013.pdf

[86] http://www1.cnnic.cn/IDR/BasicData/

[87] http://www.oecd.org/general/chinaovertakesusasworldsleadingexporterofinformationtechnologygoods.htm

[88] http://www.brookings.edu/research/papers/2012/02/23-cybersecurity-china-us-singer-lieberthal

[89] https://globalconnections.hsbc.com/united-kingdom/en/tools-data/trade-forecasts/cn

[90] Economist Intelligence Unit data.

[91] http://www.thejakartaglobe.com/news/hackers-paradise-or-host-nation-indonesian-officials-weigh-cyber-threat/

Besides US espionage, with which Russia is familiar from the cold war decades, the country's primary concern remains software. Russia's attempt to produce hardware was unsuccessful, owing to the complexity of supply chains and high costs; hence, it tends to import end products. Although initial attempts to nurture domestic software and Internet industries were also difficult, the government has made it clear that it intends to develop such products (similar to China, which still intends to develop its own operating system, OS, even after the initial failure of Red Flag). Because of Mr Snowden's taking refuge there, Russia has also been in the spotlight internationally. Although, according to one source, the average Russian probably does not care much, this is seen as a political and diplomatic win in geopolitics, and underscores the increasing importance of the politics of cyber-security more broadly.

Summary of policy responses in emerging markets

Cyber-security in many emerging markets has only recently become an important political issue, as they start to catch up from a relatively low base level of digital development—and encounter the challenges that come along with digital dependency. In response, countries such as Russia, India and Indonesia all have new cyber-security strategies under way, or are refining them to account for recent developments. Depending on their political alliances, the Snowden revelations or geopolitical friction with China are key factors propelling emerging markets to improve their national cyber-security. In general, efforts focus on securing ICT infrastructure.

Huawei would benefit from targeting other emerging markets with its services, particularly those in countries where the Chinese government has strong contacts and influence. However, until the perception of China as a potential geopolitical threat—or, at least, that of government and corporate collusion—changes, there appears little Huawei can do to improve its fortunes in respect of network infrastructure in certain emerging markets. The more pertinent question is what Huawei can do to help improve its overall image abroad and its recent moves towards greater transparency and support for international cyber-security initiatives are certainly good ways to go. One particular area of interest might be the current lack of IP protection in software, in which Huawei could emerge as a leader by establishing international co-operation and thereby build a strong reputation, at least among consumers. There is widespread mistrust of Russian companies, yet, globally, consumers have taken to Kaspersky Lab's software security. Huawei could similarly provide a bottom-up approach by targeting this segment first. In particular, given Huawei's business offering, a mobile-phone-security solution may not only improve its image, but also make business sense.

Conclusions

Given the global increase in cyber-dependency, combined with a lack of comprehensive international agreements on cyber-security, it is likely that cyber-threats will continue to affect the global economy, as well as international politics, in a number of ways. Developments in this regard are rapid, as illustrated by the frequent Snowden leaks, but one thing is certain: trust and norms are lacking, while dependency on ICT is growing, and with a rise in reliance comes a rise in risk. The extent of the cyber-security challenge remains to be seen, but, if history can serve as a guide, the task will also become greater, particularly as countries such as China progress towards an information society.

© The Economist Intelligence Unit Limited 2014

Table 2: The Patriot Act and other policies: too far?

Country	Name	Year
UK	Regulation of Investigatory Powers Act	2000
US	USA PATRIOT Act	2001
Canada	Anti-Terrorism Act	2001
Australia	Intelligence Services Act	2001
Netherlands	Intelligence and Security Services Act	2002
Sweden	Changes to defence intelligence activities (commonly referred to as FRA law)	2006/07
Indonesia	Regulation 82 of 2012 on Electronic System and Transaction Operation	2012
Vietnam	Decree on Management, Provision, and Use of Internet Services and Information Content Online (Decree 72/2013-ND-CP)	2013

By taking into account various levels of digital development, one can estimate the global, regional, and country-specific impact that cyber-threats have today and will have in the future. For instance, emerging markets, such as Indonesia and Vietnam, are now following in the footsteps of many developed countries by introducing various forms of monitoring. In turn, this leads to a better understanding of the potential geopolitical sticking points associated with cyber-security at various stages as countries progress.

For example, the cyber-domain may be viewed as "borderless", but there are borders in cyberspace too, as the online environment is dependent on physical infrastructure, operated by various business entities. It is an important point because, as demonstrated in the recent uprisings in Egypt, a country's government does have some ability to shut down the Internet. The US has similarly considered a "kill switch", which would enable it to stop incoming traffic in case of attack.

Policy always struggles to keep pace with the march of technology, and the world is still formulating its political and policy responses to cyber-threats. Some key issues and trends to watch are outlined below.

- **The Snowden impact:** Although cited as an embarrassment to the US government, the impact within the country is viewed as relatively minor according to sources—and not even the Republican opposition has exploited the issue to any great extent.

Experts around the world are also unsurprised at the revelations. "Spying is simply what spy agencies do," is one wry assessment of the non-revelation from an expert commentator. Another says that all governments try to infiltrate or regulate the Internet somehow (although with varying degrees of success). The most shocking aspects of the revelations are the methods and scope of the US efforts, in particular the co-operation with commercial entities and the targeting of allies and other world leaders, as well as the tactics used both by US and UK authorities to try to suppress the leaks.

But almost everyone else seems in agreement that the case hurt long-term US interests, particularly in advanced ICT markets such as Europe and China, which have the ability to develop on their own or with help from other countries, thereby circumventing current US dominance in certain ICT segments.

© The Economist Intelligence Unit Limited 2014

Therefore, the Snowden episode will likely strengthen the case for localisation or regionalisation of ICT standards and data storage.

- **Espionage and trust:** Although it may be obvious that intelligence agencies do what they can to gather information, when their actions are seen as disproportionate to the potential risk, it affects trust, particularly among supposed allies, which in turn affects the prospects for greater international co-operation. In particular, the revelations by Mr Snowden have caused uproar across much of the world. For example, in Mexico, Antonio Meade, the foreign minister, called the spying allegations there “an abuse of trust between partners”.[92] Sources also cite the speech by Dilma Rousseff, the Brazilian president, at a recent UN meeting as evidence of broken trust and the difficulties in restoring it, especially as she also cancelled a state visit to the US because of the Snowden revelations.

There is a feeling that the only way to deal with the issue is to restore trust through transparency, although no government has taken any meaningful steps in this regard, in part because there are no international agreements regarding politically motivated cyber-attacks. Making the case for global co-operation, therefore, becomes ever more difficult and a key question will be whether ICANN can retain its strong hold over Internet management.

- **Emerging technologies and localisation:** Although the temptation is great to replace foreign ICT systems with domestic ones, most countries do not have the capability. For those that do, it can be costly and inefficient. However, many governments see advantages to promoting domestic capacity in emerging technologies, such as cloud computing. Cloud computing not only brings with it complex issues, such as extra-territorial investigatory powers with regard to internationally stored data, but can also simplify the process of localisation, making protectionist policies both more appealing and easier to implement. The US government already has its own cloud, Europe is building one and other countries are certainly considering it in order to avoid data travelling through unknown channels.

Businesses themselves have little say in the grand scheme of cyber-security, as they must adhere to national regulations, some of which are increasingly dictated by national-security concerns or protectionism, rather than pragmatism. The problem is compounded by the lack of international forums to establish global norms. Without strong institutions, there is the strong likelihood of an increasingly complex cyberspace future, driven by the usual great-power politics.

[92] http://www.economist.com/news/international/21588890-foreign-alarm-about-american-spying-mounting-sound-and-fury-do-not-always-match-0

Chapter Three: Trade and the ICT sector

Overview

This chapter addresses the various multilateral and mega-regional trade agreements currently under discussion that will affect global ICT supply chains. It discusses the challenges facing negotiators, particularly in light of Edward Snowden's revelations, with regard to establishing rules on key issues of the day, including cross-border data flows, data localisation and e-commerce. Finally, it looks at the likely future of trade, presenting best-, worst- and middle-case scenarios for Huawei in terms of the impact on supply chains.

Introduction

Over the past 15 years, cross-border trade in ICT goods and services has increased significantly, much faster even than global trade as a whole. This is due, among other factors, to advances in technology and the spread of the Internet, rising demand for these products in developed and developing countries alike, and company-level strategies aimed at exploiting wage differentials between countries. Underpinning all of this, however, was the reduction in global-trade barriers that resulted, firstly, from the completion of the so-called Uruguay Round of multilateral trade talks, which came into effect in 1995, and thereafter from the Information Technology Agreement (ITA) and the ITA's expansion through the accession of various countries, particularly China. Without these agreements, there would be far less trade in ICT products than there is today; supply chains would still extend beyond borders, but they would be much shorter and, as a result, technological advances would be fewer and products more expensive overall.

The preceding sections have shown how the ICT sector itself is changing and how, relatively recently, the politics surrounding the sector have changed, not for the better and perhaps irrevocably. The trading system is also undergoing changes. The past decade has demonstrated that expansive, multilateral trade deals are no longer possible, at least not on the scale they once were. Even less ambitious deals, such as the one just completed at the Bali ministerial meeting, are proving incredibly difficult to pull off. This is leading to a situation where, in most instances, the WTO has become more of a "guardian of the rules",[93] rather than a forum for achieving greater liberalisation. As will be discussed, an updated ITA—or ITA 2—is one of the few important exceptions in this area, but its completion is far from assured.

Meanwhile, as global trade talks have careened from failure to failure (or minor successes, as in the case of the Bali agreement), countries have opted to pursue trade liberalisation by other means, namely in the form of bilateral and regional free-trade agreements (FTAs). After more than a decade of small and medium-sized agreements, efforts are now underway to complete a series of "mega-regionals," such as the US-led Trans-Pacific Partnership (TPP), the US-EU agreement called the Trans-Atlantic Trade and Investment Partnership (TTIP), and the China-led Regional Comprehensive

[93] Interview with external expert. We also made this point in our Brave New World report to Huawei in 2012.

© The Economist Intelligence Unit Limited 2014

Economic Partnership (RCEP), which is based on the ASEAN + 6 framework. To date, the smaller FTAs have likely had negligible impact on global ICT supply chains, but these much larger agreements could provide either economic incentives for ICT firms to restructure their supply chains or contain rules and standards that compel them to do so.

The overriding problem confronting global trade in ICT products, however, sits at the intersection of cyber-security, geopolitics and trust. Cyber-security and geopolitics, while always present in the last two decades or so, have never been as prominent as they have been over the past 12-18 months and that is directly a product of a deepening trust deficit. As a result, there are now increasing attempts by governments to restrict cross-border data flows, to create national clouds, and to inhibit e-commerce. All of these policies, and others like them, could function together—and even in isolation—to disrupt international trade and, consequently, global supply chains.

A lack of trust presents a major problem for trade and trade relations. Trust is a precondition for trade, not a product of it, although trade between nations can help to improve overall relations. When countries accede to the WTO or sign FTAs with each other, a certain level of trust must already be present. Of course, enforceable rules with real penalties are written into these agreements because that trust is not unconditional. But, if trust is eroded, then trade can go along with it. This is especially true in sensitive industries, like ICT.

The WTO and cyber-security

In The Economist Intelligence Unit's 2012 *Brave New World report* for Huawei on megatrends that are going to shape the global economy and geopolitics in the coming decade, we spent a chapter laying out various scenarios for the world trading system. The most likely scenario then—the move towards greater regionalisation—remains the most likely scenario a year on. All of the reasons we cited then are still relevant today, including the global power shift, a mismatch in levels of ambition, and the difficulties surrounding the remaining issues, such as agriculture and non-tariff barriers.

The Economist Intelligence Unit's scenario for the WTO was that it would remain relevant as a "guardian of existing rules", while achieving piecemeal liberalisation through a series of plurilateral agreements, which are essentially side agreements among coalitions of countries willing to move forward on select issues. When it comes to cyber-security and global ICT supply chains, the WTO has a particularly thorny rule to guard, the National Security Exception (NSE) contained in General Agreement on Tariffs and Trade (GATT) Article 21. In the *Brave New World report*, we explained that the two biggest threats posed to the WTO as a guardian of existing rules were, firstly, that the Dispute Settlement Body (DSB) would become overburdened as more countries shrugged off the "glasshouses constraint";[94] secondly, a major global power would ignore a DSB decision that it could not accept for its own domestic political reasons. Here, we look at the NSE in the context of those threats and the rise of cyber-security.

The National Security Exception(s): Ticking time-bomb?

One of the areas where cyber-security, trade and global ICT supply chains may one day come into serious conflict at the WTO is over the usage, interpretation and adherence to the NSE contained in Article 21 of the GATT. The most relevant parts of the article are as follows:

[94] This is a play on the English phrase, "People in glass houses shouldn't throw stones." Because so many countries are believed to have violated WTO law in one way or another during the global financial crisis, there were few countries willing to take disputes to the WTO for fear of counter-suits. With more cases being brought in 2012, this constraint appeared to be loosening.

> Nothing in this agreement shall be construed
>
> (a) To require any contracting party to furnish any information the disclosure of which it considers contrary to its essential security interests; or
>
> (b) To prevent any contracting party from taking any actions which it considers necessary for the protection of its essential security interests
>
> (i) Relating to fissionable materials or the materials from which they are derived;
>
> (ii) Relating to traffic in arms, ammunition, and the implements of war and to such traffic in other goods and materials as is carried on directly or indirectly for the purpose of supplying a military establishment;
>
> (iii) Taken in time of war or other emergency in international relations; or
>
> (c) To prevent any contracting party from taking any action in pursuance of its obligations under the United Nations Charter for the maintenance of international peace and security.

This article, and similarly worded provisions elsewhere, have been invoked a number of times over the years, but in none of these instances has a challenge resulted in a formal ruling from the DSB.[95] Some argue that this is in fact one of the article's strong suits: it can force parties to a dispute to seek out informal solutions, rather than adjudication.[96]

Others argue, however, that the NSE is something of a "ticking time-bomb" under the WTO.[97] If a country invokes the NSE, essentially no one can stop that country from doing what it wants to do, since the exception is "self-judging".[98] That, so far, there has not been any particularly egregious abuse of the NSE is evidence of both widespread restraint and trust, which together serve as the foundation of the trading system as a whole. The understanding is, therefore, that no country will actually invoke it unless it is *necessary*, as the language of the article stipulates. But there is not a lot of certainty around how much longer this will hold true, hence the ticking-time-bomb reference.

Everyone does agree that, both overall and with specific reference to cyber-security, chances are slim that there will ever be a serious challenge to the NSE. The simple reason for this is that any challenge that makes it to adjudication at the DSB will likely result in the defendant ignoring the decision if the DSB rules against it. This would "break the system", according to one interviewee, since the WTO is now only really as important as its ability to maintain and uphold the rules. Insofar as invocations of the NSE impact Huawei's business globally, there is really nothing it—or the Chinese government—can do about it.

In terms of plurilaterals, negotiations are now underway to conclude an updating of the original ITA, or ITA 2 as it is commonly called. The original ITA was almost singularly responsible for the expansion of global ICT supply chains and is often referred to as the greatest success at the WTO since the Uruguay Round. Firstly, the original ITA, how it was negotiated and how it expanded through accession over the past 16 years will be examined. Then, we will turn to the current negotiations for ITA 2, the issues facing those negotiations, and the potential impact if an agreement is not reached.

[95] Arguably the highest-profile case to date is the European Community's challenge of US sanctions against Cuba in 1996. The dispute was settled by other means.

[96] External interview.

[97] External interview.

[98] See, for example, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2079608

Information Technology Agreement: Past, present and future?

Getting to the start

In the early 1990s, as noted in the first chapter, private and public-sector actors alike began to realise the enormous potential of the rapid growth in, and globalisation of, the ICT sector for unleashing greater economic growth across the globe. Although the Uruguay Round agreement that created the WTO had just been completed, the agreement did not cover ICT products to a great degree, a fact that the private sector, especially, saw as a problem that needed to be addressed.

And it would indeed be the private sector, through various country-level and international industry associations, that pushed for what would eventually become the ITA. Politicians and bureaucrats, for their part, were weary of pursuing another difficult round of negotiations so soon after the Uruguay Round. The EU and Japan, in particular, hesitated, with both claiming that the concessions they had just made were "big enough to digest" for the time being. But, following lobbying from the private sector—especially large private-sector companies that did not have strong loyalties to any one country—as well as discussions among the leading countries, a decision was made to move ahead.[99]

The agreement itself

From the start, the ITA was designed as primarily a market-access agreement, meaning that it would deal with tariffs and leave the majority of non-tariff barriers to later work. However, even dealing with tariffs schedules—generally considered easier to negotiate than non-tariff barriers—proved difficult. Tariffs on ICT products were not that high to begin with; in fact, at least compared to other industries, they were considered sensitive. Average bound tariffs in the seven categories of the ICT products covered by the agreement were around 15% and average applied tariffs were between 3% and 6%. But, as the experts interviewed for this study continually pointed out, with margins so thin in the sector, phasing out these tariffs were what made it possible for the globalisation of ICT supply chains to commence.

Before getting to tariff reduction and elimination, however, agreement needed to be reached on which products would actually be included in the ITA. For the purposes and scope of this report, the range of products covered is less noteworthy than is the framework that was established to incorporate additional products over time. The annex to the agreement contains a provision that requires participants to "meet periodically" to review and expand the product coverage. These meetings began in 1998, the year after the ITA was implemented and were then—and still are now—led by the ITA committee.

For the praise that has been heaped on the ITA over the years (see box below on trade expansion), its main failing has been that, although member countries have met periodically as required, they had not added a single product to the original list since 1997. By way of comparison, a similar agreement covering pharmaceuticals—an industry as much driven by innovation and product turnover as the ICT sector—has been expanded three times over roughly the same period; the pharmaceuticals industry also shares with the ICT sector the dominance of a number of firms with weak or no loyalties to their home governments.

[99] For a history of the ITA negotiations, see http://www.wto.org/english/res_e/publications_e/ita15years_2012full_e.pdf

Membership expansion

Although the ITA has not expanded in terms of product coverage, it has expanded by other means, namely, the accession of new member countries. When the ITA first came into effect, there were 28 members, representing 42 countries in total. That number now stands at 48 members, representing 75 countries in total, with Russia being the latest country to join. As of the last full accounting, ITA members are responsible for 96% of global ICT exports and 90% of total imports.[100]

There have been four basic avenues to ITA accession. They are:

- countries that join of their own volition, such as Egypt and Kuwait;
- countries that join to satisfy a condition in their free-trade agreement (FTA) with the US, such as Honduras and Nicaragua;
- countries that join because of EU enlargement, which requires new members to join the ITA;
- and countries that join as a requirement of the WTO-accession protocols, such as China and Vietnam.

At this point, only five major countries have not joined the ITA: Argentina, Brazil, Chile, Mexico and South Africa. These countries are often labelled "free riders" because, unlike the Agreement on Government Procurement, the ITA is "multilateralised", meaning that market access is extended on a most-favoured-nation basis, even to countries who are not signatories to the agreement. Of these five, Chile will likely be required to accede to the ITA, old and new, as part of its participation in the Trans-Pacific Partnership (TPP). It is uncertain at time of writing whether the other four countries will join the ITA.

The Future: ITA 2 negotiations

The future of global ICT supply chains will be influenced greatly—but certainly not solely—by the outcome of the negotiations aimed at updating the ITA. Negotiations looked to be heading towards a conclusion in November 2013 when the members met in Geneva for what was expected to be one of the final rounds of talks. However, China surprised everyone by sending negotiators to that meeting without any real licence to negotiate, and with a long list of products that their government wanted excluded from the final agreement.

Although that list has not been made public, it is believed that, besides base stations and next-generation multi-component semiconductors, most of the products on it were either lower-value-added parts and components or more consumer-oriented electronics. In the course of our discussions with international experts, two specific points came up with reference to the Chinese list of exclusions. The first was that the products that China identified for exclusion are products for which it currently enjoys a massive trade surplus; in other words, where exports far exceed imports. They are also products that can easily be manufactured in another Asian country with low-cost labour, such as Laos and Cambodia. Should China eliminate tariffs on these products, it is likely that production would shift out of China, reducing or eliminating the country's surplus in these products. Keeping the tariffs would also prevent or delay countries like Laos and Cambodia from starting their climb up the ICT value chain.

[100] Ibid. It should be noted that one condition of the ITA is that it has achieved "critical mass" in terms of trade coverage, which was set at 90% of global trade.

The second point made was that the composition of the list seemed to suggest that China's economic planning involved Chinese companies staying at the low end of the value chain longer than had been expected by industry experts. The problem highlighted here was that international trade negotiations cannot be conducted in good faith with countries that are attempting to negotiate on the basis of a 5-10-year plan for their domestic economy, especially not negotiations covering a sector as dynamic as ICT. This sort of negotiating behaviour was accepted to the extent that it was when China acceded to the WTO only because the US, especially, believed that China's entrance into the WTO would lead ultimately to political liberalisation, among other benefits. Now that that outcome is either much further off than expected, or not in the offing at all, countries are going to be less tolerant of China's approach to trade negotiations.

Most, however, do expect that China will compromise in the end and the agreement will be concluded. They expect this because China—and, of course, by extension, Huawei—has gained the most of any single country from the current ITA and stands to lose the most if a new ITA does not go forward.[101] Why? Without a new ITA, China is going to be denied most of the new market access that does occur, which will be allotted at the level of regional FTAs. China is party to one of the big three agreements, RCEP, but not the other two, TPP and TTIP, which together account for around 60% of global ICT trade.

The other, related point worth noting here is that, maybe more than any other country, China needs the WTO. As one expert put it, "The WTO is essentially one big FTA with China right now. Most of the rest of the world views China as a hard-core mercantilist, hard-core realist country and therefore one that is very difficult to negotiate with." If the ITA 2 fails, or if the WTO's legitimacy begins to be eroded, China could suffer the most because major countries do not want to negotiate with it outside of the WTO.

What if the ITA does not happen?

Since the confidence of negotiators or interested parties does not always translate into success, it is important to consider, briefly, a scenario in which the ITA 2 is not completed.

As discussed above, although global ICT trade has increased and supply chains have advanced over time, the original ITA is severely out-of-date and, with the exception of a small number of countries, there is little room for expansion through new membership (at least in the short-to-medium term). If an agreement is not reached, according to the interviews conducted for this report, blame is likely to be placed with the Chinese government. While most major ITA members have brought to the negotiations very short lists of products for exclusion, the 100+ products allegedly on China's list suggests a long way to go, perhaps too long.

In the absence of an updated ITA, while market access for products under the initial ITA will remain the same, any new market access, and new product coverage, will need to be achieved using alternative approaches. For an ITA to be completed, it must reach a "critical mass" of 90% of global trade in the products covered. Given China's central position in global ICT supply chains, which results in sizable exports and imports, there is no way an updated ITA can be completed without it. In other words, the other members cannot go forward with an ITA 2 without China.

[101] Interview with external expert.

© The Economist Intelligence Unit Limited 2014

The mundane result of this, according to a Western interviewee supportive of China's participation in the ITA and dismissive of the US treatment of Chinese ICT firms, is that global trade will simply be less efficient. But the interviewee was also quick to point out that, if the TPP and TTIP do both happen, more than 60% of global ICT will still be covered. This would not be an optimal result by any measure, but it may be one that TPP and TTIP member countries are willing to accept if China proves stubborn over its long list of ITA exclusions.

For Chinese firms, this would leave only new and improved market access to countries in the RCEP, provided that agreement is even completed and assuming that China will not be able to join either TTP or TTIP (which we still believe is highly unlikely in the short-to-medium term, mainly for political reasons and due to the nature of China's economic system). The Association of Southeast Asian Nations (ASEAN) is a fast-growing source of end-demand for ICT products and has the potential to integrate more fully into global ICT supply chains. Plus, the presences of India and Japan in RCEP increase its appeal, although it does not make up for being outside of the TTP and TTIP.

The mega-regionals: TPP, TTIP and RCEP

As a transition to discussion of the so-called mega-regional FTAs, it is important to emphasize that the market-access provisions in the current ITA take precedence over any market-access provisions contained in bilateral and regional FTAs and so, too, would any provisions contained in an ITA 2 take precedence over those contained in TTP, TTIP and RCEP. In fact, most trade agreements do not address ICT market access for that reason and, instead, if one or more countries party to the agreement is not already an ITA member, simply require that country or countries to accede to the ITA.

When it comes to the ICT sector, some bilateral and regional FTAs, therefore, concentrate on related issues that are not necessarily covered by the ITA or not covered well by the WTO. This is especially true of those agreements led by the US, such as the TPP. The US often refers to these issues—along with others covering the environment and IP—collectively, as "21st-century issues". In the main, the disciplines relevant to the ICT sector and ICT trade include cross-border data flows, data localisation, and e-commerce. The way these are handled in the TTP, TTIP and, perhaps to a lesser extent, RCEP, is likely to have an influence on how they are handled elsewhere, as long as there is no new WTO agreement that provides similar coverage.

One problem for any forward-looking analysis of the impact that these agreements may have on ICT supply chains is that, since the agreements are not yet complete, it is not known exactly how the issues will be handled. The TPP is the furthest along of the three mega-regionals, so there is slightly more information to base analysis on; additionally, it is assumed the TPP will be modelled, in part, on the South Korea-US FTA (KORUS), for which the final text is publicly available. TTIP and RCEP are both in the very early stages and, consequently, little is known other than that, in the TTIP, the Snowden revelations have put considerable strain on certain aspects of the negotiations.

What follows will therefore be based mostly on the TPP. As a general rule, however, we can expect the TPP to be the most extensive, although, as will be shown, the US is receiving far more push-back than expected. The TTIP is likely to be less extensive than the TPP, not only due to the Snowden revelations, but also because the EU as a whole will have more leverage than do the smaller TPP

© The Economist Intelligence Unit Limited 2014

countries. Finally, in the case of RCEP, and as discussed in the Brave New World report last year, since trade agreements in the Asian region tend to be more about codifying existing rules than creating new ones, we expect much lower levels of ambition.

E-commerce

As would be expected, the US is pushing for the most liberalisation possible in this area. It wants, above all, goods and services delivered electronically to be given the same treatment as those that are delivered physically (that is, non-discrimination).

But this will encompass more than just treatment. The US sector, for example, is adamant that the TPP allow e-commerce to be subject to the agreement's dispute-settlement provisions, a stipulation that faces considerable opposition from developed and developing-country members alike.[102] One US-sector representative interviewed for this report said that failure to include dispute settlement for e-commerce was a "total no go" for the companies he represents, as it would provide an opening for other countries to carve "big chunks" out of market access.

In the end, our view is that some countries, such as Australia and New Zealand, will barter away their objections here for greater market access elsewhere, specifically pertaining to agriculture. The other countries that are allegedly opposed to dispute-settlement jurisdiction over e-commerce, including Singapore and Malaysia, can probably be brought around through a combination of coercion and concessions in other areas.

The US will face a much more difficult test on this in the TTIP negotiations, mainly because of France's unmoving position when it comes to the "cultural exception".

Cross-border data flows

There is considerable overlap between this issue and e-commerce, but cross-border data flows are not limited in purpose just to those that serve e-commerce.

The KORUS FTA was actually the first FTA—the first international treaty, in fact—to include specific, binding rules on cross-border data flows.[103] We suspect, however, that the US is pushing for more stringent commitments than are contained in KORUS, as the KORUS language affords considerable leeway, requiring only that the two countries "endeavor to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders".

We already know that a number of TPP member countries have pushed back against US efforts in this area, not least Australia and New Zealand, both of which voiced serious concerns about how this would clash with their own domestic privacy laws and rights. In the end, the US will likely need to relent on this issue in order to get the agreement concluded and, therefore, language closer to KORUS than the US may have wanted is likely to be used.

While privacy and data protection are key, they are not the only considerations when it comes to cross-border data flows. National security, and, consequently cyber-security, is at least the equal of privacy and data protection in this regard and, in the eyes of governments, perhaps even exceeds it as a priority. A number of countries—most prominently, Brazil—are using the combination of both

[102] See, for example, the leaked memo providing an overview of country negotiating positions prior to the 20th round of negotiations held in Salt Lake City, US, in November. Available at: http://wikileaks.org/IMG/pdf/tpp-salt-lake-positions.pdf

[103] Joshua Meltzer, The Internet, cross-border data flows, and international trade, Center for Technology Innovation at Brookings, 2013.

privacy and national security to justify policies that require "data localisation". Few, if any, of the TPP members have attempted to go this far with their policies, although restrictions of varying levels are in place. But that does not mean they will not make the attempt, which is why the US favours stronger language, and is reportedly attempting to have local- server requirements be subject to a "necessity test" in the TPP.

Interestingly, most experts—including all of those interviewed for this report—are sceptical, if not outright dismissive, of the efficacy of data localisation as a means by which to ensure either national cyber-security or data privacy. In some of these cases, it might just be that certain governments lack a nuanced understanding of cyber-security and, consequently, these efforts represent an over-reaction. In others, there is an unmistakable element of protectionism. But the problem for the US, according to one trade expert, is that the Snowden revelations have seriously damaged any moral authority it might have otherwise been able to use in negotiating this issue.

Rules of origin[104]

Although their coverage is broad, rules of origin (ROOs) have tended to be aimed at a small number of sectors, including textiles and apparel, automotive products, and, more recently, foodstuffs. The variety of calculations that are applied to determine ROOs can range from relatively straightforward to incredibly complex—so complex and cumbersome that they, in effect, function as higher barriers to trade than tariffs in certain instances. Specifically in the ICT sector, one interviewee recounted the story of the top trade lawyer at an ICT company, who spent six months working solely to determine the origin of a single product. There are so many components, and so many rules governing those components, that, for a company with an inventory of 10,000 products, it can strain economic logic to comply with ROOs for all products.

Bilateral FTAs offer almost no compelling reason for ICT firms to consider reconfiguring their supply chains, because only two countries are involved. That may change with the mega-regionals, and especially in the case of the TPP, which includes a number of countries in Asia, the hub for most global supply chains. As one expert put it, over time and in light of the differing tariffs and rules and standards, companies are going to look harder at the ways in which they can locate a sufficient percentage of their supply chain within these regional trade agreements, in order to satisfy ROOs.

Conclusions

There is still time

To the extent that any or all of these agreements will ultimately affect ICT supply chains—and, again, without knowing the final exact provisions and disciplines, it is hard to know their precise impact—there is still time before they come into effect, perhaps even a significant amount of time. This fact gets lost in almost all discussions of these agreements, especially in the press, which seems to assume that, once the agreements are signed, all the hard work is over.

Beginning with the ITA, as noted above, negotiations have been disrupted by Chinese demands for extensive product exclusions. Assuming it will take at least another 2-3 rounds of talks before an

[104] Although not necessarily a 21st-century issue like those detailed above, we include it here because it has the potential to affect ICT supply chains, especially in the context of mega-regional agreements.

© The Economist Intelligence Unit Limited 2014

agreement can be reached, it could be another 6-8 months, if not longer, before ITA 2 is concluded. After that, the agreement will need to pass through two-thirds of member-country legislatures before it can enter into force, adding 3-6 more months. If roughly correct, that would take us into mid-2015. And even when the ITA 2 does enter into force, tariff-reduction schedules are likely to be such that the impact on ICT supply chains is not felt until 2017 or even beyond.

The TPP, which is much further along than both TTIP and RCEP, is still likely at least two years away from actual implementation. Negotiations were supposed to be completed by the end of 2013 but this was not met. Talks will continue into 2014 and may not be completed until mid-year. If they are completed earlier, that will be a strong sign that some of the more ambitious aspects of the agreement, including those that cover ICT and are, therefore, relevant to Huawei, have been softened for the sake of completion.

Figure 5: Prospective timelines of ITA, TPP, TTIP, and RCEP

■ Negotiatic □ Legislation 🟥 In effect

	Q1 2014	Q2 2014	Q3 2014	Q4 2014	Q1 2015	Q2 2015	Q3 2015	Q4 2015	Q1 2016	Q2 2016	Q3 2016	Q4 2016	Q1 2017	Q2 2017	Q3 2017
TPP	■	■	■	■	□	□	🟥								
TTIP	■	■	■	■	■	■	■	■	□	□	🟥				
RCEP	■	■	■	■	■	■	■	■	■	■	■	■	□	□	🟥
ITA	■	■	■	■	□	□	🟥								

Source: The Economist Intelligence Unit.

However, even when the deal is agreed, it will not be sealed. It will still need to pass the respective legislatures of all the signatories before it can come into effect. For a number of TPP countries, this is not much of an issue, especially for those that, in effect, have rubber-stamp legislatures, such as Singapore and Vietnam. In others, like Japan, Australia and New Zealand, although passage is not necessarily assured, defeat of a TPP bill is, nevertheless, highly unlikely. Then, there is the US. The Obama administration has put off the fight over the establishment of a Trade Promotion Authority (TPA), which would allow the president to send any trade agreement to the US Congress for a yes-or-no vote and without the potential for filibuster. Until recently, it was assumed that the TPA Bill would pass more or less without incident. Recent developments suggest otherwise. In separate letters to the president, a small group of 23 tea-party Republicans in the House and a much larger group of 151 House Democrats wrote that they would not support TPA legislation. These groups, even together, do not have enough support to block the TPA Bill, but it is still a worrying indicator for the future ability of the US to conduct trade negotiations in good faith.

The TTIP, which would also come under threat from a failure to grant Mr Obama the TPA, is still a year away at best. Both sides claimed from the outset that they were aiming to reach agreement on a "single tank of gas", meaning relatively quickly. Yet, the first round of negotiations has been clouded by the Snowden revelations and the second round was cancelled due to the government shutdown in the US. The third round took place in mid-December, but, if the TPP—let alone most other FTA negotiations—provides any guidance, there are still many rounds left.[105]

© The Economist Intelligence Unit Limited 2014

Scenarios for Huawei

The best case for Huawei, for global ICT supply chains, and for the world trading system as a whole, would be for the WTO to re-emerge as the predominant forum for advancing trade liberalisation. Notwithstanding the recent success in Bali, we retain our view from the Brave New World report that this is extremely unlikely in the short-to-medium term, covering at least the next 5-7 years. As such, we present below the best-, worst- and middle-case scenarios for Huawei and for global ICT supply chains, based on what we feel is more realistic.

Table 3: Best-, worst- and middle-case scenarios

	ITA 2	TTP	TTIP	RCEP
Best-case	✓	✗	✗	✓
Worst-case	✗	✓	✓	✗
Middle-case	✓	✓	✓	✓

Best case: ITA 2 without the mega-regionals

The expansion of global ICT supply chains was made possible by a number of factors, but none more important than the extension of greater market access, provided by the initial ITA. Importantly, this market access was granted in more or less uniform fashion to all WTO members, whether signatories to the ITA or not.

As China, and, of course, Huawei, thrived under this system, it makes sense that the best-case scenario for both is for the system not only to remain in place, but to be improved upon. That, theoretically, is what the ITA 2 should accomplish; it is also the best case for the industry and global ICT supply chains more broadly.

At the same time, if the two mega-regionals that do not include China—TTP and TTIP—were for some reason to fail, while the RCEP was completed, that would have at least two positive implications. One is that Huawei would not find itself at a disadvantage in key EU markets vis-à-vis its US competitors.[106] The second is that Huawei would likely enjoy a certain measure of preferential treatment versus those same US competitors in RCEP countries, should that agreement go through.

Worst case: No ITA 2, no RCEP, but TPP and TTIP are completed

Without an ITA 2, all progress on ICT market access at the multilateral level would stop, leaving the mega-regionals as the only other viable means for lowering tariff and non-tariff barriers. New market access, new standards and new regulations would be set to varying degrees by these agreements, with the US-led TPP being the most aggressive, followed by the TTIP and, finally, RCEP.

Middle case: ITA 2 and all three mega-regionals

As explained above, it will take time—perhaps a considerable amount—but this is the most likely scenario: the ITA 2 is finally agreed to, as are all three of the mega-regionals now under negotiation. For Huawei, on the plus side, the ITA 2 would provide it with improved access to nearly all of the world's key ICT markets.

[105] To the extent that the US is at the centre of most of these negotiations, it should be noted that its negotiators have, in succession, gone from TPP negotiations in Salt Lake City to the WTO Ministerial in Bali, to TPP negotiations in Singapore, and now back to Washington, DC, for TTIP negotiations. And all of this at a time when the US Trade Representative (USTR) has had its funding cut due to sequestration. This will inevitably have the effect of slowing down any negotiations in which the US is involved.

[106] Under this and all other scenarios, Huawei would remain effectively banned from the US market.

© The Economist Intelligence Unit Limited 2014

Conclusions and implications for Huawei

Owing to Edward Snowden's revelations, cyber-security has never been as prominent in public discourse as in the past year, and rarely has the level of trust in technology providers and governments been so low. With trust as a precondition of trade, it is unsurprising that the mega-regional trade agreements currently under discussion—particularly those in which the US is a key player—face new challenges. Meanwhile, policy and legislative reactions are under consideration in the US, EU and elsewhere to improve cyber-security in general and data privacy in particular, often by localising the issues, rather than working to rebuild international trust. Some affected multinational ICT firms, who cannot simply turn inwards to look at a domestic market, are taking their own measures to increase transparency and improve trust, while hoping that governments will follow suit.

The most significant responses discussed in this report are summarised in the table below, along with implications for Huawei.

Table 4: Key responses to heightened concern over cyber-security, and implications for Huawei

Entity	Response	Implications for Huawei
US government	National Security Agency (NSA) Bills have been proposed to limit NSA powers and restore faith in US ICT-sector players.	Weak legislation would have little impact. Strong legislation would be positive for US ICT firms, but may be negative for Huawei, as it could be construed as weakening national security and could therefore lead some politicians to push harder to exclude foreign firms from sensitive sectors. Either way, Huawei should continue with its current approach of focusing on confidence-building through consumer, rather than carrier, business in the US.
European Commission	A key pillar of the digital agenda for Europe is establishing a European Cloud Partnership. This is to counter fragmentation into national clouds, but could serve to protect the region's digital economy. The Commission will issue guidance, which is later likely to become law.	Although responding to US infringements of privacy, this could equally affect Chinese ICT firms. Tighter security standards and rules on cross-border data flows are being developed, as well as common procurement requirements. Huawei will need to structure its European cloud-computing business accordingly. It should also continue to position itself as a company at the forefront of cyber-security practice.
Budapest Convention	Article 32b on extra-territorial search and seizure of data by law-enforcement authorities is likely to be revised, and the Convention will push for a new international treaty to more extensively protect privacy and procedural rights.	Huawei may need, in future, to answer questions about what is legally required from it under Chinese law and how it can ensure compliance with European privacy rights. This could be thorny, due to the differing approaches to human rights in China and Europe.
Wassenaar Arrangement	Including cyber-security technologies on arms-export control lists.	Huawei will need to keep abreast of how this ties in with other security and privacy rules in the EU, and ensure any relevant technologies, such as deep-packet inspection, are deployed in line with evolving practice.

© The Economist Intelligence Unit Limited 2014

Table 4: Key responses to heightened concern over cyber-security, and implications for Huawei

Entity	Response	Implications for Huawei
US tech firms	In February 2014, Facebook, Microsoft, Google and Yahoo started publishing the number of government requests they had received. Microsoft has also started giving cloud customers the option of choosing in which location their data are stored.	Huawei could consider taking similar measures to build trust, anticipating upcoming legislation in the EU and elsewhere in order to remain at the forefront of cyber-security best practice.
Trans-Pacific Partnership mega-regional trade agreement	Until an ITA 2 is concluded, the TPP could be very influential on trade rules with regard to cross-border data flows, data localisation, and e-commerce. Its rules will be heavily influenced by the US, although other countries' data-privacy and security concerns will limit the openness of data flows.	Through new tariffs, rules and standards, the TPP may incentivise or even compel member countries to re-route at least some parts of their ICT supply chains out of non-member states, including China. Huawei, therefore, has a strong interest in an ITA 2 being completed as soon as possible.

It follows that Huawei should take an active interest in the evolution of regional agreements, domestic legislation and the behaviour of other multinational ICT firms, in order to stay one step ahead of the game in terms of norms on cyber-security and data privacy. It will need to be sure of how its domestic legal obligations as a Chinese company affect its ability to comply with more stringent EU requirements. It should also distance itself from China's image as a rather weak cyber-security environment, as it is already doing through various initiatives promoting best practice in supply chains; this could be taken further by also promoting higher industry standards in terms of consumer-data protection. This would help to counter the negative perception of Huawei as a company willing to help governments monitor their populations, a perception that was evidenced in the 2012 allegations that Huawei deep-packet-inspection systems were offered to Iran's security establishment.

One option is for Huawei to take unilateral measures similar to those adopted by Microsoft, in order to inspire consumer confidence in its services, particularly with regard to cloud computing. Yet, with a view to building long-term trust in the industry as a whole and in Huawei specifically, it would be more effective to establish a forum to develop and co-ordinate industry standards on cyber-security. With certain industry players unwilling to co-operate directly with Huawei, a neutral space for such a forum might be found in academia. Experts on the technical aspects of cyber-security, along with others focusing on international politics and trade, could enable a less biased and more objective discussion to develop than a purely sector-led, or public-private sector debate would allow.

However Huawei decides to proceed, it should keep in mind that trust is the key to successful trade, especially in sensitive industries. With geopolitical headwinds in East Asia, strong anti-China lobbies in the US and deep-rooted concerns over privacy and security in the EU, Huawei does not have an easy road ahead. Its current proactive efforts to become not just a trusted partner, but an industry leader in cyber-security, are the right approach, but will be more effective if it can pursue this agenda in a co-operative international forum.

© The Economist Intelligence Unit Limited 2014

While every effort has been taken to verify the accuracy of this information, The Economist Intelligence Unit Ltd. cannot accept any responsibility or liability for reliance by any person on this report or any of the information, opinions or conclusions set out in this report.

Cover image - ©Shutterstock

The Economist Intelligence Unit

LONDON
20 Cabot Square
London
E14 4QW
United Kingdom
Tel: (44.20) 7576 8000
Fax: (44.20) 7576 8500
E-mail: london@eiu.com

NEW YORK
750 Third Avenue
5th Floor
New York, NY 10017
United States
Tel: (1.212) 554 0600
Fax: (1.212) 586 1181/2
E-mail: newyork@eiu.com

HONG KONG
6001, Central Plaza
18 Harbour Road
Wanchai
Hong Kong
Tel: (852) 2585 3888
Fax: (852) 2802 7638
E-mail: hongkong@eiu.com

GENEVA
Rue de l'Athénée 32
1206 Geneva
Switzerland
Tel: (41) 22 566 2470
Fax: (41) 22 346 93 47
E-mail: geneva@eiu.com