
# Intelligence and Security Committee

## Foreign involvement in the Critical National Infrastructure

***The implications for national security***

Chairman:
The Rt. Hon. Sir Malcolm Rifkind, MP


# Intelligence and Security Committee

## Foreign involvement in the Critical National Infrastructure

### *The implications for national security*

Chairman:
The Rt. Hon. Sir Malcolm Rifkind, MP

Presented to Parliament
by the Prime Minister
on behalf of Her Majesty
June 2013

Cm 8629 £8.75

Any enquiries regarding this publication should be sent to us at committee@isc.x.gsi.gov.uk

ISBN: 9780101862929

Printed in the UK by The Stationery Office Limited
on behalf of the Controller of Her Majesty's Stationery Office

ID 2565323 06/13 29949 19585

Printed on paper containing 75% recycled fibre content minimum.

## CONTENTS

## TELECOMMUNICATIONS AND THE UK'S CRITICAL NATIONAL INFRASTRUCTURE

1. The UK defines its Critical National Infrastructure (CNI) as "*certain 'critical' elements of infrastructure, the loss or compromise of which would have a major, detrimental impact on the availability or integrity of essential services, leading to severe economic or social consequences or to loss of life*".[1] This includes assets such as energy supply pipelines, transport infrastructure and water supplies. In the UK, the CNI is now largely in the hands of private enterprises that are driven by commercial considerations. However, given the importance of the CNI, the decisions they take may have wider implications for national security.

2. Certain telecommunications networks are considered to be part of the CNI: given the importance of telecommunications to our daily lives, any disruption to the integrity or availability of the network could have severe and wide-ranging consequences. Since the privatisation of the industry in 1984, strong competition has emerged; there are now hundreds of different providers. However, BT remains responsible for large parts of the UK's telecommunications infrastructure. In 2003, it embarked on a major £10bn rationalisation and upgrade project commonly referred to as 21st Century Network. A number of companies were selected to supply the various equipment required, one of which was Huawei, a Chinese telecommunications company. A contract with Huawei to supply some of the transmission and access equipment, including routers,[2] was signed in 2005, with this being deployed across the network from January 2007.

3. There is, potentially, a conflict between the commercial imperative and national security, as a result of increasing private ownership of CNI assets combined with the globalisation of the telecommunications marketplace. It is important to ensure in such situations that the correct balance is struck: Government must be clear what its strategy is when it comes to deployment of equipment – particularly where this has been developed or manufactured by foreign companies – within the UK's CNI and have effective processes in place for considering these issues. We have considered the relationship between BT and Huawei in this context.

[1] *Centre for the Protection of National Infrastructure, 'Critical National Infrastructure', www.cpni.gov.uk/about/cni (accessed 22 January 2013).*

[2] *Routers are devices that forward data 'packets' between computer networks, either domestic or commercial. In this context, they relay data at high speed along the fibre optic lines that comprise BT's communications network.*

## HUAWEI AND THE CHINESE STATE

4. Huawei was founded in 1987 by Ren Zhengfei, a former officer of the People's Liberation Army. It is the second largest telecommunications equipment company in the world, with over 150,000 employees and turnover of around £20bn. Huawei is a major supplier to many telecommunications companies globally; in the UK, this includes BT, O2, TalkTalk and Everything Everywhere. Huawei provides them with mobile handsets, routers and other equipment; its equipment permeates the UK's fixed and mobile telecommunications infrastructure.[3] Huawei employs 650 people in the UK and plans to increase this to 1,350 over the next five years.

5. Most of the concerns surrounding Huawei relate to its perceived links to the Chinese State. As the Committee noted in its last Annual Report, 20% of detected cyber attacks against UK interests demonstrate levels of sophistication which indicate that they are more likely to be State-sponsored, or related to organised crime. China is suspected of being one of the main perpetrators of State-sponsored attacks, which are focused on espionage and the acquisition of information. In this context, the alleged links between Huawei and the Chinese State are concerning, as they generate suspicion as to whether Huawei's intentions are strictly commercial or are more political.

6. However, Huawei strenuously denies that it has direct links with the Chinese Government or military, claiming that it receives no financial support from the Chinese Government and that it is 98.6% owned by its employees. Nevertheless, *** there is a lack of clarity about its financial structures.[4] Moreover, Huawei's denial of links to the Chinese State is surprising, given that such links to the State are considered normal in China. As the Government Communications Headquarters (GCHQ) explained:

> *This close relationship between commerce and the state is seen in China as normal and acceptable because success is deemed to be for the benefit of all*.[5]

7. When questions first arose concerning Huawei's links to the Chinese State, Huawei launched a large-scale PR campaign to demonstrate that they could be trusted as a telecommunications equipment supplier. In March 2011, the company published the names of its board members in an attempt to distance itself from allegations of close ties to the Chinese State. Huawei also published what they described as a 'White Paper' on cyber security entitled 'Cyber Security Perspectives: 21st Century Technology and Security – A Difficult Marriage'.[6] Written by John Suffolk – Huawei's Global Cyber Security Officer, who was

---

[3] *It is alleged that Huawei was able to win many contracts by stealing technology from its rivals and then undercutting them on price – both Cisco Systems and Motorola launched legal proceedings alleging infringement of intellectual property (the cases subsequently being settled).*

[4] ***.

[5] *Written Evidence – GCHQ, 28 April 2011.*

[6] *John Suffolk, 'Cyber Security Perspectives: 21st Century Technology and Security – A Difficult Marriage', 4 September 2012.*

formerly the Chief Information Officer for the UK Government – the report attempted to rebut the allegations, claiming that they are based on false assumptions and prejudices. According to Huawei, these include: paranoia; country discrimination; a complex legal and regulatory landscape with no global coherence; and a rapidly changing telecommunications marketplace, resulting in a challenging risk management environment.[7] The report concluded that any solution to these concerns must involve industry and governments working together across national boundaries.

8. Building on the perception that the UK is a 'friendly face' in its battle to win major overseas contracts, Huawei last year announced a £1.2bn research investment in the UK. Given the current economic climate, this sizeable investment was welcomed by the Government. Predictably, this was also seized upon by Huawei as evidence of its reliability; the company's press release was a thinly veiled retort to foreign governments that have hindered their business expansion plans. The CEO, Ren Zhengfei, is quoted as saying, "*over the past eleven years we have found [the UK] Government to be transparent, efficient and practical. The UK is an open market, which welcomes overseas investment.*"[8] Some media comment hinted that this investment in the UK was largely motivated by Huawei's broader objective to break into the US market.

9. Huawei's PR campaign appears to have fallen flat thus far, as other countries have taken an increasingly critical stance towards the company's involvement in their national telecommunications networks. In the US, the House Permanent Select Committee on Intelligence (HPSCI) recently published a scathing assessment of Huawei's reliability in an 'Investigative Report on the US National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE'.[9] Their report concluded that "*the risks associated with Huawei and ZTE's provision of equipment to US critical infrastructure could undermine core US national-security interests*".[10] Meanwhile, the Australian Government has decided, reportedly on national security grounds,[11] to exclude Huawei from involvement in their National Broadband Network, a similar upgrade project to that being pursued in the UK by BT (albeit that the Australian network is owned and funded by the Australian Government).

10. It appears that the considerable suspicion with which politicians in both the US and Australia continue to regard Huawei remains due primarily to the perceived influence of the Chinese State over the company which, in their view, deems Huawei a security risk. As Chris Johnson, a former CIA senior analyst on China, told a US news programme:

> *I think it really boils down to an issue of will the company take some steps to make themselves, you know, more transparent about their operations, and what*

[7] *Ibid.*
[8] *Huawei press release, 11 September 2012.*
[9] *'Investigative Report on the US National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE', HPSCI, 8 October 2012. ZTE is another major Chinese telecommunications company.*
[10] *Ibid.*
[11] *See 'Australia Bars Huawei From Broadband Project', New York Times, 26 March 2012.*

*their ultimate goal is, especially this relationship with the Chinese Government, with the Chinese Communist Party and with the People's Liberation Army.*[12]

11. Huawei continues its PR battle to demonstrate independence. Most recently, in January 2013, Huawei's Chief Financial Officer, Cathy Meng (daughter of Ren Zhengfei), promised greater transparency and openness, particularly around how the company is owned. However, media analysis continues to suggest that despite its claims of employee ownership, appointments to the board remain tightly controlled.[13]

[12] *Chris Johnson, CBS, '60 Minutes'.*
[13] *'Huawei Pins Hopes on Fresh Face', Financial Times, 21 January 2013.*

## HUAWEI'S ENTRY INTO THE UK TELECOMMUNICATIONS MARKET: WHAT WENT WRONG

12. Whether the suspicions about Huawei are legitimate or unfounded, we consider it necessary to ascertain how the company came to be embedded in the heart of the UK's CNI. What this Committee's investigation has revealed is a disconnect between the UK's inward investment policy and its national security policy.

13. BT first notified Government officials in 2003 of Huawei's interest in the 21st Century Network contract. However, the Committee has been told by the Cabinet Office that officials chose not to refer the matter to Ministers, or even inform them, until 2006, a year after the contract had been signed (a full chronology is at Annex A). The Committee sought to understand the reasons behind this failure:

- Initially we were told that it was because officials concluded that there were no means available by which Huawei's involvement could be blocked and, therefore, that there was no decision to be taken by Ministers.[14]

- However, this now appears not to have been the case. The Cabinet Office has since acknowledged that such powers do exist,[15] and that officials were aware of this at the time but assessed[16] that the potential trade, financial and diplomatic consequences of using them would be too significant.[17]

- We have subsequently been informed by the then Secretary of State for Trade and Industry, the Rt. Hon. Patricia Hewitt, that she did discuss the contract with BT. However, this was in relation to the competition aspects of the decision (and the implications for UK business) rather than any security concerns. Officials did not take the opportunity of her involvement to raise the security issues with her.

There was no justification for failing to consult Ministers about the situation when BT first notified officials of Huawei's interest. Such a sensitive decision, with potentially damaging ramifications, should have been put in the hands of Ministers.

[14] *Written Evidence – Cabinet Office, 27 July 2011.*
[15] *The Government's powers to intervene in such contracts are governed by the Telecommunications Act 1984, Section 94, Subsections 1–2a and 6, and include requiring operators to purchase only approved products and requiring access to software source code.*
[16] *This assessment included advice from Treasury Solicitors and the regulator, Ofcom.*
[17] *Written Evidence – Cabinet Office, 29 November 2011. The Cabinet Office noted that the Government would have to compensate BT for any losses associated with the use of these powers.*

14. The handling of the BT/Huawei case highlights a number of weaknesses in the UK's approach to deployment of equipment within the CNI. First, there is no general requirement on companies that own CNI assets to inform or consult Government prior to awarding a contract, whether that be to a UK company or a foreign company.[18] Instead, the Government relies on informal processes or the private company taking the initiative themselves. This is far too haphazard an approach given what is at stake. It means that the Government may not be made aware of contracts involving foreign companies from potentially hostile states until they have already been awarded. Clearly this does not always allow for any assessment of national security implications or a strategic approach to managing any risks identified. The Government is therefore sometimes put in the position of trying to shut the stable door after the horse has bolted.

15. Second, even where companies take the initiative to inform Government – as happened in the BT/Huawei case – there is no proper process for ensuring that Ministers are informed or consulted. The failure in this case to consult Ministers seems to indicate a complacency which was extraordinary given the seriousness of the issue. This is further compounded by a surprising lack of clarity as to which Minister would be responsible for such decisions. While it was officials from the Department of Trade and Industry (now the Department for Business, Innovation and Skills) and the Cabinet Office who decided that it would not be desirable to block the BT contract, it was eventually the Home Secretary who was first informed about the security issues, despite the fact that the organisation which provided the necessary technical advice was the Communications-Electronics Security Group (CESG),[19] which reports to the Foreign Secretary.[20] CESG had been tasked by the Cabinet Office, which reports neither to the Home Secretary nor the Foreign Secretary. It would also appear that the Telecommunications Act 1984 empowers the Secretary of State for Culture, Media and Sport to make the final decision, though we have seen no evidence of any involvement by that department.

[18] *There is one very limited exception in the case of companies that own CNI assets and are also required to maintain a permanent interception capability under Section 12 of the Regulation of Investigatory Powers Act 2000 (RIPA). Companies which have been given a notice by the Secretary of State under Section 12 of the Act are required to notify Government of any developments that are likely to affect the company's interception capabilities. Such developments might include the awarding of a contract to a foreign company, if the involvement of that company could affect the provision of the interception capability.*

[19] *CESG – part of GCHQ – provides policy and assistance on the security of communications and electronic data to central Government, the wider public sector and the CNI.*

[20] *Written Evidence – Cabinet Office, 27 July 2011.*

16. Third, it appears that there continues to be confusion as to whether the Government does or does not have any power to intervene. The Foreign Secretary told the Committee:

> *I think we will have necessary power, but we will have to judge this at the time if that situation arises... it wouldn't be impossible if we decided on the balance of evidence that we needed to take some such action.*[21]

The Cabinet Office subsequently indicated that the powers did exist under the Telecommunications Act 1984. However, its legal advice suggested that use of these powers would be likely to prompt a judicial review and the Government would have to compensate the telecommunications company for any losses incurred. In written evidence, the Cabinet Office said that "*the power of direction in the 1984 Act is not well suited to mitigating those risks*".[22] While the powers do appear to exist, they are nevertheless ineffective. This comes back to the issue of Ministerial involvement: had the matter been referred to Ministers, then they could have taken a view on whether they wished to ask Parliament to provide more appropriate powers, if that was deemed necessary.

- **The Government's duty to protect the safety and security of its citizens should not be compromised by fears of financial consequences, or lack of appropriate protocols. However, a lack of clarity around procedures, responsibility and powers means that national security issues have risked, and continue to risk, being overlooked.**

- **The BT/Huawei relationship began nearly ten years ago; the process for considering national security issues at that time was insufficiently robust. The Committee was shocked that officials chose not to inform, let alone consult, Ministers on such an issue. We are not convinced that there has been any improvement since then in terms of an effective procedure for considering foreign investment in the Critical National Infrastructure (CNI). The difficulty of balancing economic competitiveness and national security seems to have resulted in stalemate. Given what is at stake, that is unacceptable.**

  - **The National Security Council should ensure that there are effective procedures and powers in place, and clear lines of responsibility when it comes to investment in the CNI. Crucially, the Government must be clear about the sequence of events that led to Ministers being unsighted on an issue of national importance, and take immediate action to ensure that this cannot happen again.**

[21] *Oral Evidence – Foreign Secretary, 26 January 2012.*
[22] *Written Evidence – Cabinet Office, 27 July 2011.*

## SECURITY CONCERNS OVER HUAWEI'S EQUIPMENT: POSSIBLE IMPLICATIONS

17. While the way in which a foreign company was allowed to gain such a foothold in the UK's CNI was clearly not managed correctly, the question now is whether or not that foothold has implications for the UK's national security. When Ministers were finally informed about Huawei's involvement in 2006, it was because approval was being sought to carry out checks on Huawei's equipment. ***.

18. ***.

19. *** the Security Service had already told us in early 2008 that, theoretically, the Chinese State may be able to exploit any vulnerabilities in Huawei's equipment in order to gain some access to the BT network, which would provide them with an attractive espionage opportunity.[23] Furthermore, the Committee understands that the Joint Intelligence Committee (JIC) had previously warned that if a hostile actor were to exploit such an opportunity, an attack "*would be very difficult to detect or prevent and could enable the Chinese to intercept covertly or disrupt traffic passing through Huawei supplied networks*".[24] *** these assessments underline what could, theoretically, be at stake through Huawei's involvement in the UK's CNI.

20. We questioned how the Government would react in the event of an attack, if it was detected. The Cabinet Office explained that they would "*have the option of putting pressure on the Communications Service Providers [CSPs] to terminate any contract with Huawei. But HMG [HM Government] would have to have firm evidence of Chinese attribution.*"[25] This 'option' seems feeble at best. The Committee is concerned at the apparent absence of any strategy to monitor or react to potential breaches.

21. Any vulnerability, even as a result of an innocent mistake rather than malicious intent, would call into question whether a product is sufficiently well engineered. An insecure product would risk a third party exploiting its weaknesses to access UK networks for hostile purposes. ***. GCHQ said that "*we are confident that the UK network has not been at risk… at any stage because of the mitigations that BT have had in place from the outset*"[26] and that the "*set of measures adopted by BT and Government… together form coherent mitigation*"[27] of any risk. Indeed, as our investigation continued, GCHQ was increasingly concerned to impress upon us that:

> *BT has acted responsibly in investing significant money and manpower to manage this risk. They have done so willingly and in full cooperation with*

[23] *Oral Evidence – Security Service, 24 January 2008.*
[24] *JIC(08)106 (extract).*
[25] *Written Evidence – Cabinet Office, 29 November 2011.*
[26] *Written Evidence – GCHQ, 25 February 2013.*
[27] *Written Evidence – GCHQ, 25 March 2013.*

*CESG. The mitigations implemented by BT since 2004 have resulted in a well-managed communications infrastructure drawing on products developed in a global market. In this sense they might be considered an exemplar.*[28]

22. While we are reassured by GCHQ's confidence in BT, we also note that they acknowledge that the risk of unauthorised access cannot be entirely eliminated. We therefore remain concerned that there is no guarantee: any weaknesses or vulnerability in equipment deployed on UK networks could – through no fault of the operator – have serious security implications.

- ***.

- **While we note GCHQ's confidence in BT's management of its network, the software that is embedded in telecommunications equipment consists of "*over a million lines of code*" and GCHQ has been clear from the outset that "*it is just impossible to go through that much code and be absolutely confident you have found everything*".[29] There will therefore always be a risk in any telecommunications system, worldwide. What is important is how it is managed, or contained.**

[28] *Ibid.*
[29] *Oral Evidence – GCHQ, 24 January 2008.*

## MANAGING THE RISK – THE CYBER SECURITY EVALUATION CENTRE

23. CESG, *** worked with BT immediately to confirm that BT's network architecture was sufficient to protect the network from exploitation, and it also continued its own research ***. Following Huawei's expansion into other CSPs, in 2010 the Government engaged directly with Huawei UK, highlighting its security concerns and suggesting the establishment of a Cyber Security Evaluation Centre, now commonly called the Cell.*** Huawei was persuaded to take action in order to increase UK suppliers' confidence in the security of Huawei products. GCHQ has told the Committee that this "*mitigation work*" is underpinned by a written agreement between HMG and Huawei, which has so far been adhered to. However, GCHQ also notes that "*on occasions there has been pushback from Huawei senior staff who have been seeking to reduce the overheads associated with the [requirements]*".[30]

24. According to GCHQ, the mitigation strategy comprises four elements:

- Technical architecture – making sure that the network is designed to make exploitation difficult and monitoring easy, as well as providing layered defence. As a consequence, Huawei's equipment is "*limited in network scope to minimise overall systemic risk*".[31]

- Contractual liabilities – HMG encourages CSPs that are considering using Huawei equipment to use the Cell (see below) and to include particular contractual requirements to support the mitigation strategy. GCHQ describes this strand of the mitigation strategy as "*the most fragile part*". The Committee has been told that use of the Cell is voluntary: of the five CSPs that use Huawei products, only three make use of the Cell's facilities. The Government has told us that use of the Cell is encouraged only where a company is using Huawei equipment to provide services to the Government or as part of the CNI infrastructure, or operating at a scale that could have a significant impact. Nevertheless, we question its assessment that the two major broadband providers which do not use the Cell are not operating at a scale where using its services would provide extra mitigation.

- *** company engagement – GCHQ undertakes its own technical work to validate and build on the findings of the Cell. ***.

[30] *Written Evidence – GCHQ, 9 January 2013.*
[31] *Ibid.*

- The Cyber Security Evaluation Centre within Huawei, known as the Cell.[32] This is a key element of the strategy (although we note that it does not work in isolation, and would be ineffective without the other elements). We examine the work of the Cell in more detail below.

25. The Cell is funded entirely by Huawei and staffed by security cleared UK personnel, ***. When the Cell was opened, Huawei described it as being "*like a glasshouse – transparent, readily accessible, and open to regulators and our customers*".[33] However, we note that the Cell is nevertheless under Huawei's control, rather than the Government's. We questioned whether the staff,[34] who are paid and employed by Huawei, are sufficiently independent of Huawei to provide the necessary level of assurance about the company's activity. GCHQ acknowledged the risk, but explained that there are measures in place to manage it:

    - First, the staff in the Cell undergo an "*enhanced security process ***. As a result of this process some people have not been employed.*"[35]

    - Second, the Director of the Cell is an ex-GCHQ Deputy Director, "*of 40 years experience*",[36] whom GCHQ "*trust to provide assurance to the Government and UK CSPs about Huawei's products*".[37] Furthermore, "*he is the only non-Chinese employee in the entire company who has full executive power over budgets and hiring. The technical staff in the Cell are managed entirely within the Cell and have no reference to any Chinese national for pay, bonus, evaluation or promotion. The overall budget of the Cell, including staff costs, is managed solely by the Director of the Cell and he is the only one who has management links to China. The design of the Cell means that the Chinese have minimal influence on those working there.*"[38]

    - GCHQ also considers that there are "*considerable benefits*" to the staff in the Cell being Huawei employees. "*Primarily, it is easier for HMG to influence Huawei through employees, rather than third party contractors. In order to manage the risk long term, we must raise the engineering and security competence in the Chinese R&D [Research and Development] function. Recent exposures of flaws in Huawei equipment by the security research community – which every vendor endures to some degree –*

[32] *Other risk mitigation measures include: BT monitoring critical systems, implementing stringent security procedures surrounding physical and remote access to equipment, and good personnel security practices on 'patching' systems when security updates are released.*
[33] *'Huawei Opens Cyber Security Evaluation Centre in the UK', Huawei press release, 6 December 2010.*
[34] *As of January 2013, there are 22 people employed in the Cell, all of whom are UK nationals. They are all either ex-Government staff, industry experts or recent graduates.*
[35] *Written Evidence – GCHQ, 9 January 2013.*
[36] *Written Evidence – GCHQ, 8 April 2013.*
[37] *Written Evidence – GCHQ, 9 January 2013.*
[38] *Ibid.*

*[have] proved the need for this strategic engagement.*[39] *Our success in driving significant change in the company has been in no small part due to the reach back the Cell has – and uses – on our behalf. Experience of independent third parties (e.g. EWA Canada) [shows] that they do not have sufficient influence on the larger corporate machine.*"[40] However, while we agree that this may result in improved engineering standards, it does not appear to provide any further protection for the UK against the risk of vulnerabilities deliberately created for malicious purposes. Furthermore, the comparison used is with third party contractors, as opposed to GCHQ itself.

- GCHQ also cited the benefits of the staff, as Huawei employees, being given unfettered access "*to corporate tools such as the Defect Tracking System which allows them to access directly the vulnerabilities database and to track resolution progress. Access to such a system is tightly controlled and almost never given to third parties.*"[41] However, we note that this implies that more limited access to the Defect Tracking System is occasionally given to third parties, and therefore this would not appear to be sufficient reason to let Huawei run the Centre. Furthermore, while commercial considerations might well limit the extent to which Huawei would share such data with other companies, such concerns would not apply to GCHQ.

While we recognise that there are some benefits associated with the current staffing arrangements for the Cell, these do not, in our opinion, outweigh the risks of Huawei effectively policing themselves.

26. Turning to the work of the Cell, it is intended to test all updates to Huawei's hardware and software for high-risk components before they are deployed on UK networks; however, it is not expected that every single vulnerability will be found. (GCHQ assesses that any attempts to exploit any vulnerability will almost certainly be prevented or detected by the other mitigations in place, and the design of the technical architecture will enable CSPs to monitor activity.) In written evidence, the Cabinet Office has stated that the aim of the Cell is "*to reduce the risk of using Huawei equipment to a similar level to that of established manufacturers – including large American suppliers*".[42] The Committee has been told that "*these flexible and appropriate measures*" – referring primarily to the Cell – provide "*huge mitigation*" and "*work very well*".[43]

27. While that may well be the case in the future, the Cell was only due to become fully operational at the end of 2011 (six years after Huawei won the contract). The

[39] *As GCHQ notes, engineering flaws are frequently discovered in all vendors' equipment. For example, Cisco publishes a list of vulnerabilities discovered in their equipment, providing enough detail for users to rectify the error but not enough for a third party to 'craft an exploit'.*
[40] *Written Evidence – GCHQ, 9 January 2013.*
[41] *Ibid.*
[42] *Written Evidence – Cabinet Office, 27 July 2011.*
[43] *Written Evidence – Cabinet Office, 29 November 2011.*

Cell is, however, currently operating at reduced capacity, both in terms of staffing and remit, and witnesses have conceded that it is too soon to tell how effective it is. In order for the Cell to be able to provide security assurance, it requires access to the product and platform code for the equipment, which Huawei only began to release in March 2012.[44] GCHQ told us:

> *... [Huawei] had not previously released both [product and platform code]. The Cell recommended a solution which Huawei has accepted and the first platform code was downloaded in March 2012. This should now enable the Cell to develop their role and fully assess the products.*[45]

It nevertheless acknowledged that this had been a "*major issue*" with the functioning of the Cell. In response to the Committee's concerns in this area, GCHQ subsequently provided further information to explain that BT operates terms and conditions with Huawei which have provided extra assurance since the start of the contract in 2005, and that the Cell is only intended to "*scale that protection to other providers*".[46]

28. The Cell has provoked considerable interest around the world. An article in *The Economist* described it as the "*unlikely fulcrum of the balance of power in the world of telecoms*".[47] While this description is perhaps exaggerated, the Cell is undoubtedly an important step towards developing a cyber security partnership between Government and industry. Setting up the Cell at its own cost was a major step for Huawei; it required significant financial investment ***. Nevertheless, there is a strong commercial argument for Huawei to co-operate in the UK in order to prove their trustworthiness to other foreign governments. As Huawei told the US House Permanent Select Committee on Intelligence:

> *As a global company that earns a large part of its revenue from markets outside of China, we know that any improper behaviour would blemish our reputation, would have an adverse effect in the global market, and ultimately would strike a fatal blow to the company's business operations.*
>
> *Our customers throughout the world trust Huawei. We will never do anything that undermines that trust. It would be immensely foolish for Huawei to risk involvement in national security or economic espionage.*[48]

- **The UK Government has been able to leverage Huawei's reputational concerns to encourage it to invest in the Cyber Security Evaluation Centre (the Cell) and become more transparent about its equipment and business practices. This is a significant achievement. However, we question why the**

[44] *All software begins life as 'source code' – a readily understood (almost English) version of the program. At this stage it is relatively easy to identify any improper coding. It is must be converted to a computer-readable code before it can be used.*
[45] *Written Evidence – GCHQ, 20 April 2012.*
[46] *Written Evidence – GCHQ, 25 February 2013.*
[47] *'The Company that Spooked the World', The Economist, 4 August 2012.*
[48] *Charles Ding, Corporate Senior Vice President, Huawei, 'Testimony to HPSCI', 13 September 2012.*

**Cell is only now approaching full functionality, over seven years after the BT contract was awarded.**

- **Given these delays and the lack of evidence so far that it will be able to provide the level of security assurance required, we recommend that the National Security Adviser conducts a substantive review of the effectiveness of the Cell as a matter of urgency.**

- **More fundamentally, while we recognise that the Government does not expect the Cell to find every vulnerability, and that there are other mitigations in place, we remain concerned that a Huawei-run Cell is responsible for providing assurance about the security of Huawei products. Before seeking clarification, we assumed that Huawei funded the Cell but that it was run by GCHQ.**

  - **A self-policing arrangement is highly unlikely either to provide, or to be seen to be providing, the required levels of security assurance. We therefore strongly recommend that the staff in the Cell are GCHQ employees. We believe that such a change is not only in both Huawei's and Government's interests, but that it is in the national interest.**

  - **We note that GCHQ considers that there are advantages to the staff of the Cell being employed by Huawei. On the evidence that we have seen thus far we have not found this argument to be compelling. If, after further work is done to explore this issue, there are found to be insuperable obstacles to the Cell being staffed by GCHQ employees, then as an absolute minimum:**

    - **GCHQ must have greater oversight of the Cell and be formally tasked to provide assurance, validation and audit of its work; and**
    - **Government must be involved in the selection of its staff, to ensure continued confidence in the Cell.**

## THE STRATEGIC VIEW

29. This investigation, though prompted by, and focused on, Huawei's involvement with BT, is not just about a single contract, a single company or a single risk management strategy. This is a much broader, indeed global, challenge; the debate surrounding Huawei is merely indicative of a much wider issue. As the Cabinet Office told the Committee:

> *... the commoditised communications marketplace, where products can be manufactured anywhere in the world, contains inherent risks.*[49]

30. A paper on this issue by Microsoft noted that:

> *It is now incontrovertible that the Internet has transformed the way we live and work, and that it has presented both immense opportunities and challenges… ICT systems are indispensible to critical infrastructures and government operations… in light of our increased dependency on cyberspace [there is] concern that sophisticated adversaries will taint the supply chain, inserting functionality into products and services that grants one entity control over another organization's ICT systems, perhaps to steal information, alter information, or deny service at a critical moment.*[50]

31. Most telecommunications companies, wherever their headquarters are, source equipment which has been manufactured or developed in China. While, on the face of it, the strong rhetoric emanating from politicians in Australia and the US appears to be backed by decisive action, it is worth noting that these countries will already have Chinese-manufactured or -developed equipment in their CNI. As a representative of ZTE said, "*If every vendor with 'ties' to China's market is excluded from the US market, where will US carriers purchase telecom infrastructure equipment?*"[51] Any policy which seeks to block all Chinese companies from any future contracts relating to CNI projects is not only impractical but, crucially, given the predominance of Chinese-manufactured and -developed equipment, is unlikely to result in the national security protection envisaged.[52] There are probably only two companies worldwide that would be able to create an end-to-end 4G system using their own equipment: Huawei and Sweden's Ericsson. There are other companies that could supply elements of a 4G system; however, any company will almost certainly manufacture parts in, or source components from, China.

---

[49] *Written Evidence – Cabinet Office, 29 November 2011.*

[50] *Microsoft, 'Cyber Supply Chain Risk Management: Toward a Global Vision of Transparency and Trust', 25 July 2011.*

[51] *Zhu Jinyun, Senior Vice President for North America and Europe, ZTE, 'Testimony to HPSCI', 13 September 2012.*

[52] *The US's experience with tyres is a useful cautionary tale: the New York Times reported that the decision to impose a duty on Chinese tyres may have protected up to 1,200 jobs but it cost American consumers $1.1bn in higher-priced tyres. The consequential Chinese decision to impose a tariff on American chicken parts cost US poultry producers $1.1bn. The tyre tariff has since been allowed to expire. 'A Closer Look at Some Disputed Claims', New York Times, 17 October 2012.*

32. BT and other major UK telecommunications companies that use Huawei as a major supplier have reinforced this point. In a statement, BT said:

> *We clearly recognise that increased globalisation of the telecoms industry means there is a diverse range of cyber threats to consider when building and securing networks. BT takes a risk management approach on the use of components from Huawei.*[53]

33. It is this risk management approach that is key, and what the UK must focus on if it is to safeguard its national security without stifling free trade and innovation. Government must have a proper procedure for assessing the risks – as we have mentioned previously – and also for developing a strategy for managing those risks. Crucially, this should be an integral part of the process, both before and after contracts are awarded, and not merely an afterthought.

- **While we have considered the risks around the telecommunications infrastructure, the same issues apply to any aspect of the UK's CNI. Where there is a privately owned company answerable to shareholders, many of whom may be based abroad, there will almost inevitably be a tension with national security concerns.**

- **It is not practicable to seek to constrain CNI companies to UK suppliers, nor would that necessarily provide full protection given the global nature of supply chains. The risk to the CNI cannot be eliminated, but Government must ensure that it is managed properly. There must be:**

  - **an effective process by which Government is alerted to potential foreign investment in the CNI;**
  - **an established procedure for assessing the risks;**
  - **a process for developing a strategy to manage these risks throughout the lifetime of the contract and beyond;**
  - **clarity as to what powers Government has or needs to have; and**
  - **clear lines of responsibility and accountability.**

  **When it comes to the UK's Critical National Infrastructure, Ministers must be kept informed at all stages.**

- **We do not believe that these crucial requirements existed when BT and Huawei first began their commercial relationship. From the evidence we have taken during this investigation, the procedural steps that we have outlined still do not appear to exist. However, as we went to press, we were told that the Government has now developed a process to assess the risks associated with foreign investment into the UK. Whether these processes are sufficiently robust remains to be seen: the steps we have outlined must exist to ensure that Government does not find itself in the same position again.**

[53] *'BT: Working With Huawei Isn't a Security Issue', PC Pro, 11 October 2012.*

## CONCLUSIONS AND KEY RECOMMENDATIONS

**The Committee's investigation into the handling of the BT/Huawei case highlights a number of weaknesses in the UK's approach to investment in the Critical National Infrastructure (CNI).**

- **The Government's duty to protect the safety and security of its citizens should not be compromised by fears of financial consequences, or lack of appropriate protocols. However, a lack of clarity around procedures, responsibility and powers means that national security issues have risked, and continue to risk, being overlooked.**

- **The BT/Huawei relationship began nearly ten years ago; the process for considering national security issues at that time was insufficiently robust. The Committee was shocked that officials chose not to inform, let alone consult, Ministers on such an issue. We are not convinced that there has been any improvement since then in terms of an effective procedure for considering foreign investment in the CNI. The difficulty of balancing economic competitiveness and national security seems to have resulted in stalemate. Given what is at stake, that is unacceptable.**

  - **The National Security Council should ensure that there are effective procedures and powers in place, and clear lines of responsibility when it comes to investment in the CNI. Crucially, the Government must be clear about the sequence of events that led to Ministers being unsighted on an issue of national importance, and take immediate action to ensure that this cannot happen again.**

- *****.**

- **While we note GCHQ's confidence in BT's management of its network, the software that is embedded in telecommunications equipment consists of "*over a million lines of code*" and GCHQ has been clear from the outset that "*it is just impossible to go through that much code and be* absolutely *confident you have found everything*".[54] There will therefore always be a risk in any telecommunications system, worldwide. What is important is how it is managed, or contained.**

- **The UK Government has been able to leverage Huawei's reputational concerns to encourage it to invest in the Cyber Security Evaluation Centre (the Cell) and become more transparent about its equipment and business practices. This is a significant achievement. However, we question why the Cell is only now approaching full functionality, over seven years after the BT contract was awarded.**

  - **Given these delays and the lack of evidence so far that it will be able to provide the level of security assurance required, we recommend that the National Security Adviser conducts a substantive review of the effectiveness of the Cell as a matter of urgency.**

[54] *Oral Evidence – GCHQ, 24 January 2008.*

- **More fundamentally, while we recognise that the Government does not expect the Cell to find every vulnerability, and that there are other mitigations in place, we remain concerned that a Huawei-run Cell is responsible for providing assurance about the security of Huawei products. Before seeking clarification, we assumed that Huawei funded the Cell but that it was run by GCHQ.**
  - **A self-policing arrangement is highly unlikely either to provide, or to be seen to be providing, the required levels of security assurance. We therefore strongly recommend that the staff in the Cell are GCHQ employees. We believe that such a change is not only in both Huawei's and Government's interests, but that it is in the national interest.**
  - **We note that GCHQ considers that there are advantages to the staff of the Cell being employed by Huawei. On the evidence that we have seen thus far we have not found this argument to be compelling. If, after further work is done to explore this issue, there are found to be insuperable obstacles to the Cell being staffed by GCHQ employees, then as an absolute minimum:**
    - **GCHQ must have greater oversight of the Cell and be formally tasked to provide assurance, validation and audit of its work; and**
    - **Government must be involved in the selection of its staff, to ensure continued confidence in the Cell.**

- **While we have considered the risks around the telecommunications infrastructure, the same issues apply to any aspect of the UK's CNI. Where there is a privately owned company answerable to shareholders, many of whom may be based abroad, there will almost inevitably be a tension with national security concerns.**
- **It is not practicable to seek to constrain CNI companies to UK suppliers, nor would that necessarily provide full protection given the global nature of supply chains. The risk to the CNI cannot be eliminated, but Government must ensure that it is managed properly. There must be:**
  - **an effective process by which Government is alerted to potential foreign investment in the CNI;**
  - **an established procedure for assessing the risks;**
  - **a process for developing a strategy to manage these risks throughout the lifetime of the contract and beyond;**
  - **clarity as to what powers Government has or needs to have; and**
  - **clear lines of responsibility and accountability.**

  **When it comes to the UK's Critical National Infrastructure, Ministers must be kept informed at all stages.**
- **We do not believe that these crucial requirements existed when BT and Huawei first began their commercial relationship. From the evidence we have taken during this investigation, the procedural steps that we have outlined still do not appear to exist. However, as we went to press, we were told that the Government has now developed a process to assess the risks associated with foreign investment into the UK. Whether these processes are sufficiently robust remains to be seen: the steps we have outlined must exist to ensure that Government does not find itself in the same position again.**

## ANNEX A – HUAWEI'S INVOLVEMENT IN THE CRITICAL NATIONAL INFRASTRUCTURE: A CHRONOLOGY

**2003:**

- BT put out to tender a contract to provide equipment for its 21st Century Network – a £10bn project to upgrade BT's communications network by 2014. This will allow all of BT's traffic – including its landline services – to be carried over fibre optic cables (rather than copper wires) and transmitted using Internet Protocol technology, resulting in significant financial savings.

- When BT became aware of Huawei's interest in the contract, it notified officials at a National Security Information Exchange working group.[55] In written evidence, the Cabinet Office has told the Committee that "*there was no formal process in place to assess this type of national security concern. There is an effective informal process that is well established and recognised by the telecommunication companies as beneficial to their interests.*"[56]

- Officials established a cross-departmental working group which first considered whether it was possible to issue a direction to BT to block the contract. They initially concluded that there were no legal means available to do so, though they later acknowledged that "*under section 94 of the Telecommunications Act 1984 it would have been possible for a direction to be placed on BT to prevent them from using Huawei as a supplier*".[57]

- They also considered that blocking the contract "*could have had serious diplomatic and trade implications as well as exposing the government to a potential claim for hundreds of millions of pounds in compensation from BT under a provision in the 1984 Act that makes the Government liable to offset any losses sustained in complying with the direction*".[58]

**2004:**

- The Intelligence and Security Co-ordinator[59] wrote to BT offering technical assistance and reminding it of its legal obligations, but noting that it was the company's decision whether or not to award Huawei the contract, stating: "*BT will have to take its own commercial decision on such matters.*"

- September 2003–October 2004: The Intelligence and Security Co-ordinator established a cross-department working group, under the chairmanship of the

---

[55] *The National Security Information Exchange working group was set up under the National Infrastructure Security Co-ordination Centre (NISCC) – a predecessor to the Centre for the Protection of National Infrastructure.*
[56] *Written Evidence – Cabinet Office, 27 July 2011.*
[57] *Written Evidence – Cabinet Office, 29 November 2011.*
[58] *Ibid.*
[59] *The Intelligence and Security Co-ordinator's role was subsumed into the position of National Security Adviser in May 2010.*

Director of the Communications-Electronics Security Group (CESG), to investigate options.

**2005:**

- The Secretary of State for Trade and Industry took an interest in the contract, but from a competition perspective. Officials did not notify her of any security concerns.

- March: NISCC paper issued. The first recommendation was that "*Service Providers should not use an untrusted supplier's equipment*".[60]

- December: BT awarded Huawei the contract to supply some of the transmission equipment.

**2006:**

- January: The Intelligence and Security Co-ordinator wrote to the Home Secretary to seek agreement to assist BT (at its request) to monitor Huawei's work. This was the first time that Ministers were made aware of the security concerns (three years after officials were first notified).

- Following the Home Secretary's agreement, a Joint Next Generation Risk Mitigation Management Board was formed and met monthly, then quarterly until June 2008, chaired by BT and the predecessor of the Cabinet Office's Office for Cyber Security and Information Assurance.

- BT established its own security teams to work with GCHQ to provide assurance around Huawei equipment and contractual standards.

**2008:**

- December: *** CESG worked with BT to ensure that the network architecture was sufficient to protect the network from exploitation ***.

**2010:**

- February: The Government raised concerns about Huawei equipment with Huawei UK, and proposed the establishment of a security centre.

- The Cyber Security Evaluation Centre (the Cell) launched in November. GCHQ described the role of the Cell:

> *The Cell has not been created to look at every piece of hardware or software destined for the UK market. It will assess hardware and software upgrades prior to their deployment. While this will not provide full risk mitigation, it will provide ongoing lifecycle assurance to updates at Huawei's expense, which will contribute to an overall risk reduction strategy.*

[60] *Written Evidence – GCHQ, 25 February 2013.*

*The Cell will also randomly sample new hardware and software prior to initial deployment on the UK infrastructure but its main role is to assess the updates as this is where CESG believe any malicious code is likely to be hidden. ***.*[61]

**2011:**

- January: CESG, BT and the then Government Chief Information Officer briefed Huawei HQ in China on issues discovered with its equipment. Huawei confirmed that it would rectify the problem.

**2012:**

- The Committee sought confirmation that the Cell was now fully operational and appropriately resourced. GCHQ told us:

  *It currently has 18 staff, three in the recruitment process and approximately 5 vacancies to fill over the next FY [financial year]. The Cell is led by an ex-GCHQ Deputy Director. Whilst the Cell has made significant progress, there is further work required to ensure that the Cell delivers the level of security assurance to satisfy GCHQ and HMG.*[62]

- GCHQ also alerted the Committee to another issue that was, until recently, impeding the functionality of the Cell:

  *A major issue, which was hindering the Cell's development, has recently been overcome. Huawei HQ had been concerned about releasing all their product and platform code out of China; they had not previously released both. The Cell recommended a solution which Huawei has accepted and the first platform code was downloaded by the Cell in March 2012. This should now enable the Cell to develop their role and fully assess the products.*[63]

[61] *Written Evidence – Cabinet Office, 27 July 2011.*
[62] *Written Evidence – GCHQ, 20 April 2012.*
[63] *Ibid.*

## ANNEX B – INTERNATIONAL COMPARISONS

Given the international nature of the concerns about Huawei, it is useful to consider the approaches taken by other governments.

**United States**

There is much criticism of Huawei and ZTE in the US. As well as the House Permanent Select Committee on Intelligence's (HPSCI's) investigation, there is currently legislation pending in Congress which seeks to address supply chain risk in the context of Government procurement actions. However, on 18 October 2012, there were press reports that the White House had concluded a review into the risks associated with Chinese suppliers to US telecommunications companies. According to the reports, the US Government found that there was no evidence that Huawei is guilty of spying on the US. However, it did note that "*sloppy coding*" created vulnerabilities that could be exploited by third parties. We understand that the Government Accountability Office – the equivalent of the UK's National Audit Office – has launched a wider inquiry into the use of equipment manufactured abroad in US telecommunications networks.

**Australia**

The question of Chinese involvement in the Critical National Infrastructure (CNI) is also particularly pertinent in Australia at the moment following the Australian Government's controversial decision to block Huawei from the National Broadband Network. There has been some backlash to this announcement from opposition parties and the subject looks set to remain under discussion for some time. Indeed, Huawei executives recently appeared before an Australian parliamentary committee where, according to media reports, they were questioned about "*Huawei's relationship with the ruling Chinese Communist Party, whether communist cells formed part of the management structure and whether the company had ever installed "back door" provisions in computer hardware that would allow hackers potential access*".[64] As at the HPSCI hearing, Huawei denied all allegations and claimed that it is a victim of anti-China discrimination.

**India**

India is also cited in the media as a government that is working to exclude Huawei. However, according to analysis by Microsoft, India's approach centres on promoting indigenous innovation rather than legislating to block specific foreign companies. While this approach has obvious benefits in terms of local economic development, it can also be seen as "*a major impediment*" to importers and may result in retaliation in the form of economic protectionism by other countries.[65] Despite the difficulties Huawei has experienced in building its reputation in India, it is now its second-largest

[64] *Bianca Hall, 'Chinese Tech Giant Appeals Against Broadband Ban', Sydney Morning Herald, 15 September 2012.*

[65] *Microsoft, 'Cyber Supply Chain Risk Management: Toward a Global Vision of Transparency and Trust', 25 July 2011.*

research base outside China, demonstrating that hostility from the host government is not an insuperable barrier to business success.[66]

**China**

The country which takes the firmest approach to protecting its CNI is, unsurprisingly, China. As well as an "*aggressive indigenous innovation effort*", China requires that the manufacturer must be controlled by Chinese persons or the State; they must confirm that the product contains no vulnerabilities or back doors; and products with encryption technology must receive approval from the Office of State Commercial Cryptographic Administration.[67]

[66] *Morgen Witzel and Tanmoy Goswami, 'Case Study: Huawei's Entry to India', Financial Times, 17 September 2012.*

[67] *Microsoft, 'Cyber Supply Chain Risk Management: Toward a Global Vision of Transparency and Trust', 25 July 2011.*

# THE INTELLIGENCE AND SECURITY COMMITTEE

*The Rt. Hon. Sir Malcolm Rifkind, MP (Chairman)*

| | |
|---|---|
| *The Rt. Hon. Hazel Blears, MP* | *The Rt. Hon. Paul Goggins, MP* |
| *The Rt. Hon. Lord Butler KG GCB CVO* | *The Rt. Hon. George Howarth, MP* |
| *The Rt. Hon. Sir Menzies Campbell CBE QC, MP* | *Dr. Julian Lewis, MP* |
| *Mr Mark Field, MP* | *Lord Lothian QC PC* |

The Intelligence and Security Committee (ISC) is an independent Committee established by the Intelligence Services Act 1994 to examine the policy, administration and expenditure of the three UK intelligence and security Agencies: the Security Service (MI5), the Secret Intelligence Service (MI6) and the Government Communications Headquarters (GCHQ). The Committee also examines the work of the Joint Intelligence Organisation and the National Security Secretariat in the Cabinet Office, Defence Intelligence in the Ministry of Defence, and the Office for Security and Counter-Terrorism in the Home Office.

The Prime Minister appoints the ISC Members after considering nominations from Parliament and consulting with the Opposition. The Committee reports directly to the Prime Minister and through him to Parliament, by the publication of the Committee's reports. The Prime Minister may ask us to look into a matter, but most of the time we set our own agenda.

The Committee has an independent Secretariat currently hosted by the Cabinet Office. The Committee also has access to a General Investigator to undertake specific investigations covering the administration and policy of the Agencies; financial expertise from the National Audit Office; and a Legal Advisor to provide independent legal advice.

The Members of the Committee are subject to Section 1(1)(b) of the Official Secrets Act 1989 and are given access to highly classified material in carrying out their duties. The Committee holds evidence sessions with Government Ministers and senior officials (for example, the Head of the Security Service). It also considers written evidence from the intelligence and security Agencies and relevant government departments. This evidence may be drawn from operational records, source reporting, and other sensitive intelligence, or it may be memoranda specifically written for the Committee.

The Prime Minister may publish the Committee's reports: the public versions have sensitive material that would damage national security blanked out ('redacted'). This is indicated by *** in the text. The intelligence and security Agencies may request the redaction of sensitive material in the report which would damage their work, for example by revealing their targets, methods, sources or operational capabilities. The Committee considers these requests for redaction in considerable detail. The Agencies have to demonstrate clearly how publication of the material in question would be damaging before the Committee agrees to redact it. The Committee aims to ensure that only the bare minimum of text is redacted from the report. We also believe that it is important that Parliament and the public should be able to see where we have had to redact information, rather than keeping this secret. Under the existing legislation the Prime Minister has the power to redact material without the Committee's consent, making a statement to that effect when he lays the report before Parliament. To date, this has never happened.


Published by TSO (The Stationery Office) and available from:

**Online**
**www.tsoshop.co.uk**

**Mail, Telephone, Fax & E-mail**
TSO
PO Box 29, Norwich NR3 1GN
Telephone orders/General enquiries: 0870 600 5522
Order through the Parliamentary Hotline Lo-Call: 0845 7 023474
Fax orders: 0870 600 5533
Email: customer.services@tso.co.uk
Textphone: 0870 240 3701

**The Houses of Parliament Shop**
12 Bridge Street, Parliament Square
London SW1A 2JX
Telephone orders: 020 7219 3890/General enquiries: 020 7219 3890
Fax orders: 020 7219 3866
Email: shop@parliament.uk
Internet: http://www.shop.parliament.uk

**TSO@Blackwell and other accredited agents**

ISBN 978-0-10-186292-9