The UK's Intelligence and Security Committee (ISC) has been busy lately. Before the recent revelations about the UK's possible involvement in the PRISM programme run by the National Security Agency (NSA) in the US, the ISC last week published a report which deserves more attention. The subject of this report is the security implications for the UK of foreign involvement in the provision of services and equipment for the country's Critical National Infrastructure (CNI). Nick Watts, &#65533;Deputy Director General of the U K Defence Forum reports.
The UK's CNI is of importance to national security because of the effect it has underpinning modern life and the economic well-being of the country. Since privatisation in 1984 the telecommunications market has become more competitive, but BT retains a major proportion of the UK's telecoms infrastructure. In 2003 BT began a &#65533;10 bn modernisation programme. Huawei won a contract to supply transmission and access equipment including routers in 2005; this equipment was deployed throughout the BT network from 2007.
Concerns have been expressed about the links between Huawei and the Chinese state. The ISC has previously noted that 20% of detected cyber-attacks against UK interests show evidence of state sponsored sophistication. China has been suspected of being one of the main perpetrators of such attacks. This raises questions about Huawei's intentions; are they commercial or political?
The company has undertaken a major PR exercise to show that it is transparent and that its links with the Chinese government are the norm in China. The ISC notes that some view Huawei's presence in the UK as a prelude to its attempt to enter the US market; so far without success. Huawei announced a &#65533;1.2bn investment in the UK in 2012. This has been welcomed by the UK government.
Huawei won a contract to supply equipment to BT in 2003. BT notified the government that it was contracting with a Chinese entity. No action was taken on security grounds and the matter was not referred to minister until 2006. It was felt to be politically difficult to endanger relations with China, seen as a potentially lucrative market. The government had powers to limit the supply of equipment to a CNI company, but it chose not to do so. The ISC recommends that this matter is examined by the National Security Committee and that guidelines are issued to companies that furnish elements of the UK's CNI; currently there are no such guidelines.
Ministers were only advised of security concerns in 2006 when authority was sought to undertake checks on Huawei's equipment. The ISC was informed about this matter in 2008, noting that vulnerabilities in BT's network could be exploited by a third party. The Joint Intelligence Committee (JIC) noted that any such breaches would be difficult to detect or prevent. Subsequently BT has invested in mitigating measures to try to address this matter, but there appears to be no guarantees against potential breaches. Following Huawei's expansion to supply other telecoms service providers in 2010 the UK government engaged directly with the company. The result has been the establishment by Huawei of a Cyber Security Evaluation Centre, known as the cell. This is staffed by Huawei employees who are vetted by the UK government. This is seen by the government as a useful solution to the problem, as it assists Huawei with their reputational problem. The ISC notes however that this is still a self-policing exercise and not all of the service provider that use Huawei equipment participate in the testing activities of the cell.
It is now recognised that countries' CNI infrastructures represent a significant element in their national economic well-being. Contractors source components and elements of their service provision through a global supply chain. A large part of this is based in China. Chinese companies have the technological know-how to supply end to end equipment in modern telecoms such as the 4G network. It is not possible to exclude any Chinese components in supply chains. Accordingly it is up to individual nations to ensure that they implement adequate

risk mitigation measures beforehand and not as an afterthought.
The ISC believes that the UK government needs to establish better practices arising from this episode. There is evidence of a lack of joined up-ness in the way various government agencies responded to Huawei's entry into the UK market. Security concerns were not upper-most in the minds of officials. The establishment of a Huawei funded equipment testing centre was an attempt to mitigate risks, and there is some evidence that the government and BT have contrived to ensure that any sensitive material is routed in a way that is secure.
However, the report notes that there is no guarantee that Huawei equipment cannot be accessed by a third party. This may not affect government secure communications but it might affect commercially sensitive information passing over the networks of telecoms companies that use Huawei equipment or it could result in some as yet unforeseen cyber-attack in the event of future tensions between the UK and China.
The report notes that Huawei sees the UK as a strategic foothold on the way to entering the US market. It will also use this as a means into other EU markets. It has co-operated in the establishment of an equipment testing centre, to ensure that its equipment does not have exploitable vulnerabilities. The UK for its part needs inward investment, especially in high tech industries. For the time being Huawei will need to do more to show itself free of interference or other undue influence from the Chinese state. It is still blocked from entering other markets such as the US and Australia.