Government Response to the Intelligence and Security Committee's Report of Session 2013-14: Foreign involvement in the Critical National Infrastructure

Presented to Parliament
by the Prime Minister
by Command of Her Majesty

July 2013

Cm 8662 £6.25

ISBN: 9780101866224

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

ID 2576522 07/13 32045 19585

Printed on paper containing 75% recycled fibre content minimum

GOVERNMENT RESPONSE TO THE INTELLIGENCE AND SECURITY COMMITTEE'S REPORT ON FOREIGN INVOLVEMENT IN THE CRITICAL NATIONAL INFRASTRUCTURE

The ISC's report contains a number of recommendations and conclusions. These are set out below (in **bold**), followed immediately by the Government's response.

A. 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.

B. 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.**

The Government accepts the Committee's conclusion that the processes of considering national security issues at the time of the BT/Huawei case in 2003-06 were insufficiently robust. In particular with hindsight, we agree that Ministers should have been informed.

The Government does not agree with the Committee's statement that there have been no improvements since then or that national security issues are overlooked. Indeed the National Security Council (NSC), which was not in existence at the time of the BT/Huawei contract, can and does consider similar issues today in order to ensure that HMG's approach balances economic prosperity and commercial competitiveness with national security. At working level this is brought together by cross industry-government groups.

It is important that this balanced approach is taken. Boosting trade and investment is a key part of the Government's plan for growth and we are working hard to develop our economic relationships with key trading partners, including China. At the same time, the Government works with major Communication Service Providers (CSPs) in the UK to ensure that their networks and the services they provide are appropriately secure. Our work with Huawei and their UK customers gives us confidence that the networks in the UK that use Huawei equipment are operated to a high standard of security and integrity.

The Government recognises this is a fast changing environment and will continue to regularly review procedures in this area.

C. 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"*. There will therefore always be a risk in any telecommunications system, worldwide. What is important is how it is managed, or contained.

The Committee rightly highlighted GCHQ's confidence in BT's effective management of their communications network. Notwithstanding this, we agree with the Committee that no complex telecommunications system – or any ICT system for that matter – can be totally invulnerable and that what is important is how these risks are managed.

D. 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.**

It should be noted the Cell was not established until 2010, and was only required as Huawei gained further contracts with other UK CSPs. Prior to this, BT, with support from GCHQ, had been undertaking their own security risk mitigations. The Cell was established to scale the UK's protection across other CSPs as Huawei's presence in the UK increased. It forms only one part of an end-to-end risk mitigation strategy that the UK has developed and would be less effective without the other parts of the mitigation.

The Government agrees with the Committee's recommendation that the National Security Adviser should carry out a review of the Cell. He will do so and will report to the Prime Minister later in the year.

The National Security Adviser will write to the Chair of the Committee following the conclusion of the review.

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

The Government notes the Committee's concerns and as detailed above will consider these as part of the NSA's review of the cell.

F. 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.

G. 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.

The Government shares the Committee's view that it is not practicable to seek to constrain Critical National Infrastructure (CNI) companies to UK suppliers, nor would it provide any greater protection given the global nature of supply chains.

The Government also welcomes the Committee's recognition that a risk based approach is the correct way forward when considering portfolio investment into the UK's critical national infrastructure. Foreign investment in, or ownership of, CNI would not automatically create

risks related to the operation of that CNI, hence the need to consider matters on a primarily case-by-case basis.

Since the creation of the NSC the Government has put in place an approach which enables it to assess the risks associated with foreign investment and develop strategies to manage them. The NSC, created in 2010, brings together the economic and security arms of the Government and is the forum that ultimately balances the risks and opportunities of inward investment decisions. The NSC is supported by cross-Whitehall coordination by officials who identify and assess any risks in pipeline investment opportunities and bring these to the attention of Ministers. As asserted earlier, the Government recognises this is a fast changing environment and will continue to regularly review these processes.

Lead Government Departments are responsible for managing the protective security approach for their CNI sectors, identifying priorities, monitoring implementation of mitigating measures and agreeing what level of residual risk is acceptable. This is conducted in close collaboration with infrastructure owners and operators and with bodies such as the Centre for the Protection of National Infrastructure. Departments are aware of their responsibility to manage the risks, ensure they consult the relevant experts, and decide when issues should be escalated either to ministers or the NSC as the situation demands. For each case, the decision-making process is signed-off by senior officials and Ministers within the asset-owning department.

Ministers also have at their disposal a number of measures, both legislative and regulatory, that enables the safeguarding and control of operational investments. To ensure they remain fit for purpose, the powers of Government are kept under regular review and consideration given to the question of whether any new powers are required.

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 978-0-10-186622-4