Thank you for your letter regarding the Government response to your Committee’s Cyber security report. I note your concern that our response does not cover sufficiently some of the issues you raised in the report. I will attempt to address your concerns through this letter and through the offer of a further private briefing session on certain sensitive issues you have raised.

On the subject of the funding of the Defence Science and Technology Centre, as with all areas of Government, we must stay within our budgets and use the resources at our disposal carefully. The allocation of £18 Million to the Cyber and Influence Centre was at that time judged to be appropriate. Since our previous correspondence I am pleased to report that approximately £25 Million is now available with the possibility of further increases in year. I believe this is a reasonable budget for the year, although we do of course keep this under review reflecting the rapidly changing nature of cyber operations.

In your letter you enquired about the Foreign Secretary’s Ministerial Group on Cyber. The group has held four meetings under the Foreign Secretary’s chairmanship over the past two years. However, it is important to note that ministerial engagement on Cyber across Government is much broader than this. The Minister for Political and Constitutional Reform chairs a supporting Delivery Group on Cyber. Ministers also chair the Cyber Growth Partnership with industry representatives and the Partnership on Cyber Crime. In addition, since the Government gave evidence to the Committee, the National Security Council (NSC) has held a dedicated discussion on cyber security, as well as considering cyber in the context of a number of other issues of concern. The NSC is due to return to the subject of cyber shortly.

As we stated in our evidence, the MOD does not have a standing role in the cyber protection of Critical National Infrastructure (CNI). The Centre for the Protection of National Infrastructure (part of the Security Service) promotes good practice across the companies delivering our CNI, as well as managing ‘Information Exchanges’ to promote

The Rt Hon James Arbuthnot MP
Chairman
House of Commons Defence Committee
House of Commons
London SW1A 0AA
the sharing of information on cyber threats and vulnerabilities that could affect specific CNI sectors. The Cabinet Office, through the Office for Cyber Security and Information Assurance (OCSIA), operates a broader Cyber Security Information Sharing Partnership to help companies across all industry sectors access threat information. OCSIA is presently reviewing cyber security support to the CNI to ensure that all sectors are receiving the appropriate levels of support to address the particular challenges presented by a rapidly developing cyber threat. This work will inform the infrastructure security and resilience processes that are centrally managed by the Cabinet Office and Home Office, and MoD will remain closely involved in this process.

I am happy to address the other points in your letter by means of a private briefing in the Department, which will allow me to expand on the detail, particularly in some of the sensitive areas that our earlier response was not able to cover. As you can appreciate, much of the necessary information is protectively marked, which limits the extent to which it can be publicly released after the briefing.

I have asked my staff to make contact with the Committee Clerk about the arrangements.

I hope that this letter, and the subsequent briefing, gives you the assurance you seek and demonstrates that Defence is taking its responsibilities in Cyber security extremely seriously.

As cn,

THE RT HON ANDREW ROBATHAN MP