&#65533; By Nick&#65533;Watts,&#65533;Great North News Services
&#65533;
After the hoopla that surrounded the launch of the Government's Cyber Security Strategy, there has been a deafening hush from government. Yesterday the House of Commons Defence Select Committee returned to the topic. A number of former government advisers and experts gave evidence. MPs are trying to understand the scope of the cyber threat and the way in which government, through its various agencies, is responding to it.

  The Government in the cyber security strategy spoke of the cyber threat as being "transformational"- &#65533;to start with MPs wanted to know just how transformational was it? The answer seems to be that this is a technology which has applications in a variety of areas. The challenge for government is to recognise this and not to get too "stove piped" in the way it is addressed. Although a strategy paper is a good way to unify government thinking, inertia in Whitehall was one of the matters that needed to be dealt with, according to one former government advisor. As a measure of how transformational the cyber threat is, it was stated, the pace of change in this domain was very swift; faster than any bureaucracy can deal with. More forward thinking and horizon scanning will be needed to ensure that the UK is at least within touching distance of developments.

Aside from the defence element, threats exist for the financial service industry as well as government departments such as HM Revenue and Customs; any area which deals with data or on-line financial transactions is vulnerable. The priority for the defence sphere is to protect its own internal networks against the risk of financial loss, given the amount of money the MOD handles. Similarly the MOD's own network needs to be secure against hacking and Denial of Service attacks, so that its network does not grind to a halt, should it be attacked.

Turning to the risks against which the UK should be protected, one former government security advisor characterized 4 main types: criminality, espionage, subversion and sabotage. An enemy will look for weaknesses and exploit them. The Stuxnet attack was an example of a bespoke attack directed against a known target. This requires a large effort. A more plausible attack would be against a vulnerable and widespread facility, such as smart grids. The UK's Critical National Infrastructure needs to be protected against such attacks.

The current expression of the risk of State versus State attacks is the theft of information which is useful. This can range from strategic information to early sight of developments in the high tech or pharmaceutical industries. A state sponsored attack might come via proxies, such as Hezbollah acting on behalf of Iran. Cyber assisted war is possible, for example attacking an enemy's air defence network. In this new domain of warfare seconds matter. The Victorians adjusted to changes such as the telegraph and the railway. It changed the way commanders could communicate and move troops. We are just beginning to understand the true measure of how transformational this new technology is.

One challenge that government must deal with is the question of recruiting and retaining sufficient numbers of well qualified technologists who can understand the implications of new technology and translate them into coherent policy. This applies across government, from the centre in Whitehall, through the departments and into the research and development arena. Naturally enough sufficient funding will remain a central issue. The UK must also ensure that its sovereign capability is safeguarded. This will need good co-operation with industry, as government cannot keep abreast with developments and does not own the Critical National Infrastructure. Something which government can be thinking about ahead of the next strategic defence and security review.