The House of Commons Defence Select Committee (HCDC) published its report on the MOD's approach to Cyber Security on 9th January. It rightly draws attention to the extent of the UK's defence capability's reliance on cyber related technology. This is both an advantage and a risk. The advantage lies in the UK's expertise in this area. The risk lies in the central nervous system of the UK's defences becoming paralysed.

The report notes that the MOD's most important task in the cyber domain is the protection of its infrastructure. This is generally summarized as Information Assurance (IA); ensuring that the MOD's network is able to operate, and that the information within it is secure. This in turn requires a coherent doctrine and training for MOD staff and in the services to ensure that everybody is "cyber-savvy". The Committee implies in its report that the MOD hasn't quite got a handle on the matter, although it stops short of outright condemnation. Part of the problem seems to lie in the extensive nature of the MOD's activity and perhaps a feeling that certain areas are not "front-line" so not at risk. Practitioners who work on cyber security questions recognize that there is no real front line anymore.

The advent of the cyber security domain and the attendant demands on the MOD comes at a time when the Department is undergoing large scale transformation. Despite additional resources being directed to this area the underlying turbulence is having the effect of driving good people out, such that the MOD (and perhaps Government generally) lacks adequate skilled staff. The MOD's budgetary pressures, including a reduced R and D budget only adds to the challenges.

The particular challenge of cyber security lies in the speed with which any attack might manifest itself, and the speed of reaction. The nature of asymmetric warfare is to attack the enemy where they are most vulnerable. Whilst the MOD's infrastructure may be safe, there may also be back ways into critical infrastructure such as power supplies and telecommunications which could disrupt everyday life. This is a Government wide problem and the report notes that the MOD is but one part of the UK's defence and security apparatus. Local government or utilities are just as vital to the nation's well-being in many ways as the military.

The report draws attention for the need of Government to ensure that cyber security measures are adopted on a nationwide basis. This is especially the case where the supply chain for both the IT and defence industries are concerned. Part of the solution to this lies in simple things such as good communication within and between industrial partners and government departments.

The report encourages Government to be a little more proactive in promoting what is emerging as one of the principal threats to the UK's well-being. A Maginot line mentality will not do. One can almost hear the Chairman's tone of disappointment; could do better.