By Nick Watts

The UK government is due to release the latest version of its Cyber Strategy – what opportunities exist for defence contractors?

The UK has a privileged view of the cyber threat thanks to its signals intelligence relationship with the USA and other allies. Both the US and UK have recently formed dedicated cyber units in their defence ministries to address this threat. During the formulation of the National Security Strategy (NSS), the government became increasingly aware that underlying every major threat was a discrete cyber threat. Consequently cyber was mentioned as one of four Tier one risks to the UK in the NSS. In the subsequent SDSR the government announced an additional £650 million over 4 years to resource work on this threat. The new money is to fund a "transformative national cyber security programme".

Most people are aware of such things as anti-virus programmes on their personal PC; or of the risk of on line fraud. Corporations are also increasingly aware of the threat from so called Hacktivists; ideologically motivated hackers who seek to damage them. But it goes beyond that. Nowadays military operations are dependant on secure communications and data links to enable a swift and accurate response to emerging threats. The GPS system is an example of this. So the news that the Taliban have been able to intercept the video data being streamed from a drone in Afghanistan will have concerned many. This demonstrates how low the barriers to entry are in this domain.

This new form of warfare is not gong to go away. It has been dubbed the fifth domain, alongside Land, Sea, Air and Space. How can the UK leverage its privileged position to secure advantage for contractors seeking to develop opportunities at home and overseas?

The Cabinet office leads the cross governmental effort, with MOD and GCHQ playing a significant role. There are 18 agencies or departments with a direct operational interest in countering any cyber threat. A comparison can be drawn with the effort the government put into developing a resilience capacity following the terrorist attacks of 2001 and 2005.

Recent moves by defence contractors to acquire cyber capability by organic growth or acquisition represents a sensible response to the changing threat environment.

The MOD itself is about to produce its own White paper which will outline what equipment and technology the MOD and the UK's defence sector will be investing in. In the Green paper consultation earlier this year, much was made of the MOD's wish to invest in the technology and capability which it felt was absolutely necessary to maintain the capability needed if the UK was to remain a credible player on the world stage. Key to this will be operational sovereignty in crucial areas like secure communications which embraces the cyber domain.

Any cyber strategy must be set in a wider context. The UK government is hosting a high level conference at Lancaster house on 1-2 November in the hope of establishing some

internationally accepted norms. A legalistic approach to this problem would be impossible to police, given the speed of development in the IT world; and the speed with which hackers and others react to counter measures. Some more authoritarian regimes prefer such a legalistic approach, however, as they recognize that legal interpretation and sanction would take a long time, by which point the culprits will have covered their tracks.

So any cyber strategy must seek to boost the UK's ability to influence the conversation internationally and to protect the UK's open economy. This will depend on effective Information Assurance (IA) measures. The need for effective IA applies as much to retail banks as it does to Critical National Infrastructure and to our military capability. The extent to which the world's economy has digitised is reflected in the fact that in 1995 there were 16 million web users; today that figure is 1.7 bn. Terrorists or others looking for a vulnerable point to attack a country will exploit weaknesses in its cyber infrastructure, as happened to Estonia in 2008 and Georgia in 2010. A Cabinet office study estimated that in the UK in August 2010 some £4.4bn worth of transactions took place on line. The government is looking to deliver more and more services on-line. The savings to central government by delivering services this way can only be guessed at. But the corollary of this would be the need for effective cyber security if the UK is not to be paralyzed in the same way that Estonia was.

The UK has a good reputation in this domain internationally, so the government should stress the opportunities for links with trusted allies in addressing this threat. Both NATO and the EU are developing capabilities to counter the cyber threat, and this was one of the joint areas for further exploration mentioned in the Franco-British defence co-operation treaty. So alongside resilience, the second pillar of any cyber strategy must be partnerships with trusted allies overseas, as well as domestically. Within the UK companies and enterprises must be encouraged to share best practice and joint development of solutions to newly emerging threats.

So far so good, but recent reductions in spending on R&T must be concerning at a time when the cyber threat is rising. The government's allocation of funding to address this threat must be seen as a down payment against additional funds which will be forthcoming once the full scope of the cyber threat becomes apparent. This domain represents an opportunity for the UK to seize an early advantage internationally. Both industry and government must co-operate to exploit this, as well as safeguarding our national security interests. The new Secretary of State at the MOD will want to keep an eye on this.

This article first appeared in Jane's Defence Weekly. Reproduced by kind permission of the author.