Adam Dempsey, Research Associate UK Defence Forum

In the aftermath of last week's Strategic Defence and Security Review (SDSR) many industry analysts were quick to paint a bleak future for the UK's defence sector. Further job losses are expected as hardware is retired, personnel numbers reduced and service contracts terminated. The global marketplace is unlikely to offer much in the way of respite. The United Kingdom joins France, the United States and others in seeking to offset shrinking domestic markets via exports. A crowded marketplace is further exacerbated by challenges from states with more 'joined-up' defence-industrial bases and emerging market entrants. The £650 million allocated to cyber security by the SDSR may provide new opportunities. Yet the specific nature of the UK's cyber security requirements remains unclear. Indeed, total clarity does not appear to be on the horizon.

What the SDSR makes very clear is that threats to national security emanating from cyber space are likely to increase over the next five to ten years. Whilst cyber attacks from hostile states cannot be ruled out, the actions of cyber terrorists and criminals are perhaps of greater concern. In 2009 alone 51% of all known malicious software threats were identified. The language of the SDSR also suggests that Government departments are not yet capable of fully addressing the threat. As a result, the £650 million allocated will support a National Cyber Security Programme that seeks to transform the Government's response in partnership with the private sector.

Greater clarity may be provided with the publication of the Defence Industrial Green Paper by the end of the year, followed by a White Paper in 2011. In advance of such publications, the increased emphasis upon cyber security has influenced a raft of recent mergers and acquisitions (M & A). During the third quarter of 2010 more than a third of all defence M & A concentrated on cyber security capabilities. The most high-profile acquisition was the EADS subsidiary Cassidian's purchase of the UK's Regency IT Consulting. According to Jane's, the purchase reflects Cassidian's overall cyber security strategy for the UK market. The purchase also suggests that defence companies are positioning themselves to ensure that they will benefit from the clarity that future Government documents may offer.

Cassidian's purchase of Regency IT Consulting also reflects the growing cyber security opportunities emerging throughout the international marketplace. As other markets – and indeed governments – seek to mitigate the threats posed by a cyber attack M & A focussed upon cyber security solutions are likely to increase. A cursory glance of Regency's website may also provide an insight into the public-private cooperation to be forged by the National Cyber Security Programme. Underpinning Regency's services is the practice of managing information-related risks with Information Assurance (IA). From the development of IT infrastructures through to the storage of information, IA seeks to ensure that authorised users only have access to privileged and confidential data.

As is to be expected Regency's website also outlines the type of services it offers. Yet if the U.S. cyber security market is anything to go by certain services offered to the Government may

not make company websites. U.S. cyber security programmes have been estimated to be worth $11 billion. As these focus upon the protection of IT infrastructures, hardware and networks they also provide another indicator of possible contents for UK programmes. However estimates that approximately 75% of cyber opportunities are 'black' also suggests that aspects of the Government's programme may remain a largely grey area. Of course, the upcoming Green Paper may make the UK's cyber security strategy more clear. But if the machinery of government decides to replicate its American counterparts future documents may also make bold proclamations whilst keeping exact details to a bare minimum.

Indeed, such high levels of confidentiality make perfect sense when national security is at risk. One only need look at havoc wreaked by the Stuxnet virus on Iran's nuclear facilities at Bushehr or India's main television satellite to appreciate that a cyber attack is often against networks that societies take for granted. Giving challenges to cyber security more information on infrastructures ensures that the perpetrator maintains the upper hand. Accordingly, the specifics of national cyber security strategies – and purchases – may remain a grey area for some time to come.