From the fog of war to the blizzard of information: Big data and defence

As the military and security worlds become increasingly reliant on smart ICT systems for campaign planning and communications, a problem is beginning to become apparent: how best to handle the data that is gathered. Modern operations rely on communications to enable commanders in the field to reach back to the firm base for both technical and political guidance, and to reach forward to unit commanders. Remotely Piloted Aerial Systems (RPASs) pass continuous video feeds back to HQ for analysis. At the same time modern fifth generation aircraft such as the F35 transmit large amounts of information about its engineering and sensors performance. Welcome to the world of Big Data, writes Nick Watts.

Except that Big Data is nothing new. At a recent conference arranged by the Royal United Services Institute (RUSI) to examine the topic of Information Superiority in Defence, frequent reference was made to the fact that Big Data existed "out there in the real world." Anybody who has a supermarket loyalty card will understand the concept. Millions of items of data are processed everyday by retailers, which helps them to keep track of consumer preferences and manage inventory levels; then to send consumers prompts about offers at their local outlet. The trick is in handling this large amount of information, or data set.

Modern computers process large amounts of information in a short space of time. A Megabyte (MB) is the equivalent of 500 pages of text: a Terabyte (TB) is the equivalent of 300 hours of video streaming. It is easy to see how processing large amounts of data can be useful to the defence and security worlds. The recent Snowden revelations about NSA and GCHQ retrieving large amounts of meta data on telephone and internet communications shows that these agencies possess capability to handle Big data, but what about its application on operations in Afghanistan and future events?

What became apparent during the course of this conference was the size of the challenge to Defence a modern operation presents in terms of the amount of data generated. Every interaction between security forces and the local population generates information. Battlefield exploitation (forensic analysis in the civilian world) also generates digitized fingerprints and other biometric data. Modern medical techniques which use telemedicine results in saving lives,

but this also requires the use of precious bandwidth – Satellite communications for the most part.

The challenge to Defence is how to manage the information in a timely manner: how to maintain systems which are up to date and how not to get ensnared in the kind of IT fiasco which seems to bedevil the public sector; and how to keep all of this traffic secure. The way that this challenge is being dealt with is instructive. Where possible the MOD would prefer to have a system that is as much like the "real stuff" that service personnel use at home. This means both applying Commercial Off The Shelf (COTS) applications and keeping contracts on a smaller more manageable scale.

As part of the Levene Review the MOD has undertaken to put the management of information at the heart of the way it does business. As part of the Defence re-organisation, information related activity is being built into Joint Force Command (JFC). Henceforth JFC will "own" all the Information and cyber capability in the MOD. This has given rise to a two headed beast the Information Board which is co-chaired by the Joint Force Commander and the Permanent Under Secretary. Underneath this will sit a 3 star equivalent Chief Information Officer; JFC will also host the MOD's Information Systems and Services (ISS) which was previously housed by Defence Equipment and Support (DE&S).

Some observers feel that this effort is no more than moving the chairs around and that the real challenge for the MOD as with other defence ministries will be how to speed up the procurement system to enable it to cope with the protean nature of the information domain. In a challenging budgetary climate the positioning ahead of the 2015 SDR is beginning. Information and the related cyber domain are seen by MOD as "key enablers". These are going to be built into any future capability planning.
The next SDR could turn out to be a re-run of the Dreadnought campaign waged by Admiral Jacky Fisher. The proponents of "old" style conventional war fighting will be hard put to make their case against those who see the future of defence in the realms of cyber and information systems enabling RPASs and PGMs to deal with the enemy at range while Special Forces intervene surgically to knock out key commanders and HQs. MOD will have to work with other government departments (FCO, DFID) in future campaigns; their systems will have to talk to each other. All of this will have to fit into coalition operations which will pose security challenges in passing classified information. If the UK is to retain its cutting edge in future operations it must have platforms and systems which can talk to each other as well as to the humans who will operate them.

Trying to predict the future of this domain isn't easy – which inclines commanders and politicians towards caution. Recent sessions of the Public Accounts Committee loom large in the thinking of those charged with the good stewardship of public money. In this domain technology is leading and defence is following. The civil servants are rightly wary of industry representatives offering panaceas, but at some point they have to take the plunge. One speaker quoted Henry Ford, alluding to what the public wants: "if I had listened to my customers, I would have produced a faster horse!"