

By Nick Watts, Great North News Services

The bi-annual arms fair DSEI took place in London during September. Amidst the usual array of armoured vehicles, weaponry and warships, one trend became very clear. Whilst most of the conventional defence industries are standing still waiting for new programmes to be announced, the cyber world has become very busy indeed.

Most governments seem to agree that, for the time being at least, the risk of a significant land based state on state conflict is minimal. The legacy of Iraq and Afghanistan, and budget constraints, means that armed forces have got the equipment they are going to need for the next 5 years. Up-grades and service life extension programmes looks like keeping conventional defence contractors ticking over for the time being.

By contrast the cyber scene is buzzing. There were a series of well attended seminars on the theme of cyber security and related matters over two days at DSEI. There was plenty of discussion about just what is meant by cyber security – or cyber war. The danger of getting lost in semantics was evident in seminars discussing a cyber regime, or a cyber doctrine. In part this was due the absence of the expected cyber strategy paper, which is sitting in the cabinet office awaiting publication. Even an appearance by Home Office minister James Brokenshire couldn't fill the void, as he largely said what people expected him to say.

Industry seems to be at a chicken and egg moment. It seems to be waiting for the government to say something, anything, in the hope of discerning the direction of travel that the UK will take. Doctrinally the government is constrained by the enormity of the subject it is trying to embrace. Whilst recognizing the huge benefits to the UK economy of a digitized world and the efficiencies that can be derived by delivery of services on-line, the risks of cyber crime are equally huge.

A recent study has calculated that cybercrime costs the UK economy £27 bn annually. This figure is an estimate because of commercial sensitivities surrounding this matter. One approach being advocated by speakers at DSEI was for business to recognize the considerable financial and reputational risk they run by not maintaining resilient IT systems. Trying to create a 21st century Maginot line will have the same effect – the criminals and others will find a way past it. Being able to defend critical information in a system which may be compromised offers one solution. Recognizing that ultimately security relies on the human dimension is another.

Criminal activity centres on the opportunities for on-line fraud or identity theft. This is a worry to the financial services community. However, the risks to industries such as pharmaceuticals, scientific and technical industries from data theft or loss of intellectual property is actually greater. It is estimated that £9 bn is lost annually in this way.

Alongside the criminal element are what are called "hacktivists" those who are motivated by either ideology or revenge, to cause embarrassment to high profile companies. This can be

crashing a web-site or leaking telephone numbers to other activists. The pharmaceutical and energy industries are often attacked in this way. Targeted industrial espionage is another threat. Hacktivism has one benefit, in that the IT industry tends to respond to these attacks by developing the cyber equivalent of anti-bodies to deal with them, but it is a cat and mouse game.

Underlying this is the deeper more sinister threat of cyber attacks initiated by states. These arise for two reasons. Firstly scientific and technological competition; to get access to western know how without having to go through the hoops of research and development. Secondly to develop an understanding of security and defence information. Straight forward spying without the need for any agents in-country.

Most of the elements of critical national infrastructure are now owned by commercial entities; utilities, transport and telecommunication links, for example. These are areas which could possibly be attacked by a state of state sponsored actor, which wishes to harm our economic well being. Ensuring the integrity of this system will be the first priority of any likely cyber strategy. Getting industry to work together to address this problem will be the second. How this will be managed remains to be seen. But the message is clear. This is the threat the UK government is most exercised about.

Consequently defence contractors are examining their offerings to be able to respond. Who will be the winners and losers? Maybe this is the opportunity for new players to arise. Think of Research In Motion (RIM) – which stole a march on the market with the BlackBerry; or General Atomics, who did the same with Drones. Maybe there is a company out there with a clever application, waiting to seize the moment.....

Update 30th September : Ultra Electronics buys AEP Networks (secure comms) for \$57.5 million to boost its cyber security business.