The hacking stories just keep on coming. Of course, The News of the World is the big one at the moment, matched, for the moment at least, by the hacking of The Sun's website by celebrity – and proficient – hacking group LulzSec.

Other interesting stories on hacking exploits keep cropping up, but are perhaps not getting the same high-profile coverage. One well worth having a look at is the fact a Pentagon supplier recently lost 24,000 files to a foreign intelligence service.

There are several interesting things about this hack:

1) It was an unidentified defence contractor, and not the Pentagon, that lost the files.
2) The Pentagon believes the perpetrator was a foreign intelligence service.
3) The response has been a confirmation by the US military that cyberspace is a legitimate theatre of war.

That it was a military contractor that was hacked, and not the Pentagon itself, is significant. A chain is only as strong as its weakest link. The Pentagon itself might have the best security systems and procedures imaginable. But if its contractors do not have comparable standards it can all be for nought. As more and more business moves into the "cloud" this is going to become a matter of increasing concern. There is an element of irony here.

The internet was born of a US Department of Defense-sponsored research project into survivable networks. The network is robust in that it deals well with sudden node failures but the systems that run on it seem to be much less robust.

It is significant that the Department of Defense has reacted by calling for increased research and development that will provide protection from system vulnerabilities.

The Pentagon believes the perpetrator was a foreign intelligence service. This really is not surprising. Internet based espionage is just another variation on signals intelligence.

Despite efforts by authors such as Ian Fleming and John Le Carre, the image of espionage as the work of James Bond and George Smiley characters is outdated.

Human Intelligence gathering (HumInt) has not been the main source of useful intelligence for decades. SigInt (the common abbreviation for signals intelligence) has, according to Geoffrey Robertson (in "The Justice Game") been the main source of intelligence for Western powers since at least the 70s.

Of course, excessive reliance on SigInt took a hammering following the Iraq war, but it should not come as a surprise that Intelligence agencies have strong capabilities in cyberspace hacking. Nevertheless, it is interesting to see that confirmed.

Perhaps what is most interesting though is that the Pentagon has declared that cyberspace is a legitimate theatre of war and that offensive capabilities are needed as well as defensive ones.

There is a great asymmetry in the internet. It is much easier to attack a site than defend it. We have all seen, only today, organisations such as LulzSec (apparently made up of only six people) humble a huge organisation with an attack.
It only needs a poorly-written piece of code, a misconfigured firewall or an unpatched operating system to give the hacker an opportunity. It is intriguing to speculate what sorts of attacks might be possible if the might of US military were thrown behind this.

It’s also intriguing that attacks in cyberspace may be responded to with military action. These are certainly interesting times and are probably going to become even more interesting.