The U K Defence Forum's Euan Grant was in the audience for a Global Strategy Forum briefing at the Houses of Parliament on 20th March.

Speaker General Peter Pace, USMC (retd.) was the Chairman of the US Joint Chiefs of Staff during President George W Bush's second administration began by highlighting that as both VCJCS and CJCS it was his responsibility to identify the capabilities and vulnerabilities of the USA's offensive and defensive cyber warfare capabilities, a clear indicator that such responsibilities are now part of the command duties of all senior commanders. As such, he knew what his nation could do offensively, but not what its defensive capabilities were as these were obviously dependent on the opponent's own offensive capabilities. Currently, attackers have the advantage.

Gen. Pace's current view is that the threats are from nation states, terrorists, criminals and hackers, currently more or less in that order but with blurring of the distinctions likely to increase.

As advantage currently lies with the attacker, the situation now is comparable with the introduction of nuclear weapons. The biggest factor in encouraging non-use is the deterrent effect. However, actual use of a cyber-weapon inevitably alerts the defence sooner or later, so, while CJCS Gen. Pace always advised President Bush that, when considering response options, other means should be considered before exercising a response in kind. An offensive use can be considered an act of war and broadcasts your own capability creating vulnerability to reverse engineering. Stuxnet in 2010 was pointed out as the exemplar of such nation state to nation states actions.

The risk of creating unintended consequences is high, e.g. an attack on power plants or grids could hit many non-targets.

Well known early generation cyber attacks were typically DOS (denial of service) attacks using multi sourced botnets and were brute force attacks which did not actually alter data. Examples include : In 2007 against Estonia from inside Russia and "from" Vietnam, Egypt and Peru, in 2007, and in 2008 against Georgia, mainly "from" the US.

Within a few years, terrorists will have botnet attack capabilities. Certainly, nation states can currently close a national grid and other very high priority targets are banks, stockmarkets and oil and gas installations (Aramco 2012).

Currently, nation states have the capability to introduce long term Trojan Horses, well before any possible activation by the use of "sleeper codes". This capability will be available to terrorists and hackers in five to ten years.

In relation to theft of intellectual property, especially of strategic significance, the Chinese are searching our brains every day. They had details of the F 35's airframe even before it flew. Attacks have been launched against not just Lockheed Martin but against the less well defended systems of sub-contractors.

What can be done, should be done, and how. The solutions probably require a 20/80 approach.

20 % of the answers are in the hands of government, which has to protect itself and ensure education of others. The private sector is the other 80% and must work itself and with government. While separate sectors must do their own bit, within these there must be unity of command, as Gen. Keith Alexander has within the US government, reporting directly to the DNI and DHS. The US military needs to upgrade Cyber Command to a full command comparable to those for Army, Navy, air Force and Space.

There needs to be greater cooperation with the private sector and allied countries through use of special joint testing operations and discussions with states which are potential partners or competitors, somewhat along the lines of joint submarine rescue training exercises with Russia. In such cooperation, it is essential to only let in the "known good". That is the vital default option.

In the Q & A a variety of scenarios and issues were raised.

Was defence possible against the effects of electromagnetic pulses (EMP)? Gen. Pace believed not, but pointed out that such an attack could obviously not be covert given that it was a

capability only available to a known few.

Was it currently possible to shut down London for a month? Yes.

Would the cyber bomber always get through? The reply was the USA cannot currently defend against its own known offensive capabilities.

What about further thoughts on unintended consequences, especially regarding Iran? Gen. Pace pointed out that, unlike Iran in relation to its nuclear programme, no state had as yet been subjected to physical kinetic attacks in response to cyber attacks, a point doubtless noted by Iran, Pakistan and North Korea.

Are we moving towards a situation where the ability to identify the sources of attacks will be reduced or lost? Gen. Pace stressed that attribution is indeed extremely difficult, and it is relatively easy to disguise sources, as indicated by the examples quoted earlier in the presentation.

China and Russia were reported to be creating their own national Internets. Are western countries shooting themselves in the foot by using non-Windows systems? Gen pace replied that the current Internet , "Internet One", was in a Wild West state and now and in the future the need was to build an Internet Two with both greater preventive security measures and subject to stricter rules on misuse. From the governmental national security point of view there was a need to enhance currently known capabilities to create active defences which can automatically attack the attacker. Some parts of the private sector, including financials, must be deemed national security assets with appropriate levels of defence and resilience. The current state of the art in cyber defence is that it is at the good hygiene stage, with prevention being more effective at present than the cures available.

It would be useful to note the similarities of views regarding offensive cyber warfare with those of Dr. Thomas Rid of Kings College London, who spoke at KCL on 15th March, ahead of the April publication of his book "Cyber War will not take place". His central theme was that the risk of comparable retaliation would greatly limit the prospects of cyberwarfare in a manner similar to the MAD (Mutually Assured Destruction) strategies of the Cold War, an argument consistent with Gen. Pace's views on the importance of maximum restraint regarding the use of offensive

capabilities.