Workshop C1

Cyber security – quantifying risks, clarifying responsibilities and building resilience

Chair
David Francis, *Chief Security Officer,* **Huawei UK**
Expert speakers
Cheryl Martin, *Head Cyber Security Practice for Business Consulting,* **CGI**
Dr Jamie Shea, *Deputy Assistant Secretary General for Emerging Security Challenges,* **NATO**

The speakers covered the following areas thereby starting at the bottom of the chain with the equipment providers then building via corporate to national level threats:

- David Francis covered the suppliers' point of view, outlining the Huawei end to end assurance program, calling for aligned assurance techniques and metrics.
- Cheryl Martin addressed the corporate and utility customer perspective, providing attack and threat statistics from a range of sources, highlighting the scale of the issue.
- Dr Jamie Shea covered the national and military view of the threats, and explained how the nature of "attack" and war had fundamentally changed.

Noteworthy points arising from the open discussion:

- A number of contributors wanted to share experiences, which demonstrated that everyone had been directly touched by cyber-attacks in one way or another. It was noted that Lloyds had moved Cyber from 11 to 3 in their list of risks.
- The key topic of interest was: how do we encourage consumers and corporate to take basic measures? There was agreement that if we could achieve this then it would be a strong step forwards. The delivery of education needs to inform without scaring consumers away from the digital economy. Measures in this area to date have not been as successful as hoped.
- There was discussion on whether cloud computing is intrinsically more or less secure than local storage. The view was forwarded that neither is intrinsically secure, and that the cloud can be more secure than local storage if appropriately implemented.
- The digital divide between those countries who had invested and those who had not was discussed in terms of whether or not information should be shared, and whether those that have invested have a duty of care to help those who have not.
- The use of cyber to attack physical national assets became a lively topic, with examples from the floor. The session explored how physical attacks on a country's assets in the past would have required military hardware and therefore would have been a clear act of war, yet by using viruses these attacks are now more nuanced (e.g. the Iranian nuclear facilities).