Asymmetric Threats Contingency Alliance

Inaugural Session – 28th November 2002

Debate Summary – Key Findings

The event was held under Chatham House rule so no particular individual can be attributed to any of the points raised nor can the attendee list be released. It was agreed that the key findings would be made available in recognition of broader interests.

Purpose

- ATCA must be more than just a special interest group – the asymmetric threat issues arising from conventional as well as unconventional – Chemical, Biological, Radiological, Nuclear and Digital (CBRN-D) – means must be addressed in a meaningful and practical way.

Values

- In pursuing the War on Terror, we must go further than just emphasising our collective vulnerabilities but deepen our understanding of the values that we are trying to protect in pursuing this war on terrorism. Business leaders must clarify their role in terms of what they have to offer and protect in this regard.
- There are many differences in culture and values within the Islamic world itself, but there has been a tendency for certain fundamentalist elements within these societies to be united by a common antipathy towards the West.
- Attack is not inevitable from a society just on the basis of having different or incompatible value systems. The real danger is more from the outright rejection of values from within the same society by those who have been brought up to follow them.

Digital Terrorism

- It is important not to exaggerate the risk of digital terrorism and there is no justification for equating hacking with terrorism.
- The tools hackers are capable of deploying can be effectively used by terrorists when used in conjunction with conventional weapons to amplify their damage and disruption. Such blended threats are more likely.
- Digital attacks can be put into two categories – Data attacks and Command & Control (C2) attacks. The distinction between protest or crime, ie, “Data” and cyber terrorism, ie, C2 lies in the differences between these two categories.
    - Command & Control attacks are usually not possible without insider help and are very different from Data attacks, both in terms of their essential nature and in the degree of damage they make possible.

    - It is very difficult for hackers to know where to really hurt an organisation's network once they have gained access – for this reason the importance of the insider cannot be underestimated.

- The Falun Gong movement in China has been very successful in their protests using digital warfare as a propaganda tool by spoofing Chinese state radio and television content by hijacking Chinese communication satellites.
- The Vitek Boden incident is the only known and closely understood incident of Command & Control type attacks – we should not become too fixated on this single incident in attempting to deal with these risks.

Digital risk in small to medium size enterprises

- Digital risk can be the cause for certain SMEs going out of business, both in terms of the cost of prevention and the cost of recovery.
- Small to medium size enterprises are in general very poorly informed in regard to digital risks.

Terrorism and the Insurance and Reinsurance industries

- The main problem with terrorism cover today is that the current risk distribution systems are archaic and mainly intended for more general property and casualty cover.
- Premiums for terrorism cover can be easily priced but cannot be made affordable with the risk distribution systems currently in place.

Challenges for business

- The current climate of risk aversion was manifest in the business world well before 9/11.
- Physical terrorist attacks are making a very significant impact on trade and the conduct of business.
- We must appropriately address the issue of export licences and standardise best practices for business to prevent supporting terrorism inadvertently.
- It is irresponsible to just sell Broadband on its own. It is better to sell it as a package incorporating proper security measures both to prevent attacks directly on the user and to prevent the victim machine being used in DDoS attacks. Some companies are already selling Broadband with appropriate security measures in place such as firewalls, intrusion detection and anti-virus tool kits.

Fallout of the War on Terror

- Organised crime can perceive the War on Terror as causing difficulties for their interests.
- There is a need for greater democratic oversight in the War on Terror especially in regard to the use of Special Forces, the necessity of fair trials and a proper legal definition of terrorism.

Key issues to be addressed in the next ATCA session:

- Ways of addressing cross-border threats collectively between international organisations and individual governments and their agencies.
- Changing the nature of Information and Intelligence sharing both within organisations and between the public and private sectors.
- Use of specialists from the private sector by the government and military in the War on Terror.