Asymmetric Threats Contingency Alliance

Inaugural Session – 28th November 2002

DK Matai, Chairman and CEO, mi2g

My Lords, Ladies and Gentlemen

Thank you for joining us for the inaugural session of the Asymmetric Threats Contingency Alliance (ATCA). It is a great pleasure and honour to address you this evening with strong reinforcement from such a distinguished panel of experts. Please feel free to contribute to the discussion, which will take place under Chatham House rule.

In recent weeks our Prime Minister, Tony Blair, and the Home Office have reminded us of the potential threat from terrorists, including the use of unconventional weapons.

Having said that, it is interesting to note that the proposed session for ATCA on 2nd October was postponed owing to industrial action on the Underground. This week, the Fire Union's strike is forcing the Ministry of Defence to provide national cover and hampering the capability to respond effectively should a sudden emergency arise.

So, all the conjecture about terrorists and potential threats pales in comparison to the unpredictable 'threat' from within!

Background to ATCA

When we were invited last year in October by Andrew Pinder, the UK eEnvoy, to discuss the world beyond 11th September, we looked at asymmetric threats from a variety of perspectives. We looked at systems both from a computer, infrastructure and buildings perspective as well as people. People play a vital role in running the business, but may not have been seen as the crucial component that could get wiped out in the event of a terrorist attack as opposed to the backed up data.

For example, some of the organisations that suffered a heavy and direct blow in the World Trade Centre incident such as Marsh, Morgan Stanley and Cantor Fitzgerald, had their IT backup systems available the next day. Unfortunately their workforce had been decimated. How does business respond to such a challenge in the years ahead?

We examined the subject of Asymmetric Warfare in detail with a distinguished panel of experts in November last year at Lloyd's. The insurance and reinsurance exclusions for terrorism cover and their impact were examined closely.

In March this year, we discussed the people issue of Asymmetric Warfare at the British Computer Society's Information Security Specialist Group through a keynote speech.

The subjects of digital risk and business continuity within the insurance and reinsurance sector were then looked at by **mi2g** within a colloquium organised by the International Underwriting Association in May this year.

The Asymmetric Threats Contingency Alliance

The terrorist attacks of 11 September 2001 as well as the recent incidents in Yemen, Indonesia, Pakistan and Russia have introduced the West in particular and the world at large to the risk of asymmetric warfare. The purpose of ATCA is to promote the discussion and awareness of these threats facing today's society among decision makers and facilitate better understanding and co-operation between government and business when it comes to both mitigating and responding to all forms of terrorist attacks.

With the explicit mention of the United Kingdom - amongst other G-8 countries - by Osama Bin Laden in a recent audiotape as a target for further terrorist attacks by al-Qaeda, there is a requirement to act now and identify ways in which the impact of any such incidents would be mitigated.

Looking into the future, there is possible action against Iraq by US and UK forces. There has been an open threat from a range of radical organisations that they will embark on causing terror and economic disruption should this materialise. No doubt, some of this rhetoric is empty and it pulls a veil over the real threat from the few who may have been planted as sleepers in the past.

Simulation

Modelling the threats from asymmetric attacks be they manifest in cyberspace or in the physical world from chemical, biological, radiological or nuclear (CBRN) threats is of significance to the emergency response planners, operational managers as well as the insurance and reinsurance industry.

Post the Oklahoma bombing, US authorities carried out a simulation to study the effects of a biological weapons attack that unleashed the smallpox virus. By the end of the simulation the disease had spread to 25 states and 15 other countries.

Expert Panel

Please allow me introduce our panel of speakers that have agreed to join us this evening:
Adrian Ballardie, Chief Executive of Axa Corporate Solutions UK, will be speaking to us about the current state of terrorism reinsurance in the US and the activities of the Digital Risk Working Party at the IUA.

Rudi Bogni, Chairman of MedInvest International and a Director of Old Mutual, will be speaking on the social implications of digital crime.

Dr Ian Davis is Director of the British American Security Information Council and will brief us on the key security threats in the post 9/11 world.

David Handley is the Director of Group Strategic Analysis, BAE Systems. Previously he has been with the UK Foreign Office for 27 years with particular experience in the Middle East. David will be speaking about the "War on Terrorism": Who is a threat and who is not? And addressing the response of the international community to those threats, led by the US.

Professor Jim Norton is a Board Member at the Parliamentary Office of Science and Technology and will speak on the subject of Distributed Denial of Service (DDoS) attacks.

Garth Whitty, Head of the Homeland Security and Resilience Programme at RUSI, will be speaking on the subject of Weapons of Catastrophic Effect.

Finally, I would like to discuss the role played specifically by digital attack and its evolution into a particularly dangerous tool when used as an adjunct to conventional weapons.

Technology led asymmetric warfare

The big fault line visible in the world today lies at the junction of radicalism and technology. Terrorists have organized themselves to penetrate open societies and turn the power of modern technologies, on which we depend, against us.

We started collecting data on overt digital attacks on computer systems across the globe in 1995. From only a handful in the first three years, the number of attacks taking place has now crossed 70,000 in 2002. Some years have seen a 10-fold increase!

The most significant findings from our intelligence database are that trends in digital attacks act as a barometer of political tensions worldwide. It is interesting to note that in recent months the trend of attacks against online systems based in the United Kingdom has escalated – 211 overt digital attacks on the UK in August grew to 479 in September followed by a sudden explosion of activity in October, where a total of 2,253 attacks were recorded. And that is not all.

We have seen that there has been a tendency for hackers to choose the "low-hanging fruit" such as ill-prepared small to medium size business enterprises. This is the age of automated attack tools that are freely available on the Internet. As soon as any software vulnerability associated with a particular operating system or application becomes public knowledge, the release of tools exploiting that vulnerability takes place within a few hours.

The large and well-protected government or corporate networks which will often require relatively greater time, skill and experience together with extensive "social engineering" are as a consequence much harder to penetrate.

The effect of distributed attacks is the same. Economic damage is caused and confidence suffers.

Blended Threats

Equating hacker groups who cause damage with terrorist organisations that kill people with powerful explosives may not be justified. Having said that, the biggest threat could still be a blended threat: digital attacks that cripple emergency response, transport or telecommunications with some insider help, could be employed by terrorists in conjunction with physical attacks to magnify the effects of their intended disruption and damage.

In recent months, information about critical infrastructure has been ferreted via the Internet; this has been traced back to IP addresses in Saudi Arabia, Kuwait, Pakistan and Indonesia.

Sophisticated computer programs used by engineers to find stress points and weaknesses in buildings, bridges and dams had also been found at the tail end of 2001 and early 2002 in computers belonging to suspected Al-Qaeda members in Kabul, Afghanistan. So even if the ability of a terrorist organisation to conduct direct attacks against critical infrastructure is limited, cyber attacks can be used as a highly effective reconnaissance tool to precede physical attacks and to blend threats so as to magnify the impact.

Command and control attacks

There is growing concern about "Command and Control" digital attacks, which would impact the critical national infrastructure such as: telecommunications, electricity production and distribution, water storage and distribution, nuclear power plants and gas facilities. This would require extensive insider help.

Former or present employees, who may have specialist knowledge of critical infrastructure and the operation of the SCADA, PLC and DCS systems can execute an attack from the outside, as in the case of Vitek Boden in Australia, who was convicted last year of hacking into a computerised waste management system and causing raw sewage to be pumped into public waterways.

Addressing the threat of digital warfare

It has been our experience that certain organisations have suffered incredible losses through a digital attack exploiting software vulnerabilities that were exacerbated by the lack of a proper data back-up regime. One would assume that this was an easy to implement process.

The correct approach to digital security lies significantly more in configuration management and systems integration than in the security considerations made when developing a single piece of software – given enough time, hackers can usually find a way in – the most important issue clearly lies in limiting the damage that can be done by applying patches regularly.

Of course, configuration management is not the only issue – it is usually the case that where really heavy damage has occurred - be it from hacking, viruses or worms - it has usually been with local insider help from within the victim organisation.

It is crucial therefore to apply security precautions in the area of personnel vetting and monitoring, ensuring that an individual can be completely trusted before they are in any position to cause harm to an organisation and instituting policies to prevent the success of common social engineering tactics.

Also, there is a requirement to have the correct legal contracts with personnel, customers and suppliers.

The USD 50 Billion that was reserved by insurance and reinsurance companies post 11th September has led to a significant increase in premiums and a raft of exclusions in most policies. Yet, risk cannot be managed effectively without invoking some insurance measures. The growth of risk exclusions by insurance companies in the area of cyber-crime and terrorism in the past for many areas has necessitated the deployment by vulnerable corporations of alternative methods of risk transfer, but the passing of the Terrorism Risk Insurance Act in the US by both houses of Congress last week will effectively void most of these exclusions on commercial lines insurance policies and allow much needed government backing to be implemented. In the UK we have the Pool Re system for terrorism cover which is not comprehensive. The UK government is currently hoping to extend this system without having to implement new legislation.

Prediction for the future – Government intervention

It is unlikely that governments will choose to remain oblivious to the challenge of daily digital attacks on their citizens and their livelihoods given the economic damage being caused.

Laws will have to be passed throughout the civilized world that will declare cyber attacks that spark fear and cause damage to life and assets as equivalent to physical-world terrorism at an international level. The perpetrators of such attacks will have to be dealt with as terrorists.

Defence has always been about securing trade routes and markets. Given that several Trillion Dollars of trade is routed digitally, counter-attack-forces with electronic weapons that can disable attacking systems from various parts of the world will ultimately need to be deployed with Governments' backing. Counter-attack-forces will save businesses a lot of lost time and money in dealing with rogue, politically motivated, digital attacks from radical and criminal groups scattered across the world and within the nation.