Asymmetric Threats Contingency Alliance

Second Session – 3rd April 2003

DK Matai, Chairman and CEO, mi2g

Ladies and Gentlemen

Thank you for joining us for the second 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 particular, I would like to thank HSBC for making the facilities available today and welcome the National Infrastructure Security Co-ordination Centre (NISCC), the Parliamentary Office of Science and Technology as well as the eEnvoy's Office this afternoon.

Richard Hackworth from HSBC and Peter Burnett from NISCC will be shortly presenting their views to ATCA.

What do we mean by Asymmetric Threats? In essence, any threat which is disproportionate and can destroy a bigger and more organised system is asymmetric. So, 11th September is an example of an asymmetric attack as is a Chemical, Biological, Radiological, Nuclear, Digital or Suicide attack that disrupts our way of life and doing business.

One must not underestimate asymmetric threats like SARS – The Severe Acute Respiratory Syndrome. SARS has become a global issue as cases have been reported in over 16 countries. Large numbers across Asia's economies are catching the region's killer virus, with growth forecasts falling and one brokerage warning the disease could do more economic damage than the war in Iraq. From China to Singapore, the economic outlook is worsening as people cancel flights to areas afflicted with SARS.

Air Canada has just filed for bankruptcy protection. Several other airlines such as Swiss Air and Sabena went bankrupt in the wake of 9/11. Most global airlines acknowledge that this is the worst period for the aviation industry in a long time.

Two incidents took place over the weekend, which are worth reflecting on.

Incident Number 1

Imagine this.

It is a cloudless blue sky in Netanya. Side walk cafes are packed with local people and visitors at lunch time.

An instant later, a young Palestinian wearing blue jeans and athletic shoes walks towards the entrance of the London Cafe and detonates a six and a half pound pouch of nails and shrapnel. The explosion tears a hole through the Palestinian's torso, spews his body parts across umbrellas, flowerpots and sidewalk bricks and injurs at least 30.

“We are told . . . to walk with our gas masks, and then it's a suicide attack that hits," said a victim.

The militant group Islamic Jihad claimed responsibility for that attack stating the bombing was conducted in retaliation for the deaths of Palestinians and as "a sign of support for the Iraqi people and to encourage them to remain steadfast."

In the past 30 months of fighting between Israel and groups such as Islamic Jihad and Hamas, dozens of young men and some women have been sent into Israeli cities, where they've killed hundreds through their suicide missions.

Incident Number 2

Imagine once more.

On Saturday morning, the checkpoint near Najaf in Iraq is not bustling exactly, but fairly crowded.

Then a taxi approaches. The driver is dressed in civilian clothes. Four soldiers surround the car and order him out for a search of the car.

The taxi explodes when the man follows orders to open the trunk.

The hopes of the Coalition Forces of a swift victory have faded in the face of tough Iraqi resistance and guerrilla tactics such as the suicide bombing on Saturday that killed those four American soldiers.

That night Iraqi Deputy Prime Minister Tareq Aziz said the war was going well for Iraq and defended the use of suicide bombers. "When you fight an invader by whatever means available to you, you are not a terrorist; you are a hero," he said.

The radical Palestinian group Islamic Jihad said it had sent would-be suicide bombers to Baghdad, and Iraq said 4,000 willing "martyrs" from across the Arab world were already there to dislocate and dismember allied forces.

Egyptian President Hosni Mubarak said the war on Iraq would have "horrible consequences" and produce "100 new bin Ladens."

Crucial Battle for Hearts and Minds lies Ahead

The war is "against" Iraq. The "coalition troops" are "invading forces". And a suicide attack is a "martyrdom operation". This is how the US-led military campaign is depicted on some of the Arab world's most popular satellite television stations.

Amid strong competition between channels, Arab television world coverage feeds popular perceptions of the war as an illegitimate attack in which civilians - by accident or design - are the primary victims.

It is likely that this type of coverage will lead to the mobilisation of some Islamists to carry out atrocities in the UK or the US.

During the Gulf War in 1991, the Arab and Islamic populations were primarily receiving live telecasts from Western media such as CNN and the BBC. On this occasion, Al-Jazeera and other Arab channels are broadcasting live images directly to the same people. Disturbing TV images are now being brought to the attention of the Western population through continuous digital attacks on websites mirroring the striking content. This is likely to polarise cultures further. If the battle for hearts and minds is lost, this could sow bitterness for years to come, perhaps fuel radicalism and accelerate the recruitment of potential terrorists and their facilitators.

Islamic hacker groups appear to be inspired by Arab satellite channels like Al-Jazeera and Abu Dhabi TV beaming live images of bombings in Iraq and their impact on the civilian population.

The shocking images of dead children were recently broadcast by Al-Jazeera, the Arab satellite channel and then used to suggest in the words of the hackers that, “innocent blood is shed because of greed, and the people are so blinded they don't realise it.” The frame captures were mirrored on several 100 Western sites defaced by politically active hackers such as USG (Unix Security Guards), a group with members from Morocco, Egypt, Eastern Europe and Gulf countries that sprung up in May 2002.

The Pro-American and US Patriot Counter-Attacks

Al-Jazeera's English and Arabic web sites have suffered a series of Denial of Service (DoS) attacks since 25th March. Al-Jazeera has faced criticism from the United States for re-broadcasting Iraqi TV's footage of American PoWs.

Several thousand news and information sites carrying anti-war or anti-American content have been targeted recently by a series of massive denial of service attacks. Pro-Islamic and anti-war digital attacks continue with similar speed and ferocity as on the day the war started.

The National Infrastructure Protection Center (NIPC) operated by the FBI recently warned against patriotic hacking. The sophistication and organisation of the DoS attacks on some of the information web sites, which have recently come under fire despite their complex hosting architectures, is significant.

Informed sources in communication with the **mi2g** Intelligence Unit are inclined to believe that the DoS hackers exhibit skill-sets indicative of a corporate, government or military connection. It could be in the interest of "patriotic American hackers" to silence information sites like Al-Jazeera and Zone-h on the web although nobody has claimed responsibility yet.

Suppression of information sources on the web, censorship or vandalism may not augur well for the future as confidence in Internet services is eroded.

The worldwide economic damage caused by digital attacks in March – primarily protesting the war with Iraq – is estimated to be between $2.9 and $3.5 Billion Dollars so far. The overall economic damage from digital attacks and malware like the Slammer worm is estimated to be between $17.3 and $21.2 Billion Dollars in 2003 up until the end of March. [**mi2g** Intelligence Unit]

The Threat from Weapons of Mass Destruction

mi2g examined the relative feasibility of deploying different forms of weapons of mass destruction including Chemical, Biological, Radiological or Nuclear (CBRN), digital (D) and suicide (S) means.

The research covers a multiplicity of issues involved in the effective deployment of weapons from ease of access for the potential terrorist to the estimated cost involved in acquiring them.

There are multiple issues involved in deploying CBRN-DS weapons effectively

1. How easily can a potential terrorist get hold of CBRN-DS weapons?

C – Chemicals can either be manufactured in makeshift laboratories from reagents that can be obtained openly at low cost or be stolen.
B – Biological agents are always highly secured and their access and quantity is closely monitored.
R – Radioactive material can be stolen from hospitals and medical clinics. It is already established that terrorist groups have a definite interest in producing dirty-bombs or radiological dispersion devices.
N – Procuring nuclear weapons is difficult. Access to nuclear programmes or capability is necessary.
D – Anybody with a computer and some training can carry out a devastating digital attack over time.
S – Anybody with the willingness to die for a cause can amplify the impact of conventional explosives.

2. How easily can a CBRN-DS weapon be deployed?

C – Although there are transportation and dissemination difficulties when using large quantities of chemicals, there is no need for mass casualties for an attack to be successful - a small scale attack on the subway system of a major city with a handful of casualties would cause mass panic and paranoia.
B – This would depend on the nature of the bio-agent used. An airborne virus with a long incubation period and high infection rate could be successfully used as a biological weapon.
R – Dirty bombs are easy to assemble and deploy once the materials have been obtained.
N – Fissile Material is very difficult to transport without detection and then activate with appropriate expertise.
D – It is easy for a skilled hacker, of which there are about 10,000 worldwide, to carry out a devastating attack with appropriate insider knowledge.
S – Anybody who is sufficiently determined can be misguided and trained by experts to carry out a suicide bombing task.

3. What is the inherent danger of being caught or exposing the identity of other terrorist accomplices?

C – Low trace capability (chemical could originate anywhere)
B – Medium trace capability (bio-weapons can be traced back to first contact or outbreak)
R – High trace capability (radioactive isotope is tagged - source will be revealed)
N – Very high trace capability (radioactive isotope is tagged - source will be revealed)
D – Zero trace capability (can act on internet through proxies)
S – Low trace capability (without claims of responsibility)

4. How big could the target-sphere be?

C – Local
B – Local or regional
R – Local or regional through wind or water currents
N – Local or regional through wind or water currents
D – Global
S – Local or regional

5. What is the perceived "psychological" impact of a CBRN-DS attack on a big target?

C – Local fear
B – Regional or global fear. If a bio attack was made to work, it would have the maximum psychological impact of all types of attack. People are always susceptible to paranoia about personal health.
R – Global fear
N – Global fear
D – Global fear
S – Global fear

6. What is the cost of the material and logistics involved in launching a CBRN-DS attack?

C – Low (less than USD 50,000) - Costs would be mainly training and transportation. Lethal chemicals can be stolen.
B – Medium - high (over USD 100,000) - If this was ever done, materials would be stolen in small quantities and cultured at low cost - the expense would be basically in containment prior to release. Alternatively this would have to be done by bribing or blackmailing staff with the necessary access.
R – Medium (over USD 50,000)
N - Very high (over USD 1 Million)
D – Negligible (under USD 1,000) - At the most, the cost of a second hand or stolen computer. Internet cafes can also be used.
S - Low (zero + resources) – Resources and training.

Research by **mi2g** has revealed that a 'blended' terrorist approach, combining the dual threats of chemical and cyber warfare alongside conventional bombs delivered through suicide means, may represent the most worrying threat to western society as these are the most likely tactics to be employed by terrorists in the coming years.

The research suggests that the risk from biological, nuclear or radiological weapons is less grave.

Survey Results

Thank you very much for participating in the survey for CBRN-D business continuity. The collective results yield to the following conclusions:

1. 63% of the organisations do not have business continuity capability in case of a disaster.

2. 42% of the organisations do not have the capability to inform staff worldwide of the occurrence of a major disaster and are incapable of identifying critical assets and key staff

3. Almost half of all organisations do not have designated staff responsible for disaster recovery

4. 53% of all organisations are incapable of mobilizing a backup supplier for continuing their processes

5. 63% of the organisations are either unaware or do not have proper insurance cover for a CBRN-D type disaster

Conclusion

On September 11th 2001, USD 50 Billion of damage was caused and 3,031 lives were lost tragically. In comparison, the cost of the asymmetric operation was negligible: neither the planes nor the fuel within them that caused the mega structures to fail belonged to the terrorists.

The war with Iraq may exacerbate the threat from asymmetric attacks as witnessed by the surge of politically motivated digital attacks which have already cost in excess of USD 10 Billion in economic damage over the last nine months.

Based on the rankings of CBRN-DS threats, the most likely asymmetric risk scenario in the years to come would involve conventional or chemical bombs blended with suicide attacks and amplified with simultaneous digital attacks that cripple emergency services and stop people from being able to use air or rail transport, banking and credit card infrastructure at the same time.

There is a need for a robust business continuity capability within most businesses and government departments that will allow those organisations to deal with large scale asymmetric attacks and prevent systemic risk. This comprises:

1. Awareness and Understanding: We need to begin wider and more inclusive research and debate into the issue of asymmetric threats. We need to understand the inadequacies and deficiencies in countering these threats by so-called conventional methods – such as ‘military solutions’ which are unimaginative and doomed to failure since they will invariably exacerbate rather than resolve the underlying tensions.

2. Preparedness: Although an attack can have devastating consequences, with adequate forward planning it is possible for medium to large businesses to survive an attack and continue to function. Businesses need to develop customised business continuity plans to prepare for worst-case scenarios and must be operating in a way that can optimally mitigate the effects of any major disruption or loss of critical assets.

maintaining balance between hysteria and paranoia with due diligence of foresight and preparation.

3. Business and Politics Overlap: We must recognise that in today's interconnected world, business no longer exists in a vacuum. Business is inextricably related – and, just as important, is seen to be related – to politics.

4. Deal with Root causes: Our society must understand the importance of dealing with the root causes, as opposed to focusing on merely the effects. For example, as many threats emanate from the Middle East-related issues, it means championing the need to address the primary root causes of the region's violence and instability – namely the Israeli-Palestinian issue – so that we may all combine efforts to make the world a better and safer place.