mi2g

# The World Beyond 11th September

# Focus on Asymmetric Warfare

1 Whitehall, RTC, 22nd October 2001

Keynote Speech

**DK Matai - Chairman & CEO – mi2g**

***Introduced by Andrew Pinder***

***eEnvoy to Cabinet Office, UK Government***

## Contents

My Lords, Ladies and Gentlemen

## 11th September was a tragedy for the families of the victims

11th September was a huge tragedy for the families of over 5,300 victims of The World Trade Center and the Pentagon attacks using the hijacked aircraft. We cannot begin to imagine the psychological impact of the trauma that has engulfed their families, friends and colleagues at work who have lost loved ones forever.

Words are impotent in describing the tragedy. The dramatic size, scale, speed and ruthless efficiency of the multiple attacks left all of us shocked, nauseated and stunned. Commercial aircraft in the United States were immediately grounded. Interstate trains and buses were not running. The US experienced a man made catastrophe like none before in history. The perpetrators of the crime were not immediately known.

With the casualties, the horror and the shattering of US assumptions about themselves, **nothing** will be as it would have been. The road maps to the future have been redrawn. We live in a different world.

The UK is a part of the reworking of this future. President George W Bush has a strong advocate and ally in Prime Minister Tony Blair. The complex global coalition that has been swiftly put together would not have taken hold so effectively without British involvement and commitment to the “War against Terrorism”.

## Battle for Hearts and Minds

This is a battle for hearts and minds as much as it is a battle for air supremacy and ground combat “to smoke out” the Al-Qaeda organisation and Osama Bin Laden. With every passing day of war, there are stronger dissenting voices heard from different parts of the Muslim world. Faith will play a big part in this war.

## Biological warfare and hoaxes

The multiple Anthrax cases, which paralysed Capitol Hill in Washington last week for which 34 people tested positive, have led to a number of hoaxes on both sides of the Atlantic thereby exacerbating the problem. The House of Representatives was shut down. Offices of the Dutch and Irish Premiers also received hoax parcels causing them to shut down.

Fear and anxiety are the beginning. The undermining of business and consumer confidence is already evidenced on the world markets. Dow Jones, NASDAQ and the FTSE are all yo-yoing up and down. Interest rates are being cut to the lowest for decades. More panic could set in if there are new terrorism incidents or hoaxes reported that have not been envisaged or suddenly appear. The British Government’s timely laws to give hoaxers tough sentences are apt. A lot more needs to be looked at in combating this international threat.

## Psychology

The focus of the terrorists is to attack the population's confidence and monetary stability. Theatrical attacks with clear messages of dissent in the digital or physical world do undermine confidence. Whether it is the televised annihilation of the World Trade Center or men wearing spooky suits searching for Anthrax in the Senator's Offices in the US or the Liverpool Post Office in the UK, all such activity undermines society's confidence.

The psychological fall out from these events has been a double-digit percentage growth in the sale of anti-depressant, anti-psychotic and sleeping drugs in the US and elsewhere. Medical personnel are extremely concerned about the real possibility of depression, anxiety and mass hysteria, which could lead to distrust in officials, government services and established businesses. The destabilising effect of these developments on the US society, economy and government would be considerable and may well be intended. The rest of the world will also suffer the consequences; some xenophobic.

## Asymmetric threats

Any threat, which is disproportionate, such as the risk of a small group attacking a large country or a few individuals killing thousands is described as asymmetric.

The perpetrators of terrorism on the US were a group of individuals with different nationalities and a common faith. About 20 of them ended up killing over 5,300. The ratio is 1:250. This is the sad example of asymmetric threats, which can be launched by a small team against a nation state or a global business. All the power of a nation state cannot deal with the speed and stealth of such a small sophisticated and motivated team mounting an asymmetric attack.

With the American Declaration of Independence in 1776 and the French revolution in 1789 arrived the modern concept of a nation state with all the rights for her citizens enshrined in the constitution. The sovereignty of the nation state is now being superseded by the sovereignty of the individual because of access to low cost travel, communications and computing power.

In the 21st century, asymmetric warfare is going to be multi-dimensional. It will be fought on land, on the seas, in air and outer space as well as through cyberspace.

**The first dimension of asymmetric attack is land.** Guerrilla warfare is what the US and UK Special Forces are going to encounter in Afghanistan. There is no classic army waiting. There will be hit and run ambushes both within and outside Afghanistan.

**The second dimension of asymmetric attack is the sea.** On 12th October last year, two suicide bombers steered a small boat up to the USS Cole while it was refuelling in Aden harbour in Yemen and detonated explosives, blowing a 60-by-40 foot hole in the steel hull. The blast killed 17 sailors and injured 39.

**The third dimension of asymmetric attack is air.** The 11th September terrorists did not have an airforce or an ICBM – Inter-Continental Ballistic Missile – to attack the World Trade Center and Pentagon. They hijacked ordinary commercial airliners, fully laden with fuel, and flew them in a suicide mission into the towers and the Pentagon. This was the first time trained pilots hijacked aircraft and used them as missiles. The Pentagon building did not envisage such an attack and consequently was not prepared.

**The fourth dimension of asymmetric attack is outer space.** There are more than 350 commercial satellites in orbit today. There are several ways in which satellite systems have been disrupted. The simplest has been the use of brute force. Sending a signal up to a given satellite and simply jamming it.

**The fifth dimension of asymmetric attack is cyberspace.** Cyberspace encompasses digital systems, communication channels and media including television, radio, eMail, telephone and connected computer and mobile devices. Cyberspace has made history out of geography and has unified people regardless of where they are. In Cyberspace people sharing a common faith can meet, exchange ideas and plan ways regardless of whether they are, for example, in Jakarta, Islamabad, Teheran, Baghdad, Beirut, Cairo or Casablanca.

### Cyberwarfare's first pivot is as a community fragmenter / propaganda machine

In the battle for hearts and minds, the Al-Jazeera satellite channel is able to reach Muslims in not just the fifty member countries of the Islamic conference but also the 1.3 Billion Muslims anywhere in the world that have access to satellite broadcast. In the Gulf war in 1990, CNN was the main conduit of minute-by-minute information. The Arabs were getting information from CNN just like the rest of the world. It was easier to control public opinion then. This time round, Osama Bin Laden and his accomplices are using Al-Jazeera and so are other zealots mixed in with extremely credible Arab and Western leaders. Only Al-Jazeera is allowed to get maximum coverage of the Allied Bombings by Afghanistan's Taliban. The US and UK may be winning the aerial bombardment war but the battle for hearts and minds is controlled in part by Al-Jazeera. Their commentators speak from a faith point of view, which is more convincing and appealing to an Islamic audience in comparison to the BBC World Service and CNN.

### Cyberwarfare's second pivot is attack and counter-attack on digital systems

In the industrialised world we live in a digitally connected society where business and government services rely on first class computing and communications capability for logistics and distribution. The damage that an asymmetric electronic attack can do to our industrialised society is greater than what could be inflicted on a developing or under-developed country. Afghanistan need not fear an electronic attack but we have to be ready for it.

### Evidence of cyber attack - Lessons learnt from the Serbia-NATO cyberwar

During the bombing of Serbia by NATO forces in April 1999, a stream of virus-carrying eMails and denials of service as well as piracy hack attacks were targeted at over 100 businesses, media groups, public organisations and academic institutions in a number of NATO countries. Government and military facilities were also hit. The contents of the messages left behind were normally highly politicised attacks on NATO's aggression.

### Misdirected bombing and counter-attack

On 7th May 1999 the Chinese Embassy in Belgrade was struck. Three Chinese were killed and 27 injured. China sympathetic hackers from across the globe attacked US Government digital systems and US online businesses. The internet host computers of the Energy Department, Interior Department and the National Park Services were cracked. The Whitehouse web site also came under attack and was defaced.

### China-Taiwan cyberwarfare

A CIH virus emerged from Taiwan that disabled several computers in China as well as many other countries in Asia on 26th April 1999. Between June and August 1999 many digital networks in China and Taiwan came under mutual attack. Databases – some belonging to top government agencies - were damaged or copied.

## Recent attacks

Hackers in many Islamic countries including Pakistan declared a cyber jihad on the US and Britain last week, only days after the FBI issued a warning predicting as much. Also last week, Pakistani hacker group G-Force defaced the site of the National Oceanic and Atmospheric Administration (NOAA) Center, part of the US Department of Commerce, leaving a message promising more of the same type of attacks.

The day before yesterday, G-Force Pakistan defaced a site operated by the US Department of Defense (DoD) with a message about terrorism and Islam. The defaced page included several photographs of “Muslim children killed by Israelis”. The message on the DoD site – Defense Test & Evaluation Processional Institute (DTEPI) – posted by G-Force read, “We have suffered through the ages and will suffer no more. This is the era of cyberwarfare, where once again the Muslims have prevailed. We will not rest till every node, every line, every bit of information contained in our suppressors has been wiped out, returning them to the dark ages.”

The FBI warning, issued a week ago, said: "Many Muslim groups around the world have significant experience in launching sophisticated and sustained cyber attacks. In this context, a variety of pro-Muslim hacker groups, such as G-Force Pakistan, the Pakistan Hackerz Club or Doktor Nuker, could use these tactics against the US and its allies."

The G-Force Pakistan defacements carried the message that in the coming month they would deface 1,500 US, British and Indian websites. The group also said that it had highly confidential US data that will be given to Al-Qaeda. The group also warned of an Al-Qaeda Alliance Online involving other hacker groups, which it said would start attacking sites "soon" in a bid to convey its message.

## Defence expertise

Historically, politicians in the US and UK have challenged their defence forces to provide adequate defence capability within limited resources. The focus has been on the physical dimensions – land, sea, air and outer space – and not on cyberspace. There is no defence capability for sustained counter-attack in cyberspace.

Cyber warfare poses threats directly to lower level infrastructure in all government departments and commercial institutions. It is unrealistic to expect the Ministry of Defence to provide 'defence' against such threats and, in any case, the expertise needed is relatively fast moving and cannot be 'trained' into people over a short period of time. The expertise lies with those who understand the technologies used to pose the threats, gained through experience, such as electronic attack and counter-attack special defence companies. All this may change in the years ahead post September 11th.

## High profile attacks on economically sensitive targets

On 1st February last year, Sir John Bond, Chairman of HSBC spoke at the World Economic Forum in Davos and said that HSBC security was “fully stretched” repelling a hacker team that tried 150 million passwords in 2 days.

On 5th February 2001, the computers of the World Economic Forum were hacked by anti-globalisation activists. The culprits stole 80,000 pages of sensitive personal information such as cell phone numbers, eMail addresses, passwords and 1400 credit card numbers of forum participants, including UN Secretary General Kofi Annan, former US President Bill Clinton, Israel’s Shimon Peres and Palestinian leader Yasser Arafat and Microsoft’s Chairman Bill Gates. This electronic security breach contrasted sharply with the impenetrability of the Davos conference centre, which was protected by roadblocks and barbed wire barricades.

## Low profile attacks on economically sensitive targets

The much more scary attack is a subtle manipulation. On October 3rd last year a Dutch hacker, Gerrie Mansur of Hit2000, warned NASDAQ and CBS's Marketwatch.com that he could have altered their web sites in a subtle way. Mansur gained access to the global.asa file from the Web servers of the news sites. This file regulates who gets access to what applications on the Microsoft IIS server. It also contains the global settings for the applications. NASDAQ's global.asa file contained the password to the site's main database.

*What happens if terrorists use a Mansur type vulnerability exploit to buy and sell options by subtle share price manipulations that are not declared public? Or change words in particular reportage on the digital media?*

NASDAQ-100 and NASDAQ Japan sites were hacked in December 2000. Two months ago, on 24th August NASDAQ halted trading in Brass Eagle's stock (XTRM) after a hacker broke into Brass Eagle's computer systems and mass eMailed hundreds of press releases containing fake financial statements over the Internet. This kind of vulnerabilities exploitation can be a nightmare for regulatory authorities, share options traders and individual investors.

## Share price fall as a result of eAttack

In early March 1999, the world's largest online auction site – eBay was hacked by an American student going under the handle of Magic FX. The market capitalisation of eBay was US$ 21 Billion. MagicFX took root access of eBay computers by guessing passwords, which allowed him to change prices, place false statements and images as well as divert traffic to other sites and down the entire eBay network. eBay declared "administrative outages" on several days in June, July and early August 1999. The market responded unfavourably to all these "administrative" outages and eBay's share price fell from US$ 209 on 27th April 1999 to US$ 75 on 4th August. The market capitalisation fell by US$ 16 Billion during those troubled months.

## The single biggest failing of 11th September – fragmented intelligence

The single biggest failing of Western Intelligence Agencies in not having picked up the 11th September attacks is their fragmented electronic intelligence gathering systems, which have no capability to unify knowledge management and analysis.

*Consider the number of different intelligence agencies in any one country involved in the collection of data - both overt and covert - in the modern democratic world. Consider the exponentially increasing volume of that data and the nature of it: voice, image, video, fax, text and symbols – both hidden as well as encrypted.*

It is an Herculean task to collect, sift, analyse and act on this intelligence data if the key pieces of knowledge are not to be missed. This cannot be done manually and we need really smart technology solutions to help us.

If the threat and targets are international, the Allied countries' knowledge management and analysis systems handling intelligence data need to be able to talk to each other. This has not been true for Agencies even within the same country, especially the US, who up until now jealously guard information that they collect themselves. They do this to safeguard the reputation and budgets of their own organisations. This has to change; this is outdated thinking after September 11th. Agencies must share information and they must be able to share and process it electronically and securely.

## One country cannot go it alone

Finally, no one country, even the size of the US, can be sure of collecting all the relevant data. No one Agency and no one country is able to judge the worth of the fragments of intelligence it collects, be it names, dates, places, intentions or rumours without putting it with information collected by other Agencies and countries. The peer process of validation is essential to verify and deepen the intelligence gathered.

The picture is not a clear one at any stage until the end. It is a mosaic made up of fragments as much as it will be made up of large pieces, and no one Agency will know if the piece it holds fits with pieces held by others unless they exchange. Again this can only be done swiftly via electronic means and it must be done securely.

So one of the greatest needs before 11th September was for upgraded secure knowledge management and analysis systems that were interoperable across Agencies within one country and between countries. That need is now paramount. The US, UK, most of NATO as well as Australia and New Zealand need to have interoperable Knowledge Management and Analysis Systems (KMAS) and tools for mining intelligence data. These new KMAS tools need to be able to cope with other countries of Eastern Europe, the Middle East and Asia.

This is an enormous challenge and we believe that the US and UK Governments must be aware of it. Whether they are or not, they should know that computing organisations like mi2g are thinking of it and already designing such secure systems for large multi-nationals in financial services that face the issue of connecting fragmented databases because of mergers and acquisitions and need to unify the customer image from a customer relationship management (CRM) standpoint.

## Protection and civil liberties – loss of privacy

In order to reassure its citizens, the government needs to act and be seen to reassure its people and be seen to deploy a series of counter measures. Individual freedom and protection through security always carries a trade off. For example, in the City of London video shots are taken of drivers in cars as they enter the “ring of steel”. This slows the traffic down and reduces privacy. Business cannot function without confidence so we all submit to scrutiny from the multiple cameras all over the City.

## What you know, have or are?

When it comes to the issue of mass identification, we have to begin with something that people carry such as a Passport, Driving License or business ID card and something that they know such as a password or specific knowledge. This needs to be coupled with something that they are – such as their fingerprint - to tighten security.

## Biometric security

A lot has been said about Smart ID Cards and Biometric security since 11th September. The truth is that biometric security – fingerprint recognition, facial recognition, voice recognition - is not 100% accurate. It can only be used as an adjunct and not the mainstay. Even if the margin of error for a very advanced top of the range facial recognition system at an airport is 99.9% accurate for argument; if 1 Million passengers walk in and out of Heathrow every week, the number of false alarms would be 1000. This is unacceptable in terms of disruption caused.

## ID cards

If all travelling passengers were to carry an ID card at an airport, which they do, the Passport still does not solve the problem of a fundamentalist or religious zealot causing chaos if he has decided one fine day to act the devil. So the whole issue of authentication, confidentiality, data integrity and non-repudiation of bona fide presence, communications and transactions is a critical issue and has to be solved through a multi-pronged approach.

## Human intelligence

*The next question to consider is how does one deploy people with the Knowledge Management and Analysis Tools to outsmart the malevolent people who are one step ahead and constantly figure out ways to outsmart the system?*

The reality is that 70% of all complex attacks take place through insider knowledge and assistance and not political activists who go it alone. Disgruntled employees in sensitive places have been suborned, coerced, brought into believing in some faith or indeed volunteered their services. This is seen in banks when complex fraud or hack attack takes place. It is seen in large multi-nationals, in the breach of government services security and even in the planning of 11th September. More attention needs to be given to the value of human intelligence, where the information is collected in situ at the grass roots level.

When guaranteeing the security of large digital systems the only way forward is to combine knowledge management and analysis tools with human intelligence via managed security services. Large digital systems need to be monitored by experienced security specialists who are central to ensuring reliability, availability, maintainability and scalability of systems that already have a sufficiently layered security architecture.

## Conclusion

This war on terrorism must be won decisively and effectively. As in all wars, our defence must excel aggression, the same holds true for this war. We will need to understand that:

1. Laws will have to be passed throughout the 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.

This process has begun with the US Senate passing the "Uniting and Strengthening America (USA) Act" earlier this month. In the UK, under the Terrorism Act 2000, enacted into law in February this year, people who endanger lives through the manipulation of public computer systems will be punished under the anti-terrorism law as would any other terrorist.

2. New investment is now necessary on interoperable knowledge management and analysis systems that can allow data to be shared easily from different sources and agencies collecting intelligence as well as investing in more human intelligence on the ground. Nothing significant can be achieved without this sharing capability.

3. Defence has always been about securing trade routes and markets. Given that several Billion Dollars of trade is routed digitally, counter-attack electronic weapons that can disable attacking systems from other parts of the world will ultimately need to be deployed by Governments as part of their defence shield. This will save commercial operations a lot of time and money in dealing with rogue, politically motivated, electronic attacks from the rest of the world and malevolence from within which end up costing Millions in lost revenues.