Asymmetric Threats Contingency Alliance

Third Session – 18th February 2004

DK Matai, Executive Chairman, mi2g

Your Royal Highness, Your Excellencies, My Lords, Ladies and Gentlemen,

It is a great honour and privilege to introduce and participate in the third Asymmetric Threats Contingency Alliance – ATCA – meeting, kindly hosted by VISA International. Please feel free to contribute to the discussion, which will take place under Chatham House rule.

In essence, any threat which is disproportionate and can destroy a larger and more organised system is asymmetric. So, 11th September or 9/11 is an example of an asymmetric attack as is a Chemical, Biological, Radiological, Nuclear, Digital or Suicide – CBRN-DS – attack that disrupts our way of life and doing business. Nearly two and a half years have passed since 9/11 and it is useful to note that a tragedy on that scale has thankfully not re-occurred. Why is this so?

The world is a changed place post 9/11: ranging from the ritual of removing shoes at US airports before every departure to the introduction of biometric facial and fingerprint recognition devices upon arrival. Technology is being used in every way to control borders and apprehend organised criminals and extremists both in the physical world and in cyberspace. Emails and voice communications are being monitored for keywords both in the US and by other intelligence agencies across the Western world. Sharing of that intelligence is still not taking place as fast as it could.

Every country and global corporation faced with national insurgence, trans-national extremism and organised crime will ultimately need to migrate closer towards Total Information Awareness Systems (TIAS) in the years ahead. Every citizen and permanent resident of a country, employee or sub-contractor of a corporation has to be equipped with an identity card with biometric tags and governments as well as corporations need to be aware of their stakeholders' movements across borders and the frequency with which their travels, entry and exit out of specific cities, valuable complexes and public places take place.

Co-operation between Western, East-European, African, Middle-Eastern, Far Eastern, and Latin American intelligence agencies has been rising to combat the dual threats of trans-national terrorism and organised crime. Organised crime is the increasingly active handmaiden of extremism because it benefits from instability and actively encourages it.

From drugs, illegal immigration and small armaments trafficking through to video, audio and software piracy, child pornography, contraband and counterfeit goods, online banking and credit card fraud, the global organised crime industry now has an estimated take-home gross profit of between $1 and $1.5 trillion per annum

according to several government agencies. This profit is roughly equivalent to the GDP of the UK, the fourth largest economy in the world. However, the Knowledge Management and Analysis Systems (KMAS) that can inter-operate on collective data still need to be built.

About $200bn is conduited through untraceable man-to-man financial networks like Hawala banking controlled through bankers in Pakistan, UAE, Egypt and Switzerland but active in over 150 countries. The Hawala system has been partially responsible for facilitating every type of organised criminal activity and extremism including the handling of finances for the proliferation of WMD technology to countries as diverse as Libya, Iran and North Korea.

The fifth dimension of asymmetric warfare is cyberspace. This is the new frontier into which extremists and criminals are moving. The cost of entry is low and chances of getting caught are lower still. Computers and communications not only perform information flow and order fulfilment in the new economy, they are a vital component of the command and control that makes our societies' critical economic infrastructure tick.

Financial services, power supply, transport, emergency services, food and health services are all reliant on computer based equipment, which in turn is increasingly susceptible to hacker attack, viruses and worms as well bandwidth clogging caused by digital traffic jams.

The digital traffic jam caused by the MSBlast worm is often cited as another contributing reason for the dysfunctional US power stations that were unable to balance the load on 14th August last year and caused the largest power outage in history. The cascading failure led to the collapse of electric power to the entire North East of America and affected major cities like New York, Detroit and Toronto. The UK, Sweden and Denmark as well as Italy and Switzerland had power outages near the same time.

Fundamentalist hacking activity is rising and has been getting more sophisticated over the last two years. A number of hacking groups from Kashmir, Pakistan, Morocco, Turkey, Chechnya, Saudi Arabia, Kuwait, Indonesia and Malaysia are collaborating with each other and anti-globalisation groups based in the West to target international and domestic online assets. Large and small businesses, government computer networks and home computers have all been targeted with resultant business interruption damage in tens of billions of dollars.

The intimate involvement of criminal syndicates originating from the Russian Federation; China and Taiwan; Pakistan and UAE; Brazil and Columbia is aiding and abetting the extremist agenda in many instances.

Identity theft, phishing scams targeting over 20 major banks in the world and credit card fraud are all rising and provide cover for licit and illicit organised crime and extremist activities.

From spam to malware proliferation, the use of home computer zombies is growing. Every single computer on the planet, which can be recruited for malevolent purposes, is being targeted either as an end-target or a go-between for launching Distributed Denial of Service attacks followed by extortion or ransom demands. A number of companies have paid up. Some zombies are also used for illegal file sharing and mail relays. The cost of digital crime worldwide per annum now exceeds $205bn pa.

The fourth dimension of asymmetric warfare is outer space and it is only a matter of time before a commercial satellite is hijacked to broadcast extremist propaganda in the same way that the Falun Gong hijacked the Sino satellite in August last year and broadcast its agenda instead of the China Central Television scheduled programmes that reach half a billion people.

Chinese and Russian hackers have been approached for selling their skills through the black market in this area to political and religious extremists. What would be the result if a message were broadcast across a country that ideologists belonging to a particular faith have destroyed their parliament building or well-known monument?

The battle for hearts and minds is already under threat because of the suggestions by a range of satellite channels like Al-Jazeera that some Western broadcasters are biased and serve to project their governments' agendas.

The third dimension of asymmetric warfare is the sky. Multiple warnings from Western and Middle Eastern intelligence suggest that a 9/11-type tragedy may be repeated at some point. A number of flights to Washington, Los Angeles, Riyadh and other cities have been suspended as a result in the last two months.

The catastrophic nature of such an event would multiply significantly if WMD material were on board the aircraft as it was detonated over a city as opposed to colliding into a skyscraper. Though fighter-jet counter-measures exist, will government officials have the willingness to shoot down a hijacked aircraft and lose 250 people if necessary to save thousands on the ground?

The second dimension of asymmetric warfare is the sea. Yet security measures for port facilities and ships have lagged far behind the strict rules enforced at airports and aboard aircraft since 9/11.

The United States, after multiple warnings that shipping is at risk, is leading a rush to plug those holes. There is evidence that Al-Qaeda terrorist groups have taken note of the value and vulnerability of the maritime sector.

With commercial ships transporting 80 percent of the world's traded goods, it is important to note that vessels, ports and other links in the maritime economic chain are tempting targets. At some point in the future a major shipping route could be blocked by an attack that cripples and sinks a large cargo or oil carrying ship blocking a congested shipping route like the Straits of Malacca and Gibraltar; or the Suez and Panama Canals.

One to three million ocean-going containers a year are handled by each major port, and any one of them could hold illicit ready cash cargo, extremist living cells or even WMD components – all three of which have been found worldwide at some point in the last three years. A rising trend in piracy compounds concerns. Pirate attacks on ships in the first half of 2003 jumped 37 percent over the same period of 2002, to 5.9 attacks per 1,000 vessels.

The possibility of terrorists' linking up with pirates to hijack commercial vehicles containing liquid natural gas or liquid petroleum gas and crashing it into a port is of great concern to maritime nations. Security has tightened further in 2004:

1. Under US pressure, the International Maritime Organization of the UN, now requires port facilities, stevedoring companies and owners of ships larger than 500 tons to make detailed plans for responding to terrorist threats.

2. Leading container terminals across the world are seeking to install additional fencing and more closed-circuit TV cameras to watch for intruders at the water's edge.

3. Leading container terminals are also installing radiation detectors, to guard against concealment of a radioactive "dirty bomb" inside a container. In a deal with the US Department of Energy, Rotterdam is to become the first port outside the United States to use such detectors.

4. The US Department of Homeland Security is introducing a "smart box" program aimed at making containers more tamperproof by encouraging shippers to use electronic sensors for the containers' doors.

The first dimension of asymmetric warfare is land. A number of suicide enabled explosions in Iraq, Israel, Russia and other countries like Kenya, Morocco, Turkey, Saudi Arabia, Pakistan, India, Indonesia and Philippines, suggest that this dastardly tactic has become a global phenomenon. No religion, including Islam, supports suicide bombings. The targets have been identified with governments, multi-nationals and not-for-profit organisations like the United Nations.

Through suicide bombings, one or two people can hold thousands to ransom and kill hundreds. Several thousand innocent civilians have died or been maimed since 9/11 as a result of suicide bombings. There is a growing concern that suicide bombers may use WMD at some stage, which could have longer-term consequences.

Although there is no straightforward way to deal with this threat, further investment in tracking border activity and illegal immigrants using false identities is essential. Many suicide bombers do not live within the communities that they bomb but are invariably found to have arrived through a cross-border checkpoint a few hours or days earlier. They have then received their destructive payloads via criminal syndicates / sleepers.

National immigration checkpoints need to be equipped with the correct detection mechanisms and underlying databases that are no longer dependent on easily forged paper identities but utilise the permanence of physical biometric characteristics. This also points to the need for Total Information Awareness Systems (TIAS) and Knowledge Management Analysis Systems (KMAS).

It is vitally important that we in the West understand the history and tradition, which has led to cultures and countries becoming unique in the way that they are. Whilst there is no perfect form of government and there is no right or wrong way of living, mutual-respect and shared universal values for the good of humanity are well worth preserving and enhancing in all societies.

We have a responsibility to educate our populations across the globe to be able to see the others' point of view. In building this inter-faith understanding we encourage trade and industry, which can solve the long-term problem of unemployment, loss of self-respect and belonging.

The answer to fighting terrorism over the coming decades lies in the dual approach of embracing technology to construct national and international Total Information Awareness Systems (TIAS) and Knowledge Management Analysis Systems (KMAS) whilst eliminating poverty, raising education and awareness levels, as well as promoting the understanding necessary for a multi-faith tolerant society.

