Cyberland Security:

Organised Crime, Terrorism and The Internet

Oxford Internet Institute, University of Oxford – 10th February 2005

DK Matai, Executive Chairman, mi2g

Chairman, Your Excellencies, Ladies and Gentlemen,

It is a great privilege and an honour to be invited to give this talk at the Oxford Internet Institute. There are many familiar faces here and I would like to take this opportunity to extend our heartfelt thanks for your support and friendship over the years.

Any threat which is disproportionate and can destroy a larger and more organised system is defined as asymmetric. Traditionally, nation states have concentrated on symmetric threats like nation-to-nation warfare.

The knowledge garnered for this presentation on asymmetric warfare relates to the many facets of cyberland security, including organised crime, terrorism and the Internet, and comes from two independent streams:

1. Directly from distinguished colleagues who serve on the board and advisory board of **mi2g** and the very capable members of the **mi2g** Intelligence Unit. They have all contributed substantially to the contents of this presentation. So, first and foremost I seek to acknowledge their vital role and contribution and thank them.

Since 1995, we have built the world's largest digital attack database, which we fondly call SIPS – Security Intelligence Products and Systems – and this gives us a unique perspective on the dark side of the Internet. We have established profile databases on over 7,500 hacking groups across the world and monitor Internet hacker and malware attacks activity in real time across more than 20 strategically located nodal points. We also have over 9,000 relationships with CEOs, CFOs, CIOs and CSOs in large corporations, government agencies and not-for-profit entities across the world that provide us with confidential information on digital risk manifestations and their business continuity priorities. We are pleased with the level of co-operation and encouragement we have received from international law enforcement agencies and UN agencies to develop SIPS.

2. Some of what we seek to discuss falls under the auspices of **ATCA** - the Asymmetric Threats Contingency Alliance – a body we set up post 9/11 to examine the rise of asymmetric techniques of warfare and also to look at chemical, biological, radiological, nuclear, digital and suicide (CBRN-DS) enabled techniques and weapons proliferation. I

THE QUEEN'S AWARDS FOR ENTERPRISE: INNOVATION 2003 would like to thank members across all parties of the House of Lords, House of Commons, Parliamentary Office of Science and Technology, Lloyd's of London syndicates and the insurance market, government security agencies on both sides of the Atlantic, as well as financial services players like HSBC and VISA International for their generous support and encouragement of this organisation over the years. We are truly indebted.

With ATCA, we have looked at the use of asymmetric attack techniques in North and South America; Britain and mainland Europe including Russia; North Africa, the Levant including Israel and Palestine; Gulf Co-operation Council countries including Saudi Arabia; Iraq and Iran; Pakistan, India and Sri Lanka; as well as Indonesia, Malaysia, Australia, Japan and China. We have also looked extensively at the links with organised crime.

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, according to several government agencies, the global organised crime industry now has an estimated take-home gross profit of between USD 1.25 and USD 1.5 trillion per annum. 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.

So, let us begin with the five main themes of this presentation:

1. Resilience – Human society is evolving and both the good and bad elements have been present in society throughout history. As our society adopts new tools and technologies, it becomes more dependent on them. The new dependencies can lead to exploitation if the criminals and radicals can see a way to circumvent the safeguards. The Internet and most forms of modern technology are no exception. No matter how bad the situation gets or is perceived to be, human beings have a remarkable tendency to innovate and get out of a specific hole. However, in order to solve a problem we need to be aware of the problem itself and the processes behind it.

2. The challenge to the Nation State – The sovereignty of the nation state extends to its borders and that is as far as the rule of that national law goes. The law enforcement agencies have no vested power to go any further. The trans-national organised criminal syndicates and extremists understand and exploit this. They operate across nations to evade being caught and also to ensure that any one nation state's services are not fully aware of their activities. In this way, they are able to undermine the sovereignty of the nation state. They use the Internet extensively because it grants anonymity as false identities can be relatively easily created and discarded in this medium.

3. The sovereign individual – In the past, only nation states or very wealthy individuals and corporations could finance overseas operations. Today, if we look at the low cost of air travel, ubiquitous free access to high quality information and the very low cost of international communication – all partly or completely enabled by Internet technology – any individual or small cells can execute an operation anywhere, anytime and without the need for significant finance. The costs involved in executing the 9/11 tragedy or the Madrid bombings on 11th March 2004 were not very high. The sovereign individual is no longer a mythical figure, he exists in the 21st century. He or she can choose to live anywhere and yet project a chosen identity somewhere else via the Internet and mobile telephony. The greatest danger to modern civilisation comes from "sovereign individuals," smaller cells or entities that are not nations. Therefore, the intelligence to understand, anticipate and counter the attacks of such groups is far different and much more complex than normal intelligence operations interpreting the political, economic and military threats of nations.

4. Ideology and Faith – As an individual or a group of individuals feel that they are sovereign they begin to act that way. If they share a common ideology regardless of distance or national boundaries, the Internet provides easy-to-use tools to advance that ideology. This common ideology could be “anti-globalisation protest”, “religious fundamentalism”, “selling counterfeit goods” or “fighting AIDS in Africa.”

5. The role of War – The French philosopher Teilhard de Chardin presents “ideas acceleration” during a period of war, which takes place routinely in society. He emphasises the way that geography and distance are eliminated as human minds coalesce to solve a problem or fight a common enemy. In some ways, we are again in that phase with the so-called “War on Terrorism” and its many offshoots, and the Internet is the vehicle helping to reach the sub-stages of that “Omega Point.” However, the radicals are already embarked on a similar voyage of discovery based on large distance collaboration and it is not at all clear who the winners of the various battles are likely to be. Teilhard de Chardin said, "The age of nations is past. The task before us now, if we would not perish, is to build the earth."

New Patterns

When we overlay digital attack data with physical attack information, interesting patterns begin to emerge:

1. Physical terrorism and radical digital attacks go hand in hand because a common ideological commitment drives them both. In many instances, including the Bali, Riyadh and Istanbul bombings, there were a series of digital attacks at the same time or slightly before that originated from hackers based in those countries on the West and their own governments’ computing infrastructure. In most cases the hacking groups behind those attacks were part of larger global coalitions and involved hackers, not just from Indonesia, Saudi Arabia or Turkey, but also from other Islamic countries, Russia, Central Asia and Latin America. Higher the number of digital attacks originating per capita the greater the political and social instability in that country. Russia, Turkey, Brazil, Saudi Arabia, Egypt, Morocco and Pakistan all fall into this category.

2. Political instability and criminal profiteering are intertwined. Criminals are most rampant in failed states and quickly cash in as war generates even more chaos through hubs. Afghanistan and Iraq are prime examples and it is worth noting the way in which Karachi in Pakistan, Mumbai in India and Dubai in the UAE act as hubs for organised criminal syndicates operating throughout the Middle East.

There is a view held by bankers that when the proportion of criminal GDP to total GDP exceeds 20%, democratic and civilised society breaks down and failed states are the result. Such a proportion, while it may have been surpassed in countries like Afghanistan, Somalia and Congo, it is not impossible to reach even in major Western democracies such as USA, Germany and Italy, as history has shown. The problem with it is that the last mile of the organised crime cancer goes very fast and is no longer perceived because people and society’s guardians get used to living with it.

3. Rapid development creates more opportunities for criminals. Brazil, Russia, the Indian-subcontinent and Greater China are strong bases for large-scale organised crime and also for trillion Dollar outsourcing arrangements per annum. The criminal syndicates are steadily recruiting members in local call centres and other outsourced services, manufacturing plants and software development centres for garnering customer

confidential information, planting monitoring devices and Trojan Horse malware or more sophisticated bugs in software modules.

4. Traditional Mafiosi or Triad gangs have now developed modern hacking capability and use of the Internet and mobile texting for various forms of “Hawala” banking, barter trading and covert communications. Money given in one part of the world followed by an Internet, text message or face-to-face meeting translates into the same amount of cash being delivered by hand in another part of the world. Hawala communicates through man made codes and methods that defy the most sophisticated technology that anyone would want to deploy against it.

The Western financial system and the associated governments are completely unaware of the large-scale transactions involved. About USD 200bn per annum 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.

5. Financing wars and delivering weapons for guerrilla and more substantial forms of warfare requires criminal syndicates as facilitators. Warlords exploit their own criminal syndicates to generate cash to finance their war effort. Organised crime proliferates in multiple directions once it finds a home.

We have also conducted some interviews with hacker groups and virus writers who work for financial gain, glory or ideological reasons. In many instances, the organised criminal entities behind phishing scams, spam engines and relay farms, as well as pornography purveyors have diversified out of counterfeit, contraband goods and narcotics into banking and credit card fraud and then further afield.

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 with identity management and surveillance built in. Internal employees within corporations are the biggest source of financial fraud and other serious malevolent activities. They collectively cause the largest proportion of financial and associated brand damage, and in some cases lead to the outright failure of their enterprise. An identity card with biometric tags will be needed for every citizen and permanent resident of a country, as well as every employee and sub-contractor of a corporation. Alternatively, low cost biometric terminals might direct verification of a specific biometric against a central database thereby eliminating the need to carry any identity card in the future.

Also, governments and 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.

The challenge for TIAS lies in balancing the need for surveillance with the need for liberty and privacy. Some observers feel that the US has already gone too far in the direction of surveillance and that the proven benefits from surveillance have, so far, been small or negligible.

Governments need to realise that no solution can be perfectly capable, no matter how much technical assurance it may carry. The effectiveness of technology is at the mercy of good governance and building trust within the community. Checks and controls do not work as effectively as trust building initiatives.

This leads to the need for constant and critical administrative overview of the data in a TIAS. Some bright people must be rigorously trained to be able to join up the intelligence mosaic in a TIAS and not jump to the wrong conclusion, as such a system requires high quality metadata to allow system queries and challenges to be handled intelligently. The administrative and support load that this will place on the overall system - in terms of bright people, training and finance - should not be underestimated.

This is vital and will have two benefits:

1. Eases the path to critical review of each individual's data whenever needed; and
2. Demonstrates to those concerned about civil liberties that safeguards are in place and the chance of an innocent being targeted are substantially mitigated.

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 extremism and organised crime.

There are five dimensions of asymmetric warfare – cyberspace, outer-space, sky, sea and land. In each of these dimensions we see the coming together of organised crime and extremist activity, increasingly facilitated by the ubiquity of the Internet. Beginning with the fifth dimension, which cements the other four, we will count down:

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 the chances of getting caught are even lower. Computers and communications not only perform information flow and order fulfilment in the new economy, they are vital components 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 as 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 2003 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 three years. A number of hacking groups from Kashmir, Pakistan, Morocco, Turkey, Chechnya, Saudi Arabia, Kuwait, Indonesia and Malaysia are collaborating both with each other and a fringe of anti-globalisation groups based in the West in order to target international and domestic online assets.

Large and small businesses, government computer networks as well as home computer owners have all been targeted by organised criminal syndicates and radical hacking groups. The resultant identity theft, financial fraud and business interruption damage exceeds tens of billions of dollars in each category.

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. As much as 25% of organised criminal syndicate activity is perfectly legal, ie, licit, because they also need a safe facade behind which they can carry out their nefarious activities without challenge.

From spam to malware proliferation, the use of home computer zombies is growing. Every single computer on the planet that 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 and identity theft at the domestic level is rising. Some 11.5 million zombies configured as thousands of “Botnets” are used for illegal file sharing and mail relays according to the latest **mi2g** Intelligence Unit data. The cost of digital crime worldwide per annum now exceeds USD 250bn. Are citizens aware that their machine has been turned into a zombie for a Botnet and they may receive a call from a policeman at some stage for harbouring illicit material or activities? More needs to be done to raise awareness of the civic responsibility associated with owning a permanently connected computer. There may even be a need for computer “driver licenses” in the future so that users agree that they will at least perform checks on their machines looking for Trojan software and keep their anti-virus tool kits up-to-date, for example.

2004 can rightly lay claim to being the year that Botnets came of age as a means of delivering a distributed denial of service (DDoS) attack on selected targets. Defence against Botnets is inherently difficult and they have wide and undiscriminating consequences. Earlier in that year, criminal attacks on SCO and Microsoft showed that having a huge bandwidth connection into the Internet was no defence against thousands of computers all working in unison under a single hand. Closer to home, during the Cheltenham Gold Cup meeting, criminals used Botnets in an attempt to extort protection money from online bookmakers. Botnets can deliver multi giga-bit per second attacks. By attempting to mitigate damage, ISPs may have to resort to disconnecting one, or more, of their servers from the Internet resulting in unanticipated collateral damage to many customers. In September 2004, a Botnet of 10,000 zombie machines was shut down by the Norwegian provider Telenor. This was by no means a large network. Botnets have now reached a size that entire countries, not just companies, are vulnerable.

Governments’ intervention

The **mi2g** Intelligence Unit predicts there will be a growing requirement for Governments to intervene and to mobilise counter-attack-forces that protect economic targets and critical national infrastructure constituents on a 24/7 basis.

The near doubling of hacking incidents every few months has shifted away from targeting government departments and agencies towards focusing principally on Small to Medium size Enterprises (SMEs) and large corporations where opportunity allows. The roll out of 'always on' full broadband and wireless connectivity tilts the balance against the innocent citizens and SME corporations.

The SMEs are incapable of sheltering themselves or having the budget and expertise to be able to ward off sustained digital mass attacks, which have now become a daily occurrence with widely available, automated and easy-to-use sophisticated digital attack tools. The mounting collective losses to businesses might impact on governments' revenue streams through reduced tax collection, so in the future, it will be prudent to look after individuals and the SME growth engines and not just large businesses, who on the whole have the budgets and manpower resources to look after themselves. In order to reduce the long term burden on the tax payer, new enterprises need to be incentivised that provide low cost or subsidised digital risk management and protection. They should offer practical assistance and recovery to SMEs at low cost so that effective outsourcing can occur.

Counter-attack forces

In the not too distant future, there is a likelihood that command and control attacks, which blend cyber terrorism with physical terrorism, simultaneously seek to disrupt critical economic infrastructure.

We are soon going to reach a point with always on connectivity, wireless enabled technology and IP enabled critical infrastructure, when no amount of firewalls, anti-virus tool kits, intrusion detection will work at the national economic level by way of providing adequate guarantees for the safety and security of a nation state.

Historically, politicians in civilised Western democracies have challenged their defence forces to provide adequate defence capability within limited resources. The focus has been on the four physical dimensions - land, sea, sky and outer space - and not on the new 5th Dimension, which is cyberspace. There is no real digital defence capability deployed so far - other than occasional simulations and exercises which are designed to uncover gaps in the national critical infrastructure's digital defences. The redressal lies primarily in developing counter-attack-forces, which would begin to arrest the imbalance of power between ill-motivated hackers on the one hand and little-prepared businesses on the other. The legal ramifications need to be carefully thought through along with terms for trans-national engagement.

On the legality issue, there may be scope in the longer term for some adjustment to the UN Charter to recognise the right to self-defence by pre-emptive attack. Kofi Annan has been talking about this as regards conventional war for some time, although to little effect. The required degree of proof may not always be easy to reach as has been the case for the lack of WMD found in Iraq even though the war was started by the US and her allies on that premise.

It is unrealistic to expect that any defence department can provide 'counter-attack-forces' against digital attacks for an entire nation's economic targets immediately and, in any case, the expertise needed is relatively fast moving and cannot be 'trained' into would be combatants in a short period of time.

Human intelligence

Most complex attacks take place through insider knowledge and assistance. Just one motivated individual cannot usually perpetrate complex cross-boundary physical or digital terrorism. Disgruntled employees in sensitive places are suborned, coerced or indeed volunteer their services to support a cause. This is seen in financial services when complex fraud or deeply damaging hack attacks take place. It is also seen in large multi-nationals, in the breach of government services security and even in the planning of the 9/11 co-ordinated attacks. More attention needs to be given to the value of human intelligence collected by local agencies, where the information is collected in situ at the grass roots level.

In the future, when seeking to protect the critical infrastructure constituents and business digital systems at a national level, the economically prudent way forward is to combine Knowledge Management Analysis Systems (KMAS) and counter-attack-forces with on-the-ground human intelligence sources and Total Information Awareness Systems (TIAS). Surveillance and reconnaissance dashboards of digital systems for risk visualisation will need to be managed by experienced counter-attack-forces on a 24/7 basis.

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 2003 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 had 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. This concern is echoed in the UK as American Fox News, for example, is not allowed to broadcast in this county because the broadcasting regulator does not accept that it is impartial.

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 year.

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. Bio-terrorism and Radioactive dirty bombs are particularly worrisome possibilities. Though fighter-jet counter-measures exist in many countries now including the US and UK, do government officials have the willingness to shoot down a hijacked aircraft and lose 250 people if necessary to save thousands on the ground or would there be any benefit in shooting down an aircraft carrying WMD?

The second dimension of asymmetric warfare is the sea. It is clear that 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 type 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; or for that matter the English Channel.

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, although the number of attacks has begun stabilising in late 2004 because of 9,000 Volt intruder fence installations on many ships.

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 the last year:

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 became the first port outside the United States to use such detectors.

4. The US Department of Homeland Security has introduced 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. The targets have been identified with governments, multi-nationals and not-for-profit organisations like the United Nations. No mainstream religious group, including Islam, supports suicide bombings.

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.

Some nation states have played a critical role in developing the suicide-bomber and other types of terrorist through their lax policies and ambiguous approach. Despite all that has happened in some countries, there is still evidence of ruling elites turning a blind eye or funding extremism that leads to terrorism. There are also instances of their paying the terrorists – either with money or changing their laws to accommodate them – not to carry out further attacks. All of this encourages terrorism.

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 or sleepers.

The Iranians have recently adopted the term “asymmetric warfare” and use it at every opportunity to describe their approach to a possible invasion by the United States and Israel. It covers most of their defensive operations by land and by sea, and includes the activity of the Revolutionary Guards Corps and the *Basij*. If true, it would extend to operations like suicide-bombing and small-boat attacks on tankers. Here is the evidence of asymmetric warfare beginning to make a mark on nation state defence tactics.

The political will to stop infiltration hinges on the following essential requisites for successful border security:

1. Comprehensive sensor coverage;
2. Well administered intelligence handling of the data from sensors;
3. Its correlation and interpretation;
4. Intelligent and proportionate response;
5. Competent and well-trained quick reaction forces in adequate numbers from politically acceptable nations.

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).

Next Steps

Organised crime syndicates and radicals embarking on identity theft, elaborate scams and financial fraud have now become rampant. As knowledge management based authentication systems proliferate both at airports and digital commerce sites, digital identity theft levers are being exercised by the malevolents.

We believe that this war against organised crime and extremism can be won decisively and effectively. As in all wars, our collective national defences must excel enemy aggression. Our concern is that in the absence of setting out specific responses and specific responsibilities, we are looking at another issue like world poverty where everyone knows we should be doing something about it but somehow concrete progress does not take place or takes too long. This is an ongoing series of attacks on our whole way of life and yet seems to be dealt with apparently complacently by most governments and many businesses and citizens have not woken up to the threats at all. Why are we being so shy here and why do we feel that pre-emptive war action, by invading countries whose government regimes we may not favour, is the only way forward? We need to set five priorities:

1. World Security Organisation (WSO) – In order to achieve the objective of neutralising the emerging dangers we are faced with, an international organisation empowered with the necessary resources and authority of a type similar to the World Health Organisation (WHO), and with much greater clout than Interpol needs to be set up. The WSO would be a worldwide collaboration and umbrella activation body that would run programmes in troubled regions in a similar way to the highly successful United Nations' WHO. Such a WSO may be able to set priorities, raise awareness at governments' level, deal with multiple countries and run simultaneous operations legitimately. At present the WSO is essentially the US, which as super power acts as global policeman at much cost to itself in terms of finance and long-term damage to image. The evolving dangerous environment can only be looked at holistically and policed by a body such as the WSO. Country confined domestic politicians or regional politicians may also be galvanised into setting priorities in their narrower political agendas by the WSO, which will have the long-term horizons in mind to tackle issues of this magnitude and colossal scale.

Unfortunately, the rapidly increasing rate of technological change increases the dangers society is facing exponentially. Almost any conceivable advantage over the dark forces can soon be countered. This leaves us in a continuing battle for superiority similar to the situation we now face with disease in health care where each new miracle drug soon becomes ineffective as the attacking germs and viruses mutate. The WSO would also be able to model the best case scenario or steady state we could realistically hope to achieve if all sensible actions were implemented. There is no such thing as 100% safety and security but containment and outright elimination of some forms of organised crime and extremism would be concrete steps in the right direction.

The thought of some 150 nations attempting to protect themselves individually is ludicrous. The traditional concept of national sovereignty has to be redefined. Perhaps only a dozen or even fewer nations have the wherewithal, although perhaps not yet the will, to offer some reasonable domestic protection. Only a comprehensive international level of cooperation that exceeds anything the world has yet considered will be needed in the intelligence and action areas against the “anti-civilisation” forces. The anti-terror meeting in Saudi Arabia last weekend, where HRH Crown Prince Abdullah called for a global centre for counter-terrorism, represents a positive step forward in the long-term direction of the WSO.

2. Global defence has always been about securing trade routes and markets alongside survival and the preservation of national identity. 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 as part of their 5th dimension defence shield. Effective counter-attack-forces could save businesses a lot of lost time and money in dealing with rogue, politically motivated, electronic attacks from radical and criminal groups scattered across the world and within the nation state. The key aspects of counter attack are high specificity in targeting and clearance mechanisms. Governance is vital: any action must be clear, legal and enforceable.

To illustrate the need for counter-attack forces in a broader way: the United Nations will have to alter its traditional respect for national sovereignty and only defensive measures to allow selected pre-emptive strikes. These may not be so much against whole nations as against certain areas, provinces or even cities that have become almost independent units beyond the control of the nominal national authorities in which they operate. Defensive measures alone after an attack, the normal tendency and preference for all democratic governments, may well come only after quasi-defeat due to the overwhelming impact of first-strikes in this age of WMDs, particularly those that are linked to small numbers of biological agents that can spread sickness and death to vast numbers of a population with disastrous results comparable to those of a nuclear explosion.

3. Laws will have to be passed throughout the civilised world that 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.

a. This process has already begun with the US Senate and House of Representatives passing the "Uniting and Strengthening America Act by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001" and the "Cyber Security Enhancement Act (CSEA) of 2001." The CSEA seeks life imprisonment for anyone putting lives at risk by electronic means. In the UK, under the Terrorism Act 2000, enacted into law in 2001, people who endanger lives through the manipulation of public computer systems are to be considered under the anti-terrorism law as would any other terrorist.

b. All business operations should also be required, by law, to possess a sufficiently layered and tranched security architecture so that even if one layer of defence is breached the entire set of valuable databases or command and control capabilities need not be immediately compromised.

c. Laws are only passed when a government is fully persuaded of the threat. How is a government persuaded before a catastrophe occurs?

4. Mobilisation of resources including new investment is necessary on interoperable distributed Knowledge Management Analysis Systems (KMAS), which allow data to be shared easily between different sources, starting with agencies collecting intelligence for a partial Total Information Awareness Systems (TIAS). Also, investment in more local human intelligence across the globe is essential. The expertise of the very few available people who are proficient in the technologies of the 5th dimension needs to be utilised to train the counter-attack-forces through the establishment of a national Centre of excellence for digital defence.

Nothing significant can be achieved without this cohesive sharing capability being made available to the future counter-attack-forces, who would be able to ensure reliability, availability, maintainability and scalability of the critical economic infrastructure and SME business systems in the event of hacker attacks.

Such a Digital Defence Centre could be hosted within the Security Services, Ministry of Defence or the Cabinet Office.

5. The root of the problem lies in the progressive alienation of large groups of people around the world. This alienation is not just down to religious intolerance but also deprivation of many kinds: physical, territorial, spiritual, financial and educational amongst other types. It is vitally important that we in the West understand the history and tradition that have 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 perfectly 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 all 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. In the last 50 years, the West has lost some of its deeper understanding of its own religious base and associated values, we therefore need new leadership generation programmes across the world to understand the key tenets of all the major religions, associated ethics and good governance philosophy.

The humanistic angle is a new necessity in today's global village, which civilisation has never really attempted. None of the other actions will be more than short-term delaying tactics unless humankind begins to think in much broader terms of respect, honour and even love for all other humans. Otherwise we could be facing an impossible situation in which force, persuasion and even material sharing cannot reverse the formidable forces that in today's world can be unleashed at any time by only a small number of dissident, "anti-civilisation" entities and cells.

Conclusion

The answer to fighting extremism, terrorism and organised crime over the coming decades lies in:

1. Establishing The World Security Organisation (WSO), a global collaborative venture more powerful than Interpol and just as effective as the World Health Organisation (WHO);
2. Establishing national counter-attack forces within the appropriate legal framework;
3. Embracing technology to construct national and international Total Information Awareness Systems (TIAS) and Knowledge Management Analysis Systems (KMAS);
4. Developing extensive on-the-ground Human Intelligence networks;
5. Reducing poverty levels in deprived areas from where radicals and organised crime members are recruited, raising education and awareness levels, as well as promoting the understanding necessary for a multi-faith tolerant society to become a reality.

[ENDS]

This speech, post completion, was reviewed by a number of professionals in the banking, insurance, reinsurance, government, intelligence, defence, diplomatic, legal and academic arena for which we are grateful:

1. Charles Benson, Criminal Barrister, The Chambers of Desmond de Silva QC
2. Rudi Bogni, Chairman, MedInvest International; Director, Old Mutual
3. John Burke, Head of Group IT Security Risk, UBS
4. Hervé de Carmoy, European Vice-Chairman, Trilateral Commission
5. Prof William Dutton, Director, Oxford Internet Institute, University of Oxford
6. Ram Gidoomal, Chairman, South Asian Development Partnership
7. Hans Gmuender, Former CEO Asia, XL Insurance
8. Prof Prabhu Guptara, Executive Director, UBS Wolfsberg
9. Geoffrey Hancock, Director, **mi2g**
10. Willy Hersberger, Senior Consultant, **mi2g**
11. Harvinder Hungin, Senior Advisor, **mi2g**
12. Alan Hunt, Diplomatic Director, Foreign Service Programme, University of Oxford
13. Rear Admiral John Hilton, Director, **mi2g**
14. Robin Jackson, Senior Consultant, **mi2g**
15. Alonzo McDonald, Chairman, Avenir Group; Founding Chairman, The Trinity Forum

16. Hugh McLeod, Senior Partner, Assynt Associates

17. C Thomas McMillen, Chairman, Global Defense Corp; Former member US Congress

18. Farid Nagji, Senior Vice-President and CIO, HCC Insurance Holdings

19. William Newton-Dunn, Member of the European Parliament

20. Prof Jim Norton, Senior Policy Advisor, eBusiness/eGovernment, Institute of Directors

21. Dr Peter Pop, Executive Director, UBS Corporate Center

22. Major General Bill Robins, Senior Consultant, **mi2g**

23. Will Roebuck, Senior Consultant, **mi2g**

24. Colin Sewell-Rutter, European Director, The Trinity Forum

25. Dame Stephanie Shirley, Life President, Xansa

26. Charles Tilley, Chief Executive, Chartered Institute of Management Accountants

The names of reviewers are presented in alphabetical order by last name. 91 names have been withheld on request.

Thought provoking and diverse views have been received from 117 professionals based in Canada, China, France, Germany, India, Italy, Japan, Russia, Singapore, Switzerland, UK and USA.