National Security

Report of a Conference Organized by the Institute of Defence and Strategic Studies (IDSS)

Shangri-La Hotel, Singapore
13 January 2005

INTRODUCTION

Mr. Barry Desker, Director, IDSS

In his opening remarks, **Mr. Barry Desker**, Director of IDSS, observed that the Singapore defence white paper, entitled "Defending Singapore in the 21st Century", had noted that Singapore now faced a more complex security environment, with conventional security threats being joined by new asymmetric threats emanating from international terrorism.

Mr. Desker thus noted that the National Security Conference brought together thinkers and practitioners who can help frame the development of a national security strategy and organization. The focus of the conference would be to examine the meaning of national security post 9/11 and how we should organize to meet the broad spectrum of national security threats that we face today. The conference was divided into sessions examining the main components of a national security strategy, namely, threat assessment, organization, prevention, and crisis and consequence management. It would examine the framework for threat and risk

Mr Teo Chee Hean, Minister for Defence (left), and Dr. Tony Tan, Deputy Prime Minister and Coordinating Minister for Security and Defence (right)

analyses, assess the current threat from terrorism and nuclear, biological and chemical (NBC) attacks, how militaries could keep the edge in an age of asymmetric warfare, how to prevent strategic surprise, and how we can better improve psychological resilience as well as the protection of critical infrastructure.

Keynote Address

Dr. Tony Tan
Deputy Prime Minister
and Coordinating Minister for Security and Defence

Dr. Tony Tan, Deputy Prime Minister and Coordinating Minister for Security and Defence, began his opening address by referring to the tsunami that hit the coasts of Indonesia, Thailand, Sri Lanka, the Maldives, India and other countries on the rim of the Indian Ocean on 26 December 2004. This disaster must be looked at in the context of national security and its impact cannot be divorced from regional and national considerations. The tsunami disaster not only resulted in the tragic loss of many lives but also had a significant negative economic impact on the region as a whole. In this increasingly globalized world, characterized by the interdependence of states, we are all now more vulnerable.

Like transnational terrorism, a tsunami is an event that has a low probability of occurrence, but once it does, has significant consequences. Like the SARS crisis and the new brand of militant transnational terrorism first demonstrated in the 9/11 attacks, a tsunami can be regarded as a "known unknown"—a potential threat whose origins we may recognize, but whose time of occurrence and subsequent projections we cannot predict. Dr. Tan described these as the "low probability, high impact wild cards of history".

The response to this type of unconventional threat must be pro-active. Dr. Tan stressed that the region must be prepared to confront a wide range of threats from a number of directions. Governments must look ahead constantly. They must also be prepared to be faced with strategic surprises, that of the "unknown unknowns", that is, threats that we are not aware of at this time. Governments must anticipate threats, assess the risks and plan accordingly. A more extensive, systems-based planning approach must be adopted—one that can "deal with strategic complexity, with multi-faceted, [and] multi-dimensional challenges". Dr. Tan then went on to point out that governments must begin to invest in the appropriate early warning and detection capabilities for all critical sectors, including security, the economy and the environment. He concluded that while we cannot predict the future, "we can certainly anticipate what might come, before it strikes, and prepare ourselves accordingly."

Session 1—Threat Assessment

Threat Assessment

Rohan Gunaratna (IDSS) began his discussion with a survey of Singapore's new strategic environment. This has changed in the last three years since 9/11 in favour of militancy. This is due to the failure of some governments to take the necessary appropriate actions, a situation that will remain so for the foreseeable future. Thus it is possible to conclude that terrorism will remain a "tier one" security threat for Singapore for the next five to ten years.

While the resident internal threat of terrorism has been neutralized, the external threat remains significant. In order to protect against this growing external threat, the Singapore Government must creatively harden its defences. Its security measures must not become a matter of routine. Singapore must also work with its partners in the region to change the regional environment.

Singapore has no strategic depth. Its defences for the last 30 years have taken this premise into account and have sought to neutralize potential threats at their source. This principle should continue to apply in the fight against terrorism.

The violent Islamic extremists in the region see Singapore as "America's aircraft carrier" and is therefore a high-value target. Singapore's traditional method of protecting itself through the development of a strong military force will not work as a deterrent against the threat of terrorism.

Although there exists a variety of networked and experienced terrorist groups in the region, the main threat in the immediate neighbourhood is the terrorist group Jemaah Islamiah (JI). This group enjoys strong regional support and has developed a significant operational infrastructure. It is believed that up to 400 JI members are active in Southeast Asia, and the group retains a high capacity to regenerate due to the strong support base that exists in the region and the fact that JI has not been designated a terrorist group by the Indonesian Government. JI has also been operating training camps in the Philippines since 1994. The training camp currently active is Camp Jabal Kuba in the Philippines.

JI has no operational infrastructure in Singapore and is therefore likely to plan its next attack outside the country. This will most probably be a suicide attack against a high-profile, symbolic or strategic target. These attacks are likely to be relatively few in number but each will send a very powerful message. It is important to point out that JI is currently considering a shift away from the more traditional tactics of car bombings and suicide attacks to chemical and biological

Associate Professor Rohan Gunaratna, Head, International Centre for Political Violence and Terrorism Research, IDSS

attacks, although at this time they have not yet developed the capability to do so.

In order for Singapore to defend itself, it has no option but to work overseas, unilaterally and with partners to develop a comprehensive counter-terrorism strategy. This strategy must be one that disrupts the support base, ideology and appeal of the terrorist groups.

Risk Assessment and Early Warning

John Parachini (RAND Corporation) began his presentation by asserting that the contemporary terrorism threat represents a conundrum. The challenge is to assess the risk of terrorism and identify the attackers before they strike, with access to only a small set of data for reference given the relative rarity of terrorist attacks.

In the current security climate, and in particular after the attacks of 9/11, it has become increasingly evident that although catastrophic terrorist attacks remain a rarity, they are, according to Parachini, an enduring danger that no modern government can ignore. There are a number of issues that need to be addressed: How do we prepare for a low probability event that has the potential to cause catastrophic consequences? How do we get the right balance of anti-terrorist measures?

The answer is not to start by imagining worst-case scenarios as this would result in routine security being neglected or troops being required on every street corner. Parachini stressed the need for law enforcers and intelligence authorities to "devise a strategy that involves specialized measures for commonly perceived threats, some hedging against the totally unexpected, and as much attention to policy and programmes that offer dual-use and daily benefits".

It is necessary to begin by setting the parameters of the threat. It is important to understand why we have not seen the types of attack that have been predicted. In other words, why have motivations and capabilities in some cases failed to come together? The common elements in the phenomena need to be found. A baseline of terrorist behaviour must also be established in order to ground the range of possibilities. The variables can then be altered to future circumstances, allowing reasonable assumptions to be made regarding potential future terrorist attacks.

Parachini went on to propose a conceptual approach for identifying terrorist attack strategies and tactics. The approach involves four elements and it is the interplay between these elements that provides insight into the risk and early indication of the threat. The elements are: motivations, capabilities, context and vulnerabilities. Past examples of catastrophic terrorism can then be segmented into these

Mr. John Parachini, RAND Corporation

four categories in order to allow for more accurate analysis. This conceptual approach is not predictive; rather, it will help the authorities to focus and prioritize their intelligence. This approach takes into consideration both why certain attacks have happened and why attacks that were expected did not take place after all. It is important to assess these "inhibiting factors" in order to determine when they diminish and consequently raise the threat level.

In order to avoid the tendency to merely prepare for worst-case scenario events, this type of conceptual approach must be adopted to allow for a more discriminate analysis of the empirical record.

A Framework for Linking Threat and Risk Analyses to Policy Action

Eric Larson (RAND Corporation) presented a number of lessons learnt from his previous studies on terrorism and homeland security, including a framework for linking threat assessments to policy action which was originally developed for the U.S. Army, and then went on to apply them to Singapore's August 2004 National Security Strategy, in order to offer some evaluative comments.

Larson's studies have shown that nations face a long-term threat from global terrorism, and must therefore be engaged in a long-term game of damage limitation. The most important objective is to enhance strategic depth, that is, the amount of time there is to respond to a particular threat. In order to achieve a comprehensive homeland security programme designed to deal with the full range of threats, it is necessary to develop end-to-end systems of layered defences. Larson stressed that the highest payoffs are often found in preventative activities rather than in the general hardening of targets.

The framework for linking threat to policy action outlined by Larson consists of four sub-divisions.

- **Threat analysis**: This section aims to address the question of which threats and targets warrant policy action and the magnitude of planning required for a particular response. In other words, it helps to decipher the point at which action should be taken. It is based on the assumption that the probability and magnitude of threats are inversely related. It is important to note that while this framework will help to determine the threshold for action, the decision on what warrants action is based on subjective judgment.

- **Performance levels**: This section takes the planning magnitudes which were developed in the first section and aims to establish performance levels for the plans, and ways of measuring performance or effectiveness to see if the performance levels have been met.

- **Operational concepts**: In order to achieve the demanded levels of performance by the most cost-effective means possible, operational concepts are developed, that is, "layered, end-to-end policy architectures that can provide prevention, protection and response capabilities".

- **Budgeting**: The total cost of the operational concepts and the improved homeland security capabilities that would result from their implementation are set against other government spending priorities in this section, the result often being that performance levels are reduced to a more affordable level.

Singapore's National Security Strategy is based on the strong conceptual framework of "prevent-protect-respond". It represents a thoughtful and well-integrated policy response to the threats Singapore faces. Larson concludes that adopting the sort of framework described above may reveal additional opportunities to develop more successful and cost-effective means of threat reduction.

Dr. Eric Larson, RAND Corporation

Discussion

It was pointed out in the discussion that Rohan Gunaratna mentioned that Jemaah Islamiah had not yet developed chemical, biological, radiological and nuclear (CBRN) capability and that John Parachini stated that Al Qaeda had developed a "portfolio management-like approach" to terrorism, in which it does not really need to use weapons of mass destruction as it is still successful in its use of conventional terrorist methods. Does this mean that Singapore, which has done a lot of work in hardening potential targets, actually made itself more vulnerable to a CBRN attack?

One speaker replied that JI has been a very conservative organization. Most of its capability rests in vehicle bombs. Evidence found in a training manual suggests that there is the intent to acquire more sophisticated weapons. However, there is as yet no capability to use nuclear weapons. Fifteen terrorist groups have expressed their interest in radiological, chemical and biological weapons and may have developed a rudimentary capability. However, the probability of them being employed successfully is very small. Most of the time, the JI will go for the gun and the bomb.

Another speaker noted that most terrorists prefer to use simple, safe and familiar methods. On the other hand, there are some who are interested in chemical, biological and radiological (CBR) weapons. These groups tend to engage in delusional thinking and they therefore often make mistakes. Accidents occur which provide early warning signs as it is difficult to make an effective weapon of this type.

The question of how the performance goals of anti-terrorism measures are defined was discussed. The best way to think about performance goals is to imagine that if there was an attack, what consequences would be expected if there had been no changes in policy in place and compare that to the results of any new policy initiatives. In terms of assessing deterrence performance, one should look at the evidence of groups baulking at attacking specific targets. One might also look at the ability to capture suspects and thereby prevent them from carrying out an attack.

A participant then posed the question: What is the difference between a risk analysis and a threat assessment? The question sparked a number of responses. One response was that a threat assessment examines intent and capability, whereas a risk assessment examines vulnerability and consequence/impact. Another speaker disagreed on the grounds that there is a coupling between vulnerability and intent, and therefore it is not possible to do an assessment that examines only capability and intent as suggested, because intent is related to vulnerability. In other words, if the vulnerability of a target is great, the terrorist group will be more likely to attack this target.

Session II—Organization

Keeping the Military Edge in an Age of Asymmetric Warfare

Isaac Ben-Israel (Tel-Aviv University) described how, in the last four years, Israel has faced increased levels of terrorism and in particular suicide terrorism, but has now succeeded in bringing the levels down. He went on to share some of the lessons learnt from this experience.

The point at which the Israeli counter-terrorism campaign began to substantially reduce the level of terrorist attacks was when the war on terror was "separated" from the political issue of coming to an agreement with the Palestinian leadership. In fact, to begin with, the peace negotiations were put aside altogether while Israel launched a full-scale campaign against terrorist organizations. The combined effects from the expansion of intelligence coverage, the targeted killings of many key members of terrorist organizations and the erection of a security "fence" have reduced terrorist attacks to their pre-2000 level.

One of the key counter-terrorism measures employed was the "targeted killing" or "surgical elimination" of a number of important members of the terrorist organizations that had been carrying out attacks against Israel. This method was successful due to the fact that terrorist groups are rather small. According to Ben-Israel, the number of people actively involved in a particular terrorist organization is no more than a few hundred. When the rate of elimination of key terrorists in a group reaches 20 to 30%, it significantly reduces the ability of the terrorist group to function at a level that can carry out attacks. Instead, it becomes preoccupied with ensuring its own survival.

Ben-Israel also stressed that the role that cutting-edge technology can play in developing surgical capabilities should not be underestimated. The assumption that anti-terrorist measures should be low-tech just because the terrorist apparatus is low-tech is a mistake. Science and technology, and particularly R & D, played a vital role in reducing the threat of terrorism in Israel. It must be noted, however, that the technology was directed at the core of the terrorist groups for the reasons outlined above, and not at the suicide bombers or "end points" of the "production line".

In the fight against global terrorist networks, technology can also play a vital role. All networked organizations rely upon communication and it is therefore one of their weaknesses. Intelligence technologies directed against the communication lines of the terrorist organizations targeting Israel proved highly

Professor Amitav Acharya, Deputy Director, IDSS, with Mr. Barry Desker, Director, IDSS

effective and the lesson should be applied to the global war on terrorism. Detection technologies along the border have also been highly effective in the Israeli case. Creating a "virtual fence" and preventing terrorists from entering a vulnerable area is more cost-effective than trying to detect them once they have entered.

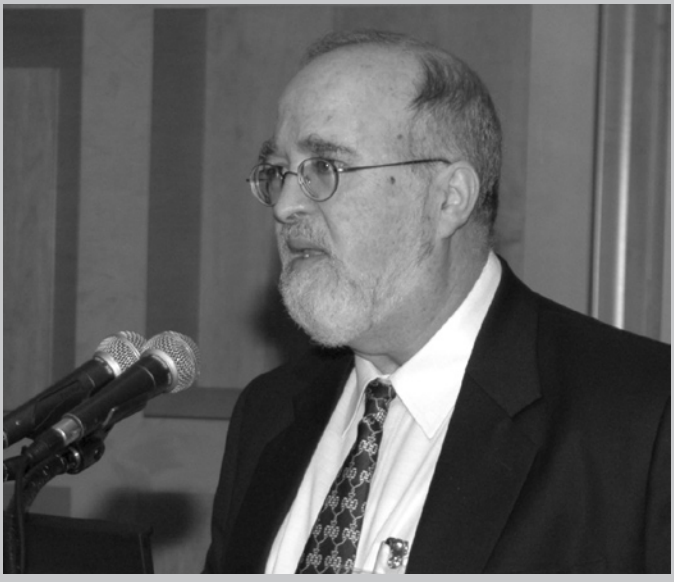
In sum, the experiences of Israel in its fight against escalating suicide terrorism are relevant in the global war on terror, the most important lesson being that technology has a vital role to play.

Discussion

In response to Ben-Israel's comment that the turning point in the Israeli counter-terrorism campaign came when the military operation was de-linked from the political dimensions of the conflict, a participant quoted British strategic thinker Liddell-Hart: "The aim of grand strategy should always be more than just winning the war; it should also be about winning the peace." Although Israeli forces have gained the advantage temporarily, for any lasting peace to be achieved, the political aspect of the conflict will have to be addressed eventually. Remembering that military operations can never be conducted in a political vacuum is of utmost importance. For example, the excessive use of force or the insensitive behaviour of military personnel towards civilians will have political repercussions and may well prove fatal to any future peace negotiations.

It was also pointed out in the discussion that the Israeli model for fighting terrorism will result in the continuation of the Palestinian-Israeli conflict for many years. This is due to the failure of the Israeli authorities to disrupt the "conceptual infrastructures" of the terrorist groups, that is, the ideological and motivational dimensions of the groups. Until these are addressed, terrorist groups will continue to operate within what is a friendly environment, and will maintain a high capacity to regenerate. Conflict management and resolution models also need to be implemented in order to achieve a more long-lasting solution.

However, a speaker responded that it was naive to presume that it is possible to negotiate with terrorists. It is only possible to start negotiations or achieve conflict resolution with the Palestinians once their political leaders are freed from the control of the terrorist organizations. In the context of the global war on terror, negotiating with extremist Islamic terrorists who want to rid Southeast Asia of any Western influence is an impossible task.



Professor Isaac Ben-Israel, Tel-Aviv University

Session III—Prevention

Preventing Strategic Surprise

Gordon Woo (Risk Management Solutions) spoke on "preventing strategic surprise" when dealing with intelligence information. Since people tend to ignore something that does not fit their worldview, he highlighted the importance of an objective assessment of intelligence information. Based on the reliability and coherence of intelligence data, the surprise element can be eliminated.

The attack on Pearl Harbor is an example of a strategic surprise that could have been prevented. The existing probability of such an attack was less than one per cent but when one considers information that was obtained but disregarded from an unreliable double agent and Japanese radio interception, there was a 20-per-cent chance of such an attack. An analogy to strategic surprise can be found in chess. One needs to be attentive to the intention, direction, timing, doctrine and weaponry of the opponent. Woo argued that the surprise factor in the September 11 attacks on the World Trade Center and the Pentagon was a result of the underestimation of the opponent's will to win.

In the recent Indian Ocean tsunami, the surprise factor could have been avoided. The science to predict a tsunami is present but because the people analysing the data are not trained in risk management, they tend to issue a tsunami warning only after they are certain of the event. He conceded that using his approach could lead to false warnings, but for him, it is better to be safe than to be caught by surprise.

Intelligence Coordination and Strategic Surprise

Richard Betts (Columbia University) took the audience through the current re-organization of the U.S. intelligence services that Congress hopes would enable the U.S. to better anticipate the next Al Qaeda attack.

The key question on how much centralization is needed has been much debated. While there is a general agreement that different departments (Department of Defence, Treasury, Homeland Security Department, FBI, CIA, etc.) are necessary, some amount of inter-department coordination is also needed. The embarrassment of the Weapons of Mass Destruction (WMD) issue in Iraq pointed to the requirement for better coordination between the intelligence agencies. One way to maximize coordination is by having a single national intelligence chief. However, while there was more questioning of the basic assumptions of reform, it was still unclear on the optimum level of coordination

Dr. Gordon Woo, Risk Management Solutions

required. Betts felt that a bureaucratic balance would evidently fall in place where the safeguarding of classified information will take priority. Current intelligence reform can also be seen as moving from a need-to-know to a need-to-share bureaucratic balance. However, while there is a move towards disseminating information as far as possible, there is also a fear of espionage.

Betts, in the hindsight of earlier reforms and re-organizations of the intelligence services following intelligence failures at Pearl Harbor, in Korea, and over the Cuban missile crisis and the Tet Offensive, is not optimistic that the ongoing reforms will succeed. He attributes this to the loss of institutional memory and observed that "many lessons of the limits of these previous attempts at reform—especially lessons involving unanticipated counterproductive side-effects of reforms—are now understood only by retirees or scholars outside the government". He thus anticipates that "it is likely that the latest big reforms in coordination will produce at least some problematic side-effects which the government will then discover all over again and grapple with in coming years".

Betts then focused on the problem of collection of intelligence, and made the point that better analyses of the data is required, as is the need for human intelligence. He also warned that the U.S. might make more demands upon its allies to provide information to fulfil their collection gaps.

Discussion

The discussion began with **Kwa Chong Guan** commenting that in traditional wars between states, one is expected to declare war. The Japanese failure to do so before their surprise attack on Pearl Harbor and other post-World War II surprise attacks, including Egypt's crossing of the Suez on the eve of the Yom Kippur War in 1973, therefore raises new problems about forecasting the outbreak of wars. In the new era of transnational terrorism, the fundamental question is whether the old techniques and methodologies for anticipating a surprise attack are applicable to analysing Al Qaeda or Jemaah Islamiah's propensity to launch a catastrophic attack on us.

The commentator further observed that we should also perhaps watch for the "problematic side-effects" that Betts anticipated would come out of the ongoing reforms of the U.S. intelligence services. U.S. allies providing information to fulfil its collection gaps is not a viable option. Conventional aggressors in preparing for a surprise attack generate a lot of noise and signals that the victim's intelligence service should be able to collect. In contrast, Al Qaeda, as an asymmetric enemy, like guerrillas and insurgents, generate a lot less noise and signals and so provide their victim with a much smaller data base to work from in anticipating the attack.

Professor Richard Betts, Columbia University (right), with Professor Khong Yuen Foong, Senior Research Adviser, IDSS (left)

Dr. Gordon Woo (left) and Mr. Kwa Chong Guan, Head, External Programmes, IDSS (right)

With respect to Woo's paper, the commentator argued that embedded in Woo's taxonomy are two fundamentally different categories of surprise. The first is the fundamental surprise that the aggressor should have launched an attack when the victim's calculations and intuition indicate he should not have attacked, as in the case of Yom Kippur in 1973. In contrast, we should not be fundamentally surprised by Osama bin Laden's intention and resolution to attack the U.S. and its allies, since he has made it very clear. What we do not know are the tactical dimensions of an Al Qaeda or JI attack. Can we, however anticipate and pre-empt this tactical surprise? Indeed, it is probable, given the inherent difficulties of Bayesian analysis, that we ultimately cannot predict a surprise attack by Al Qaeda or JI and so should be prepared to be surprised by them.

The response to this comment was that there has been a resurgence of the application of Bayes' theorem. Its use lies in the fact that it can objectively analyse intelligence information. On the question of whether the existing model could be applied to the recent tsunami disaster, it was observed that since scientists are trained in certainty and not in risk management, they did not sound an alarm when in fact they should have done so. As to the issue of whether the use of quantitative science to predict social phenomenon is useful, a speaker expressed the view that the model had its pros and cons, and that it was not really a behavioural issue but one of reliability of information.

A speaker also noted that intelligence reform in the U.S. would not stop future terrorist attacks. The report, which highlighted the fact that the CIA did not pass on crucial information to the FBI, pointed more to a procedural problem rather than one of reform. On the question of the characteristics of a robust intelligence organization, it was pointed out by another speaker that fusion centres could do a better job than individual intelligence agencies.

A participant asked to what extent the September 11 attacks were a strategic surprise given the background of the 1993 bombing of the World Trade Center as well as the bombings of the U.S. embassies in East Africa. The discussion noted that there is usually prior information but one needs to look for it. However, another view held that while prior information could reduce the element of surprise, a capable enemy would always find workarounds.

Session IV—Crisis and Consequence Management

Building Resilience in Civil Society's Psychological Response to Mass Terrorism

Anne Speckhard (Free University) observed that terrorism is used as a psychological weapon by terrorists. The erosion of borders, speed of communication and the proliferation of high-tech weaponry have markedly increased the threat of global terrorism. While governments are hardening their defences by infiltrating terrorist groups as well as securing buildings, airports and seaports, less emphasis has been placed on the resilience of the public. The general perception of most governments is that the public tends to panic in the face of disaster. But citizenry needs to be recognized as being much more resilient. From the disasters of September 11 and the hostage crisis in Moscow, it is evident that social cohesion actually increases under such circumstances.

Communication by governments is key in the immediate aftermath of a mass terrorism attack. Truth, clarity and calm are what the public comes to expect from their leaders. In this respect, it is useful for governments to prepare in advance by pre-packaging sound bites and anticipated information. The trust of government officials during a crisis is key and hence it is important to have public communication based on facts and not rumours. In other words, a comprehensive information campaign needs to be in place well before disaster strikes.

This strategic communication is important for citizens to take on civil responsibility. By embracing the role of civil society, governments can increase resilience in containing psychological contagion and post-traumatic stress disorders. Speckhard noted that the symptoms of anxiety after a crisis can be mistaken as toxic exposure and hence health facilities in a crisis-hit area can be quickly overwhelmed. In order to lower the unnecessary stress on health systems in a crisis, it is therefore necessary to empower civil society to cope with such disasters.

Resilience, Adaptive Capacity Building Overview

Steve Trevino (Booz Allen Hamilton) elaborated on the "emerging operating reality". The threats faced by states today are increasingly transnational. The common theme among terrorism, crime, SARS and avian bird flu threats, for example, is that they transcend conventional

Professor Anne Speckhard, Free University

Mr. Steve Trevino, Booz Allen and Hamilton (right), with Dr. K. U. Menon, Director, National Resilience Division, Ministry of Information, Communications and the Arts (left)

state boundaries. Conventional measures taken by law enforcement and intelligence agencies are increasingly frustrated by the networked model of these threats.

In order to build resilience against these threats, governments need to build "new operating models" based on complexity science and networks theory. Trevino argues that Singapore, having successfully dealt with terrorism and the SARS virus, provides an ideal testing ground for these models. According to Trevino, his new model seeks to build resilience at the enterprise, community, national, regional and global levels. It uses a "tri-sector" approach, where the government, commercial and civil society organizations work hand-in-hand in a networked fashion. This kind of systemic resilience is the most effective way to deal with social risk and address threats of a national as well as a global scale.

A National Resilience Strategy based on this model would involve the use of "collaborating operating environments" that will address risks real-time. This will require a comprehensive change at the organizational and cultural levels. The values of an organization will need to be adapted to the new model in order to build effective resilience operating models. As the model presented is networked, it seeks to build systemic solutions to systemic risks. This strategy will also require shareholders of all three sectors to have policy, directives, guidance, standards as well as best practices.

Discussion

A participant posed the question why government structures were primarily hierarchical when terrorist and crime networks were increasingly networked. A speaker replied that governments do not usually function well in the face of uncertainty and that the hierarchical structure might be due to political posturing. Commercial organizations, which focus only on their profit margins, also do the same. Another participant asked about the track record of Trevino's resilience model. The response was that the focus of the model was on business continuity and that having identified the core characteristics, the model provides an approach towards resilience in various industries. On the question of the key factors of a resilient organization and whether it was related to the leadership, the view was expressed that the transformation of an organization into a resilient one would require a change of the whole corporation and not just the leadership.

The discussion then focused on how governments can recover from bad decisions taken with respect to resilience. Citing the example of Italy, where a promise was made to the people that the power grid was fail-safe, a speaker felt that no such promise should have been made. In Iraq, what is needed but not forthcoming from the U.S. administration is an

apology. Without one, it is difficult to reconcile that the system has been corrected. Unlike the above, however, tsunamis are generally seen by the people as an act of God, and they are therefore willing to accept it better.

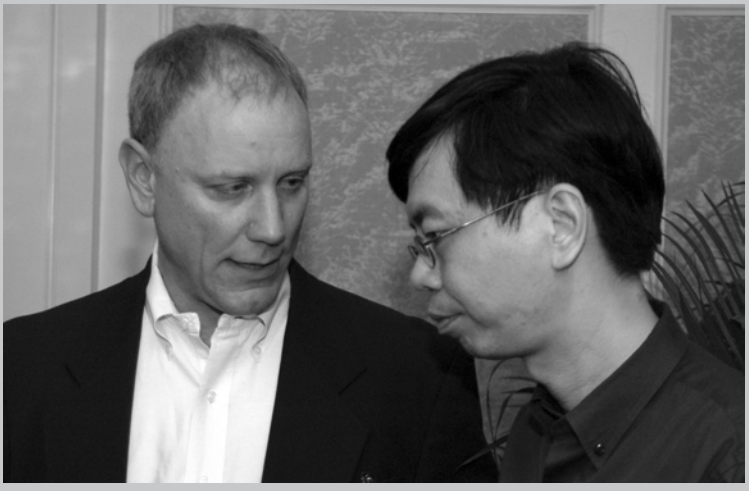
On the question of the kind of strategic communication needed to deal with terrorism, given that deterrence no longer works in this case, a speaker made the observation that governments need to tell its people that it can protect its people only up to a certain extent and that there are no guarantees.

Summary

Andrew Tan (IDSS) summed up the conference. After the September 11 attacks in the U.S., and the Bali bombings in Indonesia, Singapore's response to terrorism has been "vigorous and comprehensive". This is evident in its National Security Strategy document published in August 2004, essentially a blueprint for a comprehensive architecture that would be robust enough to detect, prevent and mitigate consequences. However, as one can never be sure, this needed to be subjected to intellectual audit, which led to this conference on national security. As Dr. Tony Tan had stated in his address, there is the need to anticipate surprises, including known unknowns, such as terrorist attacks, and unknown unknowns, such as natural catastrophes. To do so requires a systems-based approach, in order, as Woo pointed out, to engage in proper risk management.

The context of the conference was set by Gunaratna's warning regarding the continued severity of the terrorist threat, which has now morphed beyond Al Qaeda and the JI to become a generalized, long-term, ideological threat. Citing events in Iraq, Gunaratna alluded to his belief that the Al Zarqawi network there is evolving into an international terrorist organization that could pose a long-term threat even to Southeast Asia and Singapore.

The one common element in most of the discussions was the need to be systematic. As Larson noted, we could expend an entire GDP on counter-terrorism or defence, but what we need is a rational system or methodology to evaluate threats and allocate scarce resources to meet those anticipated threats. In this respect, Woo's use of quantitative decision science, for instance, is helpful in systematically managing the risk. However, as Betts also alluded to, a systematic and scientific approach should also be accompanied by the better use of our analytical abilities. Indeed, his point about the importance of human intelligence is surely also a crucial one. There is a need to be able not just to join up the dots but also to make sense of them.



Dr. Eric Larson (left) and Dr. Andrew Tan, IDSS (right)

Some participants of the National Security Conference

However, because no system can be failsafe, it is also important to focus on crisis and consequence management. In this respect, it is comforting to know, from Speckhard's paper, that the civilian population is probably more resilient than we think, and that the psychological consequences of major terrorist attack can be managed, so long as we are prepared.

Rapporteurs:
S. P. Harish
Catherine Zara Raymond

Conference Programme

Wednesday
12 January 2005

7.00 p.m. Welcome Reception
Yellow Orchid, Mezzanine Floor, Shangri-La Hotel

Thursday
13 January 2005

8.30 a.m. – 9.00 a.m. Registration

9.00 a.m. – 9.30 a.m. Opening Address
Dr. Tony Tan, Deputy Prime Minister and Coordinating Minister for Security and Defence, Singapore

9.30 a.m. – 9.45 a.m. Tea Break

9.45 a.m. – 11.30 a.m. Session I
Threat Assessment

Chair:
Mr. Barry Desker, Director, Institute of Defence and Strategic Studies

Presenters:
Threat Assessment
Associate Professor Rohan Gunaratna, Head, International Centre for Political Violence and Terrorism Research (ICPVTR)

Risk Assessment and Early Warning
Mr. John Parachini, Policy Analyst, RAND Corporation, U.S.A.

A Framework for Linking Threat and Risk Analyses to Policy Action
Dr. Eric Larson, Senior Policy Analyst, RAND Corporation, U.S.A.

11.30 a.m. – 12.45 p.m. Session II
Organization

Chair:
Professor Amitav Acharya, Deputy Director, Institute of Defence and Strategic Studies

Presenter:
Keeping the Military Edge in an Age of Asymmetric Warfare
Professor Isaac Ben-Israel, Head, Programme for Security Studies, Tel-Aviv University, Israel

Discussants:
Associate Professor Rohan Gunaratna, Head, ICPVTR
Associate Professor Kumar Ramakrishna, Head (Studies), Institute of Defence and Strategic Studies

12.45 p.m. – 1.45 p.m. Lunch
Casuarina (Tower Ballroom)

Conference Programme

1.45 – 3.30 pm Session III
Prevention

Chair:
Professor Khong Yuen Foong, Senior Research Adviser, Institute of Defence and Strategic Studies

Presenters:
Preventing Strategic Surprise
Dr. Gordon Woo, Risk Management Solutions, U.K.

Intelligence Coordination and Strategic Surprise
Professor Richard Betts, Director, Institute of War and Peace Studies, Columbia University, U.S.A.

Discussant:
Mr. Kwa Chong Guan, Head (External Programmes), Institute of Defence and Strategic Studies

3.30 p.m. – 3.45 p.m. Tea Break

3.45 p.m. – 5.30 p.m. Session IV
Crisis and Consequence Management

Chair:
Dr. K. U. Menon, Director, National Resilience Division, Singapore

Presenters:
Building Resilience in Civil Society's Psychological Response to Mass Terrorism
Dr. Anne Speckhard, Professor of Psychology, Free University, Brussels

Resilience, Adaptive Capacity Building Overview
Mr. Steve Trevino, Chief Strategist, Global Sustainability, Booz Allen Hamilton, U.S.A.

7.30 p.m. – 9.30 p.m. Dinner
The Sentosa Resort and Spa

List of Participants

1. Professor Amitav Acharya
Deputy Director
Institute of Defence and Strategic Studies
Block S4, Level B4, Nanyang Avenue
Singapore 639798
Tel: 65 6790 6213
Fax: 65 6793 2991
E-mail: isaacharya@ntu.edu.sg

2. Professor Richard K. Betts
Director
Saltzman Institute of War and Peace Studies
Columbia University
420 West 118th St. Room 1328
U.S.A.
Tel: 212 854 7325
Fax: 212 864 1686
E-mail: rkb4@columbia.edu

3. Mr. Barry Desker
Director
Institute of Defence and Strategic Studies
Nanyang Technological University
Tel: 65 6790 6907
Fax: 65 6793 2991
E-mail: isbdesker@ntu.edu.sg

4. Associate Professor Rohan Gunaratna
Head, International Centre for Political Violence and Terrorism
Institute of Defence and Strategic Studies
Nanyang Technological University
Tel: 65 6790 4491
Fax: 65 6793 2991
E-mail: isrkgunaratna@ntu.edu.sg

5. Professor Isaac Ben-Israel
Head, Programme for Security Studies
Tel Aviv University
Ramat Aviv 69978
Israel
Tel: 03 5692009
Fax: 03 6976725
E-mail: itzik@post.tau.ac.il

6. Professor Khong Yuen Foong
Senior Research Adviser
Institute of Defence and Strategic Studies
Nanyang Technological University
E-mail: isyfkhong@ntu.edu.sg

7. Mr. Kwa Chong Guan
Head (External Programmes)
Institute of Defence and Strategic Studies
Nanyang Technological University
Tel: 65 6790 6975
Fax: 65 6793 2991
E-mail: iscgkwa@ntu.edu.sg

8. Dr. Eric V. Larson
Senior Policy Analyst
Rand Corporation
1776 Main Street
Santa Monica, California 90407
U.S.A.
Tel: 310 393 0411 ext. 7467
Fax: 310 260 8145
E-mail: Larson@Rand.Org

9. Dr. K.U. Menon
Director
National Resilience Division
Ministry of Information, Communications and the Arts
140 Hill Street, #02–02
MITA Building
Singapore 179369
Tel: 65 6837 9900
Fax: 65 6837 9808
E-mail: Menon_K_U@mica.gov.sg

10. Mr. John V. Parachini
Policy Analyst
RAND Corporation
1200 South Hayes Street
Arlington, VA 22202
U.S.A.
Tel: 703 413 1100 x 5579
Fax: 703 413 8111
E-mail: John_Parachini@rand.org; johnvp@rand.org

List of Participants

11. Associate Professor Kumar Ramakrishna
Head (Studies)
Institute of Defence and Strategic Studies
Nanyang Technological University
Tel: 65 6790 6924
Fax: 65 6793 2991
E-mail: iskumar@ntu.edu.sg

12. Dr. Anne Speckhard
Professor of Psychology
Free University of Brussels
3 Avenue des Fleurs 1150 Brussels
Belgium
Tel: 322 772 1237
E-mail: Aspeckhard@brutele.be

13. Mr. Steve Trevino
Chief Strategist, Global Sustainability
Booz Allen Hamilton
19192 Greystone Square
Lansdowne, Virginia 20176
U.S.A.
Tel: 703-298-5461
E-mail: trevino_steve@bah.com

14. Dr. Gordon Woo
Terrorism Risk Analyst
Risk Management Solutions
2nd Floor, Peninsular House, 30
Monument Street
London EC3R 8HB, UK
Tel: 44 207 444 7600
Fax: 44 207 444 7601
E-mail: Gordon.Woo@rms.com

Other Participants

15. Mr. Zainul Abidin Rasheed
Minister of State for Foreign Affairs
Ministry of Foreign Affairs

16. Mr. Chiang Chie Foo
Permanent Secretary
Ministry of Defence

17. Dr. Tan Kim Siew
2nd Permanent Secretary
Ministry of Defence

18. Mr. Bilahari Kausikan
2nd Permanent Secretary
Ministry of Foreign Affairs

19. Mr. Niam Chiang Meng
Permanent Secretary
Ministry of Community Development,
Youth and Sports

20. Mr. Tan Yong Soon
Permanent Secretary
Ministry of the Environment and Water
Resources

21. Mr. Moses Lee
Permanent Secretary
Ministry of Health

22. Dr. Choong May Ling
Deputy Secretary (Security)
Ministry of Home Affairs

23. Mr. Lock Wai Han
Commissioner
Immigration & Checkpoints Authority

24. BG Choi Shing Kwok
Director, Security & Intelligence
Ministry of Defence

25. BG (NS) Lam Joon Khoi
Chief Executive Officer
National Environment Agency

List of Participants

26. Col Soh Poh Theen
Director
National Security Co-ordination Centre
Prime Minister's Office

27. Col Patrick Nathan
Deputy Director
National Security Co-ordination Centre
Prime Minister's Office

28. Mr. Lee Chin Ek
Deputy Director
National Security Co-ordination Centre
Prime Minister's Office

29. Mr. Yeong Gah Hou
Director
Joint Counter-Terrorism Centre
Prime Minister's Office

30. Ms. Sylvia Bay
Deputy Director
Joint Counter-Terrorism Centre
Prime Minister's Office

31. Ms. Lim Ai Teng
Assistant Director
Joint Counter-Terrorism Centre
Prime Minister's Office

32. Mr. Wong Woon Liong
Director-General
Civil Aviation Authority of Singapore

33. Mr. Derek Pereira
Director, Security Plans & Development Division
Ministry of Home Affairs

34. Capt Khong Shen Ping
Director (Port)
Maritime and Port Authority of Singapore

35. Mr. Soh Wai Wah
Senior Assistant Commissioner
Singapore Police Force
Police Headquarters

36. Mr. Fong Yong Kian
Senior Director, HSO
Ministry of Home Affairs

37. Ms. Lim Huay Chih
Director-Designate, Corporate Services Division
Ministry of Education

38. Mr. Tan Song Mong
Deputy Director, Security and Emergency Planning Office
Ministry of Education

39. Dr. Tan Yang Meng
Head, Delta Team
DSO National Laboratories

40. Dr. Andrew Tan
Assistant Professor & Planner of National Security Conference
Institute of Defence and Strategic Studies

41. Mr. S. P. Harish
Associate Research Fellow
Institute of Defence and Strategic Studies

42. Ms. Catherine Zara Raymond
Associate Research Fellow
Institute of Defence and Strategic Studies

43. Dr. Yvette Sulzmann
Project Coordinator
Institute of Defence and Strategic Studies

44. Mr. Joshua Ho
Research Fellow
Institute of Defence and Strategic Studies

45. Mr. Nicholas Seow
Research Fellow
Institute of Defence and Strategic Studies

46. Dr. John Harrison
Research Associate
St Andrew's University, Scotland

47. Ms. Sabrina Chua
Research Analyst
Institute of Defence and Strategic Studies

List of Participants

48. Ms. Elena Pavlova
Research Associate
Institute of Defence and Strategic Studies

49. Mr. Arabinda Acharya
Associate Research Fellow
Institute of Defence and Strategic Studies

50. Ms. Michelle Teo
Research Analyst
Institute of Defence and Strategic Studies

51. Mr. Bouchaib Silm
Research Analyst
Institute of Defence and Strategic Studies

52. Ms. Sarah Burnell
Research Analyst
Institute of Defence and Strategic Studies

53. Mr. Mohamed Ali
Research Analyst
Institute of Defence and Strategic Studies

54. Mr. Muhammad Haniff Bin Hassan
Research Analyst
Institute of Defence and Strategic Studies

55. Mr. Mahfuh Halimi
Research Analyst
Institute of Defence and Strategic Studies

56. Mr. Wong Tze Yung
Research Analyst
Institute of Defence and Strategic Studies

The Institute of Defence and Strategic Studies (IDSS) was established in July 1996 as an autonomous research institute within the Nanyang Technological University. Its objectives are to:

- conduct research on security, strategic and international issues;
- provide general and graduate education in strategic studies, defence management and defence technology; and
- promote joint and exchange programmes with similar regional institutions; organize seminars/conferences on topics salient to the strategic and policy communities of the Asia-Pacific.

Produced by **BOOKSMITH**