LAND TRANSPORT SECURITY WORKSHOP

LAND TRANSPORT SECURITY IN SINGAPORE

CURRENT REALITIES, FUTURE POSSIBILITIES

5 February 2007
Singapore

PONDER THE IMPROBABLE

DSTA
Defence Science & Technology Agency

National Security Coordination Secretariat

Public Transport Security Committee

LAND TRANSPORT SECURITY WORKSHOP

LAND TRANSPORT SECURITY IN SINGAPORE CURRENT REALITIES, FUTURE POSSIBILITIES

REPORT OF A WORKSHOP JOINTLY ORGANIZED BY
THE CENTRE OF EXCELLENCE FOR NATIONAL SECURITY AND
THE HOMELAND SECURITY AND ENGINEERING CENTRE

IN CONJUNCTION WITH
THE PUBLIC TRANSPORT SECURITY COMMITTEE

AND WITH THE SUPPORT OF
THE NATIONAL SECURITY COORDINATION SECRETARIAT

5 February 2007
Singapore

The conference adheres to a variation of the Chatham House rules. Accordingly, beyond the points expressed in the prepared papers, no attributions have been included in this conference report.

EXECUTIVE SUMMARY

On 5 February 2007, the Centre of Excellence for National Security (CENS) and the Homeland Security Engineering Centre (HSEC), in conjunction and consultation with the Public Transport Security Committee (PTSC), jointly organized a closed-door one-day workshop on Land Transport Security at the Traders' Hotel, Singapore. The workshop brought together key land transport security regulators, operators and analysts to deliberate on security issues that pertain to Singapore's land transport sector and to explore viable technological solutions to the threats faced.

The objectives of the workshop were as follows:

1. To facilitate an appreciation and understanding of how land transport security has been perceived by policymakers, operators, academics and technologists.
2. To encourage consideration and debate on "Risk Assessment and Horizon Scanning" approaches towards land transport security management.
3. To explore possible and the latest technology-based security approaches.

The first panel looked into security threats to Singapore's land transport "ecosystem" and challenges faced in the prevention and mitigation of these threats. Tristan Sim, the first speaker of the workshop, provided an overview of the operational and tactical measures that the Land Transport Authority had implemented to strengthen the land-transport sector's security baseline. The second speaker, John Harrison, highlighted the trends in terrorist activities in the region and noted that the land-transport system remains a highly vulnerable target for attack. The third speaker, Gwee Aik Chiong, spoke on the challenges faced by security providers and the steps that they have taken to overcome the problems.

The second panel explored the possibility of developing a security approach that combines both risk-based approaches and intelligence-gathering technology to effectively pre-empt and mitigate threats in the shortest possible time. The first speaker, Thomas Quiggin, opined that policymakers could make better and more informed decisions by considering risk-based approaches. He reasoned that knowledge is the only viable weapon in a security environment marked by a high level of complexity and uncertainty. Second, against this backdrop, Choy Kin Chong presented the four-pronged strategic approach that the SMRT has adopted to deal with any potential or arising terrorist threats. The third speaker, David Neo, added that, on top of installing security features at strategic spots, securing the public bus transportation system requires both the cooperation of the public and private sectors.

The third panel focused on technological best practices and how technology could be effectively harnessed to both pre-empt and mitigate threats. First, Tan Chee Ping briefed the audience on the HSEC's role in national security. In particular, he noted that the HSEC is committed to providing engineering solutions as well as building a collaborative technological network within the National Security Technology community. Second, Poh Seng Sian touched on the latest intelligence—closed circuit television surveillance technology and its ability to detect suspicious personalities and activities. Third, Lai Kah Wah examined how greater security system compatibility and interdependencies could be achieved through programme engineering. Finally, the fourth speaker, Richard Ng, explored possible areas where technology could help enhance land transport security.

Last but not the least, participants of the workshop had the opportunity to share their thoughts and hold frank discussions on land transport security during two breakout sessions. In essence, it was agreed that the land transport security community would gain from workshops that facilitate interactions among private-sector security providers, public security regulators and transport service operators, that is, a whole-of-network approach.

OPENING ADDRESS

BG Yam Ah Mee, Chief Executive of the Land Transport Authority and Chairman of the Public Transport Security Committee (PTSC), delivered the opening address. He noted that land transport security affects almost everyone and, hence, it is vital for the various stakeholders to work on and develop security solutions together. The PTSC, in his opinion, is delighted to have played a collaborative role in the first Land Transport Security workshop, which was jointly organized by the Centre of Excellence for National Security (CENS) and the Homeland Security Engineering Centre (HSEC). The workshop provided an opportunity for land transport security regulators and technologists to both network and update one another on the latest threat assessments and security systems.

The land transport system operates in an open environment where commuters could switch from one mode of transport to another with ease. According to BG Yam, it is this unique feature that makes most land transport networks vulnerable and a favourable terrorist attack target. He added that the Madrid (2004), London (2005) and Mumbai (2006) bombings have all displayed the need for effective emergency response and recovery strategies. Furthermore, given Singapore's prime and prominent role in regional and global commerce, any disruptions to the land transport network might have a domino effect on overall trade flow. As such, he reasoned, recovery and threat prevention solutions are equally important. In essence, a holistic land transport security programme should include a good mix of threat pre-emptive, mitigation and emergency response measures.

Moreover, land transport security is not limited to the protection of a single transport node. The land transport network is extensive and usually serves as a vital link between the commercial and social-political sectors.

BG YAM AH MEE, CE OF LTA AND CHAIRMAN OF PTSC, DELIVERING THE OPENING ADDRESS

Therefore, BG Yam urged participants of the workshop to pool their knowledge and experiences together and discuss possible ways to overcome land transport security challenges from a whole-of-network perspective. BG Yam ended his speech by setting three core goals for each speaker and participant to achieve during the workshop.

They were:

- to review both current and potential land transport security threats to Singapore;
- to explore the benefits of a "risk assessment and horizon scanning" approach towards land transport security enhancement; and
- to gain a better understanding of the uses of technology in security.

SESSION ONE

CURRENT REALITIES

PUBLIC TRANSPORT SECURITY IN SINGAPORE

Tristan Sim began by stating that the public transport system comprises the mass rapid transit (MRT) system, the light rapid transit (LRT) system, public buses and taxis, with about 5.1 million passenger trips made daily. The system is built around the hub spoke concept that allows for the integration of transport facilities with other facilities.

The security framework consists of three pillars: operations, capability and policy. The first primarily looks into crisis management, the second focuses on the sharing of information and networking among the different sectors and the third coordinates with other policy organizations.

In April 2004, the government established the Public Transport Security Committee (PTSC), made up of four working groups—protective security; information technology; crisis consequence management; and public vigilance and education—to identify weaknesses and gaps in the security system and implement solutions. Legislations were also amended to empower the ground staff to enforce security more effectively. For example, they are given the power of arrest.

Security measures implemented include hardening measures, such as: extra fencing at pedestrian overhead bridges along MRT tracks; the deployment of transit security officers (TSOs) at MRT stations and bus interchanges to patrol and conduct bag searches; the deployment of police MRT units (PMUs) to complement the TSOs; raising commuter vigilance and security awareness; and security exercises to test inter-agency response to multiple attacks.

TRISTAN SIM IDENTIFYING THE CHALLENGES TO LAND TRANSPORT SECURITY

Nevertheless, there are challenges ahead, namely, perennial issues such as striking a balance between enhancing security and accessibility; convenience and affordability; sustaining public attention and vigilance; and allocating limited funding.

ASSESSING THE THREAT OF TERRORISM AGAINST SINGAPORE'S LAND TRANSPORT SYSTEM

John Harrison stated that terrorist attacks are mainly driven by ideology, revenge and attack opportunities. Harrison also claimed that, increasingly, the motivation of revenge is becoming more pronounced as more of their plots are thwarted.

At the same time, opportunities for attack hinge on both the terrorists' capability and the target society's vulnerability level.

Harrison noted that terrorist attacks on iconic targets could generate high visual and symbolic impacts on a society. In this regard, terrorists not only receive the attention they sought but may also inflict psychological and economic damage on the target society.

In addition, Harrison opined that recent attacks across the globe on land transport systems have suggested that buses, trains and their stations may be more vulnerable or prone to terrorist attacks.

Furthermore, Harrison also informed that Al-Qaeda, as an international organization, is more likely to target international transport systems, such as international commercial freight, rather than local or domestic transport networks.

Therefore, Harrison argued that, given the layers of counter-terrorism measures in place in Singapore, it would be difficult to successfully launch a massive attack on Singapore's land transport system.

JOHN HARRISON ASSESSING THE THREATS TO LAND TRANSPORT SYSTEMS

Moreover, Al-Qaeda's regional influence has also been curtailed of late. Terrorist groups in the region, such as Jemaah Islamiyah, the Moro Islamic Liberation Front and the Rajah Solaiman Movement, may have the capacity to stage attacks on the public transport system.

However, locality still matters and their activities are so far concentrated in their host countries. In conclusion, while Singapore's public transport system may be vulnerable to terrorist attacks, the risk is relatively low or, to be prudent, medium.

THE PRIVATE SECURITY INDUSTRY IN THE NEW SECURITY ENVIRONMENT

Gwee Aik Chiong observed that, since 9/11, security threats to "soft" civilian targets have been broadened to include the public transport system. With more state resources channelled to Singapore's core national security interests, the private security industry has an increasing responsibility to safeguard human lives and protect both physical and economic assets. Hence, security officers of today have to be equipped beyond preventing fights, theft and shoplifting, to become the nation's eyes and ears at the street level.

An integral component of Singapore's layered defence strategy against terrorist attacks is the role of the private security industry in protecting commercial properties and private establishments.

For the state to divest some of its security functions to the private sector, it must have the requisite confidence in the sector's operational capacity and resilience. In Singapore, this is possible through the regulation of the private security industry with the formation of the Security Industry Regulatory Department (SIRD), a regulatory arm of the Singapore Police Force, in September 2004.

SIRD recognizes the need for a degree of state control over regulation while avoiding prescriptions that overly stifle innovation and immobilize the private sector's innate capacity for growth and profitability. Moreover, to promote the demand for private security, measures to enhance the standards and professionalism of the suppliers or players in the industry have to be introduced. To this end, all security officers in Singapore are screened and adequately trained before they can be deployed for duty.

As the enhancement of the overall standards of the industry has been successful thus far, the next step is to target the specialist operational competencies of security officers, who are now increasingly required to perform more specialist roles to meet the specific needs of certain segments of the community.

Gwee underscored that raising standards in the industry requires the collaborative efforts of the regulator, key stakeholders, security practitioners and buyers. In today's heightened environment, security must be an integral part of the overall day-to-day operations of all organizations. The business community, as the main buyers of private security services, therefore has a part to play. The adoption of preventive security measures to "harden" commercial buildings is an important part of a layered defence strategy against terrorist attacks, which augments

GWEE AIK CHIONG SPEAKING ON THE ROLE OF THE PRIVATE SECTOR IN LAND TRANSPORT SECURITY MANAGEMENT

other efforts undertaken by state forces in the areas of international and intelligence cooperation, including border control, community mobilization and crisis-management capability enhancement.

Efforts to strengthen partnerships with major buyers and employers of security services in the business community and enhance their level of security awareness include engaging major buyers and employers of security services and leveraging on key industry associations whenever feasible to enhance their awareness of the value of good security. A grading system for all security agencies was also implemented to provide buyers of security services with an authoritative assessment of private security companies from the regulator. This allows buyers to assess performance across agencies in deliberating which vendors to engage.

In order to improve the efficiency of private security providers in supporting land transport security, there is first a need to recognize that security is an integral and not peripheral part of overall operations. Second, there is a need for security officers to undergo specialized and continual training to keep abreast of latest developments. Third, effective communication in responding to incidences has to be enforced. Fourth, contingency plans, especially those pertaining to recovery, have to be familiarized. Fifth, adequate supervision in the form of a

system of ground supervisory checks is necessary to ensure ground vigilance. Lastly, security-related threats and other pertinent information should also be regularly disseminated to ground security staff, whenever appropriate, to enhance their security awareness, vigilance and ability to detect suspicious situations or persons quickly and efficiently.

Ground operation staff and even commuters have important roles to play in land transport security. Staff visibility serves as a useful deterrence. They can also recognize, detect and report any abnormalities in stations early.

In conclusion, the private security industry, with its large size and street level deployment, can potentially play an important role in national security. While efforts have been made to raise the standards and capability of the industry to effectively deal with current security challenges, likewise, it is equally critical that the owners of premises play their part.

QUESTIONS AND ANSWERS

Pertaining to SIRD's regulatory framework, a participant sought clarification on what the minimum criteria for a security officer to be deployed is. It was noted that while most training provided is generic, specific security needs, on a case-to-case basis, is also taken into consideration.

Observing a gap between security planners and thinkers and the security officers on the ground, another participant wanted to know how this is being addressed. A suggestion was made for training to be provided by middle-level government agencies. It was also noted that SIRD is working on the issue by identifying and presenting relevant information to the ground officers in a manner that is not overwhelming. Another observation made was that decision makers' grasp of the pulse on the ground could be enhanced with regular feedback from those on the ground.

It was also highlighted that the grading system of private security companies could serve its intended purpose of sustaining high standards if there is greater transparency in the evaluation process. It was assured that efforts have been made to fine-tune the grading criteria in line with the latest security or threat developments. Private security companies would be kept in the national security loop through periodic briefings.

It was reiterated that Singapore's public transport system is a complex ecosystem. If attacked, the losses would not be limited to the material aspect but would also affect the economy and psychology of the nation. An issue that requires more deliberation, therefore, is the prioritizing of limited resources to secure the nation. In essence, this is to avoid a situation where state resources are spread too thinly across a whole spectrum of security needs without necessarily raising its security baseline of its various infrastructure significantly. To this end, it was agreed that the Risk Assessment and Horizon Scanning (RAHS) project might serve a critical role in defining the improving current security measures.

PANEL DISCUSSION ON LAND TRANSPORT SECURITY CHALLENGES AND PUBLIC-PRIVATE SECTOR COOPERATION

SESSION TWO

ENVISIONING THE FUTURE

ADOPTING RISK-BASED APPROACHES IN LAND TRANSPORT SECURITY

Tom Quiggin began by noting that, very often, policymakers and analysts fail to appreciate the difference between the notions of risk and threat. This confusion, he said, is problematic because the failure to grasp the difference between the two ideas inexorably leads to bad policy decisions.

Quiggin explicated that the notion of threat refers to the potential of an individual or a group to exercise an action that exploits vulnerability. It does not automatically give an insight on the existing level of danger. Risk, on the other hand, is defined as the probability of harmful consequences that arises from an action taken by a source to exploit a known vulnerability.

In other words, a proper risk assessment could be highly meaningful to policymakers, as it would help to ascertain and prioritize the action or reaction needed to deal with a wide spectrum of threats.

Moreover, Quiggin noted that the current national security environment is highly complex and uncertain. This is a milieu where, on top of conventional interstate threats, there are also a multitude of asymmetric threats that can also inflict great damage to the security of societies. In such a security landscape, power alone is not able to fully address all the threats, let alone defeat asymmetric threats. In Quiggin's view, knowledge is the only viable weapon.

Therefore, Quiggin argued that when it comes to the analysis of threats and risk levels, it would be judicious to examine them from a tri-level understanding—strategic, operational and tactical. In the case of the phenomenon of trans-national terrorism, for example, a strategic-level view would refer to the ideology; an operational level view would refer to groups such as Al-Qaeda or Hamas; and a tactical level view would refer to individuals such as home-grown jihadists.

Quiggin remarked that it is also important to be aware of the distinction between capability and intentions. While capability is essentially about the ability of a source to carry out its threat, intentions refers to the desire of the source to implement its threat.

TOM QUIGGIN HIGHLIGHTING THE IMPORTANCE OF RISK-BASED APPROACHES TO LAND TRANSPORT SECURITY ENFORCEMENT

Interestingly enough, the capability-intentions dynamic (specifically, weapons of mass destruction) that most states confront today is very much an "inverse" scenario of the Cold War era.

During the Cold War, the capability to inflict mass destruction was clearly present but the intentions of the parties involved were not as clear or discernable. Now, in a post-Cold War environment, the intentions of asymmetric agents are pretty much perceptible.

However, what is not so evident is the capability of these agents to acquire and to use weapons of mass destruction.

Quiggin also raised a pertinent and policy-relevant question: At which point in the threat curve should an analyst or a policymaker start to worry and act? To this conundrum, Quiggin noted that while there would always be faint signals of potential threats manifesting across the horizon, one should start to "sit up" when these signals start to show indications of intelligence collection.

This, in effect, is the turning point of the threat curve, as it suggests that the threat source is starting to engage in planning and preparatory efforts.

That said, what should really compel the authorities to "action" would be when these signals start to show signs of capability building. When that happens, the level of threat rises inordinately and the gradient of the threat curve becomes extremely steep.

Quiggin concluded his presentation by offering his insights on a particular faint signal that may have potential ramifications on national security.

Noting that terrorists move quickly from the second-generation phase to the third-generation phase (which is essentially home-grown oriented but no less violent), Quiggin opined that future counter-terrorism efforts may well be much more complicated and complex.

SMRT'S SECURITY CHALLENGES AND DEVELOPMENT

Choy Kin Chong started his presentation by describing the operational realities confronting SMRT today.

For a start, the MRT train is already a national icon of sorts in Singapore and commuting by the MRT is very much a way of life for most Singaporeans. Second, the transportation network of SMRT is essentially characterized by a very porous layout. Third, given the heavy flow of human traffic in the SMRT network, a successful strike would almost certainly result in a massive rate of casualties. In this respect, Choy quoted the pertinent insights of noted terrorism specialist Bruce Hoffman, who said: "If terrorists want to kill a lot of people, public transport is always the preferred target, because you get a lot of people in the same place at the same time."

To be sure, other than the spectra of "conventional" terrorism (in the sense of utilizing conventional bombs), there is also a wide spectrum of threats that may well imperil the security of SMRT's network. From "deliberate" threats such as chemical, biological and radiological terrorism, crimes and sabotages, to "naturally-occurring" or "inadvertent" ones such as pandemics, accidents, fires, train collisions and derailments, SMRT faces a wide gamut of possible threats.

To effectively mitigate these multi-dimensional threats, SMRT adopts what is essentially termed as a four-pronged strategic approach to transportation network security. Briefly, this strategic approach encompasses the following key facets:

1. Protect critical assets by hardening potential targets.

CHOY KIN CHONG SHARING ON THE SMRT'S APPROACH TO THREAT AND RISK MANAGEMENT

2. Prevent incidents within SMRT's control through staff awareness training, public education and engaging government agencies in their counter-terrorism efforts.

3. Respond and mitigate major incidents via the integration of staff, equipment and capabilities into a total effort.

4. Recover from major incidents by anticipating and taking full advantage of available resources and emergency response plans.

In conclusion, Choy stressed that in order for a transportation security strategy to be truly effective, relying solely on preventative measures may not be enough. What is equally important is the recovery aspect, in which an effective restoration and disaster mitigation plan is crucial.

SECURING THE PUBLIC BUS TRANSPORTATION SYSTEM: DEVELOPMENTS AND CHALLENGES

David Neo began by pointing out that SBS operates some 2,800 buses in Singapore and quantitatively speaking, this adds up to more than 27,500 trips a day and some 2.1 million passengers daily. The total distance travelled by SBS buses works out to an astonishing 622,000 kilometres a day—equivalent to approximately 14 times around the globe daily. Quite clearly, this is a massive operational network that SBS is managing and maintaining.

SBS has undertaken a number of security measures to raise the security baseline of its interchanges and buses. For instance, SBS staff conduct regular checks of its bus interchanges and have conducted security awareness programmes for the staff and passengers to be on the look out for suspicious characters and unattended bags.

With regards to security measures implemented on buses, Neo pointed out that all bus captains are trained in the HOT protocol: an operational and on-site threat evaluation procedure. The captains also conduct bus checks at the end of each service trip. The role of the bus captain is important because SBS bus operations are essentially one-man-operations (OMO) where—unlike the traditional bus driver and bus conductor paradigm—the bus captain carries the sole responsibility of ensuring safe passages.

Despite the various security measures implemented at interchanges and on buses, Neo was quick to emphasize that challenges still abound and much more work can still be done in terms of bus transportation security. Neo stressed that SBS would always look towards incorporating more comprehensive measures to enhance and ensure the security of its transportation system.

DAVID NEO OUTLINING THE SBS' EFFORTS AT SECURING BUS STATIONS AND BUSES AGAINST TERRORIST ATTACKS

Neo ended his presentation by noting that the London "7/7" bombings evinced that public bus networks are plausible and possible targets for terrorist elements today. Securing the public bus transportation system is therefore—more than ever—an important and critical challenge for modern societies.

SESSION 3

TECHNOLOGICAL REALITIES AND POSSIBILITIES

CAPABILITY AND TECHNOLOGY ENABLERS FOR LAND TRANSPORT SECURITY

Tan Chee Ping talked about the role of the HSEC in national security. In particular, he highlighted that the HSEC was set up to harness engineering solutions and, at the same time, establish a technology collaboration network within the National Security Technology community. The workshop, Tan emphasized, was a representation of the HSEC's effort to foster greater technology appreciation through the hosting of local workshops and participating in international workgroups. Tan explained that threat-mitigation technologies in general are designed for multi-domain functions and could fit into three broad categories: (i) preventive; (ii) protective; and (iii) responsive.

Tan grouped national security technologies into two broad categories: technologies for the direct mitigation of threats and technology enablers that enable a whole-of-government approach to national security. Tan noted that technology enablers (e.g. sensor fusion) tend to have cross-domain applications. Unlike the technologies used for direct threat mitigation, each technology enabler by itself does not grant any capability to the operational agencies. This means that the government as a whole may run the risk of under-investing in these enabling areas. In order to avoid neglecting investments in these technology enablers, Tan suggested that it would be useful to group the enablers into clusters, each of which would deliver a cross-domain national security capability. As part of its ongoing national security technology road-mapping effort, the HSEC has identified four such capability clusters: (i) counter-terrorism sense-making; (ii) inter-agency collaboration; (iii) integrated awareness; and (iv) vulnerability assessment.

Tan said that it was important to use capabilities as the principal building block for technology definition as they represent the smallest complete assembly of technologies and processes that together lead to an ability to perform a specific function, task or operation.

TAN CHEE PING ELABORATING ON THE TECHNOLOGICAL APPROACH TO LAND TRANSPORT SECURITY

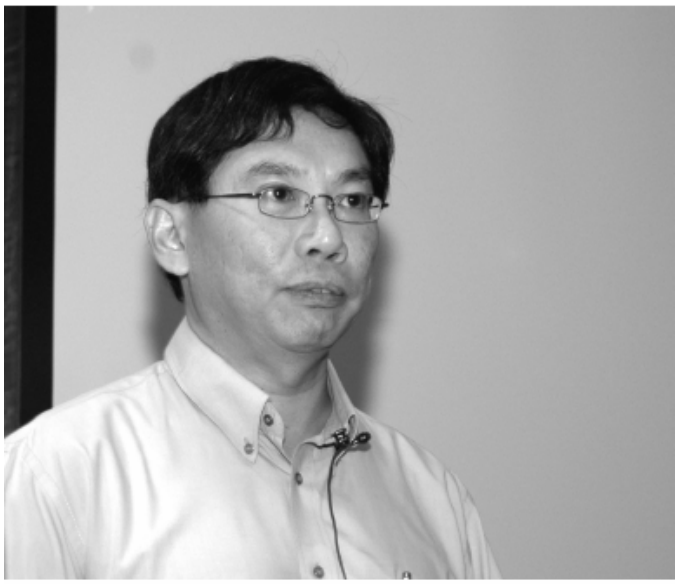
Tan concluded that inter-agency collaboration remains an essential component of the transport security system and network. An integrated and cross-platform technological approach is also necessary to facilitate better threat and vulnerability assessments, and, as well as counter-terrorism sense-making. Therefore, the HSEC is dedicated to establishing a collaborative and interconnected technological network within the land transport community and beyond.

INFRASTRUCTURE INTERDEPENDENCIES IN LAND TRANSPORT SECURITY: THE WEAK LINK?

Lai Kah Wah spoke about critical infrastructure protection and assessed the role of system interdependency in land transport security management. In addition, Lai also shared with workshop participants the various vulnerability assessment methods used by the Defence Science Organisation National Laboratories (DSO). In general, Lai noted that the DSO believes that a multi-disciplinary approach that integrates both technological and inter-agency collaboration efforts would produce highly accurate vulnerability assessments that could reflect challenges faced at the operational level.

Besides sector-based vulnerability assessments, the DSO also pursues collaborative work and joint researches with other national laboratories and agencies. In doing so, the DSO aims to refine their vulnerability-assessment skills and further contribute to critical infrastructure defence technology development. Moreover, according to Lai, the DSO also conducts dedicated researches that focus on fostering greater inter-and-intra agency system interdependencies.

The DSO has also successfully developed an "infra-interdependency model" that is capable of providing up-to-date information on, for example, changes in the "industrial ecosystem". From the model, the impact of infrastructural disturbances can be examined through scenario simulations. In other words, scenario planning is not only possible but could also produce results with a high level of accuracy. On this note, Lai concluded that the DSO's long-term aim is to design and develop a comprehensive system platform that would help advance Singapore's critical infrastructure protection strategies.



LAI KAH WAH SPEAKING ON THE ROLE OF TECHNOLOGY IN LAND TRANSPORT SECURITY

ENHANCING LAND TRANSPORT SECURITY

Richard Ng gave an overview on global transportation security threats and trends. Ng also explored the variety of security technological solutions that the land transport security community could consider adopting. In general, Ng observed that the protection of the transport network requires a multi-agency approach as attacks on the transport system often affect other critical infrastructures and social-economic installations.

Ng stressed that the transport ecosystem is more than just a collection and arrangement of "transport nodes". The network plays both iconic and supporting roles. It is, nonetheless, the key social-economic and political link for most states. As such, Ng reasoned that any major attack on the transportation network would not only disrupt commuter and service flow but also create mass hysteria and erode public confidence.

There have been no fewer than 21 terrorist attacks on buses and trains during the period 2000–2006 worldwide. Ng reckoned that the "open and exposed" nature of the public transport system rendered it vulnerable to a variety of attacks. The failure on several occasions to pre-empt or foil attacks by the international community has seen the erosion of public confidence in public transport security. Therefore, for counter-terrorism efforts to be highly effective, Ng underscored that moves to improve and facilitate greater inter-agency communication is essential.

Currently, the land transport security community in Singapore practises a communication and sensory integrative approach to security management. Ng explained that this means that a combination of surveillance, tracking and traffic controls systems is in place to both detect abnormalities and provide the necessary deterrence. Ng highlighted that the combinatory security approach has effectively enhanced security at various custom checkpoints, limited and screened vehicle flows into restricted areas.

RICHARD NG SPEAKING ON THE IMPORTANCE OF LAND TRANSPORT SECURITY RESPONSE PLANNING.

It is no longer sufficient to design security systems that could perform only unitary or specific function. Past crisis experiences have shown that an integrated system and agency-collaborative approach would be of greater benefit to the land transport security community, especially during emergencies when response time affect the overall recovery speed. Moreover, Ng also mentioned that an integrated approach would also help strengthen traffic accident and fleet/logistic security management capabilities. In conclusion, Ng noted that Singapore Technologies would continue to seek ways to enhance the technological security baseline of Singapore's land transport sector.

BREAKOUT SESSIONS

BREAKOUT GROUP 1: RISK ASSESSMENT METHODOLOGIES

Tom Quiggin started the breakout session by noting that there are at least 130 different methodologies that could be use to predict the future. A normative analysis of this situation would suggest that none of them are actually working very well. Otherwise, there would arguably be only one methodology in place. Quiggin reasoned that the basic processes of intelligence and risk assessment are more important than the methodologies themselves. If the information flows in the risk assessment process are constant and the mindsets of the individuals concerned are open to new information and change, then the process will produce good and meaningful results for decision makers. If these basic principles are not in place, then no methodology, no matter how sophisticated they might be, will solve the problems.

In general, the breakout-group participants debated on several policy pertinent issues that are worthy of further study. The insights shared are as follow:

1. There is a substantial difference between "threat" and "risk". A threat can be defined in a number of ways, but for the purposes of national security intelligence, it can be put this way: A threat is a potential for an individual or a group to exercise an action that exploits vulnerability. The key term here is "potential". The use of the term "threat" does not necessarily depict or reflect the actual danger level. On the other hand, risk can be defined as the probability of harmful consequences arising from an action taken by a source to exploit a known vulnerability. Risk can be expressed in a number of ways, but one commonly used statement is that risk could be equated to the severity of the consequences multiplied by the probability of the event occurring. Therefore, the term "risk", when used in its proper context, can be meaningful to policymakers as it implies a course of action or reaction that can be taken by them.

2. It is the response and not the event that is important to the future. It is generally agreed that any significant disruptive attack or event will have its impact magnified if there is a poorly led or poorly implemented response. In retrospect, an effective response can greatly reduce the impact of any negative event.

3. Both the potential and long-term impact of any catastrophe must be considered. The impact of an attack on an iconic target may be felt immediately but this may not be as important as an attack that has a longer-lasting or more widespread impact. Thus, losing an iconic target may have an emotional and psychological impact but the loss of a port facility or transit system is far more critical to the state in the longer run.

There is not enough data available on terrorist attacks and other such events to conduct accurate quantitative risk assessment. Additionally, the nature of the attacks and the attackers changes regularly so any data that is more than two or three years old are not exceptionally useful at any rate. Risk assessment will remain, ultimately, a qualitative exercise, supported by quantitative data.

BREAKOUT GROUP 2: NATIONAL SECURITY TECHNOLOGY ROAD-MAPPING

Chong Chan Meng presented the two main technology road-mapping methodologies that the Homeland Security Engineering Centre has adopted. This first methodology is technology-centric in nature. According to Chong, this approach is used for the development of a cross-domain competency development road map for National Security (NatSec) purposes. Basically, this NatSec technology road-mapping methodology focuses on identifying technology areas where Singapore needs in-country competencies for the development of solutions. The breakout-group participants showed great interest in this approach and even suggested that technological development could be considered from a value-add perspective as well.

The following highlights the concerns the breakout-group participants had over technology development:

1. Both the competency-development approach and value-centric approach have their strengths, and they need not be mutually exclusive.

2. Chong assured the participants that the HSEC would actively seek and take into consideration the feedback of the NatSec community. This would, in essence, ensure that technology would be of great value-add and relevance to the various NatSec stakeholders.

The second methodology that Chong shared with workshop participants concentrated on the use of a risk-based approach to help determine specific domains where technology could help to enhance and boost overall security and operational efficiency significantly. Chong illustrated to the breakout-group participants how such an approach could be implemented and be of benefit to the various land transport security stakeholders. In essence, land security regulators could prioritize and even vary their "technological investments" by weighing their options against the following:

1. The results of their threat assessments.

2. The results of their vulnerability analysis.

3. The data collected on the attack modus operandi of the various terrorist groups.

All in all, the breakout-group participants agreed that a rich combination of the different technology road-mapping methods would probably be more effective in addressing the day-to-day operational challenges and risks faced by the land-transport community. Hence, most of them reflected that they would be interested to pursue further discussions and attend future workshops or breakout-group sessions that dwell on the operational aspects of global national security enforcement methods and theories.

Rapporteurs
Yolanda Chin, Hoo Tiang Boon, Ng Sue Chia, Thomas Quiggin and Chong Chan Meng (HSEC)

Edited by
Ng Sue Chia, Kumar Ramakrishna and Chong Chan Meng (HSEC)

PROGRAMME

0830 Registration.

0900 **Opening Remarks**
BG (NS) Yam Ah Mee
Chief Executive
Land Transport Authority
Chairman
Public Transport Security Committee

Session 1:
Current Realities
Chair
Associate Professor Kumar Ramakrishna
Head
Centre of Excellence for National Security, S. Rajaratnam School of International Studies

0910 **Securing our transportation network**
Mr. Tristan Sim
Deputy Director
Public Transport Security
(Planning & Standards)
Land Transport Authority

0930 **Assessing the Threat of Terrorism against Singapore's Land Transport Security**
Dr. John Harrison
Assistant Professor
International Centre for Political Violence and Terrorism Research
S. Rajaratnam School of International Studies

0950 **Security Providers' challenges in supporting Land Transport Security**
DSP Gwee Aik Chiong
Assistant Director (Policy & Development)
Security Industry Regulatory Department
Singapore Police Force

1010 Q & A

1030 Tea Break

Session 2:
Envisioning the Future
Chair
Dr John Harrison
Assistant Professor
International Centre for Political Violence and Terrorism Research
S. Rajaratnam School of International Studies

1100 **Adopting Risk-based Approaches in Land**
Transport Security
Mr. Tom Quiggin
Senior Fellow and Coordinator
Risk Assessment and
Horizon Scanning Programme,
Centre of Excellence for National Security,
S. Rajaratnam School of International Studies

1120 **SMRT's Security Challenges and Developments**
Mr. Choy Kin Chong
Deputy Director
(Security & Emergency Planning)
SMRT Corporation Ltd

PROGRAMME

1140 **Security the Public Bus Transportation System: Developments & Challenges**
Mr. David Neo
Assistant Director
(Operations Development)
SBS Transit

1200 Q & A

1220 Lunch

Session 3: Technological realities and possibilities
Chair
Mr. Tom Quiggin
Senior Fellow and Coordinator
Risk Assessment and
Horizon Scanning Programme,
Centre of Excellence for National Security,
S. Rajaratnam School of International Studies

1400 **Capability and Technology Enablers for Land Transport Security**
Mr. Tan Chee Ping
Deputy Director
Homeland Security Engineering Centre (HSEC)
Defence Science and Technology Agency (DSTA)

1420 **Embracing iCCTV today and beyond**
Mr. Poh Seng Sian
Head Infrastructure Development Section
Police Technology Department
Singapore Police Force

1440 **Considering Systems Interdependencies in Land Transport Security**
Mr. Lai Kah Wah
Senior Member of Technical Staff
& Project Manager
DSO

1500 **Enhancing Land Transport Secuirty**
Mr. Richard Ng
Manager, Mobility Systems Division
ST Electronics (Info-Comm Systems) Pte Ltd

1520 Q & A

1530 Tea Break

Breakout Sessions: Case Study

1600 Track 1: Risk Assessment Methodologies (CENS)

Track 2: Technology Road-mapping for National Security (HSEC)

1700 End of Workshop

ABOUT THE CENTRE OF EXCELLENCE FOR NATIONAL SECURITY (CENS)

The Centre of Excellence for National Security (CENS) is a research unit of the S. Rajaratnam School of international Studies (RSIS) at Nanyang Technological University, Singapore. Established on 1 April 2006, CENS is devoted to rigorous policy-relevant analysis of a range of national security issues. The CENS team is multinational in composition, comprising both Singaporean and foreign analysts who are specialists in various aspects of national and homeland security affairs.

Why CENS?

In August 2004 the Strategic Framework for National Security outlined the key structures, security measures and capability development programmes that would help Singapore deal with transnational terrorism in the near and long term. However, strategising national security policies requires greater research and understanding of the evolving security landscape.

This is why CENS was established to increase the intellectual capital invested in strategizing national security. To this end, CENS works closely with not just other RSIS research programmes, but also national security agencies such as the National Security Coordination Secretariat within the Prime Minister's Office.

What Research Does CENS Do?

CENS currently conducts research in three key areas of national security:

- **Risk Assessment/Horizon Scanning**

The art and science of detecting "weak signals" emanating from the total security environment so as to forewarn policymakers, the private sector and the public about approaching "shocks" such as terrorism, pandemics, energy crises and other easy-to-miss trends and ostensibly distant events.

- **Social Resilience**

The capacity of globalised, multicultural societies to hold together in the face of systemic shocks such as diseases and terrorist strikes.

- **Transportation Security**

The security of land-based, aviation and maritime transport networks and increasingly, the total supply chain vital to Singapore's economic vitality.

How Does CENS Help Influence National Security Policy?

Through policy-oriented analytical commentaries and other research output directed at the national security policy community in Singapore and beyond, CENS staff members promote greater awareness of emerging threats as well as global best practices in responding to those threats. In addition, CENS organizes courses, seminars and workshops for local and foreign national security officials to facilitate networking and exposure to leading-edge thinking on the prevention of, and response to, national and homeland security threats.

How Does CENS Help Raise Public Awareness of National Security Issues?

To educate the wider public, CENS staff members regularly author articles in a number of security and intelligence related publications, as well as write op-ed analyses in leading newspapers. Radio and television interviews have allowed CENS staff to participate in and shape the public debate on critical issues such as risk assessment and horizon scanning, multiculturalism and social resilience, intelligence reform and defending critical infrastructure against mass-casualty terrorist attacks.

How Does CENS Keep Abreast of Cutting Edge National Security Research?

The lean organizational structure of CENS permits a constant and regular influx of Visiting Fellows of international calibre through the Distinguished CENS Visitors Programme. This enables CENS to keep abreast of cutting edge global trends in national security research.

For More on CENS
Log on to http://www.rsis.edu.sg/cens/

ABOUT THE S.RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES

The S. Rajaratnam School of International Studies (RSIS) was established in January 2007 as an autonomous School within the Nanyang Technological University. RSIS's mission is to be a leading research and graduate teaching institution in strategic and international affairs in the Asia Pacific. To accomplish this mission, it will:

- Provide a rigorous professional graduate education in international affairs with a strong practical and area emphasis
- Conduct policy-relevant research in national security, defence and strategic studies, diplomacy and international relations
- Collaborate with like-minded schools of international affairs to form a global network of excellence

Graduate Training in International Affairs
RSIS offers an exacting graduate education in international affairs, taught by an international faculty of leading thinkers and practitioners. The Master of Science (MSc) degree programmes in Strategic Studies, International Relations, and International Political Economy are distinguished by their focus on the Asia Pacific, the professional practice of international affairs, and the cultivation of academic depth. Over 120 students, the majority from abroad, are enrolled in these programmes. A small, select Ph.D. programme caters to advanced students whose interests match those of specific faculty members. RSIS also runs a one-semester course on '*The International Relations of the Asia Pacific*' for undergraduates in NTU.

Research
RSIS research is conducted by five constituent Institutes and Centres: the Institute of Defence and Strategic Studies (IDSS, founded 1996), the International Centre for Political Violence and Terrorism Research (ICPVTR, 2002), the Centre of Excellence for National Security (CENS, 2006), the Centre for the Advanced Study of Regionalism and Multilateralism (CASRM, 2007); and the Consortium of Non-Traditional Security Studies in ASIA (NTS-Asia, 2007). The focus of research is on issues relating to the security and stability of the Asia-Pacific region and their implications for Singapore and other countries in the region. The S. Rajaratnam Professorship in Strategic Studies brings distinguished scholars and practitioners to participate in the work of the Institute. Previous holders of the Chair include Professors Stephen Walt, Jack Snyder, Wang Jisi, Alastair Iain Johnston, John Mearsheimer, Raja Mohan, and Rosemary Foot.

International Collaboration
Collaboration with other professional Schools of international affairs to form a global network of excellence is a RSIS priority. RSIS will initiate links with other like-minded schools so as to enrich its research and teaching activities as well as adopt the best practices of successful schools.

ABOUT THE HOMELAND SECURITY ENGINEERING CENTRE

The Homeland Security Engineering Centre (HSEC) was established in November 2005 to support the National Security Coordination Secretariat (NSCS) in technology master planning for national security. Its mission is to harness, seed, and catalyse the development of engineering resources and solutions in a systemic and holistic manner to support NSCS and national security agencies in meeting the national security needs of Singapore. HSEC's key roles are in the following:

- Technology master planning, which currently focusing on in-country technology competencies that Singapore must build up and sustain for national security.
- Technology harnessing, including the building of a network of local and international technology collaboration partners.
- Technology advisory facilitation.
- Cross-domain systems architecture.

ABOUT THE NATIONAL SECURITY COORDINATION SECRETARIAT

The National Security Coordination Secretariat (NSCS) was set up in the Prime Minister's Office in July 2004 to facilitate national security policy coordination from a whole-of-government perspective. NSCS reports to the Prime Minister through the Coordinating Minister for National Security (CMNS). The current CMNS is the Deputy Prime Minister Professor S. Jayakumar, who is also Minister for Law.

NSCS is headed by Permanent Secretary (National Security and Intelligence Coordination). The current PS(NSIC) is Mr Peter Ho, who is concurrently Head of Civil Service and Permanent Secretary for Foreign Affairs.

NSCS provides support to the ministerial-level Security Policy Review Committee (SPRC) and senior-official level National Security Coordination Committee (NSCCom) and Intelligence Coordinating Committee (ICC). It organizes and manages national security programmes, one example being the Asia-Pacific Programme for National Security Officers.

NSCS also funds experimental, research or start-up projects that contribute to our national security.

NSCS is made up of two components: the National Security Coordination Centre (NSCC) and the Joint Counter-Terrorism Centre (JCTC). Each centre is headed by a director.

NSCC performs three vital roles in Singapore's national security: national security planning, policy coordination, and anticipating strategic threats. As a coordinating body, NSCC ensures that government agencies complement each other, and do not duplicate or perform competing tasks.

JCTC is a strategic analysis unit that compiles a holistic picture of terrorist threats. It studies the levels of preparedness in areas such as maritime terrorism and chemical, biological and radiological terrorist threats. It also maps out the consequences should an attack in that domain take place.

More information on NSCS can be found at **www.nscs.gov.sg**