IDSS COMMENTARIES (123/2006)

*IDSS Commentaries are intended to provide timely and, where appropriate, policy relevant background and analysis of contemporary developments. The views of the authors are their own and do not represent the official position of IDSS.*

# Critical Infrastructure Security:Why Dynamism Matters

*Ng Sue Chia and John Harrison*[*]

30 November 2006

THE 11 September 2001 attacks did not just transform lives but it also changed the security landscape. Warfare has been brought to the doorsteps of ordinary citizens and security forces have had to deal with threats beyond the traditional battlefield. It seems that the concept of total war has been applied. Anyone or anything deferring from the terrorist's belief, ideology or social-political outlook could be attacked.

The critical infrastructure network in particular has proven to be a choice target for terrorists. This is unsurprising as the volume of commuters and the access networks have to vital commercial and political districts make them attractive attack options. More importantly, attacks to the infrastructure network permit terrorists to inflict as much harm and disruption as possible to both civilians and their livelihood. There are few better ways to maximize physical and psychological damage than to attack a population while they participate in their most mundane activities – commuting to or from work. In addition, attempts to secure the public transportation network are difficult at best. To secure such locations from potential attacks, restrictions on access – which runs contrary to the public mass transit principle of convenience and public accessibility – must be placed.

Hence, especially for Singapore whose aim is to be a leading financial, information and transportation hub, this makes the protection of public infrastructure and supply chain networks all the more critical.

## Securing Singapore's Infrastructure

In both the public and private sector, a two-pronged approach to securing Singapore's critical infrastructure has been adopted. Firstly, the transportation network and vital supply chain industries have been hardened against any assault. Secondly, defence action plans have sufficient built-in redundancies in order to minimise any security gaps that can be exploited as well as effectively respond to and recover from any attacks that do occur.

Examples of this two-pronged approached abounds. Maritime protection plans display a synergy between the public sectors and private sectors with responsibility shared by the military, police, Maritime and Port Authority (MPA) and members of the supply chain network. Measures to secure the ports and waterways range from sky and water patrols, the implementation of the International Ship and Port Facility Security Code (ISPS Code) and the installation of detectors on ships and containers to track the movement of vessels and flow of goods. At the airports and MRT stations, special operation police units have been established to secure these environments. Likewise, on Jurong Island, additional security features such as

x-ray scanners and an island-wide closed circuit television (CCTV) camera system screens, scans and monitors both land and sea traffic for potential threats. This CCTV system is complemented by a round-the-clock patrol conducted by army and police units.

In general, a rich layering of security measures are in place to protect Singapore's critical infrastructure. However, how do we determine if the current security measures serve as an effective deterrence? Unfortunately, the true gauge is not the amount of state-of-the-art technology or gadgetries adopted. Rather it rests on the ability to meet current threats, anticipate future contingencies while also simultaneously remaining flexible. Key to achieving this is through a dynamic security system resistant to becoming a predictable routine.

**Dynamic Security System**

Threats are constantly evolving. As such security measures have to be just as dynamic and adjustable to changes. Although a systemic approach aids the implementation and management of security measures owing to its efficiency, it may also be unquestionably routine and highly predictable. As such, fixed solutions and standard controlled results do not necessarily imply a robust and highly adaptive defence mechanism. They may provide the illusion of security while doing little to actually increase genuine security.

There are two basic reasons why an overly routine or clockwork security regime should be a cause for concern. One, terrorists are meticulous in their pre-operational planning. Thus, they will easily map out the day, time and venue when a task force conducts its patrols. Operations are then designed to exploit identified weaknesses. Second, while a routine allows one to see what is normal and out of the ordinary, it also limits you to seeing the extraordinary as a threat while missing the ordinary. This is based on the idea that one is safest in the known environment, because one is trained what to look for based on past experience. There is tremendous value in learning from the past. But if the past becomes the sole predictor for the future, the ability to adapt to or stay ahead of the opponent becomes hampered. Learning from the past can be a strength but being wedded to a past turns that strength into a weakness.

**Solutions and the Way Ahead**

Security layering ensures that loopholes in the overall defence system are minimised. It involves the combined work of intelligence, technology and security enforcers – that is, the tactical and the operational aspect of defence. Singapore has adopted this approach and systematically ensured that the technology and manpower are well in place. The key concern here is that this approach may lead to predictability and hence undermine the intended impact of a measure. In the long-term, it helps to have some randomness in a security approach to prevent terrorists from either fully predicting the responses or the security gaps in the system.

Admittedly, this runs contrary to the transportation business model that requires strict adherence to a predictable operation schedule. An unpredicted event, mechanical failure or weather delay, can cause a cascading disruption to the entire transportation system. The opposite, however, is true with regard to a robust security system. In fact, the best way to protect a transportation system is to be as disruptive to the terrorist operation cycle as possible. What marks a robust and effective security system is not a standard set of measures or routines; it is how security personnel and technology can best react to and anticipate threats. Hence, dynamism matters for critical infrastructure security.

[*] *Ng Sue Chia is an Associate Research Fellow and John Harrison is an Assistant Professor at the Centre of Excellence For National Security at the Institute of Defence and Strategic Studies, Nanyang Technological University.*