



OTS Security Risk Doctrine

Key Messages:

Jihadist terrorism - including Al Qaeda and those inspired by them - is the greatest domestic security threat to Australia; it poses a significant challenge to Law Enforcement and Security Services.

The preferred method of attack continues to be the use of Improvised Explosive Devices (IEDs), often through suicide tactics, to cause mass casualties. Armed assault attacks aimed at causing mass casualties are also possible.

The consequences of these attacks are irreversible and must be prevented as best as possible through a process of risk management.

In this security environment there may be no prior operational warning of an attack. This places preventive security planning based on strategic intelligence at the forefront of countering this threat.

Preventive security planning must be focused on creating an environment hostile to terrorist activity.

The identification and prioritisation of vulnerabilities that could be exploited by terrorists is the central principle of preventive security planning.

Key to a hostile environment is:

- mitigating against vulnerabilities relevant to the threat;
- designing out the consequences of blast;
- the identification and resolution of suspicious activity;
- strong security culture; and
- regular preventive security exercises.

At all levels of decision making in preventive security policy and planning our focus must be on mitigating those vulnerabilities that can be exploited to cause mass casualties, particularly through the use of IEDs.

Purpose:

The OTS Security Risk Doctrine outlines the current security environment, as described by the Australian Intelligence Community, and highlights implications for preventive security regulation and planning in the transport sector.

It is provided to support intelligence-led risk-based decision making by OTS in accordance with the OTS Regulatory Philosophy and Strategic Plan.

Security Risk Doctrine:

Intelligence reporting indicates the greatest domestic security threat to Australia comes from Jihadist terrorist groups¹ associated with, or inspired by, the global violent jihad movement. Intelligence reporting indicates that some of these groups have attacked Australian interests overseas and some have a desire to conduct an attack within Australia.

Terrorist groups are capable of successful attacks

Jihadist terrorist groups are committed, knowledgeable and are capable of planning, preparing and successfully conducting terrorist attacks with a good probability of success. Terrorists will seek vulnerabilities in transport operations that enable them to meet their strategic objectives, most notably inflicting mass casualties.

The nature of the threat

Islamic terrorists are likely to consider the following strategic objectives:

- inflicting mass casualties;
- causing economic disruption;
- making a symbolic statement;
- generating public anxiety; and
- generating spectacular media imagery.

They will also consider the following factors:

- accessibility and vulnerability of a given target; and
- opportunity for attack and likelihood of success.

Improvised Explosive Devices (IEDs)

Islamic terrorists have demonstrated a preference for the use of Improvised Explosive Devices (IEDs). IEDs are versatile, cheap and relatively easy to make and use, they also fulfil terrorist's strategic objectives.

Open and accessible targets

Terrorists seek vulnerable open architecture targets as they provide accessibility and opportunity for an attack and allow for a good likelihood of success.

Transport systems are a key target

Transport systems are open architecture systems and are a key target. Those parts of the transport system that gather people in predictable places at predictable times are at most risk.

¹ Islamic Jihadist terrorism has become the most prominent form of politically motivated violence within the global setting and this is reflected within the Australian context. For the purposes of the security risk doctrine, the term terrorism, when used generically, is used to refer to Islamic jihadist terrorism, as broadly defined above.

There is likely to be no warning of an attack.

An Islamic terrorist attack could be conducted by a transnational terrorist cell, local extremists acting independently, or a collaborative effort between the two.

These groups pose fundamentally different preventive security challenges to previously seen terrorist groups.

1. Both transnational terrorist cells and local extremists are difficult security intelligence and law enforcement targets.
 - Al-Qa'ida is well resourced, disciplined and persistent.
 - Local extremists can be inspired by internet and media reporting and undertake attacks with only a few number of people involved.

It is **possible that no operational intelligence warning will precede an attack** by groups involved in the global violent jihad movement.

2. These groups seek to create terror through indiscriminate killing of the public. Suicide tactics are often favoured as they provide greater opportunity for success. These attacks are carried out without issuing a warning.

These two challenges mean that there is likely to be no warning of an attack on an Australian transport system—no operational intelligence warning and no warning on the day of an attack.

Most likely risk events

The most likely risk events involve the use of IEDs against open architecture transport operations for the purpose of causing mass casualties. Each transport mode, including passenger ferries, cruise shipping, high capacity RPT and major airports, is inherently vulnerable to this form of terrorist attack.

Alternate attack methods, such as armed assault and mixed mode attacks, should be considered. Other acts of unlawful interference that could cause catastrophic consequences, such as the actions of mentally disturbed, intoxicated or issue motivated individuals should also be considered. Attacks of this nature are equally unpredictable and as such preventive security remains important in mitigating against them.

Preventive security is at the forefront of countering terrorism

Without intelligence on specific attack planning to guide a counter terrorism response, preventive security moves to the forefront of counter terrorism efforts.

OTS is a preventive security regulator that seeks to reduce the risk of terrorism through oversight of preventive security planning within the aviation and maritime transport sectors.

Vulnerability to the threat

To attack transport systems terrorists must exploit vulnerabilities. Preventive security planning should be focused on mitigating vulnerabilities that, if left unaddressed, increase the likelihood of a successful terrorist attack.

To do this, preventive measures must be focused on the nature of the threat, the most likely risk events to operations and consequential vulnerabilities.

Australian/New Zealand Risk Management Standard AS/NZS 4360/2004 provides the framework for all risk management. The formula below—from *Security Risk Management Handbook HB 167:2006*—sets out the approach to be used for preventive security risk assessment for transport security purposes.

Risk = (Threat x Vulnerabilities) x Consequence

Note however that more specific iterations of this approach may be developed by the department from time to time for application to particular security environments or circumstances. Where this occurs, these iterations will be included in relevant internal and external guidance material.

Preventive security implications

Preventive security planning must be based on sound security risk management

Preventing *all* acts of unlawful interference against Australian transport systems is not possible. The Australian Government's policy is to manage the risk of terrorism and unlawful acts of interference through preventive security planning.

Basic Preventive Security

Basic physical security, layered security measures and defence in depth principles remain important security elements.

Human factors – Security Culture

An informed and proactive security culture across all aspect of business management and operations is vital to ensure an appropriate level of competence and to avoid complacency. In this environment security culture should focus employees on the importance of all elements of preventive security not just traditional access control and identity elements.

Human factors – drills and exercises

The complexity of the transport environment means that coordination of all those working in the industry is a challenging task. Preventive security exercises—designed to identify roles and responsibilities in preventing terrorist attacks—are important preventive measures.

Resolution of Suspicious Activity

In an environment where there is likely to be no warning of an attack—neither prior intelligence warning nor a warning on the day of an attack—any ability to disrupt terrorist activity is vital.

Transport industry employees are well placed to identify suspicious activity and contribute to the disruption of terrorist activity. Information provided by employees has assisted with the investigation and disruption of terrorist attack planning overseas.

All transport industry employees should be able to report suspicious activity, confident that such reports will be taken seriously and resolved. This is a key measure in preventing a terrorist attack.

Summary:

The Security Risk Doctrine outlines the way preventive security decision making should be approached and identifies a layered preventive security approach that is essential to ensuring a more secure transport system in the current security environment.

Preventive security outcomes should be informed by an understanding of vulnerabilities to the current threat and what is required to help mitigate those vulnerabilities.

AQ and those inspired by them are seeking to exploit vulnerabilities in the transport system to cause mass casualties, probably through the use of improvised explosive devices. The focus of OTS' work should be on ensuring that preventive security planning in the transport sector is primarily focused on mitigating those vulnerabilities through a preventive security risk management process.

Security Analysis Section*
Office of Transport Security

*This Security Risk Doctrine is developed by Security Analysis and draws on classified intelligence reporting as of September 2009. It reflects the strategic intelligence picture as it relates to preventive security planning in the transport sector. It will be updated should there be a substantial shift in the security environment. Until that time it remains current.