DISRUPTING HOSTILE RECONNAISSANCE

Owners and operators have a responsibility to understand what the current terrorist threat environment means for the security of their site and implement protective security measures that are proportionate to the level and types of threat. Information on the current terrorism threat environment can be found at: www.nationalsecurity.gov.au

To disrupt hostile reconnaissance at your site, it is important to understand:

- **What information hostiles will be looking for and why**
- **Where hostiles will go to obtain this information**
- **How far they will go to obtain the information they need**

Understanding these factors can help owners and operators to develop a security program to help disrupt hostile reconnaissance. This disruption can be achieved in three principal ways:

1. **DENY** a hostile access to the information they need to plan an attack
2. **DETECT** hostile reconnaissance through effective security, and vigilant staff
3. **DETER** hostiles by promoting the likelihood of detection and failure

1. DENY

Hostile reconnaissance can be prevented by denying hostiles access to the information they need to give them confidence to proceed with further attack planning. If the risk of detection is too high when obtaining the information, hostiles may disregard the site as a potential target or ensure they have to undertake further reconnaissance.

Owners and operators should audit what information is publicly available about their site or event and remove or edit information to make it less useful to a hostile.

Information that may be useful in planning an attack includes:

- Site-specific information (e.g. photographs, videos, floorplans, security plans, evacuation plans, virtual tours)
- Security information (e.g. specific security measures in place, patrol timings and procedures)
- Images of staff or vehicle accreditation (e.g. on websites, social media)
- Corporate information (e.g., organisational charts with staff contact details, staff, and office locations)
- Planning information (e.g. new building/development plans, security upgrades, etc)

Sources of information can include:

- Observing the location itself
- Organisational/corporate, contractor or partner websites and social media accounts
- Staff, contractor, and visitor social media accounts
- Traditional media articles in print and online
- Current vacancies or other HR/employment information packages
- Corporate printed materials (e.g. brochures, signage, posters, tickets, etc)
- Online review sites (e.g. visitor reviews such as Trip Advisor, employee reviews such as Glassdoor, etc)

Ensure your staff are aware that information they post or share about their work can provide valuable insights to a hostile on your organisation's attitude to security and potential vulnerabilities.

2. DETECT

The most effective method of detecting and disrupting hostile reconnaissance is ensuring people at your site:

- **Know what to report and where to report**
- **Know it is easy to report information**
- **Know that reports will be taken seriously**

People at your site—whether security, staff, patrons, or visitors—are best placed to detect suspicious behaviour. However, **they will be more likely to report the behaviour if it's convenient and they are confident** about how to do it.

For staff or regular site users this may involve training or education (online or face-to-face) including induction training and/or be supported by a campaign to educate and inform them about the importance of vigilance and reporting any suspicious behaviour. For visitors, irregular site users or event patrons, messaging may be promoted through sign-in procedures, ticketing or event information, posters, or public announcements.

Who has a role?

Everyone has a responsibility to help detect and prevent possible terrorist attacks in crowded places. Everyone working in or using a crowded place should be aware of their surroundings and report suspicious or unusual behaviour to authorities. This can range from security staff, employees, visitors, patrons and will vary depending on the nature of your business.

Security awareness and vigilance should be promoted among everyone working in or using a crowded place. Remember, reconnaissance can take place at any time and be conducted away from the potential target location.

As we go about our daily lives, we can keep an eye out for anything that may seem unusual or suspicious. Whether or not something is suspicious can depend on the circumstances: look at the situation as a whole. But remember, a small piece of information may be a significant part of a bigger picture.

What to look for?

It is important for owners and operators of crowded places to understand where hostiles might go on site to collect information or test security measures. Employees should have an awareness of behaviour or activity that is atypical or unusual for the environment and be able to report such incidents.

Hostiles do not comply with a standard set of guidelines and any person (irrespective of age, gender, or ethnicity) could be involved in attack planning.

Possible indicators of hostile reconnaissance could include[1]:

- People taking photographs of staff or security features of the site
- Someone taking an interest in staff/vehicle movements
- Unusual approaches to staff
- Attempts at testing or breaching security
- Someone being followed through security control points (e.g. tailgating)
- Packages/bags being left unattended
- Suspicious vehicle activity near the site

[1] Additional hostile reconnaissance indicators are included in Appendix 1.

Responding

Staff and security personnel should be prepared to receive and immediately respond to reports of suspicious activity.

Security should be encouraged to approach persons on site and politely ask questions to explain their presence or behaviour if considered unusual. Security should use a customer-service approach and ask open-ended questions such as **'Can I help you?' or 'Who are you visiting today?'**. This demonstrates that staff are not only good at spotting things that are out of place but will also do something about it.

This should be done with caution and where there is no immediate or obvious threat. If staff concerns are not resolved by this engagement (e.g., where responses are vague or evasive), staff should follow procedures for reporting and responding as appropriate to their organisation.

Once reported, security and/or management should ensure CCTV monitoring and external security patrols are focussed on recording or identifying suspicious individuals, vehicles, and items. CCTV images and incident reports should be archived as these may be required by police for further investigation or as evidence.

Security and staff should be aware of their powers relevant to their site. In many cases security do not have legal powers to prevent someone taking photos, asking them to delete photos, or to seize a camera. However, some sites may have prohibited item or other policies that prohibit photography or the use of UAS that will assist security in further responding to suspicious activity.

Recent increases in the capability and ease of use of UAS increases the likelihood of these being used for malicious purposes as they can circumvent many physical security measures. Owners and operators need to be aware of Australia's UAS safety laws[2], and their limitations. Understanding rules for UAS operators (e.g. around controlled airports or populated areas such as parks) may help in identifying suspicious activity.

Owners and operators should develop response procedures for suspected incidents of reconnaissance and rehearsals, considering:

- ensuring staff and security are trained to know what to do (taking personal and legal safety constraints into account)
- recording an incident, including evidentiary requirements
- reporting protocols
- responsibility for managing an incident
- how an incident will affect neighbouring facilities (or other building tenants), including any mutual arrangements that need to be agreed on and implemented for the reporting of suspicious activity in the precinct
- how incident logs will be analysed to detect potential hostile activity at the facility
- sharing incident information with other organisations in the precinct and emergency services
- establishing a procedure for reporting an incident to Police and/or the national security hotline. Once incident procedures are developed, organisations should exercise and review their procedures to ensure a timely, measured response and effective strategies are in place

Depending on the nature and details of the incident, owners and operators may decide to increase their security measures and/or alert level until an incident is satisfactorily resolved.

[2] Available on the Civil Aviation Safety Authority (CASA) website

3. DETER

Deterrence involves the promotion of the DENY and DETECT capabilities of a site.

One of the primary functions of protective security measures is as a deterrence to hostiles. Proactively promoting protective security can enhance the deterrent effect and heighten the perception by hostiles that they will be intercepted, and their attack will fail.

Promoting Security Capabilities

Promoting security capabilities needs to be done thoughtfully. There is a balance to both reassuring site users without causing alarm, and without giving away too much detail that could be helpful to hostiles.

For example, signage or information on your website that provides specific information about your security (e.g. what times security are on site, specific number of cameras after an upgrade, type of vehicle barriers, etc) may be exploited by a hostile.

Promotion of security capabilities must also be truthful—exaggerating your security measures can encourage the hostile and undermine the deterrence effect of your security.

Security capabilities to be promoted may include[3]:

- strong security partnerships
- staff and security vigilance
- unpredictable security patrols
- onsite CCTV coverage and monitoring
- security access procedures
- security screening of people and belongings

Messages should be promoted where a hostile is more likely to see them, e.g., public foyers, entry points, security screening points or online.

Promotion and communication strategies may include:

- organisational website and social media messaging
- local, regional or trade press publications
- posters, signs, and notices
- flyers, leaflets, pamphlets
- promotional material and memorabilia
- tickets, wristbands, bunting
- recorded PA announcements
- screen savers and visual display screens
- website cookie policies in place that log a user's IP address, keyword searches and pages/locations visited. Research indicates that the cookie policy pop up can act as a deterrent. It also indicates that the organisation makes security a priority.

Reviewing and updating these communications will demonstrate that the organisation considers security to be a priority and further enhance the deterrent effects.

[3] See Appendix 2 for more details on promoting security capabilities

Protective Security Measures

Protective security measures at your site should be proportionate to the level and types of threat. Although not exhaustive, the list of security measures below may assist to deter and deny a hostile access to your site or valuable information.

These include:

- varying times and routes of security patrols to avoid predictability
- increasing visibility of security patrols around entry points and public access areas
- ensuring security patrols identify and report damaged/malfunctioning security infrastructure
- regular auditing of access control (e.g. identification passes, swipe cards, keys) with lost or misplaced passes immediately deactivated or compromised locks rekeyed
- enhance natural surveillance along the external perimeter of a facility premises by removing or trimming excess vegetation
- CCTV systems can be used to conduct ongoing virtual patrols and monitor the environment to support security personnel on the ground
- appropriate levels of security lighting should be used to support natural surveillance of the perimeter and approaches to the site at all times of the day and night (including periods of inclement weather)
- obscure and secure perimeter windows and restricted areas to reduce the potential of reconnaissance and rehearsals of critical or vulnerable areas

NEXT STEPS

These *Guidelines* are intended to increase understanding of the hostile reconnaissance threat and assist owners and operators to disrupt hostile reconnaissance at their site.

Owners and operators are encouraged to review the considerations outlined in this guideline and determine what measures can be applied to their site or event.

- Completing the *Crowded Places Self-Assessment* and *Security Audit* to understand the threats and vulnerabilities of your site
- Audit publicly available information about your site **(see DENY)**
- Ensure staff and site users are confident in knowing what and how to report and respond to suspicious behavior **(see DETECT)**
- Encourage staff and security to approach and politely ask questions when they observe unusual behaviour **(see RESPOND)**
- Develop clear procedures for staff and security for responding to suspicious behaviour **(see RESPOND)**
- Promote and communicate your protective security capabilities to enhance their deterrence effect **(see DETER)**
- Review your protective security measures to ensure these assist in the deterrence of hostile reconnaissance **(see DETER)**
- Establish liaison and regular communications with Police, emergency responders and neighbouring organisations or precincts to enhance information exchange and develop integrated security measures and emergency response plans
- Exercising security response plans regularly with employees and other stakeholders (e.g. building management, and tenants) to ensure adequate resources are available to implement the plan

USEFUL LINKS

- Australian National Security: *Australia's Strategy for Protecting Crowded Places from Terrorism*
  - www.nationalsecurity.gov.au
- ASIO Outreach
  - www.outreach.asio.gov.au

VERSION CONTROL

This document is endorsed by the *Australia-New Zealand Counter-Terrorism Committee (ANZCTC)* and maintained by the Department of Home Affairs (DHA). DHA is responsible for the version control of this document. To preserve the integrity and currency of this document:

- major amendments must be endorsed by the ANZCTC
- minor amendments, for example to correct spelling or grammar, should be documented and forwarded to the Department of Home Affairs to be implemented and then
- a revised version sent to the CPSC to be endorsed before it is distributed

APPENDIX 1: INDICATORS OF HOSTILE RECONNAISSANCE

Employees working in crowded places and members of the public are often best placed to detect suspicious behaviour. Everyone who works in, or uses, a crowded place should be aware of their surroundings and report suspicious or unusual behaviour to authorities.

The following is a non-exhaustive list of behaviours and activities that may be indicators of hostile reconnaissance.

- unusual interest in security measures and routines, including over-inquisitive, unusual, or persistent questions by individuals
- covert photography of the location
- visits by individuals or vehicles with no apparent purpose, possibly for prolonged periods
- loitering in public areas
- weak reason or rationale for being on site if questioned or challenged
- avoiding eye contact with employees or avoiding uniformed security personnel
- leaving the area if noticed
- deliberately avoiding detection by security guards or cameras
- unusual activity by delivery/contractor vehicles
- tailgating and unauthorised access into controlled areas
- using stolen or fake clothing to imitate legitimate site users (e.g. employees, contractors, tradespersons, couriers, security or Police)—this might be identified through suspicious behaviours such as failing to conduct themselves according to protocol and improper use or wear of uniforms, etc.
- persons displaying anxious or nervous behaviours (unconscious movements such as clock checking, pacing, nail biting)

Remember, there could be innocent and legitimate reasons for these behaviours and activities. The most important thing is considering what the is baseline behaviour for the area and seeking more information to confirm or refute the initial suspicion.

APPENDIX 2: PROMOTING SECURITY CAPABILITIES

Deterrence communications should promote the security measures an organisation has without divulging too much detail. The main objectives should be to:

- **deny hostiles access to the information they need to plan an attack;**
- **deter hostiles from planning an attack because of a higher likelihood of detection; and,**
- **inform and reassure members of the public that an organisation is doing all it can to keep them safe from harm.**

The following table shows how communicating security measures can affect the hostiles and public perceptions.

Promoted capability	Hostile's perception	Public perception
Unpredictable security guard patrols	I am not able to predict the best time to conduct an attack	The organisation can effectively respond to an emergency
Effective partnership with police around a site	Everyone is alert to, and will report my suspicious behaviour	The organisation is working with police to enhance security and keep people safe
Site-user vigilance, and directives to report suspicious behavior and suspect items	I am likely to be detected in or around the vicinity and be reported to police or security	We can collectively help keep everyone safe
Onsite CCTV monitoring and intrusion detection system	I am likely to be detected and my attack will fail	The organisation is doing its best to keep people safe
Security barriers and access control systems	Any attempt to gain quick and easy entry and exit is not possible	The location is safe and secure
Website security messages—email instant messaging, cookie policy and pop-up screens	My online access and search criteria are being constantly monitored and recorded	The organisation is serious about cyber security and promoting security online
Security screening people and their belongings	I am unable to smuggle anything into the site	The location is safe and secure
Warning signs and notices	The organisation is serious about security	The organisation takes an active responsibility for security