Protecting Our Crowded Places from Attack:
Detecting and Responding to Hostile Reconnaissance

Te Whakamaru i Ō Tātau Wāhi Kōpiripiri mai i te Whakaekenga:
Te kimi me te Urupare ki te Hurahura Kairiri

New Zealand Government

Table of contents

Introduction	**3**
What is Hostile Reconnaissance?	**4**
Overview	**4**
Reconnaissance and Rehearsals	**5**
Initial reconnaissance/ intended location selection	5
Detailed reconnaissance	5
Rehearsals	**6**
Detection	**6**
Possible Indicators	**7**
Reporting	**8**
Responsibility	**8**
Response	**9**
Security measures	**10**
Next Steps	**11**

Introduction

All New Zealanders have a role to play in keeping crowded places safe.

Protecting Our Crowded Places from Attack: New Zealand's Strategy[1] / Te Whakamaru i Ō Tātau Wāhi Kōpiripiri mai i te Whakaekenga: Te Rautaki a Aotearoa has been developed to protect people working in, using, and visiting crowded places. The strategy's intent is, to every extent possible, preserve the public's use and enjoyment of these places while making them more resilient.

This document is part of a series of resources published by the New Zealand Police to help you understand the risks around crowded places, and to provide advice on how to prevent and manage those risks. This document should be read in conjunction with the Protecting Our Crowded Places from Attack: New Zealand's Strategy[2] / Te Whakamaru i Ō Tātau Wāhi Kōpiripiri mai i te Whakaekenga: Te Rautaki a Aotearoa.

These documents are regularly reviewed and updated. New information is also published from time to time.

Please check the New Zealand Police Crowded Places website[3] on a regular basis to ensure you have the latest and most comprehensive information.

[1&2] *www.police.govt.nz/crowdedplaces/crowded-places-strategy*
[3] *www.police.govt.nz/crowdedplaces/prepare-your-crowded-place*

What is hostile reconnaissance?

Hostile reconnaissance is the purposeful observation of people, vehicles, buildings, places and spaces to collect information that informs the planning of an attack against that specific and intended location.

It may also include rehearsals, where one or more elements of the plan are practised.

Analysis of previous incidents indicates that some form of reconnaissance and rehearsal will likely occur prior to an attack.

Reconnaissance efforts may be focused on areas near the intended location where potential security measures may mitigate an attack, such as security screening points, access control points or vehicle access routes.

Detection and intervention of reconnaissance and rehearsals may lead to an attack plan being abandoned and may produce intelligence leads.

This guide provides an overview of the potential indicators and protective security measures that could be considered when developing or reviewing security plans and measures to mitigate the tactic of conducting hostile reconnaissance and rehearsals through deter, detect, delay and respond.

Overview

The primary objective of reconnaissance and rehearsals is to provide attackers with information that will help them to:

- understand the location
- establish the best method of attack
- determine the best time to conduct an attack
- gather intelligence/information
- familiarise themselves with the layout of the organisation or plan of an event.

The frequency and type of reconnaissance and rehearsals conducted may vary depending on multiple factors, including:

- intended location type
- the preferred attack tactic
- level of sophistication of attack
- the amount of information publically available about the intended location (e.g. on the internet)
- familiarity with the intended location and the environment surrounding it
- level of training and experience
- risk appetite
- the presence of visible security measures, etc.

Reconnaissance and rehearsals

Reconnaissance and rehearsals can be broken down into broad stages that may occur successively or simultaneously, and may involve a number of visits to the potential intended location prior to the attack — noting that reconnaissance can take place at any time on any day and be conducted from vantage points located away from the intended location itself.

The activity may be openly or secretly undertaken via physical and/or technological means e.g. mobile phones, GoPro-style cameras and commercially available drones.

Initial reconnaissance/ intended location selection

Initial reconnaissance is usually associated with intended location and tactic selection, and may involve research using publicly available information to inform more detailed reconnaissance activity. **This can include:**

- information obtained from online maps or an organisation's website
- tours of facilities
- telephone calls and emails designed to extract confidential information
- services that provide reference material and referrals for utilities e.g. "dial before you dig"
- internet protocol look-up tools that provide the contact information of a specified IP address
- business profile information such as New Zealand Business Number
- employee social media profiles, etc.

Detailed reconnaissance

Once potential intended locations are selected, more detailed reconnaissance activity may take place. This can include physical observation and interest in:

- location of closed-circuit television (CCTV) cameras and security systems
- location and number of security personnel
- entry and exit routes
- variations in security patterns, such as timings of security patrols
- operating procedures
- changeover of shifts
- pedestrian and vehicle traffic patterns
- parking areas
- loading docks
- ability to enter or leave location without detection
- perimeter doors and fences, etc
- observing emergency tactics and responses to inform secondary attacks
- identify likely escape routes.

This detailed reconnaissance may also include making notes, sketches and taking footage or images of an intended location and its security measures. This can include:

- unsolicited approaches and questioning employees to elicit information about security measures
- probing security measures e.g.:
  - initiating hoaxes (such as placing an item for the purpose of assessing a suspicious item response or identifying emergency evacuation assembly areas)
  - attempting to bring prohibited items through screening, activating intruder detection systems
  - direct questioning to identify vulnerabilities, etc.

Rehearsals

Before carrying out an attack, attackers may conduct rehearsals. This could include walking through entry and exit points, transporting items that serve as stand-ins for weapons, or rehearsing timings and event sequences. The timings between a rehearsal and the actual attack may be short to protect operational security, and to reduce the time an organisation has to make changes to its security posture that may impact an attack's execution.

It should be noted that a rehearsal may also **not** take place, especially on a "soft location" or for an opportunistic or simple attack scenario.

Detection

The ability to detect suspicious activity is an important security measure that could assist in disrupting attack planning— noting that reconnaissance and rehearsals may factor in attack objectives, usual modus operandi and indicate the type of attack being planned.

Some of the best people to spot things that are out of the ordinary in a neighbourhood or workplace are those who are there every day. 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.

Three concepts that are useful to remember are **HOT, White Level Inspection** and **Baseline.**

- Under the **HOT** principle, anything that is **H**idden, **O**bviously suspicious or not **T**ypical to its environment could be deemed a security risk.
- **White Level Inspection:** An inspection by all staff members of their respective workplace for any articles that are unusual, suspicious or unable to be accounted for. The people in the best position to conduct these inspections are the people who know and work within that area.
- **Baseline:** There is an accepted and predictable behaviour in your environment. Spotting behaviour that is different to your baseline is key to detection.

Situational awareness should be promoted among employees and vigilance encouraged at all times in and around an organisation's area of operation— noting that reconnaissance can take place at any time on any day or night and be conducted away from the intended location area. This includes being alert to suspicious behaviour or activity that could indicate reconnaissance and rehearsals, and encouraging the timely and accurate reporting of such behaviour.

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

Possible indicators

Suspicious behaviour and activity can take a number of forms. Employees should have an awareness of behaviour or activity that is atypical for the environment and be able to report such incidents. **Possible indicators of reconnaissance and rehearsals include:**

- possession of detailed maps, blueprints and global positioning systems
- unusual interest in security measures and routines, including over-inquisitive, unusual or persistent questions by individuals
- complying with security directives when challenged, but defying directives afterwards
- reluctance to show security personnel or staff personal belongings e.g. a back pack
- theft and use of false, stolen or lost access control cards and identification passes
- visits by individuals or vehicles with no apparent purpose, possibly for prolonged periods
- unusual activity by delivery/contractor vehicles
- erratic driving
- avoiding eye contact with employees or avoiding uniformed security personnel
- weak reason or rationale for being on site if questioned or challenged
- evidence of tampering or damage to security infrastructure
- tailgating and unauthorised access into controlled areas
- scanning the location with recording devices
- maintaining secret connections between others in a group by eye, head and hand gestures
- loitering in public areas
- leaving the area if noticed
- staring or quickly looking away
- attempts to disguise identity or change appearance e.g. motorcycle helmets, 'hoodies' and multiple layers of clothing. Note there is a layer of complication to determine if someone is covering their mouth/face/eyes for hostile reasons or due to other reasons
- attempts to imitate employees, security or Police through the wearing of stolen or counterfeit uniforms - this might be identified through suspicious behaviours such as failing to conduct themselves according to protocol and improper use or wear of uniforms, etc.

Additionally, an attacker conducting a rehearsal may wear items of clothing that enable concealment of weapons or an improvised explosive device (IED). Such attire may be out of keeping with a location, event or current weather conditions.

Behavioural detection indicators are difficult to reference accurately as they can vary depending on an individual and the environment; however, anxious behaviour and nervous tendencies could include:

- patterns in unconscious movements (e.g. clock watching, rubbing hands, face touching, pacing, nail biting)
- appearance of being tense (e.g. rigid and over controlled)
- high-pitched speech
- perspiration
- heavy breathing
- shaking, etc.

A number of these indicators become obvious when the person is spoken to by anyone who looks official i.e. security, branded staff, police etc. Some behaviours are just because the person is nervous by nature but it's the response to certain things that give higher concerns to certain behaviour e.g. if a suspect is walking around the perimeter checking out exits/entrances and sees 'security' and turns around and walks off that is a red flag or if they were perspiring it could be that they have been running or its hot.

Reporting

Individuals displaying indicators (and in particular multiple indicators) of suspicious behaviour may need to be assessed as potential threats.

In broad terms, employees and volunteers should be encouraged to immediately report all suspicious activity to nominated security personnel with a focus on:

- what they saw
- when they saw it
- where the incident occurred
- what behaviour was considered suspicious.

While remaining cautious and without putting personal safety at risk, witnesses may be able to gather other relevant details to assist in resolving an incident— this could include use of personal recording devices such as a mobile phone or camera. Details could include:

- description of personal physical attributes e.g. gender, age, height, weight, hair cut/colour, scars, tattoos and ethnic origin
- description of clothing
- description of carried items
- if engaged in discussion, the individual's reaction and response, etc.
- number of people, direction arrived from, directed exited to
- vehicle description, location and registration details
- what activities or items that person may have had a specific interest in.

Immediate reporting of suspicious activity can enable security personnel to monitor the situation for further assessment and provide a response if required.

Responsibility

All New Zealanders have a responsibility to help detect and prevent attacks in crowded places.

Everyone who works in, or uses, a crowded place should be aware of their surroundings and report suspicious or unusual behaviour to authorities.

In an emergency everyone should phone 111

If the information is not time-critical, people can report suspicious or unusual behaviour by:

- completing a report at **105.police.govt.nz**, or calling Police's non-emergency number **105**
- visiting their nearest Police station[4]
- phoning Crimestoppers on **0800 555 111**
- contacting the NZSIS on **0800 747 224** or via their Public Contribution Form[5].

[4] *www.police.govt.nz/contact-us/stations*
[5] *https://providinginformation.nzsis.govt.nz*

Response

When an incident is 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 of the incident should be archived.

Security personnel should be mindful that Police may require information relating to an incident e.g. CCTV images and incident reports for further investigation and evidentiary purposes.

Security personnel should also be prepared to receive and immediately respond to reports of suspicious activity.

Responses could also include initiating casual questioning of suspicious individuals through to requesting photographic identification to enable an additional assessment of the threat. This should be done with caution and without putting personal safety at risk. Open-ended questions e.g. 'can I help?' or 'who are you visiting today?' could be used to put pressure on an individual, which could result in deceptive non-verbal cues such as:

- evasive or delayed answers which lack a normal degree of detail
- uneasy responses to conversation
- increases in voice pitch
- facial flush
- avoiding eye contact
- dilated pupils
- exaggerated yawning
- rapid eye blinking
- excessive throat clearing or swallowing
- leaving the area.

It is recommended that owners and operators develop response procedures for suspected incidents of reconnaissance and rehearsals, giving consideration to:

- ensuring staff are trained to know what to do
- responsibility for managing an incident
- reporting protocols
- security personnel response and what actions need to be taken
- when and how security personnel or employees should intervene (taking personal and legal safety constraints into account)
- recording an incident, including evidentiary requirements
- 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 information regarding an incident with other organisations in the precinct and emergency services
- establishing a procedure for reporting an incident to Police and/ or the NZSIS. 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.

Security measures

Security measures that are layered, difficult to overcome and/or predict may deter an attacker from conducting reconnaissance past the initial phase.

To mitigate any potential threat from reconnaissance and rehearsals, various security measures can be implemented. Consideration should be given to the number of on-site security personnel required to provide an effective deterrence and/or detection capability, including:

- ensuring security patrols identify and report damaged/ malfunctioning security infrastructure
- conducting security patrols around drop-off and pick-up points, public access areas and areas where large numbers of people congregate
- during times of heightened threat, maintaining awareness of security patrol patterns. If possible, vary times and routes to avoid predictability, and increase random patrols to reduce any perceived vulnerability of potential intended locations
- increase visibility of security and Police personnel in areas adjacent to, and in front of, entry and security screening points
- ensure access control cards and identification passes are regularly audited
- immediately deactivate all lost or misplaced access control cards
- ensure access control and security keys are regularly audited. Keys should be kept in the custody of trusted individuals at all times
- access control and security locks should be re-keyed if it is suspected that keys have been compromised (lost or unauthorised copies made)
- lock and install tamper alarms and/ or tamper evident seals on enclosures and cabinets containing equipment which supports critical assets or security infrastructure
- enhance natural surveillance along the external perimeter of a facility premises by removing or trimming excess vegetation and relocating waste skips and other pieces of equipment. These could be used by an adversary for concealment from detection, placement of an IED or as a staging point to conduct an attack
- 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 facility 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 key functions and assets.

In addition to the above, consider:

- establishing liaison and regular communications with Police, emergency responders and neighbouring organisations 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
- establishing effective and efficient suspicious activity reporting procedures and mechanisms that support communication and incident response—noting that reconnaissance can take place at any time on any day and be conducted away from the intended location area
- ensuring security personnel and employees receive training and briefings on most likely tactics and scenarios, including active armed offender preparedness, and IED awareness and recognition
- testing and maintaining all electronic security systems and security hardware to ensure they operate as designed
- conducting a survey of the publicly available information associated with an organisation and its facilities— sensitive information should be redacted or removed
- the use of real-time social media geo-specific monitoring tools to increase situational awareness and identify suspicious activity around an intended location
- the use of analytical tools to monitor activity on an organisation's website to identify potential acts of online reconnaissance.

Next steps

In using this document you have considered further information that will help keep your crowded place safe.

You may have noted some areas where you feel you can change your current ways of operating and develop a plan to address those areas.

If you feel there are significant gaps, or remain concerned for your location, it is recommended you complete the Protecting Our Crowded Places from Attack: Security Audit[6] / Te Whakamaru i Ō Tātau Wāhi Kōpiripiri mai i te Whakaekenga: Ōtita Whakamarutanga document to develop further plans and responses.

You may also want to contact a security professional and seek assistance from them.

[6] *www.police.govt.nz/crowdedplaces/prepare-your-crowded-place*

In the event of an attack

Move quickly and quietly away from danger, but only if it is safe to do so.

Stay out of sight and silence your mobile phone.

Call the Police by dialling 111 when it is safe.

www.police.govt.nz/crowdedplaces

New Zealand Government