跨部門反恐專責組
Inter-departmental Counter Terrorism Unit

Safe Community Newsletter

2025 Oct Issue #15

Potential Risks to Critical Infrastructures During Major Events

The term "Critical Infrastructures" (CIs) does not have a universal definition, but it generally refers to infrastructures that are essential or of great importance for the normal functioning of a government and the everyday lives of people. Due to their symbolic meaning and significances, CIs often become the target of terrorists and extremists. Large-scale or major events tend to attract large crowds, which further increase the risk of attacks on CIs. Operators should therefore strengthen the relevant security measures.

When a CI unfortunately experiences a terrorist attack or major incident, it can lead to significant casualties and cause social panic, resulting in unpredictable impacts on the public and society.

As such, we must strengthen our preventive measures, stay vigilant, and guard against individuals seeking to exploit opportunities to stage attacks on CIs.

Below are some examples of overseas attacks or plots targeting CIs during major events:

The Netherlands June 2025

During the NATO summit held in Hague, the Netherlands, about 30 rail cables were intentionally set on fire, bringing local train services to a halt. Police investigation indicated that extremists had conducted the attacks to cause serious disruption to the community.

Austria August 2024

Three concerts of American singer Taylor Swift scheduled to be held at a stadium in Vienna, Austria, had to be cancelled after local Police received intelligence of a terrorist attack. Two people suspected of plotting the attack were arrested, with one of them being a supporter of an Islamist terrorist group.

France July 2024

Hours before the opening ceremony of the Paris Olympics, three locations of the local high-speed rail network were hit by arson attacks which paralysed the transportation system. Trains on a number of railway lines had to be diverted or cancelled, with 800 000 passengers affected. Police subsequently arrested a left-wing extremist.

To reduce the risk of attack on CIs, operators may adopt the following key preventive measures:

Strengthen Security Measures

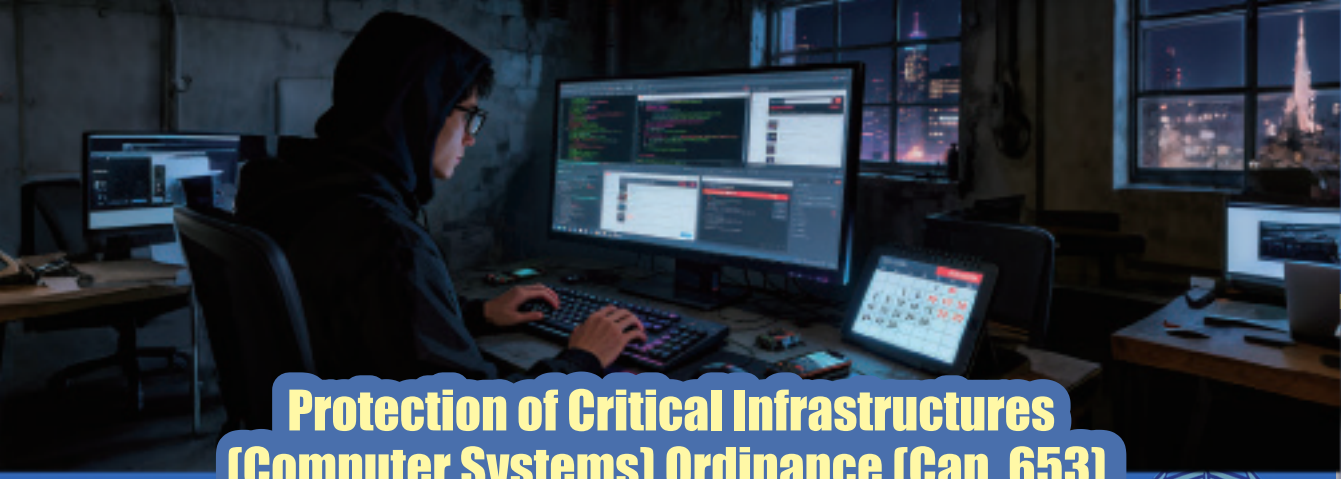
- Enhance patrol to ensure door locks and alarm systems are functioning properly
- Implement security control measures for visitors and vehicles at access points and keep proper logs
- Install CCTVs with high-definition recording functions
- Equip entrances with security screening equipment to detect potentially dangerous items

Strengthen Counter-terrorism Training and Enhance Response Capabilities

- Educate staff on how to identify suspicious persons, objects or activities, and encourage them to "Spot and Report"
- Conduct regular emergency response exercises
- Ensure that personnel are familiar with the environment and escape routes in order to assist the public in evacuation when it is safe to do so

Roles of the Public

Members of public should always stay vigilant and look out for suspicious persons or items around, especially in crowded places. Remember to "Spot and Report".



Protection of Critical Infrastructures (Computer Systems) Ordinance (Cap. 653) is set to take effect on 1 January 2026

In fact, terrorist attacks nowadays are not confined to physical ones. Extremists may also exploit technology and the cyberspace to carry out attacks.

In view of the technological advancement, the Protection of Critical Infrastructures (Computer Systems) Ordinance (Cap. 653) will come into effect on 1 January 2026 to strengthen the relevant security measures and ensure the safety of the computer systems of Hong Kong's CIs.

The Ordinance, gazetted on 28 March 2025, aims to impose statutory obligations on designated operators of CIs to ensure they adopt appropriate measures to protect their computer systems, minimising the risk of essential services being disrupted or compromised due to cyberattacks, thereby maintaining the normal functioning of Hong Kong and the daily lives of people.