「國家關鍵基礎設施防護」的思維與工作面向

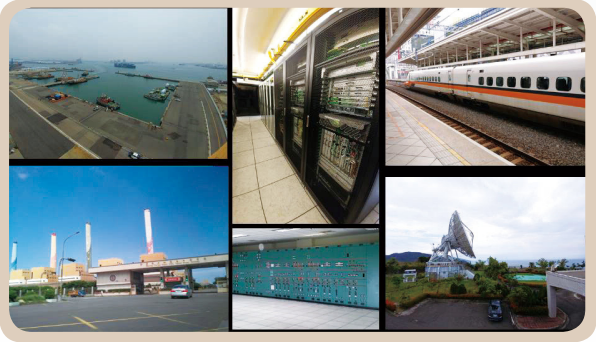
■ 國立聯合大學土木與防災工程學系助理教授　李中生博士

開車返鄉或出遊前，有一件很重要的事必須提醒：須先保養車輛，檢查並確定各項狀況良好，包括引擎、煞車、水箱、電力等系統；也需要確定車裡各項資訊傳輸儀表顯示以及監控系統正常，能夠正確告訴我們檔位、引擎轉速、溫度、油量、電力等控制資訊。然而，就算車輛狀況正常，預備充足的油料與電力也是確保能順利抵達目的地的必要條件。此外，還有一項必要的項目，那就是駕駛。在無人車技術發展成熟之前，缺了駕駛員還是無法成行的。故若我們分析開車出遊這項任務時，執行它所需要具備的條件可以歸納為：車內各項機械系統（實體）、儀表顯示與監控（資通訊），以及駕駛（人員），而燃料與電力則是必要的資源，缺乏前述任何一項條件都將使得這項任務中斷。

而「國家關鍵基礎設施」（Critical Infrastructure，簡稱：CI）所指的即是支持著國家與社會運作所需要的重要功能設施與系統，包括能源、通訊、交通、機場、港口等，而要使這些設施系統能夠正常地運作，同樣必須要仰賴「實體」、「資通訊」控制系統以及「人員」等三類必要條件，而這三類必要條件有各自不同的風險

與安全威脅。若是其中一類遭受災害影響，將進而導致 CI 功能失效，不僅會嚴重影響民眾生活，中斷都市社會運作機能，造成國家經濟重大損失，降低政府聲譽與信用，甚至有可能影響國家安全。

國內外最近幾年發生過多起 CI 防護失當案例，顯示出 CI 一旦失效將造成重大的影響層面與災害損失。因此有必要對這些「CI」進行特別的防護與管理。在我們探討那些設施是 CI 之前，我們必須先了解 CI 防護的思維。



關鍵基礎設施類型。（圖片來源：作者提供）

CI 防護思維

一、安全與韌性

美國推動 CI 防護工作已逾二十餘年，不論是在觀念上以及在作法上都值得借鏡。在 2013 年美國國土安全部提出以「安全（Security）與韌性（Resilience）」為推動目標的國家基礎設施防護計畫（NIPP）[1]。根據美國定義，「安全」是指**「利用實體防護與網路防禦來降低因為入侵、攻擊或天然以及人為災害對關鍵基礎設施所造成的風險」**。而「韌性」的定義則是指**「對於蓄意攻擊、意外，或是天然災害等威脅與突發情況能夠有所準備、調適與因應，以及在中斷後能快速恢復的能力」**。綜整上述描述，CI 的防護工作目標可以整理出以下幾點工作面向來進行說明：

（一）於平時分析威脅來源並進行防護

在 2005 年卡翠納颶風造成重大災害以及後續所發生之重大資安事件後，美國政府即要求以全災害（All-Hazards）的思維來進行分析 CI 威脅並進行防護。

全災害可區分為天然災害與人為災害兩大類，而生活在臺灣對於天然災害的類型並不陌生，包括地質災害以及氣象災害

2005 年卡翠納颶風在美國造成重大災害，不僅數千人在這次災難中喪生，各地基礎設施毀損，經濟損失慘重。

兩類。人為災害，根據美國消防工程師學會 NFPA1600 的分類[2]，則可區分為生物危害、人為意外事件、人為蓄意事件、技術事件以及其他危害等，如表一所示。在這個工作面向中，不僅需要依據 CI 的功能特性與位置，分析來自外部與內部災害威脅的可能性，更需要瞭解威脅一旦發生所可能造成的災害與衝擊影響，進而針對可能遭受破壞的項目進行防護工作。

（二）對於突發事故的處理能夠事前規劃

在此工作面向上，必須掌握設施間的相依性，以及必要的外部資源（如水、電、通訊等），做為分析連鎖性影響的根據。另應該針對不同威脅類別與程度評估可能造成設施失效的狀況、影響範圍與層面，以及災害損失等，並依照災害情境規劃處置對策以及處理程序。

（三）在災害事故發生時能夠有效因應

在此工作面向上，須仰賴有效的災害事故應變組織、機制以及處置對策，更應熟稔應變程序，包括指揮調度在內對各項應變技能進行技術與教育訓練。此外，利用演練與演習驗證、檢討並改善各項處置對策與處理程序，於平時即提升對於各類災害事故的應變能力與技術，以確保在事故發生時能夠有效因應，並降低且限縮災害影響的範圍與層面。

災害發生時，規劃設置災害事故應變組織、機制以及處置對策，可提升救災效率。圖為 2015 年復航空難，臺北市成立災害應變中心，市長坐鎮指揮。（圖片來源：臺北市政府，https://www.gov.taipei/News_Content.aspx?n=F0DDAF49B89E9413&sms=72544237BBE4C5F6&s=AF86AA6116D01948）

平時利用演練與演習可驗證、檢討與改善各項災害處置對策。圖為 2017 年臺北市舉行萬安 40 號演習，演練發生「信義區聯合行政大樓遭敵縱火及挾持民眾狀況」之應變措施。（圖片來源：臺北市政府，https://www.gov.taipei/News_Content.aspx?n=2044902FC839D045&sms=72544237BBE4C5F6&s=E82AD343E540485F）

（四）在功能中斷之後能夠快速恢復

CI 擔負重要功能，因此如何確保在災害事故下能夠持續運作，或是在中斷之後能夠快速的恢復功能，是推動防護工作最重要的目的之一。因此，國際間在推動「CI 防護」的工作上，均已導入「持續營運管理」的觀念，藉由設施功能的允許中斷時間以及目標復原時間，做為持續營運管理以及設計功能恢復手段（如備援）的目標與依據。

二、設施盤點與分級

為了推動 CI 防護工作並有效地進行管理，必須藉由設施盤點與分級建立資料庫。在設施盤點方面，依照系統功能屬性，行政院國土安全辦公室已經將我國 CI 分為八項主領域：能源、水資源、通訊傳播、交通、金融、緊急救援與醫院、政府機關、科學與工業園區；而在各主領域下亦再區分次領域，例如在能源領域之下再區分為電力、石油、天然氣、核能、化學材料等次領域。其目的乃希望以領域功能為目標，進行有系統的盤點工作，藉以掌握支持領域功能運作所必要的實體設施與網絡（如供水、供電網絡）、資通訊控制系統，以及關鍵的技術（人員）等。

在設施分級上，不僅需要評估設施的重要性，更需要考慮設施的相互影響關係。在設施重要性上可藉由「功能重要性」、「失效影響」以及「民心士氣影響」三大項目進行評量。功能重要性則建議由政府機關運作、重要資通訊系統、維生與運輸機能、金融秩序、疫病系統、治安與防救、國家重要象徵與資產、重要產業與園區、防衛動員等面向進行評量；在失效影響方面，可由設施價值、影響人數、經濟損失

表一　災害類別與項目

類別	項目
地質危害 Geologic hazards	地震、海嘯、火山、土石流、坡地崩塌等
氣象危害 Meteorological hazards	強風、洪水、暴洪、乾旱、下雪、冰雹、暴風、極端氣候、閃電電擊等
生物危害 Biological hazards	食物中毒、疫病等
人為意外事件 Accidental human-caused events	有害物質洩漏、核能事故、爆炸／火災、交通事故、燃料／資源短缺、機械故障、操作意外等
人為蓄意事件 Intentional human-caused events	罷工、惡意破壞、暴力行為、抗議示威、炸彈威脅、恐怖主義、縱火等
技術事件 Technology-caused incidents	設備故障、設施老舊、網路中斷、網路攻擊、資料遭竊、電力中斷、供水中斷等
其他危害／風險 Other hazards/risk	供應鏈中斷等

CI 防護必須由管理體系與專責單位分層負責推動與落實相關工作，我國目前由行政院國土安全辦公室負責督考各領域的 CI 防護管理工作，推動國家層級威脅情境辨識，擬定國家 CI 管理與執行策略與目標。（圖片來源：中華民國行政院，https://www.ey.gov.tw/cp.aspx?n=9DD1F33EB9A1A6CB、三立新聞）

等進行評量；而在民心士氣影響方面，則由影響國際形象、影響政府聲譽、影響民眾信心等方面評估。藉由上述這三大面向的綜合評估，將使各自領域內設施系統依重要性排序。

三、組織與合作

CI 防護是一項需要持續推動的管理工作，必須藉由管理體系與專責單位，分層負責推動與落實相關工作。我國目前由行政院國土安全辦公室負責督考各領域的 CI 防護管理工作，推動國家層級威脅情境辨識，擬定國家 CI 管理與執行策略與目標。各領域主管機關應建立推動小組，進行領域內的設施與系統的盤點與分級、災害威脅辨識，擬定領域層級的 CI 安全防護計畫，督考所轄的 CI 防護工作，並建立資訊通報與分享機制。而 CI 與系統的營運單位同樣需要導入持續運作的管理方法，擬定 CI 防護管理計畫，執行相關防護工作。唯有如此，才能夠使關鍵基礎設安全防護工作能夠在橫向與縱向上，在跨部門之間整合起來。

結語

若是以人的身體來比喻，CI 就如人體內的骨骼、血管與經脈，支持一個人所要執行的動作。正因為如此，必須要有系統地建立設施資料庫，以系統性的方式進行風險分析後並加以防護。CI 安全防護所推動的是一套風險管理程序，從設定目標、設施盤點與分級、風險評估（威脅、暴露量、脆弱度、後果）、規劃防護優先次序，進而實施防護計畫並且評量實施成效。而在推動過程當中，以「持續營運管理」的方法，在實體、資通訊、人員三個項目上進行風險管理與防護。CI 支持著國家各項重要功能的運作，因此必須要在各層面上提升其耐災韌性，並且對於變動的風險威脅能夠及時調適與因應。

參考資料

1. NIPP 2013, Partnering for Critical Infrastructure Security and Resilience, https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf (accessed on 2018/1/30)

2. National Fire Protection Association, NFPA 1600 – Standard on Disaster/Emergency Management and Business Continuity Programs, 2013 Edition.