



關鍵基礎設施 防護與工程師 之二

— 防護整備作業 探索

張清祥／前行政院 參議、土木・大地工程 技師

廖東成／蘭陽技術學院建築與室內設計系 副教授

林祐正／國立臺北科技大學土木工程系 教授

關鍵基礎設施（Critical Infrastructure, CI）肩負社會服務、國家永續運作的命脈任務，關係民眾生活至巨，如何維護其服務正常，各界關心，更是工程師基本使命。工程師不但在其規劃、設計階段著力，營運階段功能的確保的角色亦不可或缺，扮演基礎設施全生命週期的保母角色，故如何預防、因應與善後各種威脅風險等各種整備工作，值得關心、探索與究竟。國際上，尤其是美國，歷經數件重大事件之後，既有的國土安全議題，再度被關注，其中涉及關鍵基礎設施防護（Critical Infrastructure Protection, CIP）議題更是重心，而工程師原本著重的任務焦點範疇也隨之拓展，深入到全生命週期的防護整備工作。本文繼續探索工程師與關鍵基礎設施防護關係，就防護整備工作做進一步介紹，供各界參考，尤其是以專業技術服務為基本的工程師與機構，並期不吝指正。

關鍵字：基礎設施防護、整備、情境規劃、總體任務清單、目標能力要項

關鍵基礎設施為何要防護整備？

張清祥等人^[1]提出國土安全參與者與工程師於關鍵基礎設施防護應具備有的素養，涉及各種背景人物、輪廓、範疇均相當的多樣、豐富，也點出後續精進的方向。本篇針對關鍵基礎設施防護（Critical Infrastructure Protection, CIP）核心任務，亦即防護整備工作，做更進一步的探索介紹。純「整備（Preparedness）」就內涵言，一般解讀各有立場與定義，也常與「準備」一詞常交互出現，就本質言，是一體兩面。

基礎設施支撐政府的運作、社經的活動與民眾的生活，尤其是具關鍵性的設施，亦即 CIP，其重要性不言而喻。而持續（Continuity）則是一個國家／企業，甚至是個體存在的必要條件，基礎設施亦然。以美國為例，曾由總統公布其國家持續策略，揭示其持續國家的基本功能運作為國土安全推動的目標，而確保關鍵服務正常為

國家的基本功能。過去國際發生過的災害案例與經歷，造成政府、社會與企業機構運作中斷，帶來極大衝擊。維持持續運作、確保設施安全與韌性（功能正常），是設施防護基本任務，而防護的一體兩面－整備工作，更是核心。工程師此刻扮演的更是「非我莫屬」保母角色。今回溯之前的 CIP 相關介紹，如 CI 的輪廓與威脅^[2]：

關鍵基礎設施輪廓

以美國（國土安全部）說法，CI 內容包括資產、系統與網絡。其他如歐盟、澳、加、紐亦有類似定義。國內，資通安全管理法亦有類似定義。這些範疇、定義雖有差異，但防護追求目標（核心功能）並無差別。關鍵基礎設施的概念起源於二戰^[3]，與今天的認知方式大不相同的形式。以前是戰爭開始選擇敵方影響的對象為標的，亦即關鍵的基礎設施，作為攻擊的目標，藉以癱瘓對手，爭取勝利，如今戰爭已被各

種威脅所取代，關鍵基礎設施防護已經演變成一種防禦策略，亦即防護措施屬關鍵者被納入，範疇更加擴大；由於各有不同的環境、背景、年代等因素，因而有不同的主張，且差異頗大。前曾整理一些國家對 CI 的分類，整理如表 1。雖然主張分歧，但卻離不開其訴求的基本功能核心對象。

表 1 國際間一些關鍵基礎設施的範疇

對象	關鍵基礎設施範疇	備考
美國	化學 / 商業設施 / 通訊 / 關鍵製造業 / 水壩 / 國防工業基地 / 緊急服務 / 能源 / 金融服務 / 糧食與農業 / 政府設施 / 醫療保健與公共衛生 / 信息技術 / 核反應器、材料與廢棄物 / 運輸系統 / 水和廢水系統	16
英國	通信 / 緊急服務 / 能量 / 金融服務 / 食物 / 政府 / 健康 / 運輸 / 水	9
法國	糧食 / 水管理 / 健康 / 民眾活動 / 法律活動 / 軍事活動 / 能源 / 金融 / 運輸 / 通訊、技術和傳播 / 工業 / 太空與研究	12
比利時	能源 / 交通 / 金融 / 電子通訊	4
日本	情報通信 / 金融 / 航空 / 鐵道 / 電力 / 天然氣 / 政府 / 醫療 / 水道 / 物流 / 化學 / 信用卡服務 / 石油工業	13
臺灣	能源 / 水資源 / 通訊傳播 / 交通 / 金融 / 緊急救援與醫院 / 政府機關 / 科學園區與工業區	8

基礎設施的威脅

基礎設施的威脅也有多元，災害威脅呈現的多樣性、難預測性與破壞性，對人類生活造成極大的衝擊，其中有很大部分係因設施被摧毀所導致。至於威脅種類各有範圍：

1. 以美國國土安全部國家防護計畫（NIPP, National Infrastructure Protection Plan）的報告，分為五大類，即：極端氣候（Extreme Weather）、意外疏忽（Accidental/Technical Failure）、網絡威脅（Cyber Threats）、恐怖活動（Acts of Terrorism）及疫病（Pandemics）^[4]。
2. 歐盟關鍵基礎設施保護計畫（EPCIP）分人為、技術和自然災害，恐怖主義威脅優先考慮^[5]。
3. 日本將威脅劃分天然與人為災害兩大類，並各細分為 3 及 5 類。除了以人為為主要對象外，且幾乎亦與設施相關。之中 5 種人為災害包括戰爭、管理不當、行政處置欠妥、謠言、警報錯誤及人類能力不足所造成災害等^[6]。

4. 臺灣災害防救法將災害條列 22 種^[7]，主要包括風災、水災、震災等天然災害與人為等因素所造成的災害，加上生物病原、動植物疫病等對象。另依中央氣象局災害的分類，災害的發生原因主要有：天然變異與人為影響。分為天然災害、人為災害、天然人為災害與人為天然災害四類^[8]。
5. 此外亦有對威脅分惡毒力量與惡性力量（Malevolent Forces vs. Malignant Forces）^[9] 成兩大類。其中惡毒力量是威脅物理攻擊和破壞基礎設施正常運行的外部力量；而惡性力量則主要是使基礎設施惡化的自然力量。

對此，曾被整理歸納成六類^[2]，包括：天然災害（Natural Disaster）、人為災害（Manmade Disaster）、網絡威脅（Cyber Threats）、疫病（Pandemics）、老化（Aging）與管理災害（Management Disaster）。

CIP 工作是國土安全整備的一環，故探索 CIP 整備工作內涵不得不從宏觀角度切入，方得窺全貌。目前國際上各國的國土安全的整備工作，並非一步到位，而是歷經一些事件逐步演化而來，並持續進行中。回顧過去經驗，所遭遇的事件及背景，以美國經歷較為豐富，也是切入較深，或稱投入最為積極的國家。其輪廓從國家持續政策以降，包括國家整備系統（National Preparedness System, NPS）、國家關鍵基礎設施防護計畫（National Infrastructure Protection Plan, NIPP）、部門防護計畫、個別機構防護計畫，以及管理、訓練與研發等配套機制進行防護工作，值得探究、學習與介紹，是本篇探索的主要範疇。

整備作業的內涵為何？

國內機制

在行政院網頁國土安全政策會報^[10]中有全貌的介紹。國內係以全災害（All-hazard）的角度推動關鍵基礎設施防護，目前除於災害防救領域、資訊通信安全持續推動之外，有關國土安全部分，在美國 911 之後，行政院已成立了專責單位推動，從政策會報以下，包括應變機制、應變計畫與關鍵基礎設施防護等，亦積極在相關事業機構 / 單位推動，期對政府運作、社會經濟活動與民眾生活確保正常，即使遭遇各種事件、災害下亦能快速應變與恢復運作。由於環境、背景等條件不同，比起一些國家，運作機制相對精簡。

他山之石

就以美國言，國家整備系統（National Preparedness System, NPS）的建立，以國家規劃系統律定將整備計畫，將整個組織參與可執行的策略、程序和戰術方法三層級做有效的推動。整個國土安全推動輪廓以整備系統為核心，包括：預防、防護、減災、應變與復原 5 大領域任務。

關鍵基礎設施防護則有 NIPP 做為指引，運用 NPS 系統機制，以風險管理（Risk Management, RM）架構作為主軸，進行防護工作，從策略、計畫、執行與迄第一線人員應變的操作與指揮，堪稱龐大、豐富且具系統化^[11]。

在美國其 CI 民間企業佔有重要角色（曾被提出比重高達 85%），加上防護工作是龐大工程，單獨由政府推動難竟其功，其總統亦提出指令（Presidential Policy Directive 21, PPD 21）整合公、私部門，中央與地方政府，律定方向，讓所有單位能密切接合，成為夥伴關係，共同防禦可能的衝擊，構成維持國家基本功能的一環，並與其國家持續運作政策銜接。在推動過程 NIPP 2013 亦曾揭示推動核心準則，當然，整備工作必須透徹了解所處環境（威脅）狀況，進而進行防護。

防護整備關鍵工作 3 元素：

設施環境威脅如此多元，所需的防護整備工作到底需要那些？以及作業項目到底有那些？均需要相當的清楚、明確，方能有效推動。一般作業鮮有對此做詳細的探討（僅有簡單的描述或介紹），但在龐大的體系內若未分類則難以管理，遑論防護績效的評估。為改善或克服這些情況，目前也有一些作法，常見於軍事與防衛相關領域，在美國也有類似推動，其過程、

作為值得參考。於 2001 年 911 事件之後，針對防護整備推動提出指導綱要，端出一些關鍵要項，除威脅情境是基礎元素之必須掌握之外，其具體作為就是先調查任務內的任務清單 UTL（Universal Task List），作為參與者應熟悉的工作範圍、項目，也作為參與人員能力培訓推動的基礎；另外針對任務 / 工作清單如何承擔，承擔能力的標準也提出應有相對的處理能力需求，亦即目標能力要項 TCL（Target Capability List），做為整備防護工作的關鍵元素。宛如說文解字一般，將複雜的威脅情境、渾沌的任務工作與能力需求，蒐羅、整理與分類，做為整備防護工作的基礎。因此，威脅情境、總體工作清單與目標能力要項構成防護整備工作的關鍵 3 元素。

威脅情境規劃

於任何緊急或威脅狀況下應處是設施防護整備的基本功，然威脅是開放性的，任何狀況都可能出現，如何有效因應，確實是挑戰，舉世皆然。對此，在美國國土安全部國土安全委員會制定的國家規劃方案定義了國家必須準備的各種事件，目前共列出 15 種情境，參表 2。來面對一系列可能的攻擊、自然災害和其他緊急情況的威脅。雖然它們沒有解決所有潛在的威脅或危害，但它們提供了一個關於國家必須準備的事件範圍和策略框架，也給後續發展預防、防護、減災、應變和復原等整備作的方向，利於整備工作的推動。

總體任務清單（UTL）

為了支持實現國家備災目標，國土安全部、州和地方政府制定了 UTL，定義任務所需 / 可能遭遇的項目。它是在與聯邦、州、地方和部落實體以及國家協會密切協商後開發的，是一種用於協助基層實施根據

表 2 威脅規劃情境項目（美國）

1.簡易核裝置 (Improvised Nuclear Device)	9. 大地震 (Major Earthquake)
2.氣溶膠炭疽 (Aerosol Anthrax)	10. 大颶風 (Major Hurricane)
3.流行性流感 (Pandemic Influenza)	11.放射擴散裝置 (Radiological Dispersal Device)
4.瘟疫 (Plague)	12.簡易爆炸裝置 (Improvised Explosive Device)
5.吸塑劑 (Blister Agent)	13.食物污染 (Food Contamination)
6.有毒工業化學品 (Toxic Industrial Chemical)	14.外來動物疫病 (Foreign Animal Disease)
7.神經毒劑 (Nerve Agent)	15.重大網絡攻擊 (Major Cyber Attack)
8.氯氣筒爆炸 (Chlorine Tank Explosion)	

法令建立的基於能力的規劃過程的工具，UTL 是一份「活的」文件，在付諸實踐時將滾動式發展。UTL 的目的是列出需要執行的「什麼」任務，同時保留確定「誰」應該執行它們以及「如何」執行的靈活性。預計沒有一個機關或機構可以自行執行每一項任務。相反地，各個機關將需要根據自己的特定角色、使命和職能來評估和選擇任務。完全開發後，UTL 將包含有關可能影響任務績效的條件（實體、環境、政治）的通用語言以及評估績效的措施。

UTL 是一個圖書館和國土安全任務區的任務層次結構。基於能力的準備鼓勵靈活性並需要協作。更重要的是，它有助於確保全國的運營規劃人員和計畫在進行規劃、培訓、設備和其他投資時可以使用通用工具和流程，並可以產生可衡量的結果。有關指南如何促進特定國土安全能力發展的更多信息。

UTL 定義了聯邦、州、地方和部落管轄區以及私營部門需要執行那些任務，以預防、防護、應變國家規劃方案中定義的事件並從中恢復。UTL 2.1 版確定了大約 1,600 項獨特的任務。

目標能力要項 (TCL)

UTL 是定義能力要項 TCL 的基礎，這些目標能力是執行預防、防護、應變和復原等國家重大事件的任務所需的。充分發展的 UTL 和 TCL 將為各級單位提供框架，用於評估他們的整體準備成果，同時將資源做有效的配置。

TCL 是在對 UTL 中的關鍵任務進行分析之後開發的。關鍵任務被定義為在重大事件期間必須執行的任

務，以防止發生、減少生命損失或重傷、減輕重大財產損失或對成功完成國土安全任務至關重要。在 UTL 2.1 版中發現的大約 300 項任務已被確定為關鍵項目。TCL 1.1 版提出了 36 項目標功能要項。幾經演化，目前已稱為核心功能，分為 5 大領域，共有 32 項，做為整備工作能力的共通語言。如表 3。

如何進行整備作業？

在美國為例，以國家備災系統協助、指導各級政府、私營和非營利部門建立和維持國家備災的能力目標。國家備災系統包括對規劃、組織、設備、培訓和演習的指導，提供一種全國性、系統化的方法，並隨著時間的推移，建立和維持一個整備活動循環週期，參圖 1。建立和維持整備作業，其主要活動摘述如後：

鑑別和評估風險

做好整備工作首先要了解要準備那些風險以及如何準備這些風險。為了支持、標準化和衡量風險以及管理風險的活動，FEMA 通過其國家風險和能力評估產品開發了一套評估工具。評估結果為利益相關者提供數據，以通過降低風險或發展能力來進行有針對性的準備投資。再者，當綜合考評時，結果還有助於更廣泛地了解國家風險、能力和差距。此類分析每年都會呈現在年度國家整備報告中，作為後續精進的參考依據。

衡量能力需求

國家整備系統強調基於能力需求的規劃，開發和維護應對威脅和危害的知識、技能和能力，而不是為每個潛在的場景做準備。在確定相關風險後，選擇能

表 3 國家整備系統各領域所需核心能力^[11]

預防	保護	減災	應變	復原
		• 規劃 • 公共資訊與預警 • 作業協調		
• 情報分享 • 攔阻與瓦解 • 篩選，搜索和檢測	• 社區抗災能力 • 持續減少漏洞 • 防災韌力 • 辨識威脅和危害		• 基礎設施系統	
• 蒐證和究責	• 擷取控制和身份驗證 • 網路安全 • 實體保護措施 • 風險管理 • 供應鏈的完整性和安全性		• 關鍵運輸 • 降低環境影響 • 傷亡事故管理 • 消防管制 • 後勤與供應鏈 • 眾大保健 • 大規模搜救 • 現場保安與執法 • 作業通信 • 公衛與緊急醫療 • 服務狀況評估	• 經濟復原 • 衛生和社會服務 • 住房 • 自然和文化資源

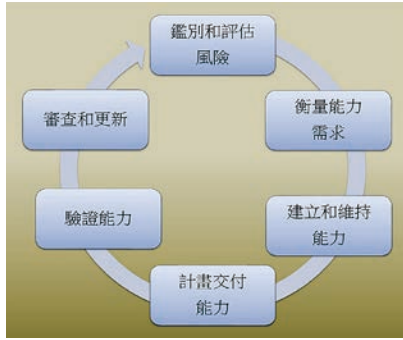


圖 1 國家整備系統 (USA)

力來應對這些風險。某些功能可能已經存在，某些可能需要開發其他方法來解決明顯的差距。如果衡量標準未達到目標，則需要解決差距，以滿足任務所需。

建立和維持能力

各單位面臨優先考慮資源的挑戰，以開發他們最需要的能力，來解決可能遭遇與嚴重後果的威脅。鼓勵夥伴合作，包括州、地方、部落和領地政府，通過規劃、裝備、培訓和其他準備活動來提高他們的能力。

如前所述，能力的發展涉及整個政府和非政府團體的許多利益相關者。為確保成功交付這些能力，FEMA 開發了國家事故管理系統 (National Incident Management System, NIMS)。NIMS 提供必要的「共享詞彙、系統和流程」，以確保預防、防護、減災、應變和復原活動的整備作業。NIMS 提供如何管理提供核心能力的資源，如何提供對這些資源的命令和控制，以及如何傳達有關這些資源活動的信息。NIMS 的主要功能包括事件指揮系統、互助指南、國家資格系統和資源分類。根據 NIMS 指南建立和維持能力可確保該能力能夠與夥伴機構相結合。一些聯邦機構也採用 NIMS 提供準備補助金的依據。

計畫交付能力

國家規劃架構規定了整備活動的協調，提供了一種讓整個團體參與並同步準備工作的方法。每項任務領域都有一個整備架構：預防、保護、減災、應變和復原機制，每一個領域都提供核心能力的策略和原則，利於能力的分享與合作。

驗證能力

在開發和規劃能力之後，透過演習得到驗證。演習提供了一種低風險、具有成本效益的方法來測試計畫、政策和程序，並確定差距、需要改進的領域和最佳實踐。為確保緊急演習系統地進行，FEMA 制定了

一套指導綱要，根據國土安全演習和評估計畫來構建其設計、開發、實施和評估。該方針包括評估能力績效、確定需要改進的領域以及在行動後報告和改進計畫中推薦糾正措施的方法。通過這個過程，各單位可以提高自己的能力和計畫，從而縮小整備的落差。

審查和更新

FEMA 確認定期審查能力、資源和計畫的重要性，並鼓勵整備工作的不斷發展。FEMA 的許多核心文件都提到了持續改進，強調適應不斷變化的威脅形勢和能力概況，以面對未來的可能威脅。

整關鍵基礎設施整備作業如何推動？

前揭的整備工作是國土安全的範疇，而其中涉及 CI 部分，則有更細緻的推動方案，亦即以整備的機制，推動 CI 的防護。

國家基礎設施防護計畫

NIPP 2013：關鍵基礎設施安全和韌性合作，簡稱國家基礎設施防護計畫 NIPP 2013^[4]，指導國家努力管理國家關鍵基礎設施的風險。其內容包括的演化歷程，2013 版提出願景、任務與目標、CI 風險環境、核心原則、協同管理風險、參與管理風險與行動呼籲等項目。

關鍵基礎設施風險的社區範圍廣泛，由所有者和運營商之間的伙伴關係組成；聯邦、州、地方、部落和地區政府；區域實體；非營利組織；和學術界。

採用整合方法管理來自實體和網絡關鍵基礎設施的重大威脅和危害的風險：

- 識別、阻止、檢測、破壞和整備對國家關鍵基礎設施的威脅和危害；
- 減少關鍵資產、系統和網絡的脆弱性；和
- 減輕事故或不利事件對關鍵基礎設施的潛在後果。

這種方法的成功取決於利用關鍵基礎設施社區和相關利益相關者的全方位能力、專業知識和經驗。這需要在夥伴之間有效共享信息，以利決策因應。NIPP 2013 還與國家整備系統保持一致，國家整備在風險、政策和運營環境的背景下，關鍵基礎設施部門和跨部門合作結構提供了一個框架來指導合作夥伴的集體活動。

NIPP 2013 的核心是行動呼籲，它指導關鍵基礎設施社區的協作努力，以在三大活動類別下提高安全性和韌性：建立在夥伴關係的基礎上；創新風險管理（強調資訊分享）；並注重結果。

夥伴關係是 NIPP 的核心

對於建立夥伴關係，特別提出七個核心原則，期以有效的資源調配，達到防護計畫的執行效果。尤其對於維生設施、通訊、能源、交通運輸、水資源管理等跨領域、跨層級管理的設施部門，做為提升安全韌性的參考依據。七個核心原則包括：

- 風險辨識與管理應由關鍵設施相關機構共同協調及整合，使得後續投入的安全防護和提高韌性的資源能有效分配。
- 瞭解跨部門間相依性及風險，有助提高關鍵基礎設施的安全與韌性。
- 相關部會、業者間必須分享關鍵基礎設施的資訊情報，有助於瞭解設施風險與相依性。
- 熟悉不同部門的觀點和優勢並建立夥伴關係，有助於設施安全防護與韌性的執行方案。
- 區域與地方夥伴關係的建立是改善關鍵基礎設施安全和韌性的關鍵。
- 關鍵基礎設施需要考量跨國合作、互助及其他合作協議。
- 資產設施、系統及網絡於規劃設計階段，即應考量安全防護和韌性。

導入風險管理與強化持續營運

NIPP 2013 延續了 NIPP 2006 提出之關鍵基礎設施風險管理架構，在 NIPP 2013 提出之風險管理架構中，強調實體、資通訊以及人員是關鍵基礎設施安全及韌性防護的三大要項。風險管理必須整體考量此三大要項，並透過目標制定、關鍵設施辨識、風險分析、管理行動執行及衡量成效等五步驟進行風險管理。更加強調的是資訊分享，藉由資訊分享串起整個程序與參與單位。關鍵基礎設施風險管理架構，如圖 2。

NIPP 2013，內容強調整體考慮關鍵設施的網絡與實體的安全與韌性，並且要求以企業手段進行風險管理，以達到降低脆弱度與失效影響後果，辨識威脅及破壞，加速應變和復原，確保關鍵基礎設施功能持續運作的重要目的。與最近推動「企業持續營運管理

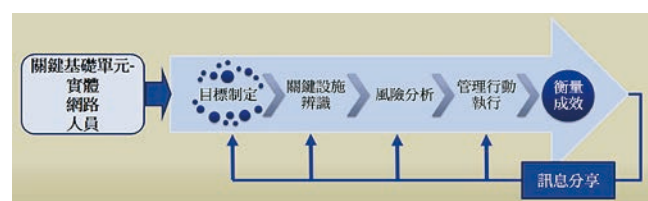


圖 2 關鍵基礎設施風險管理架構 [12]

(Business Continuity Management, BCM)」的目標一致，也與國家持續政策不謀而合。

注重結果與計畫管理

利用效果驗證，根據事件實際應變成果或演習結果，追蹤計畫成效，進而藉以調適精進。整體用計畫管理手段來推動追蹤評估目標實現的進展。

小結

利用風險管理技術，套用事後檢討機制 (After Action Review, AAR) 與計畫管理 (Program Management, PM) 精神，強調夥伴關係，推動關鍵基礎設施防護。

防護計畫階層式推動

防護計畫推動，以交通部門為例，國家關鍵基礎設施龐大，以美國當前共分 16 類，各有相對的防護計畫推動。以交通運輸部分為例，交通部門亦依照規定 (NIPP 2013)，提出防護計畫，亦即 USA TS SSP (Transportation Systems Sector-Specific Plan)。TS SSP 根據國家不同交通系統的獨特運營條件和風險格局，量身定制國家基礎設施保護計畫，NIPP 2013 則提供策略指導。

TS SSP 代表聯邦部門和機構之間的協作努力；州、地方、部落和領地 (SLTT) 政府；非政府組織；以及公共和私人關鍵基礎設施所有者和運營商，以實現共同的目標和優先事項，降低關鍵基礎設施風險。它還反映了部門夥伴關係的成熟以及推動以來該部門在應對不斷變化的風險及運營和政策環境方面的進展。此計畫係一種管理安全和韌性工作的方法，同時提高對該部門政府和行業合作夥伴的能力和資源的有效利用。

TS SSP 定義了政府和私營企業的角色和職責，並提出了目標、優先事項和活動，以管理風險並為國家安全和復原目標做出貢獻。TS SSP 並確定相關活動，包括針對 NIPP 2013 行動呼籲和國家聯合優先事項的具體行動和流程。

選定的活動還考慮了政府政策、國家整備以及國家整備系統的保護、預防、減災、應變和復原任務的核心能力的開發。負責實施活動的官員並啟動衡量方法。以上係從上到下針對管理面向指導或要求作為。在實務上的作為，交通部門所轄的，如軌道系統安全，則依循 TS SSP 為主軸，推動其防護計畫。

至於交通部門更細的任務，如在軌道系統，其安全是服務的首要考慮目標，威脅是軌道安全關鍵的議題，也防護對策之鑰，其中如：法令規章的制定、安全管理

的執行等，這些都是實務上必須克服與完善的工作。加上威脅一直都存在，難以全面掌握，尤其近年來，環境更嚴峻，既有的作為，必須調適、改善與精進。

結論與前瞻

如何在國土安全的領域下推動關鍵基礎設施防護？工程師如何於關鍵基礎設施防護整備中扮演更稱職的角色？美國推動經驗帶來相當大的啟示，其中整備工作的奠基工程，即是前揭的：威脅情境定錘、任務清單與需求能力要項等的啟發、整備系統的籌建與運作、關鍵基礎設施防護計畫推動等，為工程師拓展既有視野的關鍵基礎工作。

整備工作雖然本質涉及範疇實在太廣，而關鍵基礎設施防護亦然，「千里之行，始於足下」，雖然複雜、龐大，但本質上與當前工程師任務卻有相當大的重疊，只要觀念調整一些，目標就在眼前。前揭章節已將整備與 CIP 的輪廓摘述，惟仍有幾個觀點值得提出供參考、分享：

隨環境調適

以工程師的使命言，工程師工作除了傳通統的工程標的規劃、設計、施工與營運所關心的領域外，由於內、外在環境影響日益複雜，也直接或間接對基礎設施造成影響，有些因素是工程師不能忽略的角色。因此，從 CI 的整備工作內涵、範疇、所需的能力，與工程師角色關聯密切且具關鍵。以往任務擔負的傳統視野必須隨環境調適，以不負社會所賦予的使命。

關心整備的核心與運作

美國 NPS 包括 5 大領域，32 項核心能力，勾勒出 CIP 人員所需素養的輪廓。至於 NPS 所涉及 CIP 的部分其實很難分離出，惟可以確認的是，有些工作則非工程師專業不可。從另一角度觀察，這期間的參與者，應有工程背景從事任務，且經常亦可能橫跨多種角色，可能是指揮官、幕僚長、功能主管、領班、或純工程師；亦即，除工程專業技術之外，應考慮到設施全生命週期的所需的整備防護能力，強化在國土安全專業的素養。

技術邁向管理

工程師實際就是國土安全或 CIP 領域的專業人員。工程技術是工程師的基本素養，專業素養為在工作上所需具備的能力。以功能導向的部門，隨著時間

的消逝，工作的薰陶，原本基層的工程師角色也會隨之調整，成為主管、首長等領導者，甚至更高位階。當然，素養也隨著職位調整而變化，涉入的領域，除本身原有專業的部分外，也會（需要）提升來面對並擔負起該有的責任。若為純工程技術服務者，則亦應提升對客戶工作的認知，來強化其專業的形象。故，即使是工程師，在服務過程，「鐵打的衙門、流水的官」，隨著職位變更而調整角色，工程師也是往後國土安全與 CIP 領域的管理者、領導者。

健全機制不能缺席

一個較完整的 CIP 需有適當的配套來約制與推動，美國有其體系，且非一次到位，而是歷經內、外在條件逐漸演化而成，目前仍隨著遭遇狀況與經歷在調適，如資訊安全、疫病等狀況調整。其所耗人力、物力與資源相當浩大，有其背景，其作法足堪參考，但基於內、外的環境、體制、國情等的不同，若擬全面推廣，須考慮從制度面檢討、整合，健全機制，推動方可能事半功倍，且後續機制的優化與推動工程師不能缺席。

參考資料

- 張清祥、廖東成、林祐正 (2020)。關鍵基礎設施防護與工程師之一—專業素養探索。土木水利，47(5)，58-66。doi:10.6653/MoCICHE.202010_47(5).0011
- 張清祥 (2019)。關鍵基礎設施防護與工程師。工程，92(3) (工程與技術)。doi:http://www.cie.org.tw/cms/JournalFiles/10809_chapter08.pdf
- Oliver, D. and Haney, M. (2018). Curriculum development for teaching critical infrastructure protection. *Journal of The Colloquium for Information System Security Education*, 5(2).
- Homeland Security (2013). *National Infrastructure Protection Plan 2013 (NIPP 2013): Partnering for Critical Infrastructure Security and Resilience*. USA.
- Lazari, A. (2017). *ERNICIP Training for Professionals in Critical Infrastructure Protection: From Risk Management to Resilience*. EUR 28657 EN. Luxembourg, Publications Office of the European Union, JRC105204.
- 歐陽嶠 (2005)。防災都市計畫。國立中央大學土木工程學系主編。土木工程防災概論，藝軒圖書出版社。
- 內政部 (2019)。災害防救法。
- 辛在勤 (2015)。天然災害災防問答集。交通部中央氣象局。
- Toffler Associates (2008). *Five critical threats to the infrastructure of the future—Leading infrastructure protection experts discuss strategies for protecting your enterprise*.
- 行政院 (2022)。行政院國土安全政策會報，Retrieved from <https://ohs.ey.gov.tw/>
- Homeland Security (2011). *National Preparedness System*. USA.
- FEMA. (Last updated July 31, 2020), *National Preparedness System*. Federal Emergency Management Agency, USA. Retrieved from <https://www.fema.gov/emergency-managers/national-preparedness/mission-core-capabilities>

