主題企劃

國家關鍵基礎設施防護
——論風險管理與韌性評估

黃俊能*

目　次

壹、前　言

近年來因為氣候變遷，各種災害頻傳，造成世界各國重要之關鍵基礎設施破壞，影響社會經濟等基本活動，也給人民生命財產帶來的巨大損失。臺灣地處地震及颱風頻傳區域，為避免各種災害造成國家關鍵基礎設施（Critical Infrastructures, CIs）損害，更需要進行全面的風險及韌性管理。災害根據起因的不同可分為人為災害及自然災害，人為災害包括戰爭、空難、鐵路事故、恐怖活動等由人為所引起的事件，自然災害包括地震、海嘯、瘟疫疾病、風災等由自然因素導致的災禍，且無法完全避免，而這些自然災害往往會帶給人類社會巨大的衝擊。根據國際災害數據庫（Emergency Events Database, EM-DAT）統計[1]，全球在2000年至2021年，這22年間總共發生了8,952件天災事件，

* 中央警察大學消防學系暨消防科學研究所教授

1 https://www.emdat.be/

2 L. Labaka, J. Hernantes & J. M. Sarriegi, *A Holistic Framework for Building Critical Infrastructure Resilience*, 103 TECHNOLOGICAL FORECASTING AND SOCIAL CHANGE 21-33 (2016).

3 Sydney Perelmutter, M, Top 5 Ransomware Attacks that Shook, X'talk, *available at* https://xtalks.com/top-

期間總死亡人數約136萬人，並且有約42.1億人口受到災害影響。在數據統計中，以亞洲地區發生的天災事件為最多，在這22年間共造成3,516件天災。儘管現今科技的進步日新月異，但是隨著氣候的變遷，各種極端氣候不時發生，人為或自然等不同的因素所發生的災害卻不會因此而停止，而要如何減少災害的發生並降低災害所帶來的傷害，將會是一項很大的挑戰。

臺灣在面對各種天然災害頻傳的極端氣候之下，如何維持國家與社會的穩定發展，將有賴於國家關鍵基礎設施的正常運作。各種天然災害對關鍵基礎設施的影響遠超過其他設施，若是這些關鍵基礎設施遭受破壞，通常對社會的影響更加劇烈，不但將造成人員傷亡與設施的毀損，甚至許多基本的民生需求也都會成為問題。雖然科技日新月異，但是人們仍然無法阻止天然災害的發生，Labaka等學者認為要設計這些關鍵基礎設施完全免於各種災害的破壞是不切實際。既然無法免除天然災害風險的發生，提高關鍵基礎設施之韌性（Resilience），因此是當今風險管理與決策者最重要的目標（Labaka et al., 2016）[2]。

關鍵基礎設施包含交通系統、通訊系統、金融系統、電力系統、供水系統、醫療系統、政府機關等，攸關民生社會與國家治理之資產、系統或服務功能，均可能受損或因相互關聯性系統之癱瘓而無法發揮作用。關鍵基礎設施的安全防護在美國、英國、加拿大等國家皆有成立專責機構，歐盟訂立有歐洲關鍵基礎設施防護計畫（European Programme for Critical Infrastructure Protection, EPCIP），利用行政命令114/08/EC對於歐洲關鍵基礎設施進行調查、辨識和需求加以評估，同時提高它們的防護水準。任何現代化國家，如何預先掌握國家關鍵基礎設施（Critical Infrastructures, CIs）的各項威脅（Threats）評估、韌性（Resilience）評估及脆弱度（Vulnerability）評估，並經由全災害（All Hazards）的風險評估（Risk Assessments）過程，經由風險溝通及不同政府層級之情資與災害資訊分享機制（Information Sharing），採取各項強化關鍵基礎設施韌性或減災、防災等積極的防護作為，是當今各國政府相當重視的國家安全工作。舉凡電力、通訊、網路、水庫、橋樑、鐵路、港口、化學管線等，至重要的財務金融系統、政府運作體系、危機應變與災害防救指揮管制運作（軍隊、警察、消防、海巡等）、與重大關鍵設施之安全維護與持續運作，不論在天然災害或人為恐攻之下，都扮演不可或缺的一環。因此，要如何強化「國家關鍵基礎設施防護」（National Critical Infrastructure Protection, NCIP）應變計畫，並協助地方政府推動、落實國土安全相關工作，亦是國際間對國家安全與國土安全研究領域的重要議題。以下國內外三起例子，可以看出關鍵基礎對國家安全及社會穩定性的重要。

2021年10月，位於美國威斯康辛州全美最大的奶酪製造商施賴伯食品公司（Schreiber Foods），其生產工廠和配送中心遭到惡意勒索軟體網路攻擊

5-ransomware-attacks-that-shook-the-food-industry-3425/ (last visited Dec. 14, 2023).

4 吳依恂，「美國採取網路攻擊戰　阻止伊朗發展核武」，資安人，2012年6月4日，https://

（Ransomware Cyber Attack），連續幾天無法運營。據報導，此次駭客惡意勒索要求約250萬美元的贖金，以恢復該公司的數位系統[3]。威斯康辛州的牛奶分銷商和運輸供應商收到了施賴伯食品公司來信，告知他們該公司的電腦系統無法運作，這導致設施系統無法接受先前已訂的牛奶訂單單據，而運輸商和牛奶分銷商的下游經營者，不得不爭先恐後地尋找牛奶的替代商。雖然尚不清楚施賴伯食品公司否支付了贖金，但該公司已在幾天內成功將其系統恢復到原先的功能。此次網路攻擊造成美國市場奶油奶酪短缺的嚴重後果，而在Google搜索引擎上，「關鍵基礎設施」一詞，在0.61秒有近5.6億條搜尋結果。這表明美國私人企業食品生產供應中心，其資訊關鍵基礎設施在遭受網絡攻擊後，資訊系統是多麼的脆弱。

2010年9月伊朗核電廠受到震網Stuxnet蠕蟲（Stuxnet Worm）電腦病毒感染攻擊其核電廠控制系統SCADA（Supervisor Control and Data Acqusition）軟體[4]，重要的基礎設施竟然受到攻擊，舉世震驚，由於Stuxnet蠕蟲電腦病毒在生產過程中的干擾，被Stuxnet鎖定的伊朗Natanz鈾濃縮工廠，造成幾個月的濃縮鈾減產或零生產。據估計，該地點還遭受過早老化和1,000到2,000個鈾氣體離心機的破壞，此類攻擊可以繞過實體安全和保護設備之外的所有設備，並可能導致人員傷亡，公共安全風險和昂貴的設備損壞。此類攻擊需要高度的電腦工程技術水準，以瞭解實體過程和控制系統組件，並繞過設備防護和安全系統。此類攻擊還需要高度的網路複雜性，才能將該新攻擊編碼為客製化惡意軟體，而在欲攻擊的目標電廠中部署特定網路安全技術無法檢測到惡意軟體，而進行潛伏並置入電腦病毒，有資安專家認定，此事件是由美國策劃，對伊朗核電廠的攻擊。

臺灣國內亦有發生重大關鍵基礎失效的事件，於2017年8月15日16時51分，桃園大潭電廠因天然氣供氣突然中斷，導致大潭電廠6部機組停機，臺灣整體電力供應瞬間減少約11.94%（如圖一），全臺各地因此多處停電，之後台灣電力股份有限公司執行緊急分區輪流停電措施，至晚間21時40分正式解除，惟已造成全臺民眾不便及不安，對國內產業亦產生不少衝擊。當日全臺停電區域包括17縣直轄市、縣（市）之99個鄉鎮（市）區，共計約592萬戶用電受影響，造成部分交通號誌停擺，造成不少交通事故，受損失的廠家數：工業區部分378家、加工出口區部分32家；科學園區除竹南園區、南科園區有部分廠商受緊急分區輪流供電影響，其餘科學園區大致供電正常。民眾因電梯受困及救助案件各縣市消防局受理共計約900件。電力供應穩定，不僅是民生必需，更攸關國家安全，顯示國內電力之高度脆弱度，以及系統設計、操作流程、營運管理等諸多問題。調查專案報告中指出台電公

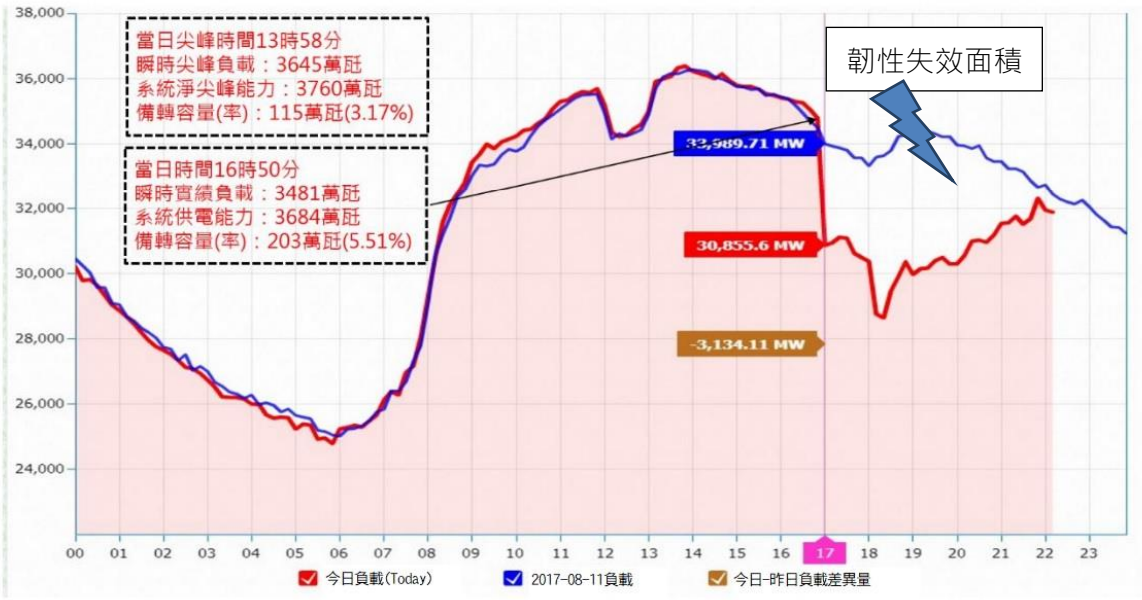
www.informationsecurity.com.tw/article/article_detail.aspx?aid=6830（last visited Dec. 14, 2023）。

5 部分內容摘錄行政院「815停電事故行政調查專案報告」，2017年9月7日。

6 余弦妙，「一張圖秒懂！ 興達電廠這個開關怎樣耽誤549萬戶」，ETtoday財經雲，2022年3月4日，https://finance.ettoday.net/news/2201175（造訪日期：112年12月14日）。

司（供應全國電力）及中油公司（供應全國天然氣）之兩大關鍵基礎設施公司其相依性（Interdependency）之重要性，特別是全臺天然氣電廠關鍵性弱點應加以強化，才能避免事故再度發生，特別是應檢討各大電廠供氣模式及將重要電動閥MOV（Motor-Operated Valve, MOV）改成分別操作模式，及委外廠商所可能造成之人為重大疏失[5]。在2022年3月3日，亦發生興達電廠開關場事故，造成臺灣地區大停電，停電戶數共計達549萬戶，其中南部地區更是此次停電重災區，影響所及包括大林廠、南火、核三廠，民營麥寮、嘉惠等機組皆全部停機，更是波及到臺南「龍崎超高壓變電所」運作，而龍崎超高壓變電所是臺灣三大電力樞紐之一，嚴重影響經濟發展及其他關鍵基礎的持續運作[6、7]。

由以上事件可以看出，無論是天然災害、人為意圖恐攻、電腦病毒、人為疏失等所造成之重大災難，都顯出關鍵基礎設施對一個現代化國家或主要都市會區有重要之影響與關聯性，如何滿足國家安全與永續性社會都市發展的條件，Nelson and Sterling（2012）等學者提出了一些都市關鍵基礎設施高韌性系統（Highly



圖一　臺灣815大斷電時序情形

（圖中右上角為電力韌性失效面積）

資料來源：台電公司

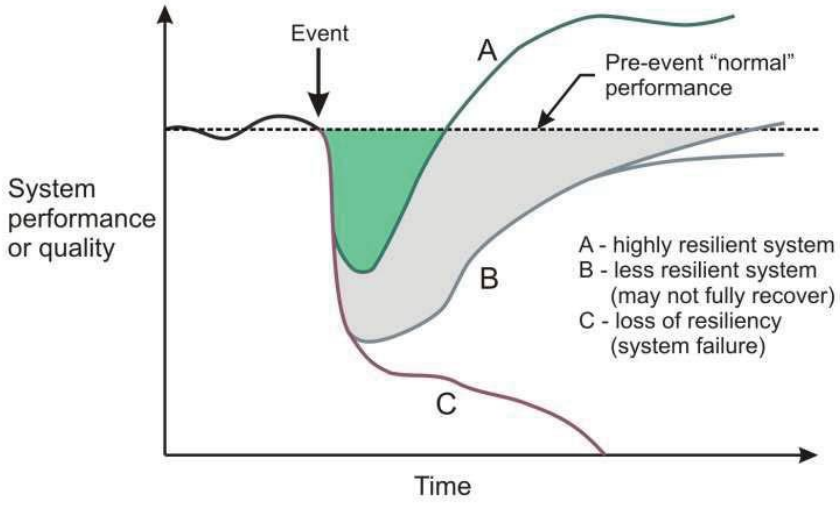
---

7 林家慶、黃俊能，關鍵基礎設施韌性之探討——以台灣輸電設施為例，《災害防救學報》，2020年12月，21期，81-103頁。

8 P. Nelson & R. Sterling, *Sustainability and Resilience of Underground Urban Infrastructure: New Approaches to Metrics and Formalism*, 2012 GEO CONGRESS 3199-208 (2012).

Resilience System）效能設計的概念（Nelson & Sterling, 2012）[8]，而這樣的思維，也應用在所有的關鍵基礎，如圖二所示，當天然災害或人為事件發生時，曲線A為最佳韌性系統設計，在災害事件發生初期，產生系統效能服務品質（System Performance or Quality）的部分失效（尚維持至少60%的服務機能），但在短期復原期程中，其系統效能服務品質可以比災害發生之前還要更佳，以補足解決關鍵基礎設施失效期間所喪失的服務功能；而曲線B會在發生初期，產生劇烈系統效能服務品質的失效（降至約只有30%的系統服務機能），但經一段長期的復原期程後，尚可維持原來系統效能之服務品質；曲線C為最差的韌性系統設計，在發生初期，產生嚴重系統效能服務品質的失能（立即降至15%以下服務機能），最後隨時間慢慢完全失去系統效能服務品質，系統亦告損壞，或因成本過高，或因修復期太長，以至完全無法修復使用，將可能造成全體社會在一段時間內，其設施功能嚴重受到影響，亦無法提供服務或運作。

2001年9月11日早上發生了震驚全世界的911恐攻事件，四架被劫持的飛機撞向了象徵美國經濟、政治和軍事實力的兩座標誌性建築，該襲擊造成2,996人死亡，這是有史以來美國本土遭到的規模最



圖二　效能回應功能概念定義

（Conceptual Definition of Performance Response Functions）

資料來源：Nelson and Sterling, 2012

9 安娜・佩斯（Ana Pais）、塞西莉亞・湯比西（Cecilia Tombesi），「911事件20週年：改變歷史的那天早上分分秒秒都發生了什麼」，BBC NEW中文，2021年9月11日，https://www.bbc.com/zhongwen/trad/world-58511295（造訪日期：112年12月15日）。

大的襲擊[9]，也從此事件後，美國與歐洲等各國先進國家，開始重視關鍵基礎設施防護的議題。文本主要目的是探討近幾年國外先進國家（美國、歐盟地區等）在關鍵基礎設施之沿革發展，包含其法制、組織、風險評估方法等介紹，作者亦針對韌性評估（Resilience Evaluation）部分作較系統性的介紹[10]。

貳、關鍵基礎設施概念界定與分類範圍（美國、歐盟、臺灣）

一、美國關鍵基礎設施之歷史沿革與演變過程

2001年9月11日恐怖攻擊事件發生11天後，賓州州長Tom Ridge被任命為白宮國土安全辦公室首任主任（Director of the Office of Homeland Security）。該辦公室主要任務是監督和協調全面的國家戰略，以保護美國國家免受恐怖主義侵害，並應對未來的任何襲擊，隨著美國國會於2002年11月通過「國土安全法」（Homeland Security Act），經過重整結合了22個聯邦部會，國土安全部（Department of Homeland Security, DHS）正式成立，作為一個獨立的內閣級部門，進一步協調和統一國家國土安全工作，成為美國有史以來，僅次於國防部的第二大部會。針對各項反恐及可能遭受攻擊的基礎設施進行定義及防護，在一份2003年總統辦公室所發布「關鍵基礎設施與重要資產實體防護國家策略」的報告之中（Office of the President, 2003），在911恐怖攻擊事件後第一次提及關鍵基礎設施的定義與清單，然而，事實上，從1980年代起，美國在公共政策在「關鍵基礎設施」名詞的定義上，一直都是在演變，而且常常也一直都含糊不清。

美國是第一個對關鍵基礎設施給出現代（冷戰後）定義的國家[11]，在1996年的總統第13,010號行政命令中指出[12]，國家基礎設施給出了定義如下：

「一重要基礎設施失去功能或遭受破壞時，將使防衛能力及整個國家安全造成嚴重性影響與衝擊。」

而任何關鍵基礎設施遭到攻擊與威脅，將影響到美國的國防或經濟安全，其中包括了8個關鍵基礎部門：電信、電力系統、天然氣和石油儲存和運輸、銀行和金融、交通、供水系統、緊急服務（包括

---

10 本文論述部分參考採用黃俊能教授國科會2021年（三年期計畫）整合型研究計畫，整合型計畫名稱「氣候變遷下國家關鍵基礎設施之韌度評估與災害防治之風險決策分析——氣候變遷下關鍵基礎設施防護與都市韌性及防災之研究（子計畫二）」（計畫編號：MOST 111-2625-M-015-004-）之研究成果資料。

11 Jakub Harašta, *Legally Critical: Defining Critical Infrastructure in an Interconnected World*, 21 INTERNATIONAL JOURNAL OF CRITICAL INFRASTRUCTURE PROTECTION 47, 48 (2018).

12 KATHI ANN BROWN, CRITICAL PATH: A BRIEF HISTORY OF CRITICAL INFRASTRUCTURE PROTECTION IN THE UNITED STATES (2006).

13 Exec. Order No. 13010 61 FR 37347 (1996). 原文：an infrastructure so vital that is its incapacity or destruction would have a debilitating impact on our defense and national security. 作者轉譯。

14 USA Patriot Act of 2001, Sec. 1016 (e), 美國愛國者法案（USA PATRIOT Act）是2001年10月26日由美

醫療、警察、消防和緊急救援）及政府持續運作等[13]。該行政命令提到了針對所述基礎設施的兩種潛在威脅，即實體威脅和對控制關鍵基礎設施的資訊或通信組件通訊射頻，或電子通訊設備等攻擊與威脅。美國第一版的「國家關鍵基礎設施計畫」（The first version of a National Plan for Critical Infrastructure）是出現在2001年的愛國法案（Patriot Act）[14]，該法案對關鍵基礎設施定義如下：

「關鍵基礎設施係指那些實體或非實體之資產，或潛在系統遭受損毀或失效時，會使得國家安全、經濟安全、國民健康或任何形式的安全保護受到重大衝擊。」[15]

國際恐怖主義在90年代中期日益增加的威脅，是聯邦政府重新思索及定義基礎設施，與前80年代時期，側重於基礎設施是否足夠，聯邦機構在90年代日益關注基礎設施保護，這方面的關注，進而導致決策者們重新定義「基礎設施」是否在安全的範圍內。關鍵基礎設施防護（CIP）成為重要議題，主要是克林頓總統在1996年7月15日，簽署一項EO13010總統行政命令（Executive Order），並成立關鍵基礎設施保護總統委員會（the President's Commission on Critical Infrastructure Protection, PCCIP）（Executive Order 13010, 1996: 37347），委員會主席是由Robert Marsh擔任，因此，此法案也被稱為馬殊報告（Marsh Report），行政命令重新定義「基礎設施」為：

「相互依存的網絡和系統之框架，包括可識別之產業、機構（包括人民和程序）、配銷能力等，對於美國的防衛、經濟安全、政府社會各項功能之全面性順利運作不受到影響，提供產品和服務可靠的流通。」[16]

雖然馬殊報告提及「重要基礎設施」對整體國家安全有重大影響，但報告並未僅提及有關「重要基礎設施」的內容，但對「重要」（Vital）一詞卻無明確的定義，而事實上，如何定義出哪些資產（Assets）是所謂的「重要」之「基礎設施」？而需要加以保護，而哪些不是「重要」？如何排序其重要性及並且加以分

國總統喬治・布希簽署頒佈的國會法案（Act of Congress）。正式的名稱為「Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001」，中文意義為「使用適當之手段來阻止或避免恐怖主義以團結並強化美國的法律」。

15 原文：Those systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. 本文作者轉譯。

16 原文：The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of government at all levels, and society as a whole.

17 https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors (last visited Nov. 1, 2023).

18 https://www.fletc.gov/site-page/critical-infrastructure-security-and-resilience-month (last visited Dec. 14,

類？各自「基礎設施」之間又是如何相互影響？是一項非常大的挑戰，也在美國的公共政策辯論上一直存在多年。

美國經歷很長一段時間在定義關鍵基礎設施之意義與內容項目，而整個演變過程也跟著國家的需求（如90代後期重視反恐）不停在變動，根據美國總統政策指令指令21（Presidential Policy Directive 21（PPD-21），美國發展出目前最新16項關鍵基礎設施的部門（Sectors）項目及聯邦主管部門[17]，如下所述（依英文字首排列）：

(一)化工產業部門（Chemical Sector），主管部門：國土安全部。

(二)商業設施部門（Commercial Facilities Sector），主管部門：國土安全部。

(三)通訊系統部門（Communications Sector），主管部門：國土安全部。

(四)關鍵工業製造設施部門（Critical Manufacturing Sector），主管部門：國土安全部。

(五)水壩部門（Dams Sector），主管部門：國土安全部。

(六)國防工業生產基地部門（Defense Industrial Base Sector），主管部門：國土安全部。

(七)緊急救護服務部門（Emergency Services Sector），主管部門：國土安全部。

(八)能源部門（Energy Sector），主管部門：能源部。

(九)財經服務系統部門（Financial Services Sector），主管部門：財政部。

(十)食品與農業部門（Food and Agriculture Sector），主管部門：農業部、衛生與公眾服務部。

(十一)政府設施部門，（Government Facilities Sector）主管部門：國土安全部與總行政管理局。

(十二)公共照護與醫療部門（Healthcare and Public Health Sector），主管部門：衛生與公眾服務部。

(十三)資訊科技系統部門（Information Technology Sector），主管部門：國土安全部。

(十四)核能反應器、核能原料與核廢料部門（Nuclear Reactors, Materials and Waste Sector），主管部門：國土安全部。

(十五)交通運輸系統部門（Transportation Systems Sector），主管部門：國土安全部及交通部。

(十六)水資源與廢水處理系統部門（Water and Wastewater Systems Sector），主管部門：環保署。

美國國土安全總統指令7HSPD-7（Homeland Security Presidential Directive-7, 2003）認定關鍵基礎設施，是根據恐怖攻擊主要的思維（90代後期），以下6項指導性政策綱領（或指導方針）概述如下：

(一)當受到大規模殺傷性武器攻擊會造成災難性的健康影響或造成大規模傷亡。

(二)損害聯邦部門和機構執行基本任

2023)

[19] 原文：Over the last few decades, our Nation has grown increasingly dependent on critical infrastructure,

務以確保公眾健康和安全的能力。

(三)損害國家和地方政府維持秩序和提供最低限度的基本公共服務的能力。

(四)損害私營部門確保經濟有秩序運作和提供基本服務的能力。

(五)透過對經濟影響的關聯性造成其他重要基礎設施和關鍵資源的負面影響。

(六)削弱公眾對國家經濟和政治機構的士氣和信心。

歐巴馬總統上任之後，針對關鍵基礎防護的重要性進行重新宣誓，更強調「韌性」（Resilience）的重要，並在2013年11月份定為「關鍵基礎設施安全性與韌性月份」（Critical Infrastructure Security and Resilience Month）[18]，在演說宣誓文中並再次強調國家安全與韌性的重要，

「在過去的幾十年裡，我們的國家已經變得越來越依賴於關鍵的基礎設施，是我們國家和經濟安全的骨幹與命脈。美國的關鍵基礎設施的複雜和多樣化，結合網絡空間和實體系統，從電廠，橋樑和州際公路，聯邦建築和大量的電力電網散布在我們國家的任何一處。在關鍵基礎設施安全性與韌性月份期間，我們決心對來自國、內外的威脅保持高度警惕，共同努力，進一步確保我們的重要資產，系統和網絡的安全……身為總統，我有將保護關鍵基礎設施的事情列為重要優先……今年早些時候，我簽署了總統政策行政命令（Presidential Policy Directive），以支撐我們的實體防禦和網絡事件強化的法令……」[19]

歐巴馬總統在宣誓文當中強調政府與民間部門之間的夥伴關係與資訊分享的重要，包括業主和經營者，相關有效資訊信息的共享，不僅在防範恐怖份子攻擊外，也包括對極端天氣和氣候變化的影響。宣誓文呼籲美國人民認識國家的關鍵設施與資源保護之重要性，並認知這個月所有適當相關活動和培訓，以強化國家安全和韌性。2018年又重新制定美國的國家關鍵基礎設施防範計畫及安全與韌性挑戰（NATIONAL INFRASTRUCTURE PROTECTION PLAN (NIPP) SECURITY AND RESILIENCE CHALLENGE 2018 FACT SHEET）。

二、歐盟關鍵基礎設施之歷史演變過程

歐盟繼美國之後，也開始致力於保護關鍵基礎設施，歐盟執委會（Commission

---

the backbone of our national and economic security. America's critical infrastructure is complex and diverse, combining systems in both cyberspace and the physical world – from power plants, bridges, and interstates to Federal buildings and the massive electrical grids that power our Nation. During Critical Infrastructure Security and Resilience Month, we resolve to remain vigilant against foreign and domestic threats, and work together to further secure our vital assets, systems, and networks… . As President, I have made protecting critical infrastructure a top priority. Earlier this year, I signed a Presidential Policy Directive to shore up our defenses against physical and cyber incidents.

[20] 歐洲執行委員會簡稱歐洲執委會，是歐洲聯盟下轄的一個超國家機關，為歐盟事實上的內閣。在歐盟政治系統中，歐洲執委會主要工作為負責執行歐洲議會和歐盟理事會的決議、提出歐洲法案和維護《歐洲聯盟條約》，歐洲執委會由27位執委組成，執委須在位於盧森堡市的歐洲法院宣誓就職。

of the European Communities）[20]對於關鍵基礎設施免於遭受恐怖份子攻擊的保護，在美國911恐怖事件發生後，歐盟委員會（European Council）首先於2004年6月召開了一次重要會議，並於同年10月20日對關鍵基礎設施給予了明確的界定，討論決定潛在關鍵基礎設施的判別標準，並列舉已確認關鍵基礎設施的項目，這也是歐盟首次對關鍵基礎設施給明確定義：

「關鍵基礎設施包含那些實體與資訊科技設施、網絡、服務與資產，一旦中斷或被破壞將對歐盟之衛生、安全及人民經濟福祉，導致成員國政府運作功能失效，造成嚴重影響。關鍵基礎設施也擴大到經濟及政府主要服務的許多範圍」[21、22]

又於2005年12月，歐盟司法和內政委員會（Justice and Home Affairs Council）呼籲歐盟委員會就歐洲關鍵基礎設施保護計畫（European Program for Critical Infrastructure Protection, EPCIP）提出建議，以期改善對歐洲關鍵基礎設施的保護[23、24]。委員會通過了通訊（2006）786法案，其中提出了一項在上述計畫背景下「識別和指定歐洲關鍵基礎設施的指令」[25]。又在2008年12月，歐盟理事會通過了理事會行政命令2008/114/EC，「關於歐洲關鍵基礎設施的識別和指定以及改進其保護的必要性評估」[26]，在該行政命令中，對關鍵基礎設施定義為：

「位於成員國的基礎設施，其破壞或干擾至少對兩個成員國產生重大影響」[27、28]

歐盟執委會是歐盟的常設執行機構，負責執行條約及理事會所做出的決策，並須向理事會及歐盟議會提出報告與建議，處理歐盟日常事務。執委會由20人組成，法國、德國、英國、義大利、西班牙各2人，其他歐盟成員國各1人〔歐盟執行委員會——維基百科（wikipedia.org）〕。

21 Commission of the European Communities, Critical Infrastructure Protection in the Fight against Terrorism (Brussels, Oct. 20 2004), COM (2004) 702 final, p. 3, *available at* http://europa.eu.int/comm/justice_home/doc_centre/criminal/terrorism/doc/com_2004_702_en.pdf (last visited Feb. 10, 2009).

22 Critical infrastructure, European Commission, *available at* https://home-affairs.ec.europa.eu/pages/page/critical-infrastructure_en (last visited Dec. 14, 2023).

23 Green Paper on a European program for critical infrastructure protection [2005] COM/2005/0576 final.

24 EPCIP, CIPedia, *available at* https://websites.fraunhofer.de/CIPedia/index.php/EPCIP (last visited Dec. 14, 2023).

25 Communication from the Commission on a European Program for Critical Infrastructure Protection [2006] COM/2006/0786 final.

26 原文：on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

27 原文：infrastructures located in Member States the destruction or disruption of which would have a significant impact on at least two Member States.

28 Council Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection [2008] OJ L 345/75 (NIS Directive).

29 同註13。

30 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on

該行政命令特別將「能源」部門（Energy Sector）和「運輸」部門（Transport Sector）指定為關鍵基礎設施的重要相關部門[29]。隨後，歐盟於2016年8月8日通過網路與資訊安全行政命令（Network and Information Security Directive）（NIS行政命令）重新審視此重要法案[30]。這是歐盟第一個區域範圍內協調網路安全和通報要求的努力成果，目標是重要通訊服務運營廠商和數位服務的提供廠商[31]。在NIS行政命令和NIS 2.0行政命令中，可以觀察到將保護關鍵基礎設施的規範轉變為硬性（強制性）的法律義務（hard legal obligations）。事實上，必須提到的是，由於該法案作為歐盟行政命令的性質，成員國仍有權將其轉化為本國法律[32]。然而，成員國有法律義務如此保護重要關鍵基礎設施，如果成員國不遵守，歐盟可能會對成員國提起法律訴訟[33]。因此，NIS行政命令和NIS 2.0行政命令（第二版本）都有半強制性，歐盟這兩個重要法案，也揭示歐盟對保護關鍵基礎設施規範的重要陳述。

在歐盟執委會在所出版的「歐洲關鍵基礎設施保護計畫綠皮書」（the Green Paper on a European Program for Critical Infrastructure Protection）（簡稱Green Paper on EPCIP）中則將「關鍵資訊基礎設施防護」（CIIP）定義為：

「基礎設施擁有者、操作者、生產者、使用者及調整授權單位，針對如何保持關鍵資訊基礎設施在受到失靈、攻擊與意外情況下能持續運作，使之維持最小限度服務，並將危害及復原降到最小的計畫與作為。」[34]

因此，關鍵資訊基礎設施防護（CIIP）應該被視為跨領域、跨機關、跨公私部門的現象，而非限定在特定的範圍或機關事務，關鍵資訊基礎設施防護應該密切與關鍵基礎設施防護部門或擁有者，從整體防護展望中緊密協調與合作。從這個定義可以看出歐盟對關鍵基礎設施重要性的強調，並著重如何在遭受攻擊後，維持關鍵基礎設施的基本運作，避免損害的

measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 OJ L 333 (NIS 2.0 Directive); NIS Directive (n 14).

31 Jan Neutze, What's Next for EU Cybersecurity after the NIS Agreement?, Microsoft, Jan. 25, 2023, *available at* https://www.microsoft.com/security/blog/2016/01/25/whats-next-for-eu-cybersecurity-after-the-nis-agreement/ (last visited Dec. 14, 2023).

32 Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C 326 art 288 (3) (TFEU); Kieran Bradley, *Legislating in the European Union*, *in* EUROPEAN UNION LAW 104 (Catherine Barnard & Steve Peters eds., 3d ed. 2020).

33 TFEU art 260 (3); Bradley, *id*. at 105.

34 Commission of the European Communities, The Green Paper on a European Program for Critical Infrastructure Protection (Brussels, Nov. 17, 2005), COM (2005) 576 Final, pp. 19, 24, *available at* http://www.libertysecurity.org/IMG/PDF/EC_-_Green_Paper_on_CI_-_17.11.2005.pdf (Nov. 2, 2009).

35 EUROPEAN COMMISSION, COM (2020) 829 final. 2020/0365 (COD). Proposal for a. DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the resilience of critical entities, Brussels,

擴大。

關於歐盟關鍵基礎設施的分類，歐盟執委會於2020年COM (2020) 829 final文件中確認了關鍵基礎設施包含下列10項[35]：

(一)能源系統（Energy）：此部分包含5項，電力（Electricity）、石油（Oil）、天然氣（Gas）、氫氣（Hydrogen）、區域供熱和製冷之重要場站（District heating and cooling）等，以上能源供應都包括生產、提煉、裂解與儲存，也包含油管、電廠、電力、電塔、開關場（變電站）、天然氣與石油的儲存（LNG system operators）、轉送與分配等場站（Transmission and Distribution System Operators），及各電力、石油及天然氣的工業控制系統SCADA（Supervisory Control and Data Acquisition）。

(二)運輸系統（Transport）：此部分包含4項，空中運輸（Air）、鐵路運輸（Rail）、道路運輸（Road）、水路運輸（Water），包含內陸及海洋與近海航運。

(三)銀行系統（Banking）：包含相關銀行機關之系統（存款、提款ATM、借貸等）。

(四)財經市場與基礎設施系統（Financial market infrastructures）：包含薪資服務與薪資結構、政府財政分配系統。

(五)醫療健康系統（Health）：包含醫療及醫院照護、醫藥、血清、疫苗生產與製藥配送、生化實驗室及生化代理事務。

(六)飲用水系統（Drinking Water）：包含飲用水儲備、水質監控、水量把關與控制。

(七)廢水處理系統（Waste Water）：包含都市與工業廢水收集、處理與淨化。

(八)數位化資通訊系統（Digital infrastructure）：包含網路交換系統（Internet Exchange）、網域提供商系統（DNS Service Providers）、資訊系統與網路防護、網際網路、雲端運算服務供應商（Providers of Cloud computing service）、固定通訊系統儲備、機動通訊系統儲備、無線通訊及導航、衛星通訊及廣播。

(九)公共行政系統（Public administration）：包含各會員國政府持續運作功能、軍隊、行政勤務、警消緊急勤務、郵政及快遞勤務。

(十)太空系統（Space）：包含各會員國地面與太空衛星基礎設施及研究項目系統。

此文件有別於「歐洲關鍵基礎設施保護計畫綠皮書」所提出的11項，其中包含糧食（糧食儲備、糧食安全與防護之確保）、公共及法治秩序與安全（如維持公共及法治秩序、防護及安全、拘留及審判行政）、化學及核能工業（包含生產及儲存、化學及核能製品的過程、如化學製品等危險物品的輸送管道）等項目有所區別與修正。

三、我國關鍵基礎設施之定義與分類

我國關鍵基礎設施之發展，主要是參考美國及其他各國發展，經由學界進行「行政院國家關鍵基礎設施防護計畫專業

16.12.2020, ANNEX (Sectors, subsectors and types of entities).

[36] 分類原係行政院國土安全辦公室委託產、官、學界進行「行政院國家關鍵基礎設施防護計畫專業服務委外研究」（自2009年12月至2013年9月三年期），參考各國理論與實務運作經驗，並結合我國國

服務委外研究」[36]，以全災害預防及防護之觀念[37]，並依據2013年國土安全政策會報及國土安全業務會議決議，規劃國家關鍵基礎設施安全防護事項，強化國家關鍵基礎設施安全防護功能，維護國家安全，確保人民生活利益等目標，訂定「國家關鍵基礎設施安全防護指導綱要」。（行政院國土安全辦公室，2018）針對國家關鍵基礎設施之定義如下[38]：

「國家關鍵基礎設施（Critical Infrastructure, CI）：係指公有或私有、實體或虛擬的資產、生產系統以及網絡，因人為破壞或自然災害受損，進而影響政府及社會功能運作，造成人民傷亡或財產損失，引起經濟衰退，以及造成環境改變或其他足使國家安全或利益遭受損害之虞者。」

我國關鍵基礎設施目前擬定出8個主領域項目，包括能源、水資源、資通訊、交通、銀行與金融、緊急救援與醫院、中央政府及主要都會、高科技園區等，有別於關鍵資訊基礎設施（Critical Information Infrastructure, CII）係指涉及核心業務運作，為支持關鍵基礎設施持續營運所需之重要資訊系統或調度、控制系統（Supervisory Control and Data Acquisition, SCADA），亦屬關鍵基礎設施之重要元件統一納管國土安全項目。在CI分類部分，我國國家關鍵基礎設施採三層架構分類，第一層為主領域（Sector），如上所述分為8個主領域，第二層為次領域（Sub-sector），第三層為次領域下的重要功能設施與系統，如表一所示：

表一　我國國家關鍵基礎設施領域分類[39]

領　域	次領域	重要業務功能	主管機關
能　源	電　力	穩定提供發電、輸電、配電、調度、監控等供電服務之設施或系統。	經濟部
	石　油	穩定供應油品，及帶動石化相關工業發展之設施或系統。	經濟部
	天然氣	提供輸儲、接收、遮斷等設備，穩定供應天然氣之各項設施及控制系統。	經濟部
水資源	供　水	提供質佳、量足、穩定供水之水源、水庫、淨水、供水、水質保護等設施。	經濟部（地方政府）

情需要，經與學者專家及政府官員討論後多次修正後核定，研究團隊成員，包括張中勇、黃俊能、簡賢文、劉建浩、呂世通、郭燿禎等學者參與國土安全辦公室委託之三年期研究與規劃。

37 全災害係指天然災害、資安攻擊、意外事件、人為攻擊、非傳統攻擊及軍事威脅等災害，係關鍵基礎設施辨識風險與威脅的主要依據。

38 資料來源：「國家關鍵基礎設施安全防護指導綱要」，行政院國土安全辦公室資訊，https://www.ey.gov.tw/Page/66A952CE4ACACF01（造訪日期：2018年12月30日）。

39 同前註，2018年7月30日版本（造訪日期：2019年12月30日）。

40 S. Paula, Regional Public-Private Partnerships – Addressing Critical Infrastructure Interdependencies and Homeland Security Preparedness, Presentation at the 2004 PNWER Annual Summit, Victoria BC. July 14.

領　域	次領域	重要業務功能	主管機關
通訊傳播	通　訊	支持通訊服務之重要設施及系統，例如：市內 / 長途 / 國際通信、行動通信、衛星通信及數據通信等。	國家通訊傳播委員會
	傳　播	支持傳播服務之重要設施及系統，例如：無線廣播電視及有線廣播電視。	國家通訊傳播委員會
交　通	陸　運	提供大眾陸上運輸服務，例如：公路運輸系統、鐵路運輸系統（含一般鐵路、高速鐵路、大眾捷運）。	交通部（地方政府）
	海　運	提供航運及商港、工業港、漁港之相關系統設施。	交通部、經濟部、農委會
	空　運	提供航空營運管理及航空運輸關聯服務。	交通部、國防部
	氣　象	提供氣象觀測、氣象預報、地震測報、海象測報及相關資訊發布等相關服務。	交通部
金　融	銀　行	1. 財金公司之跨行交易設備系統主要係提供新臺幣跨行通匯之資金調撥服務，以及ATM之提款、轉帳及餘額查詢等跨行交易服務。 2. 中華郵政資訊系統。	金融監督管理委員會、交通部
	證　券	執行全國證券、期貨市場交易及結算、交割。	金融監督管理委員會
	金融支付	支持我國支付清算系統之相關作業系統，例如：同業資金調撥清算作業系統、票據交換結算系統、中央銀行中央公債及國庫券電子連線投標系統等。	中央銀行
緊急救援與醫院	醫療照護	提供醫療照護之相關系統及醫療院所。	衛生福利部
	疾病管制	提供傳染病疫情監測與預警、傳染病防治與應變、傳染病邊境檢疫，以及生物病原檢驗與技術研發等相關系統及設施。	
	緊急應變體系	災害緊急應變中心、消防救災救護系統、相關重要設施與救護設備等。	內政部、海洋委員會、（地方政府）
政府機關	機關場所與設施	支持政府核心業務運作及重要領導權與人員辦公之重要設施與場所。	中央政府機關（地方政府機關）
	資通訊系統	支持政府核心業務運作之重要資通訊系統。	
科學園區與工業區	科學工業與生醫園區	科學園區、生物醫學園區等。	科技部

領　域	次領域	重要業務功能	主管機關
	軟體園區與工業區	軟體園區、工業區、科技工業區等。	經濟部

資料來源：行政院「國家關鍵基礎設施安全防護指導綱要」

參、關鍵基礎設施風險管理與韌性評估

一、關鍵基礎相依性概念

國際學者在探討關鍵基礎風險管理與評估時，有一重要的觀念就是相依性（Interdependency），國家關鍵基礎設施之功能失效，將損及大眾及攸關國家經濟與安全；且任何一項關鍵基礎設施之中斷，將嚴重影響另一項關鍵基礎設施及重要都會區的運作，甚至再影響回到原來之關鍵基礎設施，此現象稱之為關鍵基礎相依性，一旦當中任何一項受到破壞或威脅，則影響程度將是全面性、連鎖性及加倍性地毀損，其中相依性是研究關鍵基礎重要的課題，也就是某一關鍵基礎失效時，會影響到哪些關鍵基礎亦跟著失效，因此，到底哪些關鍵基礎設施才是一個國家至關重要的關鍵基礎設施？而其又如何影響到其他的關鍵基礎設施？關鍵基礎設施彼此間存在高度相互依賴關聯性，是研究關鍵基礎設施相當重要的觀念，依據學者S. Paula（2004）認為關鍵基礎設施的相互關聯性可以劃分成4個主要形式，分別如下[40、41]：

(一)實體相依性（Physical Interdependencies）

一項基礎設施所產生的產品或服務為其他項基礎設施所運用或使用的關聯性，例如道路橋梁等運輸系統就提供給農業食物或郵政業務或化工產品等項目運送所需，甚至緊急救護也不可或缺。

(二)資訊網絡相依性（Cyber Interdependencies）

各項基礎設施彼此間電子資訊的連結關係，亦即各項基礎設施均需要透過資訊科技或通訊系統傳達訊息來發揮運作的功能，特別是郵政船務或是銀行金融這類的基礎設施更是受資訊科技及通訊系統的連結所影響。

(三)地理相依性（Geographic Interdependencies）

各項基礎設施共通性之陸、海、空連絡運輸系統，例如鐵路、捷運、高速公路、機場、海港等有地理位置相關之關聯性。

(四)其他相依性（Other Interdependencies）

以上無法歸類者，如金融市場（網路安全等）。

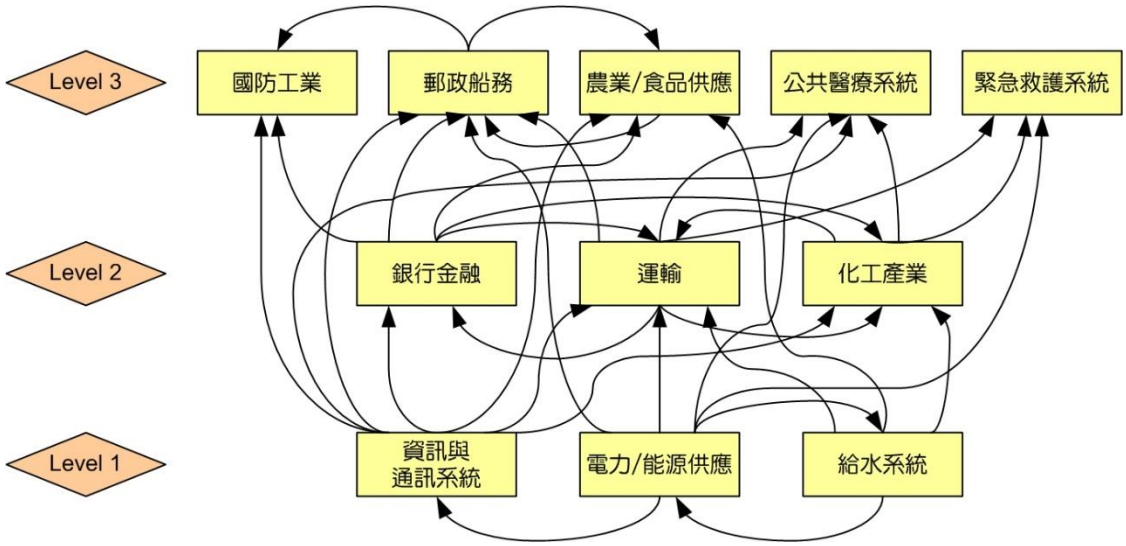
美國關鍵基礎設施研究學者Ted Lewis，將關鍵基礎設施之相依性繪製成下圖（圖三），圖中分為三個層級，Lewis認為第一層級（Level 1）最為重要，一旦發生破壞或中斷，將影響國家安全、國家經濟或區域性生活機能最為嚴重，包含電力/能源供應系統、資訊與通訊系統、給水系統，其次為第二層級（Level 2），包含銀行與金融系統、人及物品之運輸系統、化工產業，最後影響較不嚴重者為第三層級（Level 3），Lewis

41 黃俊能，氣候變遷下國家關鍵基礎設施之韌性評估與災害防治之風險決策分析——氣候變遷下關鍵基礎設施防護與都市韌性及防災之研究（子計畫二）三年期計畫(I)(II)，子計畫主持人，2022-2023。NSC MOST 108-2625-M-015-007-。

42 T. G. Lewis, Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation 57 (2006).

雖提出此三層級重要層級圖，但在其書中並無實證數據或方法，說明其分出此層級圖之作法[42、43]。

就目前來說，現今大多數國家的災難管理系統已經擁有關鍵基礎設施系統資料，但是關鍵基礎設施相依性資料卻是十分缺乏的，相關的分析與紀錄很少[44]。但是關鍵基礎設施相依性資料卻是必要存在的，例如：美國911事件營救行動時，美國重要電信公司Verizon Communications的基地台及光纖也因為世貿大樓倒塌，地下室造成淹水，而把重要通訊設施全部摧毀，所有通訊系統及華爾街股票交易系統亦完全無法運作，因為缺乏用來預測災難發生後對某些關鍵基礎設施產生的傷害，及隨後基礎設施受影響損毀之通訊與財務系統等綜合資料庫，使得救災工作困難重重[45]。由此可見，關鍵基礎設施不但是一



圖三　關鍵基礎設施相依性層次與關係示意圖（美國爲例）

資料來源：T. G. Lewis, 2006: 57

43 黃俊能、郭燿禎，關鍵基礎設施風險評估機制之建立——以台北車站重要交通場站為例，《前瞻科技與管理》，2013年5月，3卷1期，1-19頁。

44 D. Laefer, A. Koss & A. Pradhan, *The Need for Baseline Data Characteristics for GIS-Based Disaster Management Systems*, 132(3) JOURNAL OF URBAN PLANNING AND DEVELOPMENT, ASCE 115-19.

45 A. Pradhan, D. Laefer & W. Rasdorf, *Infrastructure Management Information System Framework Requirements for Disasters*, 21(2) JOURNAL OF COMPUTING IN CIVIL ENGINEERING, ASCE 90-101 (2007). .

46 R. Fisher & J. Peerenboom, Interdependencies: A DOE Perspective, 16th Annual Security Technology Symposium & Exhibition, Office of Critical Infrastructure Protection, June 28, 2000, Williamsburg,

項影響國家及都市安全、經濟安全與發展以及都會區人民生活的重大基本條件，而其所形成的交互關聯複雜體系，更是提供國家長治久安所必須。一旦這個複雜體系遭受損害時，整個國土境內及都市必產生一發不可收拾的連鎖反應（Chain Reaction）。

因此，各國均相當重視關鍵基礎設施的防護工作，紛紛投入相當多的資源與努力來思考與積極進行其應有的管理策略與相關法律規範的修訂。文獻中亦提及在如此高度相互依賴關聯性的情境，僅花大量的經費及時間在實體的防護上，無法滿足並解決易受損的公共安全及國家安全。如前所述，關鍵基礎設施為國家重要的資產，用以連續地產生或輸送重要實體物或服務[46]，這些關鍵基礎設施不局限於運輸、電信、電力系統，還包括氣體、油的儲存、運輸及給水系統和廢水處理系統等。關鍵基礎設施包括電力、電信（含軍警專用電信）、自來水、排水、污水、輸油、輸氣（瓦斯）、有線電視、路燈、下水道、共同管道、廢棄物、水利設施、銀行、學校等，各項供給都市順利運作的設施，若任何一項設施無法提供穩定運作，則國家、社會、都市區域等將陷入大小不一之災難。

二、風險管理與韌性（回復力）評估

(一)美國關鍵基礎設施防護計畫（NIPP）風險管理架構

2009年美國國土安全部公布最新「國家關鍵基礎設施防護計畫」（National Infrastructure Protection Plan, NIPP）報告是國際間最常引用的風險管理架構，美國每年投入大量的資源和資金進行關鍵基礎設施風險評估，並將重要的納入為國家安全的一項重大計畫，制定出關鍵基礎設施的風險管理架構，致力於關鍵基礎設施的災害預防與加強管理，降低災害的損失影響，而使關鍵基礎設施防護的發展程度相較於其他國家成熟。美國亦於2003年12月頒布國家安全第7號總統指令，強制聯邦政府及地方機構建立關鍵基礎設施防護的國家政策，建立和管理完整的國家關鍵基礎設施的資產、系統、網路及功能資訊資料庫，並由國土安全部、各個產業主管機構、維安夥伴共同承擔實施NIPP風險管理架構之責任。

此外，美國國土安全部門必須訂定準則、發展工具和執行系統性分析，以援助各個產業主管機關和維安夥伴進行關鍵基礎設施之防護。NIPP的目的是辨識資產、系統、網路及功能，辨識潛在威脅，辨識脆弱性因子、評估脆弱性與衡量風險，決定防護措施和優先順序，強化參與夥伴間或內部資訊共享機制、資訊防護與恢復，並且要求聯邦機構、州政府和組織、區域政府和組織、地方和部落政府和組織，以及各別關鍵基礎設施的擁有者與相關營運團體一同參與。圖四是美國NIPP的風險管理架構，該架構是一個階段式的執行步驟，採用系統性的方式來解決關鍵基礎設施的風險危害，有利於及時

Virginia.

47 黃俊能、郭燿禎，註13文。

48 A. Mottahedi, F. Sereshki, M. Ataei, A. N. Qarahasanlou & A. Barabadi, *Resilience Estimation of Critical*

作出適當決策降低風險，且表示程序的執行應該得持續地循環檢視，才能因應風險的變化，完善的做好關鍵基礎設施的安全防護。NIPP的風險管理架構是目前國際間發展最為完善的關鍵基礎設施防護架構，此風險管理架構的程序步驟如下[47]：

1.設立安全目標：定義一個共同的風險管理結果之目標。

2.辨識資產、系統與網絡：建立資產、系統與網絡的清單，並考量關鍵基礎設施的特性蒐集和調整風險管理所需資訊。

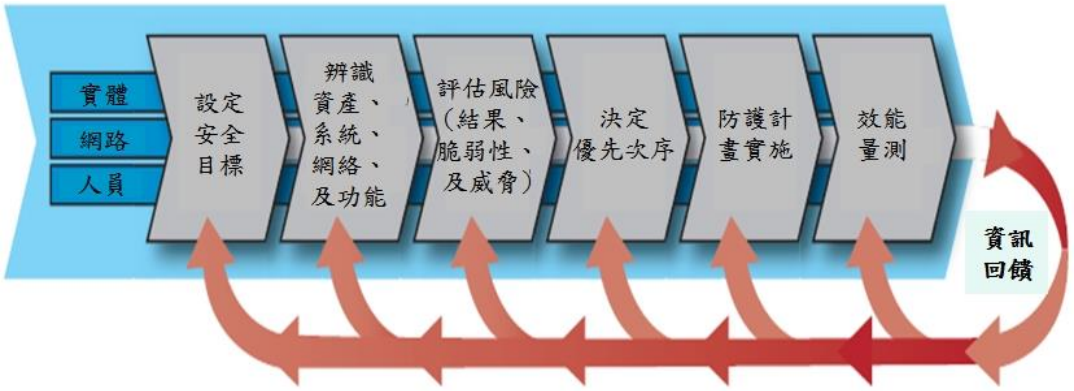
3.評估風險：針對辨識出的資產、系統與網絡進行風險的評估，包括已知與未知的各種潛在威脅，以及本身的脆弱度。

4.決定優先次序：整合比較風險評估的結果，排定關鍵基礎設施的推動及投入的最佳排序。

5.防護計畫實施：選擇適當的行動和防護計畫，集中資源的利用且妥善的管理及分配投入的資源。

6.效能量測：為達到最初設定的目標，透過績效的方式來加以檢視並持續的改善。

國內雖參考各國經驗，對關鍵基礎設施主部門、次部門、重要元件設施及部門主管機關之範圍已有所律定，但至今對於各國分析方法論部分，並無一套體系的深入研究與分析，各主管機關亦無專責單位或人員負責進行較為量化或質化之研究探討。回顧近幾年國外相關文獻與技術報告，愈來愈多學者將風險管理與韌性評估相關研究導入關鍵基礎設施防護之分析中，而風險管理的觀點，主要是對各項內、外因子作全面性風險評估，再進行風險處置，透過持續性及系統性風險資訊收集及分析而建立完善防救災體系。而韌性則是針對各關鍵基礎設施的軟硬體設施，



圖四　美國NIPP風險管理架構

資料來源：NIPP, 2009

Infrastructure Systems: Application of Expert Judgment, 215 RELIABILITY ENGINEERING & SYSTEM SAFETY

當風險發生前後如何減緩（Mitigation）、準備（Preparation）、應變（Response）及復原（Recovery）關鍵基礎設施的功能。本文作者與國科會整合型研究團隊成員，多年來進行相關關鍵基礎設施方法論之研究探討，針對全世界各先進國家所研發之各種關鍵基礎設施韌性評估方式及風險管理作法進行回顧，並已建構出屬於臺灣關鍵基礎設施之韌性評估方法及災後管理機制架構，及各類型關鍵基礎設施不同方法評估方式，以量化及質化等方式，將關鍵基礎設施之脆弱度、危害性與風險因子加以分析，提供各部會參考。根據各種風險其危害程度對關鑑基礎設施的影響，建立災前預防、災害承受、其評估方法論與工具如表二所示。

(二)韌性（回復力）評估

「韌性」這個新興的概念在管理工程系統方面的應用顯著增加（Mottahedi et al., 2021），關於關鍵基礎設施的韌性與風險評估，過往的研究者從不同的角度切入、探討這個主題[48]。Hosseini及Barker（2016）等學者對韌性（Resilience）或稱回復力之說明如下：這個詞最初起源於拉丁語「復活」（Resiliere），意思是「反彈」（Bounce Back）。韌性意味著一個實體（Entity）或一套系統（System）在經歷破壞事件後，一個實體或一套系統發生重要災難破壞後，其恢復正常狀態的能力（Ability）。

Holling（2002）發表論文「生態系

表二　關鍵基礎設施常見風險評估方法

No.	方　法	No.	方　法
1	代理人基（Agent-Base）基礎設施建模與模擬。	8	危害性操作分析。
2	CARVER2模型（關鍵性、可接受性、可回收性、脆弱度等）。	9	相依性能源基礎設施模擬系統。
3	關鍵基礎設施相依性整合工具。	10	網路安全風險評估模型。
4	相依性代理人關鍵基礎設施模擬。	11	開放式地理空間訊資訊關鍵設施防護行動。
5	財政系統基礎設施風險評估模式。	12	地理資訊系統風險地圖。
6	水資源公共設施模擬環境評估。	13	交通路網要徑分析與地理資訊系統。
7	失誤樹分析。	14	都市公共設施系統影響分析。

資料來源：本文作者整理

107849 (2021).

[49] L. H. GUNDERSON & C. S. HOLLING, PANARCHY: UNDERSTANDING TRANSFORMATIONS IN SYSTEMS OF HUMANS AND NATURE (2002).

統的韌性與穩定性」（Resilience and Stability of Ecological Systems）中對（Resilience）一詞進行了系統性的詮釋[49]：

韌性Resilience：「決定一個系統內在關係的持久性，同時也是一種能力的衡量，即這些系統吸收狀態變數（State Variables）、驅動變數（Driving Variables）和參數變化並且仍然維持自身的能力。Resilience是系統的屬性，其結果是系統的持久性或系統滅絕的可能性。」

韌性其定義適用於生態學（Ecology）、材料科學（Materials Science）、心理學（Psychology）、經濟學（Economics）、工程學（Engineering）等多個領域[50]。之後韌性被廣泛定義為：「回到最初狀態」（提供最初服務水準）[51]。McAslan學者認為韌性（Resilience）學術概念最早起於材料學領域[52]。描述木材特性以解釋為什麼有些類型的木材能夠適應突然而劇烈的荷載而不斷裂。後來幾百年間不同學者在不同領域都不斷發展了不同的概念，其基本含義變化不大，都是強調物體抵抗外力衝擊而不被折斷的能力。不同學科領域對韌性有不同學術概念的定義，自「韌性」學術概念提出以來，國際上眾多學者就開始在不同領域內不斷詮釋與發展此概念，其定義不下數百個。除此之外，還有多位學者發表論文對韌性學術概念本身的發展歷程進行了文獻綜述，例如前述Hosseini等學者列舉了跨學科關於韌性的學術定義。其他不同學者，如Allenby & Fink對韌性的定義[53、54]：

「系統在面對內外變化時保持其功能結構的能力以及在必須情況下平穩退化的能力。」

「關鍵基礎設施安全合作夥伴」（Infrastructure Security Partnership）描述「災害韌性」（Disaster Rresilience）定義如下[55]：

「阻止或抵禦，如恐怖襲擊等重大而多重危險之威脅事件，並且恢復與重建

---

50 原文：The word resilience has been originally originated from the Latin word “resiliere” which means to “bounce back.” The common use of resilience word implies the ability of an entity or system to return to normal condition after the occurrence of an event that disrupts its state. Such abroad definition applies to such diverse fields as ecology, materials science, psychology, economics, and engineering.

51 J. M. Kendra & T. Wachtendorf, *Elements of Resilience After the World Trade Center Disaster: Reconstituting New York City's Emergency Operations Centre*, 27(1) DISASTERS 37-53 (2003).

52 A. MCASLAN, THE CONCEPT OF RESILIENCE: UNDERSTANDING ITS ORIGINS, MEANING AND UTILITY 1-13 (2010).

53 B. Allenby & J. Fink, *Social and Ecological Resilience: Toward Inherently Secure and Resilient Societies*, 24(3) SCIENCE 2000 347-64 (2000).

54 林家慶、黃俊能，註7文。

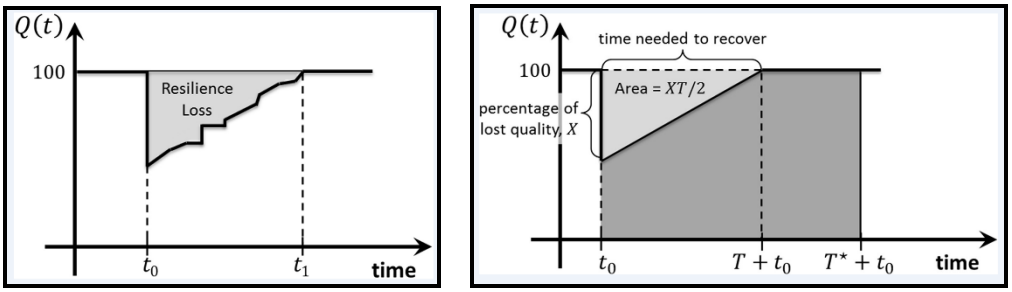
55 The infrastructure Security Partnership (TISP), Regional Disaster Resilience: A Guide for Developing on Action Plan, Reston, VA: American Society of Civil Engineers; 2006 The infrastructure Security Partnership.

56 林家慶、黃俊能，註7文。

57 Hosseini Seyedmohsen, Barker Kash & Ramirez-Marquez, *A Review of Definitions and Measures of System*

關鍵基礎設施服務使得公共安全與健康損失最小的能力。」

圖五為一般量測方法中之韌性三角（Resilience Triangle）之較簡易量測方法示意圖，三角形灰色區域即是關鍵基礎設施失效所造成之韌性損失（Resilience Loss），面積愈大，代表該關鍵基礎設施失效情況愈嚴重，圖右邊為實際發生情況，左圖為簡易三角形之計算，三角形面積是由服務品質失效及失效時間軸之乘積的二分之一（但並非所有關鍵基礎設施失效的情況都如此）。

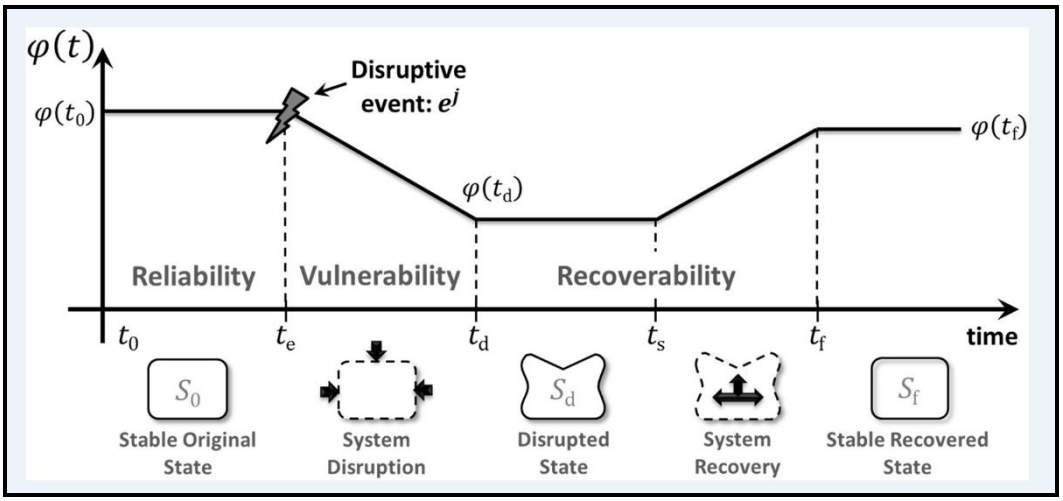


圖五　韌性（resilience）評估——韌性三角

資料來源：Hosseini, 2013

圖六所示，代表事件（Event）發生前後，依著時間推移，可以區分幾個階段，在事件前（t_0~t_e）表示關鍵基礎設施設施系統非常穩定提供可靠的服務（S_0）（Reliability），此時段代表可靠度期間（Reliability），意外災害事件（Disruptive Event）發生後，產生關鍵基礎設施系統服務下降，一直到關鍵基礎設施系統提供服務最低期間（t_e~t_d），此時段代表系統的脆弱度程度期間（Vulnerability），從關鍵基礎設施系統最低服務一直到開始漸漸修復，完全達到原先服務品質，這段期間（t_d~t_f），代表關鍵基礎設施系統處於復原期間（Recoverability）[56]。

Resilience, 145 RELIABILITY ENGINEERING AND SYSTEM SAFETY 47-61 (2016).



圖六　韌性（resilience）評估——可靠度、脆弱度、回復度示意圖

資料來源：Hosseini, 2013[57]

肆、結論與建議

一、結　論

從美國與歐盟的發展，發現重要的共同性，美國作為保護關鍵基礎設施最古老的架構，採取了非常詳細但有針對性的方法，其所給出的定義，在過去二十年中可能保持不變，但是這樣的措辭，允許美國擁有16個指定的關鍵基礎設施部門（Sectors），每個基礎設施都有許多次部門（Sub-Sectors）。歐盟即使提出了修訂NIS行政命令的提案，歐盟關鍵基礎設施架構，就沒有涵蓋與美國架構相同數量的部門，並保持各會員國的自主權。

其次，值得一提的是，美國和歐盟架構中對關鍵基礎設施的定義，都強調國家安全或經濟安全，其主要方法防禦。另一方面，歐盟關鍵基礎設施架構的重點仍然是「關鍵、社會和經濟活動」為主。因此，歐盟似乎更傾向於經濟成長方式，而美國與其他國家，如日本和中國等立場，則是以國防或防衛為基礎。

另一點很明顯，美國和歐盟的關鍵基礎設施私部門所擁有與經營的比例要比我國大得很多，因此，為歐美國家必須考慮私部門經營利潤追求目標，與國家安全的雙重目的考量，甚至有助於將服務或基礎設施指定為關鍵或必要性的辯論。相反，就我國而言，政府是大部分關鍵基礎設施的擁有與經營者，如台電公司、中油公司、桃園國際機場等，政府都是唯一或是最大股東，因此，我國關鍵基礎設施防護作法與歐美的作法大不相同，例如美國核電廠防護，是由持槍保全人員負責，而國內則由警政署保安警察負責。國內保全

[58] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (24 June 2013) UN Doc. A/68/98 para 20;

人員依保全業法不得配槍，對於關鍵基礎設施防護不具嚇阻效力，亦無任何抵禦能力，經濟部（電廠、煉油廠、水壩... ... ）與交通部（機場、高鐵、重要場站... ... ）等所屬重要關鍵礎設施，應重新盤點其重要影響性，與警政署討論其防衛能力，配署必要保安警力，以強化關鍵基礎設施防護之能力。

在國際法中，沒有明確具有約束力的規則，指示所有國家採取一切措施專門保護其關鍵基礎設施，或不損害其他國家的關鍵基礎設施，都沒有強制約束力，從烏俄戰爭中俄軍攻擊核電廠週邊設施，可以完全理解，聯合國明定之相關規定，都只是透過軟法（Soft Law）來進行監管或規範，儘管如此，這個問題在國際法中越來越多地得到探討，主要是在非約束性規則（Non-Binding Rules）（擬議法）（lex ferenda），特別是在關鍵基礎設施網絡規範（Cyber Norms）的背景下受到規範。網絡規範是網絡空間（Cyberspace）中可接受的國家行為的自願非約束性標準，其運作方式與氣候變遷法背景下的自願承諾相同。具體而言，國家、國際組織和非國家行為者一致認為，這些表述儘管不具約束力，但應被採納並遵循，作為網路空間適當行為的標準。

值得一提，在各國大多同意國際法適用於網絡空間，那麼自願性非約束性規範（voluntary non-binding norms）的地位如何呢？學術界和國家實踐一致認為，關鍵基礎設施網絡規範為各國解釋、適用和實施其在網路空間的現有法律義務提供了指導，此外，它們在法律上並非無足輕重，因為它們反映了對國際法的潛在、當前和廣泛接受的解釋與效力。

在國際上，對關鍵基礎設施防護法律規範有那些重要的發展呢？不論在美國或歐盟、或是國際法（聯合國規範）等，都有明確規範規定，各國必須保護本國之關鍵基礎設施，同時不得損害其他國家的關鍵基礎設施。這一部分將首先關注聯合國在創建和頒布保護國家關鍵基礎設施免受網路攻擊概念性的嘗試，即2015年和2021年UNGGE（United Nations Group of Governmental Experts）報告、OEWG（Open-Ended Working Group）報告以及UNGA（the United Nations General Assembly）的實踐[58、59、60]。隨後，該保護架構在美洲國家組織（OAS）、上海合

UNGA Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (22 July 2015) UN Doc. A/70/174 (2015 UNGGE Report) paras 25-28; Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security (United Nations Office for Disarmament Affairs, 28 May 2021), *available at* https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf (2021 UNGGE Report) paras 70, 71(a), 71(e) (last visited Dec. 14, 2023).

59 2015 UNGGE Report (n 40) para 10; 2021 UNGGE Report (n 40).

60 UNGA, Final Substantive Report of the Open-ended working group on developments in the field of information and telecommunications in the context of international security (10 Mar. 2021) UN Doc A/AC.290/2021/CRP.2 (OEWG Report).

作組織（the Shanghai Cooperation Organization）、非洲聯盟（the African Union）和北大西洋公約組織（北約）（the North Atlantic Treaty Organization, NATO）等，都提出致力於保護各國關鍵基礎設施的國際組織背景下得到支持。即使在非國家組織區域，例如GCSC規範[61]和巴黎信任（Paris Call for Trust）呼籲[62]，兩者都包含保護各國國家關鍵基礎設施免受網絡操作影響的規範[63]。

雖然國際上與各國的國家關鍵基礎設施防護發展有長足的進步，但目前對於災害發生，不論是天然災害或是人為災害的預防，關鍵基礎設施的事前準備、發生時的反應、事後復原的研究，尚依然存在許多值得進一步探討的問題：

(一)在目前極端氣候之下，及人為戰爭與恐怖攻擊，目前能夠預測未來會發生何種危機？

(二)加重刑事司法刑度，是否可以抑制關鍵基礎設施人為破壞的機率？

(三)境外敵對勢力不在我國的領土區域，對我國關鍵基礎設施破壞（如公海範圍破壞我國的海底電纜），我國刑法效力是否有能力處罰？

(四)重要關鍵基礎設施之週邊土地，是否限制不當買賣與開發（包含境外投資）？

(五)國際法（聯合國相關規定）對關鍵基礎設施的破壞是否有約束力？

(六)危機可能會如何演變？以及應該採取何種保護措施以避免重複發生？

(七)如果各種風險是無法避免的，該如何事前強化或事後復原關鍵基礎設的運作？

(八)在缺乏歷史資料之下，國家關鍵基礎設施該如何進行風險評估？

(九)關鍵基礎設施的韌性如何評估？有哪些構面或指標？

(十)關鍵基礎設施的硬體系統性架構該如何評估其韌性？

(十一)目前關鍵基礎設施相關的周邊組織（如承包商、供應商）風險管理成熟度如何？目前關鍵基礎設施單位的危機與風險處理措施是否足夠應付當前的危機？

(十二)風險發生後的災後關鍵基礎設施復原機制？優先順序？以及防治策略的選擇？

二、建　議

關鍵基礎設施防護觀念在國際上與國內已發展多年，美國推動關鍵基礎設施防護工作已逾二十餘年，特別是在911之後更加成熟與健全，應當是目前全球在關鍵基礎設施研究與實踐的領先者。在2013年美國國土安全部提出以「安全

---

61 Global Commission on the Stability of Cyberspace, 'Advancing Cyberstability' (Global Commission on the Stability of Cyberspace, November 2019), *available at* https://cyberstability.org/report/22 (GCSC Report) (last visited Dec. 14, 2023).

62 'The Call' (Paris Call For trust and security in cyberspace), *available at* https://pariscall.international/en/call (Paris Call for Trust) (last visited Dec. 14, 2023).

63 Global Commission on the Stability of Cyberspace, *supra* note 61.

64 「網路安全暨基礎設施安全局」（CISA）下設立聯合網絡防禦協作辦公室（JCDC's office），由具代表性的聯邦政府單位所組成，包括國土安全部（Department of Homeland Security, DHS）、司法部

（Security）與韌性（Resilience）」為推動目標的國家基礎設施防護計畫（National Infrastructure Protection Plan, NIPP）。根據美國NIPP的定義，「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」。綜整上述風險管理與韌性概念，關鍵基礎設施的防護工作目標，在國內尚有很大的檢討空間，歸納出以下幾點來進行說明：

(一)我國關鍵基礎設施防護組織與法律位階過低、公私部門防護概念亦非常薄弱

關鍵基礎設施防護課題，過去被視為非傳統安全（Non-Traditional Security）之探討範圍，如以美國為例，自1983年開始對民生「基礎設施」產生重視，近年由於911恐怖攻擊事件，日益嚴重的國際恐怖主義威脅，導致美國政策制定者在國土安全方面的重新定義「基礎設施」並成立了有史以來最大的安全部會「國土安全部」，並成立專屬單位「網路安全暨基礎設施安全局」（The Cybersecurity and Infrastructure Security Agency, CISA）主管關鍵基礎設施防護（包含關鍵基礎設施資訊安全）[64]，顯見美國對關鍵基礎設施和關鍵資產（CI and Key Resources）更加重視，並由國家公布「實體保護關鍵基礎設施和關鍵資產的國家戰略」（The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, NSPP）及2009年「國家關鍵基礎設施防護計畫」（NIPP）勾勒出美國政府對整體國土安全戰略的重要組成細節，而美國實施這項戰略，明確定義出「關鍵基礎設施」和「關鍵資產」等，及各國發展及立法位階看來，其重要程度實在不容小覷，反觀國內，國內在法案之立法程序上，甚至尚未有明確訂定，實落後先進國家相當大的距離，而國內各公私部門對於「關鍵基礎設施防護」之概念亦非常薄弱，美國積極投入關鍵基礎設施防護多年，在總統行政命令、政策、策略、法案上作出多項宣示及完成立法，要求所屬部門（如能源部、國防部、交通部等）皆需積極投入各項重要關鍵基礎設施防禦計畫，為與其他聯邦部門和機構，包含州、地方、區域、地區和部落，及私部門和其他外國國家等，一起合作完成CIP工作要務，歐盟所屬會員國亦是極積投入相關立法與防護政策，國內在重要關鍵基礎

（Department of Justice, DOJ）、美國網路司令部（United States Cyber Command, USCYBERCOM）、國家安全局（National Security Agency, NSA）、聯邦調查局（Federal Bureau of Investigation, FBI）和國家情報總監辦公室（Office of the Director of National Intelligence, ODNI），與自願參與的夥伴合作、協商，包括州、地方、部落和地區政府、資訊共享與分析組織和中心（ISAOs/ISACs），以及關鍵資訊系統的擁有者和營運商，以及其他私人企業實體等（例如：Microsoft、Amazon、google等服務提供商）合作進行網絡防禦協作防護關鍵基礎設施。

65 S. Paula, Regional public-private partnerships – Addressing Critical Infrastructure Interdependencies and Homeland Security Preparedness, Presentation at the 2004 PNWER Annual Summit, Victoria BC. July 14.

設施法案立法程序上，尚處空白，僅是行政院下屬國土安全辦公室或近日成立之數位部等，進行相關行政命令等作為，美國與歐盟等先進國家作法，實值得借鏡參考。

(二)風險管理與韌性評估工具導入的重要性

美國過去幾年中，針對關鍵基礎設施之防護，以從原先被動回應計畫思維（Re-action planning and Response Paradigm），轉向成為整全主動性之策略（Comprehensive Pro-active Strategies），不單只是災難發生時所需要進行之救災回應，更進一步建構完整及有效之預防預警措施，這種思維已改變了原先傳統之被動式緊急救災管理法則（Paula, 2004）[65]。從NIPP的架構看來，美國主導各中央部會、地方政府、及私部門產業，皆是利用風險策略管理的手段來進行各項風險的控管，包含風險辨識（Risk Identification）、風險評估（Risk Assessment）、風險分析決策（Risk Analysis and Decision）、風險執行與控制（Risk Implementation and Control）、資源分配（Resources Allocation）、韌性評估等，有一套較為量化及邏輯科學的方式，較能說服公、私部門對於政府的作為認同，並且美國為了推動具科學客觀的研究基礎，挹注大量經費給全美相關大學與關鍵基礎設施防護研究機構，反觀國內，目前各關鍵基礎設施部門皆無一套完整的評估方法與工具，亦無專屬研究團隊或是大學相關系所院校研究中心協助進行跨部門、跨學門、跨科學的研究與評估等研究方法與工具開發，美國的作法可以作為國內重要參考依據。

(三)加重刑罰完全抓錯了重點，關鍵基礎設施重視事前預防，而非事後災後復原

關鍵基礎設施的概念，是持續穩定不中斷的提供各項旅客運輸、物資產品與各項服務的流通（Steady Flow of People, Products and Services），在各種天然或人為（或超載使用）的災害情境下，各種重要物資：油、氣、電、水都能穩定的供應，也就是持續營運（Continuity）的概念，因此，加重刑罰事後處罰並無濟於大規模災變的嚇阻，與災害所造成大範圍的影響。所以，關鍵基礎設施防護重點在於防護（Protection），在於預防（Prevention），在於主動式（Proactive）防範，完全有別於一般消防的災害管理概念，重視救災的緊急應變（Emergency contingency）概念，目前各部會的關鍵基礎設施演習，過度重視災害復原的演習內容，對災後事件發生時被動式（Reactive）回應，完全抓錯了關鍵基礎防護的重點，事前防範且零容忍失誤及大範圍破壞，才是關鍵基礎設施防護的正確思維。而如何進行重要關鍵基礎設施的盤點，是重要的工作，由國際上先進國家經驗，盤點關鍵基礎設施應考量下列幾項要素：

1.人口影響：全國使用人數、區域使用人數、衝擊人數、客戶數等。

2.經濟衝擊：全國經濟影響衝擊、地區經濟影響衝擊。

---

[66] 黃俊能主持研究計畫，「108-109年核子保安風險管理與危機處置之研究」，原子能委員會委託研究，2019年。

3.相依性影響：如主要供電失效，將影響南北交通高鐵、臺鐵、都市捷運等，天然氣中斷，將影響大潭電廠發電等，進而影響全國供電。

4.人民政府的信心及民心士氣的喪失。

盤點出關鍵基礎設施的重要性與影響性，如何強化關鍵基礎設施的韌性與持續營運機制？以經濟部所屬重要生產電廠（如大潭發電廠）為例，重要輸電線路、輸油管路、輸氣管路，及重要節點（Notes）（如龍潭超高壓變電站、輸氣海管陸管交集點通霄配氣站等），都是需要加強其防護水準、並增加所有重要關鍵資產的備載容量〔增加天然氣第三、第四儲存量，與任何必要的備援機制（Redundancy）〕。

(四)強化人為內部威脅防制

關鍵基礎設施不論是實體或是網絡，大部分會以封閉性系統設計為原則，因此，外部攻擊較為不易，所以關鍵基礎設施防護另一項重點，即是防範人為內部威脅（Insider Threat）（內賊）破壞的可能性，也是關鍵基礎設施保防（Personnel Security）重要防護策略，人為內部威脅應注意控制3項重要項目，包含侵入性（Accessibility）、授權性（Authority）、知識性（Knowledge）等，對於擁有這三項權力（或能力）者，皆需受到嚴格管制，不論其職位有多高，亦或授權的外包廠商，都應該建立各種防範機制，可以利用二人機制（Two Person Rule），或三人機制（Three Person Rule）操作機制等防呆系統設計方式，來防制有心破壞的內部人員（包含維修廠商）。

對於如何達到防範水準，美國核電廠人員管制與適職方案是最佳的參考範例。以美國為例，美國商用核能電廠持照者（如國內台電核電廠）必須建立一套能夠闡述可信賴因素之內部威脅減緩計畫（Insider Mitigation Program），其必須與實體防護方法相結合，降低內部人員製造不利行為的可能，其內容至少包含[66]：

1.內部威脅計畫要素／關鍵組合。

2.初始安全性確認。

3.藥物和酒精測試。

4.心理評估包括臨床和定期的醫學評估。

5.年度審查。

6.定期重新檢視安全性。

美國時代雜誌曾報導過：「美國核電廠難防大規模攻擊，並指出警衛缺乏必要的訓練和武器且美國政府對核電廠所定的安全標準過低，有警衛表示，他們可能未準備好防制像911事件那麼大規模的恐怖攻擊。」本文參酌國外相關文獻提出下列參考建議事項，供國內關鍵基礎設施業主對人為安全進行重要防護工作盤點：

1.安全防護檢查：每半年實施定期安防總檢查，並召開安全防護會報實施檢討，以發掘缺失、檢討改進、列管追蹤。

2.實施安全防護宣導：每月將安全維護案例宣導資料於各關鍵基礎設施內網實施宣導，提高員工安全警覺及處置能力。

3.保安模擬演練：配合年度緊急計畫

演習，以美國核電廠為例，每四年實施保安演練二次，提升員工及保警應變制變能力。

4.危機管理、應變作業：召開「危機管理、應變小組」會議，適時處理緊急應變業務。

5.與治安機關聯繫：與軍、警、情報單位簽訂支援協定，與治安機關聯繫。

6.危安狀況之通報：發生重大危安狀況時，立即陳報，並通報相關單位。

7.監測並限制不適任人員繼續在廠內工作：安全查核新進人員或包商、有酒精反應人員限制進入管制區域、定期尿液或毒品篩檢含（承包商、支援單位、外籍人員）後再依規定不定時抽驗。

8.保安檢查：提升門禁管制檢查，廠內巡查工安、保安巡查、現場檢驗員與包商監督。

9.擬定保安計畫：以核電廠為例，由外而內劃分5區，分別為財產區、控制區、保護區、緊要區及輻射管制區，層層包圍，各層間皆有堅固阻隔圍籬，並保留50公尺以上之緩衝區域。

10.強化備援系統：核電廠為例，廠區之緊急用供水、供電系統亦應加強備援方案，且列為保安重點，應配置守護與巡邏警力。

11.型塑公平、包容、多元的國際社會（歐美國家為例）：宗教種族衝突，主要源起於西方社會長期以來對穆斯林在政治、經濟、種族各個層面的歧視，能減少恐怖份子的滋生，並促使恐怖組織放棄恐怖攻擊手段改採合法的平和手段表達訴求，如此方能真正治標又治本地解決恐怖主義的問題。