



關鍵基礎設施防護與工程師

行政院參議 / 張清祥

關鍵詞：關鍵基礎設施防護、整備系統、安全與韌性、持續營運

摘要

基礎設施是國家永續、社會經濟、人民生活的根本，其扮演關鍵角色無庸贅述，倒是近年來國內外遭遇到的事件所造成的衝擊、驚嚇令人不安，如何確保其功能正常是個極其嚴肅的議題，除了設施業主之外，尤其肩負基礎設施的孕育者-工程師角色，值得進一步探究。古往今來，設施提供服務本是建設的初衷，而從其規劃、設計、施工，以迄營運各階段的決定與作為都會影響到服務表現，如何確保是值得去關注。隨著時代的邁進，環境境況的急遽演化，以往的作為模式已難符合及因應未來的變化。本文就基礎設施防護於國內、外，尤其是歐、美的一些作法，探索當前的趨勢及遭遇的議題與工程師該有的角色提供參考，並期能促動（trigger）各界專家、先進預（共）謀因應，善盡專業的責任。

一、基礎設施即民生工程

基礎設施名稱對大多數民眾而言，多不陌生，尤其對從事工程專業的工作人員而言。但若深入探索，又發現某些似熟悉卻又陌生的窘狀。這也難怪，因為其範疇太廣，也歷史悠久，各有認定，即使當今，仍是各吹各的調，各吹各的號[1-3]。然就其本質言，回顧人類歷史文化的演化過程，迄今留下的工程/建物足跡多屬之。從相關紀錄可見到其繁華風光的過去，也可見到因故殘敗的景象。簡言之，就是供人類生活的設施，從都市城牆、道路、橋梁、溝渠等到如今的陸、海、空等建設都是。早期最基本目的以生活所需著眼，後逐漸伸展到各種用途為目標。後續發展，除硬（hard）目標之外，也有包括系統及人員等軟（soft）目標納入。由此可見，依需求/目的不同各有範圍，惟可以確定的是離不開與民眾生活相關。



二、定義多元

以美國(國土安全部)說法，關鍵基礎設施(Critical Infrastructure, CI)支撐起國家福利，亦即整個社會的奠基，內容包括資產、系統與網路。其他如歐盟、澳、加、紐亦有類似定義。關鍵基礎設施，也有稱為國家重要基礎設施，可以廣義地定義為提供民眾服務的系統、資產、設施和網絡，是國家安全、經濟繁榮、以及國民幸福和安全所必需的。

於國內，資通安全管理法亦有定義，即「關鍵基礎設施指實體或虛擬資產、系統或網路，其功能一旦停止運作或效能降低，對國家安全、社會公共利益、國民生活或經濟活動有重大影響之虞，經主管機關定期檢視並公告之領域。」[3]。

傳統上，設施所考慮的功能，隨著環境的變化與國際社會的變遷而隨著演化。材料也是跟著更新，設計方法、觀念也隨之調整，越來越新穎，功能表現越來精緻。然功能的維持防護也面臨更嚴峻考驗，從最近國內外巨災，如颱風、地震與人為恐攻等事件斷續發生，環境的更迭，尤其是人為的衝擊，加上先天的本質--設施龐大、範圍廣、年壽長，防護不易。過往的規劃、設計的考慮、考量也面臨越來越多的挑戰。且範疇已跨出硬體部分，設施內或間之系統、軟體部分也紛紛涉入。相對的，以往著力或關心的面向調整變成另一些具挑戰的新興議題，亟待進一步探索因應。過往國內、外經過一些遭遇事件歷程，與各所處環境與社經背景等，對於基礎設施的防護態度各有所衷。於英國、美國經過一些歷程演變，目前分別

表 1 英國關鍵基礎設施清單



表 2 美國關鍵基礎設施清單

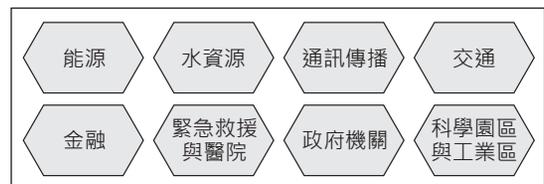


圖 1 我國關鍵基礎設施分類 [5]

篩出9項與16項關鍵基礎設施[4]，分如表1，2：

在國內關鍵基礎設施分類亦經過一些歷程研究、探討篩出，將之分為8項，如圖1。

三、基礎設施的威脅

提供服務是基礎設施基本的任務，但過



程中可能會遭遇一些事件或狀況，進而影響到功能。近年來，國際發生了一系列重大災害，如美國卡翠那颶風、911事件；日本311大地震、多次颱風；英國倫敦地鐵連環爆、法國、比利時、德國恐攻、印度洋海嘯、中國大陸南方雪災、汶川與玉樹地震、風災；臺灣的921大地震、88風災及2017年815大潭電廠事故造成全台八百餘萬戶大停電。這些災害呈現的多樣性、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毀所導致。至於威脅種類各有解讀與看法：

(一) 美國

以美國國家防護計畫(NIPP, National Infrastructure Protection Plan)的報告，不斷演化的威脅(evolutionary threats)分為五大類，即：極端氣候(extreme weather)、意外疏忽(accidental/technical failure)、網路威脅(cyber threats)、恐怖活動(acts of terrorism)及疫病(pandemics)。^[6]

(二) 歐盟

歐盟關鍵基礎設施保護計畫(EPCIP)採用全危害方法，包括人為、技術和自然災害，恐怖主義威脅優先考慮。^[7]

(三) 日本

在日本，將災種分兩大類，即天然與人為災害，並各再分為3及5類，共八類，除了以人為為主要對象外，幾乎亦與設施相關。其中5大種人為災害為：都市、產業災害、交

通災害、戰爭、管理災害。其中管理災害包括：調查簡陋、規劃與設計欠周密、施工不良、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。^[8]

(四) 臺灣

在災害防救法將災害條列22種，即：
(1)風災、水災、震災(含土壤液化)、旱災、寒害、土石流災害、火山災害等天然災害。
(2)火災、爆炸、公用氣體與油料管線、輸電線路災害、礦災、空難、海難、陸上交通事故、森林火災、毒性化學物質災害、生物病原災害、動植物疫災、輻射災害、工業管線災害、懸浮微粒物質災害等災害。

依中央氣象局災害的分類，災害的發生原因主要有：天然(自然)變異與人為影響。並分為天然災害、人為災害、天然人為災害與人為天然災害四類。^[9]

(五) 其它

另外，亦有針對21世紀面臨的關鍵基礎設施的威脅分成兩大類：惡毒力量與惡性力量(Malevolent Forces vs. Malignant Forces)^[10]。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。如：恐怖主義組織、有邪惡意圖的資通訊組織或個人。另惡性力量則主要是使基礎設施惡化的自然力量，如：時間，天氣，和疏忽的無情力量，如：老化、使用過度、技術、系統或程序的失敗等。

設施服務過程，曝露於各種環境，威脅

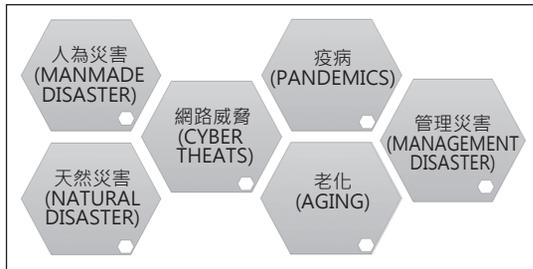


圖 2 關鍵基礎設施威脅種類彙整

複雜，除外在環境外，亦有內在本質因素，以及管理面所造成的災害。威脅雖有不同的分類，但輪廓、範圍多數重疊。

綜上，整理歸納成六類，如圖2，包括：天然災害 (natural disaster)、人為災害 (manmade disaster)、網路威脅 (cyber threats)、疫病 (pandemics)、老化 (aging) 與管理災害 (management disaster)。

四、基礎設施防護策略

設施之施設本應有其必要之服務，為確保其功能正常，適當維護或防護機制乃是必要作為。由於美國有數次颶風肆虐與911事件的洗禮，對於CIP的推動態度積極，其它國家或區域也仿效啟動，如：歐盟、加拿大、澳洲等。美國對於防護著力甚深，成立國土安全部職司此任務，即可見其企圖。歐洲如英、法、比、德等國也遭遇恐怖事件的衝擊。面對此種氛圍，基礎設施的防護機制也陸續應運出現。例如：

1. 美國2002年頒布「2002年國土安全法」[11]、2006年頒布「國家關鍵基礎設施 防護計畫」，2009年、2013年更新[6]；2007年頒布「國家持續政策」[12]與「國家持續

政策執行計畫」[13]推動相關的措施以確保國家能持續運作。2011年頒布國家整備系統 (National Preparedness System, NPS) [14]指令，旨在通過系統地準備對國家安全構成最大風險的威脅與災害，來加強國家的安全和韌性。

2. 英國：對天然災害2010年內閣提出「提高關鍵基礎設施天然災害韌性策略架構與聲明」2010年提出各設施主管部門須依全災害思維提出「部門韌性計畫」[15]
3. 澳洲：2009年決議「關鍵基礎設施計畫方案」執行強化為「關鍵基礎設施韌性」並發表國家災害韌性策略 [16]。
4. 加拿大2014年公布加拿大行動計劃的關鍵基礎設施更新版 (2014-2017) [17]。
5. 日本2014年公布「關鍵基礎設施資訊基礎設施保護基本策略」[18]。

由於一些歷史背景，美國對於基礎設施防護積極推動，堪稱最為先進與完整，且推動原來的聯邦救災總署 (FEMA) 擴編為國土安全部，推動相關事宜。目標是推動國家持續，強化安全與韌性，值得參考與借鏡。

五、服務水準與設施韌性

對於一個國家或企業，維持其既有功能或營運持續 (Business Continuity) 是主事者追求的基本目標，而基礎設施的維護為基本功。過去國際發生過的災例經驗，往往造成企業與政府機關運作中斷，造成極大衝擊，



維持持續運作、確保設施安全與韌性（功能正常），是設施管理的核心。ISO對企業持續推出ISO 23000標準，確保運作安全與韌性，亦即控制在低風險的環境，確保其服務水準。一個設施服務水準與設施風險及防護措施息息相關，可從幾個面向來描述，Petti [19]曾對於CI風險與防護措施關係的論述，其將風險（R）大小由四大因素來決定，即：威脅（T）、脆弱度（V）、後果（C）及韌性措施（Re）來決定，即

$$R = f(T, V, Re, C) \quad (1)$$

亦即關鍵基礎設施風險是威脅/災害、脆弱度、後果及韌性的函數。

其實CI服務水準（Service Level, SL）的維持與防護措施關係密切，也就是韌性的另

一種表徵，其內涵就是靠整備機制或系統的妥適程度來展現，將前揭因素重組以另一種函數來表達，即

$$SL = f(R', Re, t) \quad (2)$$

其中 $R' = f(T, V, C)$ ； t 為事件歷程。

以圖3說明，即是服務水準高低，與韌性機制功能息息相關，以圖形表示，其中A、C線為簡化狀況，B、D線則可能為實際狀況。事件發生當下、之後的設施服務水準與應處（應變與復原）高低立判，如圖A、C線。當然之前的預防、防護與減災對於服務水準的衝擊居關鍵角色，若妥適，則衝擊較小，反之則影響大，甚至完全被摧毀而失能，如圖D線。如何降低服務水準與縮短影響歷程極具挑戰。

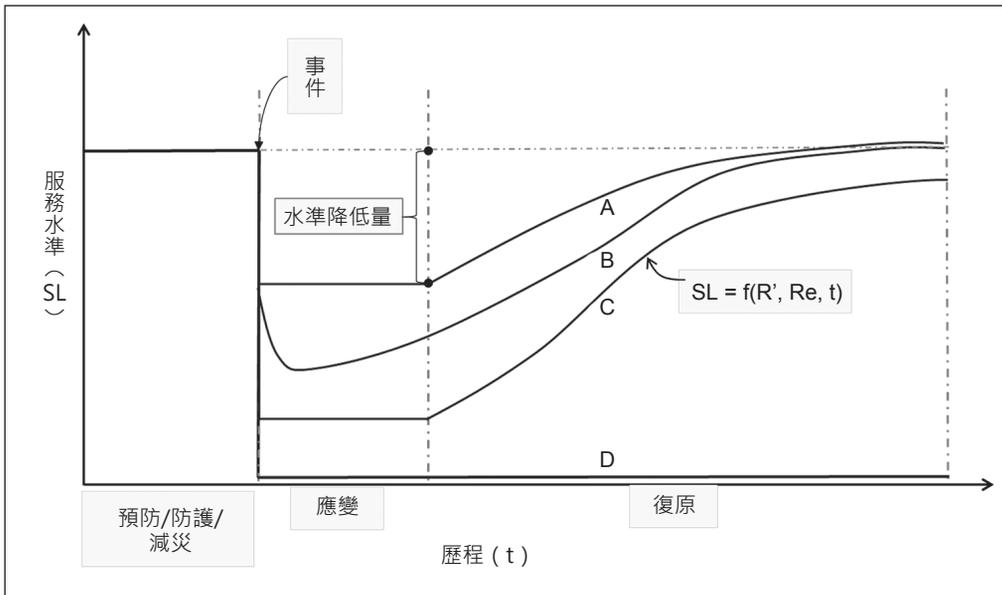


圖 3 關鍵基礎設施服務水準與整備系統運作歷程圖



六、它山之石 - 美國 CIP 推動

為推動國家基礎設施防護計畫以保護關鍵基礎設施和關鍵資源並確保韌性，美國國土安全部依其總統指令PPD 7 [20]提出NIPP [6]（該計畫的最近版本於2013年更新）指示：關鍵基礎設施必須安全，且能夠承受並迅速從所有危險中恢復。為實現這一目標需要與國家整備系統NPS相結合。並要求聯邦政府有責任加強其關鍵基礎設施的安全性和復原能力，保持國家基本功能的連續性，組織自己有效合作並為關鍵基礎設施的安全和韌性加值。

國家整備系統的建立，旨在維持和提供防護核心能力的過程，以實現安全和有韌性的國家的目標。並以國家規劃系統律定整備計畫，將整個組織參與可執行的戰略、程序和戰術方法三層級作有效的推動。整個國土安全推動輪廓以整備系統為核心，包括前揭的5大領域任務，參圖4。

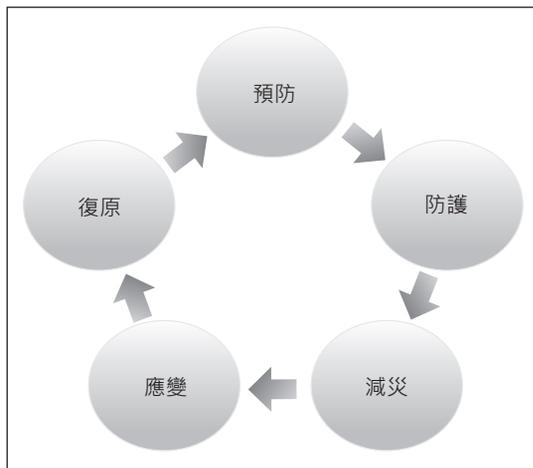


圖4 國家整備系統（美國）

關鍵基礎設施防護部分則有NIPP做為指導，並運用NPS系統，以風險管理架構作為主軸，進行防護工作。針對個別部分又細分各類的細部作為，包括第一線應變的操作與指揮，堪稱完整。

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（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。並構成維持國家基本功能的一環，亦即與國家持續運作政策銜接。

在推動過程NIPP亦揭示推動七大核心準則，包括：應協調和全面整合風險管理，以便有效分配防護資源；了解和解決跨域的依賴性和相互依賴性的風險；基礎設施風險和相互依賴性的知識需信息共享；夥伴關係需了解不同設施的獨特性；建立夥伴關係至關重要；跨國的基礎設施，需要跨境合作；在設計資產、系統和網絡時應考慮安全性和韌性。

七、國內機制

在國內，對於關鍵基礎設施防護係以全災害的角度面對，除了災害防救領域、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，行政院已成立了辦公室推動，從政策會報以下，包括應變機制、防護計畫與關鍵基礎設施防護亦積極進行，期對政府運作、社會經濟活動與民眾生活即使遭遇各種事件亦能夠如常。其推動機制，從環境因素的掌握，藉由政策會報及CIP整導綱

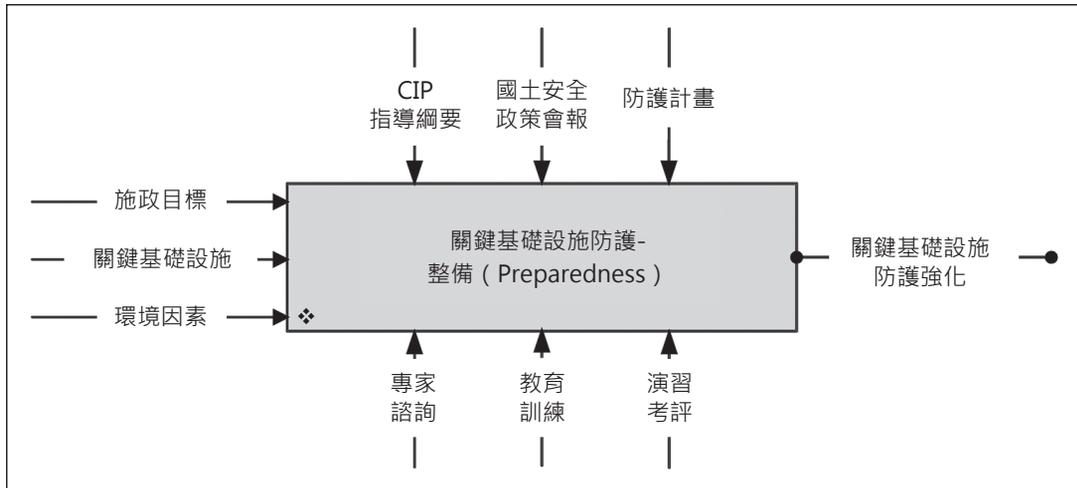


圖 5 國家關鍵基礎設施防護整備機制

要的導引，加上訓練與演習的機制，目標是強化安全與韌性的關鍵基礎設施，以達到或確保施政目標。參考圖5。另外於我國關鍵基礎設施防護指導綱要[21]亦鼓勵各主管機關與私營企業合作及研究發展，強化CIP。

八、工程師於 CIP 角色

(一) CIP 整備各階段均需要專業

以公部門為例，基礎設施開始服務後，維護是確保其功能正常的基本手段，以確保其目的，傳統維護工作，主要是定期與不定期保養，深入些的作為則會配合一些活動，如演練或演習。由於維護/養護管理作業是單位的後勤工作，一般多偏被動作為，缺少宏觀的、積極與前瞻的思維。對於肩負國家持續運作的基礎設施功能的確保，需要更完整的防護機制。

制，經常涉及各級政府、企業，當然也與各專業對象密切。基礎設施生命歷程從可行性研究開始，歷經規劃、設計、施工、營運等階段。為了達到目標要求，以擔負起服務的重任，每一階段，均有任務待執行，亦即：預防、防護、減災、應變與復原等領域之整備工作，透過風險管理手段，降低威脅、脆弱度等風險，來增加其安全與韌性。工程師於設施生命週期過程中，則擔任專業關鍵角色。當然各階段各有考量重心，以確保CI的功能。為了達到國土/企業安全抑或持續運作，設施擁有者或管理者--業主角色當然是舉足輕重，擔負所有責任，其中涉及面向龐雜，除組織內團隊外，需搭配外在的專業來協助方能成事。此任務，非工程師莫屬，亦難辭其責。

(二) CIP 整備作業於生命週期前期階段導入效益潛勢高

於整備系統，即前揭的五領域，此機

政府或企業為了某些目的，籌建一些基



礎設施來服務，為了確保完成後能持續運轉，在啟動計畫階段，防護需求即應納入考慮。亦即於可行性、規劃、設計階段作業，預防、防護與降低安全威脅應於這些階段就須進行；當然應變，甚至復原階段亦可納入。當然，CI基地的選擇，若選擇適當，可以降低營運期防護的機制或措施需求，甚至連帶可以降低災害衝擊或利於應變；相對地，若限於既有條件而無其他較妥方案，則須於防護措施著手；至於營運階段，對於預防則須從非CI著手，例如強化防護計畫應變，藉以滿足任務的需求。

以下就專業作為可能影響CI服務表現的效益潛勢高低，整理如表3，其中程度以A...E來表示，A為高，B次之，E為一般。如：設計階段，在整備過程的預防、防護與減災效益潛勢最大（均為A），應變與復原階段次之（均為B）；在施工階段整備效益潛勢則較遜（分別為C, C, E, D, D）。

九、CIP 推動前瞻

（一）威脅一直存在與加劇，防護機制需與時俱進

對設施的威脅層出不窮，除天然災害外，人為災害漸成為威脅的主流。由於高度的複雜性，難以完整歸類應處，即使利用過去的案例，也難適當的應處。目前針對特殊對象，雖有進展，但離全面災害防護仍具相當大的挑戰。基礎設施先天脆弱：軀體/規模龐大，防不勝防，然仍須有宏觀前瞻思維，並有系統規劃推動，方能事半功倍，方克有成。

（二）CIP 推動，工程師責無旁貸

對整個國家而言，災害防護方法，或多或少多已經歷過，由於先天得災害宿命特性，善後處理結果鮮少讓民眾滿意。服務讓大眾滿意是參與工作者追求的目標，其中可見到工程師涉獵的蹤影，也留下很多待改善的工作。所謂：「豫則立。不豫則廢。」未雨綢繆仍是防護基本精神，傳統工程設計思維，思考面向以天然災害颶、洪與地震為主，其它領域範圍則鮮見納入特別考量。但威脅不分對象，也處處挑戰業主利益與工程師的專業。其中安全與韌性強化議題的納入是計畫推動的核心，整備機制的5大領域與設施生命週期的各階段，尤其是規劃、設計階段，更需要此兩者的關心與參與。

表 3 CI 於整備各階段工程師參與的效益潛勢程度

整備各階段 生命週期	預防	防護	減災	應變	復原
可行性研究	A	A	A	C	C
規劃	A	A	A	B	B
設計	A	A	A	B	B
施工	C	C	E	D	D
營運	C	A	B	A	A



(三) 防護要達標，跨界合作乃必然

傳統上，政府與企業立場常處對立，但提供政府持續，民眾福祉除了政府部門外，企業亦居關鍵角色，兩者密不可分，面對險惡環境，很多狀況唇齒相依，必須攜手方能達標。另實體之外更具挑戰，實體系統多跨不同領域，加上衝擊威脅多元且日新月異，且實體防護之外，關係基礎設施功能，尚有人員與資訊系統，更添加維護的難度，加上關係設施經常以系統存在，單獨的防護為最基本，其間的相依關係，更是複雜，影響也跟著放大，這些都是橫在眼前的挑戰，跨域、跨界合作勢所必然。

(四) 風險峻，專業需求須更高

關鍵基礎設施處於複雜多變的環境，確保其服務正常，必須視野更廣、前瞻，當然需要多方的專業與素養，面對這種需求，既有的專業經驗，難以面對複雜的未來，故培養與精進是不可缺。並且宜有系統化規劃、建構、整合方克有成。

從整備系統預防、防護、減災、應變及復原各個階段，均涉及相關工程師的專業，加上新興挑戰蜂擁而至，風險嚴峻，專業需求更高，故，政府及企業、學校、研究單位與專業機構的交流、互動與合作亟待強化。

參考文獻

1. Lewis, T. G. Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation. Wiley-Interscience, 2006.
2. Giannopoulos, G., Filippini, R. and Schimmer, M. Risk assessment methodologies for Critical Infrastructure Protection Part I: A state of the art. Publications Office

- of the European Union. 2012.
3. 資通安全管理法，行政院，107年。
4. Office of the Press Secretary Presidential Policy Directive -- Critical Infrastructure Security and Resilience (PPD-21) . The White House, 2013.
5. 國家關鍵基礎設施領域分類，行政院國土安全辦公室，107年。
6. Homeland Security National Infrastructure Protection Plan 2013 (NIPP 2013) : Partnering for Critical Infrastructure Security and Resilience. Infrastructure Security and Resilience., 2013.
7. European Conference Commission COMMUNICATION FROM THE COMMISSION on a European Programme for Critical Infrastructure Protection. 2006.
8. 歐陽崎暉，防災都市計畫。藝軒圖書出版社，94年。
9. 辛在勤，天然災害防災問答集，交通部中央氣象局，104年。
10. Associates, T. Five Critical Threats to the Infrastructure of the Future. 2008.
11. Homeland Security Homeland Security Act of 2002. 2002.
12. Esq., M. J. A. National Continuity Policy. 2017.
13. Homeland Security Council National Continuity Policy Implementation Plan. 2007.
14. Homeland Security National Preparedness System. 2011.
15. Cabinet Office Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards. 2010.
16. Council of Australian Governments National Strategy For Disaster Resilience.
17. Canada National Strategy for Critical Infrastructure. 2009.
18. JAPAN The Cybersecurity Policy for Critical Infrastructure Protection. 2017.
19. Petit, F. Critical infrastructure resilience and interdependencies. In Proceedings of the 2016 National Critical Infrastructure Protection Practice and Forward-look Seminar (New Taipei City, 2016) .
20. Homeland Security. Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection. 2003.
21. 國家關鍵基礎設施防護指導綱要，行政院國土安全辦公室，107年。