國立臺灣大學建築與城鄉研究學報｜第 24 期｜2024 年 9 月｜頁 36-68
Journal of Building and Planning｜No. 24｜Sept. 2024｜pp. 36-68
DOI: 10.6154/JBP.202409_(24).0002

研究論文

基礎設施如何成為國家「邊界」：台灣關鍵基礎設施的技術政治與轉化

施柏榮 *

摘 要

關鍵基礎設施（critical infrastructure）在多數國家定義之中，是不可或缺的公共基盤、建築物與系統的集合體，它們的存在為國家經濟、社會福祉、公共安全，甚至政府的關鍵機能提供必要性的支持。本研究聚焦關注台灣關鍵基礎設施歷史形構，並且藉由技術政治（techno-politics）取逕來說明其發展與轉型。台灣關鍵基礎設施必須放置在台灣獨特的歷史、政治經濟脈絡下來進行分析，本研究指出，台灣關鍵基礎設施形構，可以被視為台灣國家邊界劃定的過程。首先，本研究先行探討美國、歐盟、日本在全球脈絡下的關鍵基礎設施政策形成與內涵；其次，描述台灣關鍵基礎設施在不同歷史時期的政策價值與思維的轉化；第三，進一步指出台灣關鍵基礎設與國家（族）建構工程呈現出共同結構（co-construct）關係；而在台灣無論是關鍵基礎設施，或是國家建構工程，都仍然存在於一個動態、不確定的「未完成」（unfinished）的狀態之中。

關鍵詞：關鍵基礎設施、技術政治、國家邊界、國家建構、國家認同

收稿日期：2023 年 12 月 19 日；修訂日期：2024 年 07 月 15 日；接受日期：2024 年 09 月 20 日。

*國立台灣大學建築與城鄉研究所博士生、財團法人資訊工業策進會產業情報研究所產業顧問兼副主任。email: d10544002@ntu.edu.tw

一、前言：關鍵基礎設施

關鍵基礎設施（Critical Infrastructure, CI）若按聯合國減少災害風險辦公室（2024）（United Nations Office for Disaster Risk Reduction）提供的定義，其意指：「提供社會、社區之社會經濟運作至關重要服務的物理結構、設施、網絡及其他資產」。此外，國際電信聯盟（2008）（International Telecommunication Union）也曾指出關鍵基礎設施是：「關鍵系統、服務和功能，若中斷或受到破壞，將對公共健康和安全、商業和國家安全，或其中的任意組合產生破壞性影響」。

如果以全球的發展歷程來看，關鍵基礎設施一詞可回溯至 1996 年 7 月美國白宮發布的第 13010 號名為「關鍵基礎設施防護」（Critical Infrastructure Protection）行政命令，該命令對於關鍵基礎設施陳述為：「某些國家的基礎設施至關重要，以至於它們的失效與破壞，將對於美國的國防或經濟安全產生削弱性的影響，這些關鍵基礎設施包括電信、電力系統、油氣儲運、銀行與金融、交通、供水系統、緊急服務與政府連續性（continuity of government）」（Executive Office of the President, 1996）。2001 年 9 月美國歷經九一一襲擊事件，並且於 2002 年 11 月成立國土安全部（United States Department of Homeland Security），該部會於 2003 年 2 月提出《國家關鍵基礎設施與重要資產實體防護策略》（The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets），對於關鍵基礎設施的關注更為提升，同時也確立國土安全部作為美國關鍵基礎設施的主管部會，專職於關鍵基礎設施的認定（identification）與優先性（prioritization）之識別。美國國土安全部對於關鍵基礎設施，給予了以下的定義：

> 關鍵基礎設施包括龐大的高速公路網絡、連接橋樑和隧道、鐵路、公用事業和維持日常生活正常所需的建築物。交通、商業、清潔水源和電力都依賴於這些重要的系統。（United States Department of Homeland Security, 2021）

相對於美國，台灣政府部門對於關鍵基礎設施的討論相對較晚，直至 2014 年 12 月才由行政院國土安全政策會報提出《國家關鍵基礎設施安全防護指導綱要》，其中對於關鍵基礎設施也給予了明確的定義、任務與配套措施。值得留意的是，如觀察《國家關鍵基礎設施安全防護指導綱要》內容，除了認定主管機關、

次領域主管機關之外，也提出主管機關必須定期對台灣關鍵基礎設施進行「盤點」、「評估」以及根據重要性擬定「防護優先順序」（行政院國土安全政策會報，2014）。

不過對於何為「重要性」的論述，以及是否存在具體的標準以及方法，其實並未清楚；其中只有提及主管機關，將就次領域主管機關提出的項目進行歸納與比較，並且藉由專案會議來檢視、審議重要性，提出排比、分級建議，以及關鍵基礎設施的項目與其分級清單。此外，2014 年《國家關鍵基礎設施安全防護指導綱要》提出之後，對於「究竟什麼是台灣的關鍵基礎設施」的討論便不曾停止，該綱要也在 2018 年 5 月提出修正，其中在策略、目標，甚至是安全防務的方法也有所差異，也再次顯現出關鍵基礎設施的內涵，會隨著不同的時間產生變化。

所謂的「關鍵」，不僅指涉對於基礎設施「重要性」認知的改變，多半也圍繞在－「何為國家威脅？」、「它們如何造成威脅？」等政治議程的設定，關鍵基礎設施的認定、評估過程，除了涉及基礎設施的技術功能之外，也多半與主權（sovereignty）、國土（territory）邊界概念呈現「共建」（co-construction）發展。換言之，關鍵基礎設施認定與排序，即為基礎設施政治（politics of infrastructure）與技術政治的一種呈現。基礎設施也絕非是單純的技術客體，而是容納各種政治價值選擇的載體，或者說它就是政治性本身（infrastructure as a site of the political itself）。本研究，也將依循著此一思考，提出兩項研究問題：

第一，台灣關鍵基礎設施的發展，如何與國家邊界建構相互關聯？

第二，台灣關鍵基礎設施作為與國家邊界、主權、國土概念共同建構之物，背後所反映出哪些的政治性（politics）與張力？

本研究主要採用文獻分析法（document analysis），以台灣為經驗案例，針對台灣關鍵基礎設施相關的政策綱要、計畫等歷史資料進行分析之外，也預期納入 2009 年至 2021 年曾經提及關鍵基礎設施之立法院「議事公報」進行梳理分析。前者，可被視為是台灣政府所擬定的結果，而後者針對不同期間議事公報解析，則可以進一步納入時間軸線，檢視在不同年份、時間之下，有關於關鍵基礎設施相關的討論內涵，包含策略、目標、防務方法是否有所差異。藉由歷史性資料，嘗試比較不同期間由政策所反映的立場與價值體系，以期待能夠完整呈現出台灣關鍵基礎設施背後的政治性（politics）以及被掩蓋的「國家認同」意涵。

除了文獻分析法之外，本研究也預期針對－台灣曾經參與關鍵基礎設施政策規畫者、利害關係人進行半結構式訪談（semi structured interview），以作為文獻

分析法的輔助方法，一方面可以補足文獻分析所可能遺漏之細節之外，另一方面也可以藉由半結構式訪談，來驗證文獻資料的正確性，已讓研究資訊更為可信。

預期的研究結構安排，第一部分將先回顧基礎設施涉及「技術政治」之相關文獻，探索基礎設施與現代國家、現代性之間的關係，尤其聚焦在探索基礎設施如何與國家治理正當性（legitimation），甚至國家認同問題的共同結構；第二部分則將回顧國際關鍵基礎設施相關的政策、計畫，分析其政策形構的特徵與過程；第三部分，則聚焦分析台灣關鍵基礎設施相關的政策與計畫，以及各類型的政治討論、辯論過程，以及關於關鍵基礎設施背後的思考與方法；第四部份作為本文結論，期望以台灣關鍵基礎設施為經驗案例，理解背後的政治性，以及其流變。

二、文獻回顧

（一）全球關鍵基礎設施發展史與轉化

美國自 2001 年 9 月歷經九一一襲擊事件後，是近代最先提出關鍵基礎設施相關定義、措施的國家。在美國政府組織的分工之中，國土安全部主要作為關鍵基礎設施的主導部會，負責國家總體性的策略規畫，其下的網路安全暨基礎設施安全局（Cybersecurity and Infrastructure Security Agency，CISA）則是被賦予基礎設施評估與分析的職責，判斷那些基礎設施對於美國而言，是具有關鍵性的作用。

美國網路安全暨基礎設施安全局，對保護國家關鍵基礎設施給予以下說法：

> 關鍵基礎設施部門的財產、系統和網絡，無論是物理的還是虛擬的，都被認為對美國至關重要，以至於它們的失效或者被破壞，將對人民的安全、國家經濟安全、國家公共健康產生削弱作用。（Cybersecurity and Infrastructure Security Agency，2021）

藉由美國的網路安全暨基礎設施安全局的說法來看，可以發現到美國對關鍵基礎設施的認知與討論，相當程度上是圍繞在「安全」（security）的討論之上。不過，其涉及的範疇相當廣泛，首先，基礎設施並不僅限於「實體」的基礎設施，也包括「虛擬」基礎設施，比如網路空間的資訊安全，也被視為是關鍵基礎設施的範圍之一；其次，有關於「安全」的討論，也相當多元化，包含人民生命安全、國家經濟、公共衛生與健康的安全，也都被進一步歸納在討論的範疇。除此之外，

美國的網路安全暨基礎設施安全局，提出了十六個關鍵基礎設施項目，期望針對這些項目擬定專屬的保護方案，來確保基礎設施能正常的運行與恢復能力。

除了美國之外，歐洲聯盟委員會（European Commission）在 2006 年之時，也提出－《歐洲關鍵基礎設施保護計劃》（European Programme for Critical Infrastructure Protection），該計畫首先關注在運輸、能源部門，希望能夠確保這些部門之下的基礎設施，可以避免受到各種自然、人員或有意、無意的威脅與危害，甚至是可以在受到衝擊之時，也能夠在可接受（acceptable）的時間內快速恢復（recover）到可以運作的狀態，不難發現歐盟對於關鍵基礎設施的內涵，與美國相當近似，同樣是以防禦可能的衝擊，來建構一個具有安全性的基礎設施網絡。但值得留意的是，歐洲聯盟委員會在《歐洲關鍵基礎設施保護計劃》之中，特別針對基礎設施的「相互依存關係」進行了描述：

> 關鍵基礎設施之間日益增加的相互依存關係，以及它們面臨到不斷變化的風險，當前的框架是不夠的。隨著這些基礎設施越來越相互依賴，一個部門的中斷，可能對其他部門運營產生直接影響，某些情況會產生長遠影響，反過來又可能破壞關鍵社會／經濟功能的依賴。諸如此類的情況，可能對成員國和整個歐盟安全產生嚴重後果，可能導致不確定性，或削弱對當局和服務提供者的信心（European Commission, 2021）。

藉由歐洲聯盟委員會有關於為什麼要識別、保護關鍵基礎設施的說明，可以發現到在確保安全之外，歐盟指出了兩項關鍵基礎設施的重要特徵與內涵：第一，不同的基礎設施之間，事實上存在著相互依賴的關係，因此，基礎設施並不能夠被視為是各別獨立的單元，而某些因為自身的損壞，而可能會造成其他部門負面影響者，則可以被視為「關鍵」；第二，關鍵基礎設施的破壞、不穩定性，可能連帶影響到民眾對於政府的「信任關係」，甚至進一步削弱政府治理的正當性。

與美國的發展背景相同，日本在 2000 年首度提出《打擊關鍵基礎設施網路恐怖攻擊的特別行動計畫》，也同樣回溯到當時的恐怖攻擊事件，並且將電信、能源、金融、鐵路、政府服務、人民醫療保健等十四個項目，納入在國家的關鍵基礎設施範疇之中。然而，比較特別之處在於，日本將電信、網路資訊安全基礎設施特別獨立出來，2013 發布－《關鍵基礎設施的資訊安全措施》，指出資通訊系統也在日本普及使用，若資通訊系統受到破壞，那麼以資通訊為基礎的電信、

電力、金融服務等部門也連帶造成衝擊與影響，甚至進一步衝擊國民的生活福祉。日本內閣府網絡安全中心（内閣サイバーセキュリティセンター）給予以下說明：

> 在應對東日本大地震時的系統故障與數據的丟失，以及面對不斷變化的社會與技術環境，有必要在複雜的網路攻擊趨勢之中，獲得知識並做出適當回應，…。以關鍵基礎設施為目標的網路攻擊情況背景來看，…，資訊與通訊技術（IT）與控制系統等操作技術（OT）融合，…。除已經實現的系統之外，也可能成為網路攻擊目標的物聯網系統，也變得愈來愈普遍。（内閣サイバーセキュリティセンター，2018: 1）

除此之外，在日本內閣府網絡安全中心，2021 年最新出版《網路安全策略》（サイバーセキュリティ戦略）之中，也多次提及應該識別關鍵基礎設施，以及必須針對關鍵基礎設施相關的營運者、利害關係人進行審查，同時，也必須針對可能的威脅，設計新的保護機制。其中，對於日本資通訊基礎設施的威脅，提出以下觀察，是日本首次清晰地描繪新型態威脅的模式：

> 隨著經濟、社會數位化的普及與快速推動，此類網路攻擊事件增加，造成人民安全、國家民主根基、國家安全動搖的局面，…。網路攻擊的隱藏與偽裝愈來愈複雜，中國正從軍事相關企業、先進技術企業等竊取資訊；而俄羅斯則是在軍事與政治上，作為國家網路活動的嫌疑對象。（内閣サイバーセキュリティセンター，2021: 8）

回顧日本有關於關鍵基礎設施政策、方針的討論，不難發現到日本對於關鍵基礎設施「何以關鍵？」討論會隨著不同的發展情境產生變化，比如 2000 年，日本關鍵基礎設施的識別，與美國相同皆是以「因應恐怖攻擊」為背景。然而，在 2013 年東日本地震發生之後，擷取於地震災害造成多方系統故障的經驗，與歐盟相似，對於關鍵基礎設施的描繪，除了更加地強調基礎設施的彈性、恢復力之外，也更聚焦在各類型基礎設施的「相互依存關係」。而且此種相互依存關係，在如今更加仰賴於資通訊基礎設施作為運作的核心，這也是何以日本內閣府特別將資通訊基礎設施獨立探索的主因，探討其作為關鍵基礎設施（重要インフラ）的重要性以及應該提出什麼樣的策略、做法，來確保它能夠持續、安全地運作。

不過，正如前述，日本內閣府對於關鍵基礎設施的重要性，也發生了轉化，而且在 2021 年時，更直接指出中國、俄羅斯、朝鮮是日本網路攻擊的主要來源；

對於日本資通訊基礎設施造成威脅之外，也指稱中國嘗試在日本的先進企業之中「竊取」重要的技術資訊。除了對於威脅認知轉化之外（恐怖攻擊、自然災害、特定國家攻擊），值得留意的是，日本對於關鍵基礎設施受到威脅所造成的影響認知也發生了變化，在人民安全、國家安全既有與關鍵基礎設施相關的論述之外，也將「國家民主根基」（国家や民主主義の根幹）納入其中，筆者認為這也顯示出日本對於關鍵基礎設施的政策論述，事實上皆處在非常動態、不穩定的過程。

回顧美國、歐盟、日本對於關鍵基礎設施的政治討論，可以進一步歸納關鍵基礎設施具有幾項特徵：第一，關鍵基礎設施不僅限於實體物理、硬體上的意義，包括「虛擬世界」有關的網路、資通訊基礎設施，也是關鍵基礎設施不可迴避的討論範疇，而且隨著資通訊成為各類型部門的技術基礎，基於此一特徵，資通訊基礎設施關鍵性必須被提升；第二，關鍵基礎設施間，呈現「相互依存關係」，這樣的依存關係，除了資通訊技術成為各部門的操作、建構基礎之外，也發生在能源與交通、能源與水利、化學與運輸等不同的基礎設施與部門的相互構成過程，而「關鍵性」的認知，也必須放置在「關聯度」的認知，換言之，當某一個基礎設施所關聯的部門相對複雜，當其發生損壞、停止運作的情況之時，就可能造成連帶影響的擴大，那麼也就意味著其有較高的關鍵性；第三，對於「為什麼必須識別關鍵基礎設施？」這涉及到一系列的政策論述（Discourse），而這樣的論述本身也使得關鍵基礎設施除了是實體、虛擬世界的建構物之外，也成為政治議程的建構物。再以美國、歐盟、日本的案例來觀察，三個國家政治實體不斷、持續產製（Encoding）關鍵基礎設施的內容與論述，這也使關鍵基礎設施的內涵持續被覆蓋、增添，也使關鍵基礎設施處在持續變動「未完成」（Unfinished）狀態。這意味著必須進一步解構（deconstruction）隱藏在其背後的政治性，也才能夠進一步瞭解關鍵基礎設施與其他論述的共同結構（co-construct）過程。

表 1 美國、歐盟、日本與台灣關鍵基礎設施推動比較

	美國	歐盟	日本	台灣
推動背景	恐怖攻擊事件（九一一事件）	各種自然、人員有意（恐怖攻擊）、無意危害	自然災害，源於特定國家資訊網路攻擊	恐怖攻擊事件、中國對於台灣實體與虛擬的滲透
主要法規或者文件	《關鍵基礎建設防護（行政命令）》（1996）、《國家關鍵	《歐洲關鍵基礎設施保護計劃》（2006）	《打擊關鍵基礎設施網路恐怖攻擊的特別行動計畫》	《國家關鍵基礎設施安全防護指導綱要》（2014）

	基礎建設與重要資產實體防護策略》（2003）		（2000）、《關鍵基礎設施的資訊安全措施》（2013）	
涉及國家權力與正當性議題	關鍵基礎設施的防護，是為了確保人民生命安全，而國家有義務確保人民生命財產安全	關鍵基礎設施如受到損害，亦會削弱人民對政府的信任與信賴關係	關鍵基礎設施的防務，是政府對於人民生活福祉的承諾，且國家也須確保不受特定國家的滲透與危害	關鍵基礎設施的防護，是確保不會受到他國藉投資、零組件輸出而產生對國家基礎設施的滲透與危害

資料來源：筆者自製

（二）關鍵基礎設施作為政治議程的經驗研究

回顧「關鍵基礎設施」相關經驗研究，大多仍聚焦在關鍵基礎設施的「工程管理」與「工程技術」問題，比如如何藉由一套理性、量化的方法或規範，降低關鍵基礎設施受到攻擊與影響的風險（Risk），以進而強化關鍵基礎設施的受災與減災能力（Moteff, 2005; White, 2019），或者用以「評估風險」的方法論或者相對應的管理技術（Theocharidou and Giannopoulos, 2015; Ongkowijoyo and Doloi, 2016）。然而，即使多數有關於關鍵基礎設施的經驗研究，聚焦在如何避免出現損壞、避免風險的發生，但也有少數經驗研究，關注到關鍵基礎設施的政治性，這類型的研究也嘗試去解構（deconstruction）關鍵基礎設施背後的政治性，或者進一步將關鍵基礎設施是為一種政治議程，試圖釐清背後的權力運作關係。

比如 Hemme（2015）以美國關鍵基礎設施的政策發展為經驗案例，美國政府在九一一的事件之後，逐漸定義了十六項關鍵基礎設施，並且必須確保關鍵基礎設施不受到自然、人為的威脅與風險，對於關鍵基礎設施的保護，則是意味政府必須持續「維持國家的安全」（National Security），甚至是政府治理正當性的來源。而 Monaghan and Walby（2015）則以加拿大警政機關對關鍵基礎設施的保護為例，指出在加拿大的案例之中，加拿大警務機關為了確保關鍵基礎設施不受破壞，便針對特定的環保運動人士進行監視，此一事件引起了極大的爭議，Monaghan and Walby（2015）認為這樣的事件反映出加拿大政府對於關鍵基礎設施保護的論述背後，隱藏著國家與企業的共謀，甚至是一種對於「政治異議」的

壓抑，此舉，也凸顯政府在關鍵基礎設施、環境保護之間的矛盾，甚至出現政府正當性危機。

除了強調政府保護關鍵基礎設施與政府正當性之間的「政治性」之外，2020年之後開始有研究者聚焦在關鍵基礎設施與「國家認同」的關係。比如 Gechkova and Kaleeva（2020）將歐洲關鍵基礎設施的保護與「難民」議題扣合，Gechkova and Kaleeva（2020）指出關鍵基礎設施停止、破壞會對於國家有效的運作造成影響，而當大量難民進入歐洲，會對歐洲的關鍵基礎設施造成衝擊之外，難民危機對於歐洲「舊大陸」之上每一個國家的「民族認同」產生新的威脅，因此，「舊大陸」的國家應該增強對於關鍵基礎設施的保護。除此之外，Crosby（2021）也嘗試將研究的視角聚焦在國家、民族認同問題之上，Crosby（2021）同樣以加拿大關鍵基礎設施為案例，不過相對於 Monaghan and Walby（2015）談論的是加拿大警政機構與環境保護團體之間的衝突，Crosby（2021）則是聚焦在加拿大警政機構與原住民社區之間的衝突，Crosby（2021）其指出關鍵基礎設施是加拿大「警務」工作的重要環節，加拿大警方內部報告卻曾經指出原住民社區，是關鍵基礎設施主要的威脅之一，因為原住民社區的出現，讓國土與基礎設施的治理，產生無法在空間上、管理上持續延展的問題，而 Crosby（2021）認為藉由加拿大警政機構將原住民社區視為威脅的案例可以發現，關鍵基礎設施保護也上升到「原住民」與「定居殖民者」的衝突，成為一種「種族化」的意識形態衝突。

回顧上述有關於美洲、歐洲關於關鍵基礎設施的經驗案例，可以發現到討論的主題都圍繞在「關鍵基礎設施」與「國家邊界」的關係之上。值得一提的是，相關的經驗研究也將關注的視角重新放置在「邊界」（Border），而這裡所指稱的「邊界」，並非指涉的是傳統對於「國界」的認知，更像是 Balibar（2002）對於「政治邊界」的觀點，「國家邊界」更像是現代國家賦予、劃定自身財產權（right to property）的「產物」，而其背後圍繞著階級、種族、國家主權、公民身份認同等複雜性因素，比如 Crosby（2021）對於加拿大警政機構與原住民社區之間的緊張關係，便呼應了如此複雜化的過程。除了 Balibar（2002）之外，Rumford（2012）也嘗試批判既存的國家邊界觀，Rumford（2012）指出需要藉由「多視角研究」（Multiperspectival Study），來切入國家邊界的討論，並且展開不同視角、不同立場來審視國家邊界的問題，比如 Monaghan and Walby（2015）試圖托出環境保護運動團體的「政治異議」，或者是 Gechkova and Kaleeva（2020）嘗試凸顯出「難

民」的視角，都可以發現與 Rumford（2012）所強調的多視角觀點相互呼應。而此種對於既有邊界劃定與認知的討論，也同樣值得融入於基礎設施的思辨之中。

除了上述關於關鍵基礎設施與獨特族群，如原住民社區、難民的討論之下。少數如 Lundborg（2011）則關注在關鍵基礎設施的形成過程，背後存在的「生命政治」意義，Lundborg（2011）指出國家關鍵基礎設施的認知過程，與政府治理的「理性化」、「生物權力」（Biopolitics）存在密不可分的關係，將關鍵基礎設施的政治性，進一步與國家之於公民的「生命政治」相互連結。

藉由上述回顧可以發現，過去有關於關鍵基礎設施的研究與討論，偏重討論關鍵基礎設施管理與方法，雖然已有部分學者如 Hemme（2015）、Monaghan & Walby（2015）聚焦在政府的治理正當性，或者如 Gechkova and Kaleeva（2020）、Crosby（2021）進一步將關鍵基礎設施與國家、民族認同、種族化問題相互連結，甚至是如 Lundborg（2011）嘗試拆解關鍵基礎設施所隱藏的生命政治的政治性。可以發現已有少部分的研究將關鍵基礎設施視為是一種乘載政治意義的技術物與政治物，除此之外，也成是指出是何種政治論述，與關鍵基礎設施產共同結構（co-construct），並且使權力得以發生。而在不同的國家可能產生不同的情境。

藉由上述文獻的回顧，我們可以發現到，確實有必要將關鍵基礎設施從單純的技術物，轉移到它所處的各種政治議程來進行探討。並且如同 Winner（2004）所述，必須進一步瞭解基礎設施的脈絡、重要性，與背後支撐起重要性的理由與論述，而且，關注它可能在不同歷史時間之下的「政治性」表現與轉化，將有助於我們去理解基礎設施更為複雜、多元化的樣貌，比如重新以多元化的視角省視「邊界」就反映了此一重要嘗試。除此之外，對於「轉化」梳理與分析，也可以幫助我們掌握各種政治價值、論述爭議，而且也能夠協助我們以一種更為動態的視角，來認知基礎設施作為一種技術政治的不穩定性。

（三）基礎設施與技術政治的批判與反思

Edwards（2003）指出基礎設施（infrastructure）形塑「現代性」（modernity）的同時，也被現代性所形塑，它作為一種「現代性據點」（modernist settlement）便與複雜的維生體系、官僚體系、物質與能源供應體系共同建構（co-construct）；因此，如果期望對基礎設施的功能與意義進行解析，就必須將基礎設施與所處的時間、空間、社會組織共同解構（co-deconstruction）。

此一說法，與 Carse（2017）認為基礎設施其實是一個「意義的歷史性問題」（Historical Problems of Meaning）的概念相仿，也就是基礎設施隨著歷史時間的遷移，其背後意義已更為多元化，而在此種意義多元化發展的過程，也反映出當代有日益擴張的「複雜系統」，在此複雜系統之上，也有更為高度分工、複雜化的社會功能，比如物流、分配邏輯。換言之，無論是 Edwards（2003）或 Carse（2017），兩者都試圖將基礎設施研究放置在不同的時空之上來進行討論，期望研究者關它所扮演的複雜社會功能。

除將基礎設施與現代複雜系統相互連結，也必須認知到基礎設施亦是現代「種種技術」（technologies）疊加與總合，以及將基礎設施視為技術物；這部分正如 Winner（2004）所提醒，研究者在探索不同的技術的同時，也必須關注技術物的政治性，所謂的政治性「是指在社會關係中的權力與權威布局，及因而發生的各種活動」（Winner, 2004: 129），換言之，基礎設施作為技術物本身，我們必須回溯其所處的環境脈絡，並且理解它的組成也將引起眾多政治立場批評與擁護，它本身即是政治場域，反映特定組織權力與權力形式。如 Winner（2004）指出：

> 若要瞭解對我們而言何種技術與脈絡是重要的及其理由，就得同時瞭解特定的技術系統及其歷史，也須充分掌握政治理論的觀念與爭議。（Winner, 2004: 150）

Winner（2004）對於政治性的定義相對廣義，並未明確指涉何種社會關係與活動。對此，部分有關於基礎設施的經驗研究，也許可以協助我們進一步理解，比如作為現代國家重要基礎設施的電力系統，Criqui（2016）以印度德里的電力系統案例指出，基礎設施擴展是社會、物質、政治產生的稜鏡（prisms）過程，上述過程，凸顯公共服務、城市結構、政治之間呈現相互依存（interdependence）的關係。同樣關注於電力基礎設施的 Verdeil（2016），則是以黎巴嫩貝魯特城市電力系統規劃來探討國家治理正當性的問題，比如以貝魯特的非正式電力系統為案例，電網圍繞著社會與政治主張，而基礎設施發展也可能是一種「政治選擇」。

從 Criqui（2016）與 Verdeil（2016）的研究來觀察，可以發現到有關基礎設施缺乏、擴張、延伸的探討，多半會聚焦在國家與人民關係，以及國家、政府如何確保人民可以獲得穩定、安全、可持續性的民生基礎資源與服務。更為重要的是，圍繞在對於政府治理品質與正當性的討論之下，也掩蓋了更多政治價值與立場，這樣的過程並非是一種穩定的狀態，而是一個充滿緊張、衝突、折衷的動態

過程。至此，可以發現兩個層面的政治性討論，一者是國家治理正當性，一者則是埋在獨特國家發展脈絡所延伸出的政治議程，如宗教、種族、階級甚至是國族意涵。

延續上述關於基礎設施所反映出來的政治課題，Nolte（2016）則以耶路撒冷輕軌（Jerusalem Light Rail, JLR）為研究對象，指出耶路撒冷輕軌的規劃與興建歷程具高度政治性，Nolte（2016）區分「政治基礎設施」（political infrastructures）以及「基礎設施政治」（politics of infrastructure）兩種用來分析基礎設施政治性的概念，並且指出強調基礎設施是政治的一種「工具」，也可能忽略掉「基礎設施就是政治性本身」（infrastructure as a site of the political itself）的討論，比如 Nolte（2016）便認為耶路撒冷輕軌就是一個差異機器（difference machine），它的出現讓許多原先就存在的立場、衝突、協商過程又可以被顯現出來。

與 Criqui（2016）、Verdeil（2016）及 Nolte（2016）強調關注於基礎設施建構過程中的緊張、衝突的論述相似，Carse and Kneas（2019）則進一步以「未完成」（unfinished）概念來分析基礎設施背後的緊張、折衷、協商關係，「未完成基礎設施」（Unfinished Infrastructures）在 Carse and Kneas（2019）陳述之中，成為一種啟發式方法，讓人們理解基礎設施背後的知識、制度、主體性的變化，並且拆解人們與基礎設施之間複雜的政治與社會關係。Carse and Kneas（2019）對「未完成基礎設施」的指涉可以是特定的基礎設施，如道路，也可是更為廣義的社會技術與治理系統，此一概念也有助於分析處於不斷變動、多元化的社會現象與課題，而此種不斷變動的狀態，也正可呼應 Nolte（2016）所述，必須同時理解到基礎設施的政治性課題，必須同時針對「政治基礎設施」（political infrastructures）以「基礎設施政治」（politics of infrastructure）來進行分析。

藉由上述相關文獻的回顧，我們可以發現到，有必要將關鍵基礎設施從單純的技術物，轉移到它所處的各種政治議程來進行探討。並且如同 Winner（2004）所述，必須進一步瞭解關鍵基礎設施的脈絡、重要性，以及背後支撐起重要性的理由與論述，而且，關注它可能在不同歷史時間之下的「政治性」表現與轉化，將有助於我們去理解基礎設施更為複雜、多元化的樣貌。在此同時，我們也必須留意基礎設施背後的不穩定、持續變動中的狀態（Criqui, 2016; Verdeil, 2016; Nolte, 2016; Carse and Kneas, 2019）。尤其是對於「轉化」的理解與分析，也可以幫助我們充分掌握各種政治價值、論述的爭議，而且也能夠協助我們以一種更為動態視角，來認知基礎設施作為一種技術政治的不穩定性。

三、台灣關鍵基礎設施的政策形構

（一）中資、中國產品與港口：國家安全為名的國家「外部防禦」

藉由美國、歐盟、日本對於關鍵基礎設施的政策論述，可以發現到我們必須將關鍵基礎設施視為一種「技術政治物」（比如，日本對於資通訊關鍵基礎設施的陳述之中，便提到訊與通訊技術（IT）操作技術（OT）的科技融合，藉此表現技術演化趨勢之外，此一技術發展趨勢也可能提高國家治理的風險），而非單純的維生系統之外，三者也強調的關鍵基礎設施的「相互依存性」與「動態性」。而這樣的發展特徵，在台灣是否存在？又是以什麼樣的方式被建構？

台灣的關鍵基礎設施的規劃，最早的推動者為－行政院國土安全政策會報，其前身為 2003 年成立的「行政院反恐怖行動政策小組」。在 2007 年之後其正式更名為「行政院國土安全政策會報」。而從該單位成立背景來看，可以清楚發現該單位的設立，主要是呼應 2001 年 9 月份美國受到「蓋達組織」的「恐怖攻擊事件」的影響；設置之初，便清楚提到其設置的目的，在於擔任行政院在反恐怖攻擊行動、災害防救、防衛動員、核子事故、傳染病疫病、毒災應變、國境管理、資訊安全議題的主要幕僚單元，藉由行政院國土安全政策會報的任務執掌來看，其最主要的目標在於協助行政院整體跨部會的行政資源，建構台灣的「國土安全應變網」，以因應各種可能出現的基礎設施危害。

行政院國土安全政策會報在 2014 年，首次提出的《國家關鍵基礎設施安全防護指導綱要》，其對於關鍵基礎設施給予了以下的說明與定義：

> 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，造成人民之傷亡或財產損失，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。……，係指涉及核心業務運作為支持國家關鍵基礎設施持續營運所需之重要資通訊系統或調度、控制系統，亦屬國家關鍵基礎設施之重要元件（資通訊類資產）應配合對應之國家關鍵基礎設施統一納管。（行政院國土安全政策會報，2014：2）

藉由檢視台灣《國家關鍵基礎設施安全防護指導綱要》對於關鍵基礎設施的內涵可以發現，台灣在 2014 年首次提出關鍵基礎設施的政策規畫中，對於關鍵

基礎設施所可能受到的潛在「威脅」並未相當明確，僅提到任何可能造成政府、社會運作受損的人為、自然災害。然而，值得注意的是，2014 年的指導綱要中，便已經將資通訊系統視為重要組成，而且指出國家必須針對資通訊基礎設施進行統一的管理，以確保國家關鍵基礎設施的調度、控制是在無慮的狀態之下。

1. 台灣關鍵基礎設施的政治議程, 始於「限制中資」投資關鍵基礎設施等

然而，倘若藉由從政治議程的角度來觀察，在 2014 年首次由行政院所提出《國家關鍵基礎設施安全防護指導綱要》之前，台灣有關於「關鍵基礎設施」的討論就已經存在，在不同的面向上，引起了眾多的爭議、辯論；此外，值得留意的是，如果按立法院的議事公報之紀錄，台灣首次將關鍵基礎設施完整納入政治議程之中，便是與 2009 年「中資來台辦法」的議案有關。時任立法委員賴清德指出：

> 其他國家對外國來本國投資，都有一些審查原則及限制。像美國的審查原則是，對於外國的投資，委員會必須考量該項投資對國家安全、外國政府控制、……，據以做成對關鍵基礎建設及科技之限制項目。英國的審查原則為，禁止危害國家安全及公共利益的投資，如敏感軍事機密；限制項目包括特定重要產業及企業，...。對外資設限，各國皆然。但是我們對全世界唯一的敵對國家—中國，竟然不設防！如果把這次開放的 100 項項目與各國限制外資投資的項目對照，……，我們對中國竟不設防！（立法院，2009: 356）

藉由上述可以發現，在台灣立法院的相關政治議案之中，關鍵基礎設施首次出現在議案之中，是出現在－「是否針對中國資金的投資項目與方式進行管制」的政治議程之中。然而，台灣關鍵基礎設施內涵為何，其實尚未具體化；此時，關鍵基礎設施被當成是一種「政治因素」被援引，關鍵基礎設施本身，尚未成為一個獨立、明確的政治議程，內在的政治性，也尚未清晰化。2010 年，關鍵基礎設施再次出現在台灣立法院的政治議程之中，但與 2009 年相當不同的是，這段時期的的討論並非聚焦在國際關係，而是水資源、農業與環境政策。

值得留意的是，在 2014 年行政院國土安全政策會報提出的《國家關鍵基礎設施安全防護指導綱要》的前兩年，台灣關鍵基礎設施又重新回到「中台政治」

關係下進行討論，一方面圍繞在是否開放、限制中資投資特定產業部門之外。時任立法委員蘇震清指出：

> 世界各國對於是否開放外資參與基礎建設，多數都是採取嚴格限制的保守態度。例如美國禁止外資投資關鍵基礎建設，至於其他重要產業、設施也有嚴謹的審查機制，其外國投資委員會更結合國安、財政等單位所組成。日本、荷蘭、法國限制外資投資鐵路、機場大眾運輸（立法院，2012a: 78）。

另一方面，也在網路攻擊與「資通安全」討論，引起劇烈的辯論，時任國家安全局副局長張光遠指出：

> 中共為全面掌握我國防、政治、外交、兩岸等發展動態，對我發動網路攻擊竊密對象已由政府機關、駐外館處，轉向民間智庫、電信業者、委外廠商等，並轉變思維攻擊我較疏於防護網路節點設施或車輛交通號誌儀控設備、寬頻路由器、工業微電腦控制器、網路儲存系統等嵌入式系統裝備，預判未來恐擴及我國關鍵基礎設施（立法院，2012c: 7）。

藉由上述可以發現，2013 年由國防委員會邀請國安局針對－「我國如何因應網軍與駭客攻擊並強化資訊安全措施」進行報告一案，可以視為是台灣關鍵基礎設施，成為獨立的政治議程的重要轉捩點。諸多討論的議題與內涵，也成為台灣在 2014 年《國家關鍵基礎設施安全防護指導綱要》先聲。若進一步解析國安局在－「我國如何因應網軍與駭客攻擊並強化資訊安全措施」的陳述，可以發現在相關的討論，已經開始應用「國土防禦」概念來充實關鍵基礎設施建構的正當性，比如國安局對於強化資訊安全措施的說明。時任國家安全局副局長張光遠指出：

> 加深我國總體防禦縱深，強化電信關鍵基礎設施防護：我國為高度資訊化社會，……，然各類通訊均需透由骨幹網路進行通訊傳輸，故面對日益嚴峻的資安威脅與挑戰，除加強個人資安防護觀念，更需結合國內電信業者力量，前進部署防護措施至電信骨幹網絡，組建多層次防禦縱深機制（立法院，2012c: 7）。

2. 轉向「滲透」的防禦思考，禁止中企產品應用在台灣關鍵基礎設施

延續國安局有關於強化台灣國家資訊安全措施的討論，在同場委員會的議程之中，也出現了對於台灣在國家戰略、國際競爭格局上的爭議。比如，時任立法委員姚文智指出：

> 為什麼馬政府要把台美之間 2007 年好不容易建立起來的資通安全論壇擱在一邊呢？……，何況剛剛很多委員都提到美國發生的問題。最後是有關博勝系統的問題，你們在報告中提到，為了增加防禦縱深，要和民間合作，強化電信關鍵基礎設施；我們一方面要排除中國網軍介入，包括他們的廠商，另一方面也要擴大民間合作（立法院，2012b: 54）。

延伸觀察行政院國土安全政策會報提出的《國家關鍵基礎設施安全防護指導綱要》，不難發現到該指導綱要，對於關鍵基礎設施的內涵，相當程度上延續了 2013 年第 3 會期外交及國防委員會第 20 次全體委員會的討論，而相較於 2009、2010 年，台灣在 2013 年之後，已然將關鍵基礎設施視為獨立的政治議程，並且引起了眾多關於國家戰略、國家定位、國際競爭格局選擇的政治討論：一個清晰的例證是 2018 年 9 月由國家資通安全辦公室發布的《國家資通安全戰略報告：資安即國安，打造安全可信賴的數位國家》便是由總統府所直接指引，綜合考量了全球資訊武器化、國際政治經濟局勢轉變等議題，將資安與國家基礎設施整合探討，並進一步上升至「國家安全」議程之中（行政院資通安全辦公室，2018）。

2020 至 2021 年之後，由於美中貿易戰、科技戰的發生，台灣對於關鍵基礎設施的討論更加劇烈，除了上述數位政府議題，許多討論也反映出台灣處在美國、中國大國競爭的宏觀環境變化與國際政治關係、媒體輿論對於台灣「國家安全」新想像與認知。而這樣的安全或危機的想像，圍繞在更深層的「滲透」的概念。比如 2020 年有關於關鍵基礎設施與「危害資安產品」的議案，時任立法委員的羅美玲和張世杰指出：

> 但查至 109 年 10 月止，行政院尚未公布危害國家資通安全產品廠商清單。……，惟近年中國資通產品的安全疑慮高漲，且台灣所面臨之國家安全疑慮的深度與廣度亦與他國不同，仍有必要儘速進行相關評估。爰請行政院積極加速推進危害資安產品廠商清單制訂作業，供各機關、學校、公營事業及八大關鍵基礎建設等明確遵循（立法院，2020: 254-5）。

藉由上述關鍵基礎設施，再次於立法院引起的議論之中，可以發現到論述的內容與 2012 年「我國如何因應網軍與駭客攻擊並強化資訊安全措施」相較之下，雖然兩者都聚焦在國家層級的資訊安全（cyber security），不過，2012 年關注在台灣應用資通訊技術為基礎的關鍵基礎設施，是否會受到中國網路「外來」攻擊，而 2020 年之後，相關的政治論述則是聚焦在台灣的關鍵基礎設施，是否會因為應用了「危害產品」而被進一步在內部受到「滲透」，所指涉的安全、危害內涵已然更加的隱微，且擴展的範圍也更為全面。除代表 2020 年之後，台灣與中國敵對關係的論述更加深化之外，可再細究的是，產品是否會受到「滲透」的討論，也將國家安全性維護的思考，進一步與國際貿易、全球產品供應鏈的經濟活動相扣合，此舉，除了反映台灣相關政治議程被納入到美國、中國大國競爭格局中，也進一步將關鍵基礎設施的內涵賦予更為抽象的想像。

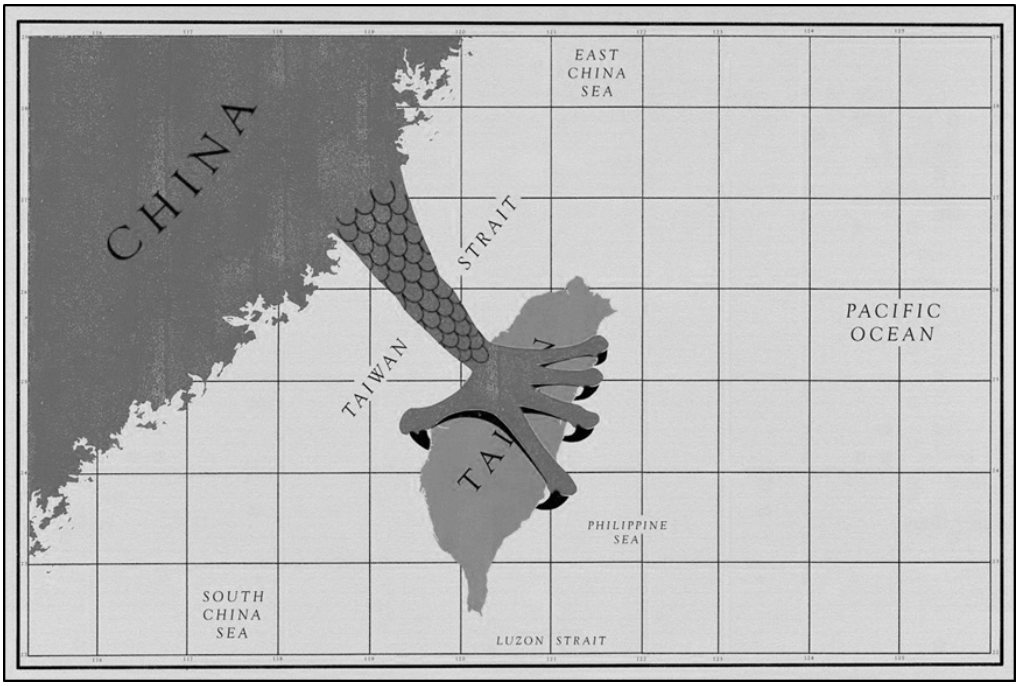

圖 1 《外交》（Foreign Affiair）雜誌描繪台灣受中國威脅之意象（資料來源：Mastro, 2021）

3. 東方海外航運公司向港務公司承租高雄港 65、66 號碼頭事件

倘若「危害資安產品」意味著一種對於虛擬接口（virtual Port）的滲透防禦，在同樣的思考之下，台灣實體的港口（port）－高雄港在 2021 年 8 月也同樣引起

具有中資色彩的企業如承租高雄港碼頭，是否會對於台灣產生國家安全的疑慮。相關的討論出現在 2021 年高雄市議會的議案之中。時任高雄市議員林于凱指出：

> 這個事情也是國安議題，就是中資入侵高雄港。……，中共透過「高明的股權交易」實質控制高雄港的碼頭。……你看一下這個高明貨櫃碼頭公司後面的股權比例，政龍投資就占了三成，政龍後面的人物有誰，我們等一下再來講。政龍就是由中資中遠、中國海運及招商國際三個合組的，占高明 30%的股份，它號稱港資，其實後面都是中資（高雄市議會，2021: 13）

事實上，東方海外貨櫃航運公司承租高雄港 65、66 號碼頭是否會對於台灣的國家安全造成疑慮，相關的討論在 2018 年 9 月就已出現在日經亞洲（Nikkei Asia）的一篇名為：「台灣悄悄讓中國國營公司接管港區」（Taiwan quietly lets Chinese state company take over port area）的報導之中，該報導中指出蔡英文總統相對於前一任總統來說，雖然對於中國採取更為強硬的對抗，但卻開放中國遠洋運輸集團（China Ocean Shipping Company, COSCO）集團下的東方海外貨櫃航運公司（The Orient Overseas Container Line, OOCL）繼續承租高雄港碼頭感到疑慮，日經亞洲（2018）也進一步將此事件放置在美中大國對抗的格局之中，探索中國是否藉由國有企業的海外投資手段，來達到控制其他國家的脈絡中來進行探討。

圖 2 高雄港第 66 號碼頭（資料來源：Li, 2018）

若觀察高雄市議會於 2021 年的討論內涵，可以發現到大致上與日經亞洲的論述一致，皆質疑投資高雄港的企業背後，是否具有「中資」色彩，以及是否會削弱台灣政府對於關鍵基礎設施的控制力。除高雄市議會之外，經濟部投資審議委員會（2022）也提出了「跨部會密切合作確保高雄港營運安全」，強調該案已經過投資審議，已要求中資持股比率須低 50%、持股不得超過其他非陸資最大股東，並且要求對投資事業，不得具有控制能力等限制條件。然而，值得一提的是，除了對於「中資」的討論之外，此一案例也提到了資訊與監控的「技術」。時任高雄市議員林于凱指出：

> 高明貨櫃碼頭配備的自動化智慧型橋式起重機可監控碼頭狀況。……，而我們港口管理系統使用的是韓國作業系統。不過我們看一下硬體部分，高明碼頭採用的是振華重工的設備，它是什麼？是中國國企。…，台灣高雄港是最重要的港口，不管是軟體或硬體，它掌握在中國手中都是有疑慮的。而這個起重機設施，上海振華重工目前在全世界市佔率 70%，……，如果還有 30%其他公司市場，我們為什麼不考慮呢？……。……智慧化的碼頭監控系統？它就是一個資訊傳輸的節點，高雄港所有貨運吞吐、所有貨料的移動，全部都在他的監控底下（高雄市議會，2021: 13）。

藉由上述議案對於的東方海外貨櫃航運公司承租高雄港的爭議，可以發現到對於台灣關鍵基礎設施「外部防禦」作為有二，一者是藉由投資的限制與審查，另一者則是排除中國企業所生產的資通訊產品，此一案例恰巧呼應上述兩個案例（限制中資投資特定產業部門、禁止中企產品應用）的政治內涵。值得留意的是，高雄港碼頭的投資爭議，也恰巧融合了實體、虛擬兩個港口（port，或稱為接口）的外部防禦意象，顯現「接口」往往是容易受到滲透之處，無論對於實體的海運碼頭，或是對於虛擬的資訊傳輸接口，都是必須強化保護、控制、防禦的地方。

綜整上述三個案例，可以發現台灣關鍵基礎設施的建構與美國、歐盟、日本相同，保有相當動態、不穩定性，「關鍵基礎設施」作為一種「空的意符」（empty signifier），背後的意義不斷被不同的價值、能動者所產製。這樣的說法，也可與 Laclau（2005）《民粹理性》（On Populist Reason）一書所提出的觀點相互映照。

Laclau（2005）提出了「空的意符」以及「浮動的意符」（floating signifier）兩種政治建構的實踐觀，「空的意符」在 Laclau（2005）觀點之中，是一種表達

普遍觀念的政治思想與結構，其作用是將每一個群體，綁定到一個集體身份之中，而「浮動的意符」則進一步擴張，指出某個政治物或詞語，對於不同的人來說，可能意味不同的內涵，而這與解釋的人或權力單元，如何進行詮釋與表達其背後含義有關。無論是空的意符或是浮動的意符，都反映出背後複雜化的政治論述與建構過程，它們亦顯現出特定的政治意識與論述的鬥爭（Barros, 2023），其具備的批判性概念，能夠進一步論證關鍵基礎設施作為一種技術物、政治物，其無法以單一意義來詮釋，除此之外，研究者也必須讓它持續保有「開放性」，因為，關鍵基礎設施可能也指涉了一個不穩定、建構中的集體身份。

將關鍵基礎設施的建構視為「空的意符」，也適用於分析台灣關鍵基礎設施的建構過程，比如台灣與中國之間的「敵我關係」，便是台灣關鍵基礎設施最先、最為核心的政治議程。此一過程在 2014 年行政院提出正式指導綱要之後仍持續發生。除此之外，由「限制中資投資台灣關鍵基礎設施」、「中國資通產品視為危害資安產品」、「東方海外航運公司承租高雄港」三個案例，可以發現台灣關鍵基礎設施的政治議程，皆提到在「國家安全」的考量下，針對可能會被他國滲透的基礎設施，無論是虛擬資訊數據接口（Digital Port），或是實體的貨運港口（Port），台灣都必須強化保護，以防禦外在的挑戰。在此一論述之下，真正的關鍵作用力為劃定「敵我關係」的「邊界」。

除了上述三個案例之外，台灣在不同時期之間，也不斷出現將關鍵基礎設施納入於國家安全的議論。比如 2024 年 4 月 30 日內政部警政署保安警察第二總隊擴編，內政部便提及該組織的擴編、轉型，是為了因應全球國際地緣政治情勢的變化，灰色地帶衝突及新型態恐怖攻擊的威脅逐漸興起，比如滲透、無人機攻擊等，因此，必須擴編組織、增加警力員額來，防護台灣的關鍵基礎設施（內政部警政署，2024）。藉此也可再次映照出，以國家安全為名的台灣關鍵基礎設施的建構過程，背後的關鍵作用力是劃定「敵我關係」的「邊界」。

（二）eID、半導體與護國神山：新國家與國族的「內部生產」

1. 數位身分識別証 eID

2015 年至 2019 之間，關鍵基礎設施在立法院的政治議程之中，多數仍延續先前有關於是否開放中資？以及如何強化對於他國資金的審查機制的討論之上。然而，進入 2019 年之後，關鍵基礎設施的討論開始融入更多新興議題，其中，

又有許多政治的討論面向落於政府與人民的數位治理（E-Governance）的關係，以及此種新型態的數位治理關係，會不會進一步轉化成為新的資訊安全風險。

如 2019 年 8 月由行政院推出－「數位身分識別證（New eID）」政策方案，在立法院便引起了諸多的討論，而且也涉及到多元化的關鍵基礎設施認知，擴充了台灣關鍵基礎設施的內在政治，也再次驗證關鍵基礎設施的動態特徵。如國家發展委員會法制協調中心（2019），便嘗試釐清 eID 與政府基礎架構之間的關係。時任國家發展委員會法制協調中心參事林志憲指出：

> New eID 為智慧政府服務的基礎架構，是在保護個人隱私與資訊自主下運作。New eID 是智慧政府服務的基礎架構，可使政府加速將創新科技導入客製化民生服務。New eID 係作為身分辨識之鑰匙，並採行「eID 版面個資揭露最小」、「隱私資料加密保護，需民眾同意及需內政部授權方能讀取」等做法保護隱私及資訊自主。（立法院，2019: 349）

圖 2 台灣數位身分證（eID）換發範例 （資料來源：內政部，2021）

除了國家發展委員會（2019）將 eID 視為實現智慧政府、數位政府「基礎」的論述之外，eID 與關鍵基礎設施的連結則是出現在 eID 背後的資訊系統建置，比如內政部（2017）對於 eID 資訊安全的說法：

> 為確保 New eID 各相關系統（如 New eID 製發管理系統及自然人憑證管理系統等）將依循關鍵基礎設施安全防護指導綱要提升防護能量，並符合資通安全管理法規範，執行資通安全責任等級 A 級之公務機關應辦事項，導入資訊安全管理制度、資安監控中心等，且建置過程將由第三方廠商做獨立驗證。……。New eID 相關系統將建置於內政資料中心之內網環境，透過「共用雲端基礎服務」優質基礎設施與網路資安環境，完善整體資訊安全防護（內政部，2017）

事實上，有關於 eID 資訊安全的討論，除了一般性關於公民隱私、資料保護的討論之外，也有許多議論牽涉台灣與中國獨特的政治關係，比如 2019 年 9 月邀請內政部以「新式數位身分證之法律授權」為題內政委員會報告，便有不少的立法委員以不同面向提出 eID 可能出現的「國安問題」。比如，時任立法委員的許毓仁指出：

> 現在中共針針對我們即將換發數位身分證，埋了很多駭客洞在裡面，這個是掌握到的情資。部長這個很重要，我們的標書都是公開的，他們看不到嗎？他們當然看得到，而且每個月都在嘗試，我們的健保資料已經被突破了，戶政資料也有被入侵的可能性，所以資安漏洞是國安問題（立法院，2019: 381）。

同樣聚焦在資料安全與「國安問題」之上的，還有時任立法委員的鍾佳濱，其亦指出：

> 2020 年 10 月數位身分證要上路，你們這裡說現在的紙本身分證揭露 11 項個資，以後數位身分證只有 5 項個資，其中有沒有包括照片？...。說到人臉辨識，我們說人在做天在看，但在中國是人在做黨在看，海康威視的人臉辨識到處都可以識別，...。在台灣，現在已經有 136 支海康威視的監視器入侵台中，今年行政院發布「各機關對危害國家資通孜全產品限制使用原則」，結果馬上就有人爆料台中的地下道有這些，市政府就很緊張趕快換掉，...所以今天很多對數位身分證的關注，其實我覺得現在根本不需要數位身分證，只要有一張臉就夠了（立法院，2019: 381-2）。

回顧上述兩個與「中國」有關的 eID 在執行層面的議論，不難發現中國造成的台灣國家安全因素，仍然是 eID 討論的重要基調之一，除了「中國駭客」之外，新興的生物、臉部辨識技術也成為討論的要角之一。比如 eID 的個資規畫之中，是否包含了公民的「相片」？以及如果在 eID 遺失的情境，甚至是台灣由於採用中國所製造的監視器，而使得台灣公民的臉部特徵被中國企業所擷取之時，那麼是否會對於國家、公民的安全產生危害，這些都成為了延伸出來的新興辯論之處。

整體而言，eID 的政治議程值得進一步被關注的原因有二：首先，eID 建置必須以確保國民的資訊安全為前提，因此相關的晶片、資訊系統與後台資料庫，必須依循《國家關鍵基礎設施安全防護指導綱要》進行規範；其次，相較 2014 年之前，台灣關鍵基礎設施的核心討論，eID 所能引起的討論更為的多元化，其中至少包含兩種內涵，一種仍是放置在台灣、中國獨特的國際政治關係之下來思考特殊情境發生之時，如何確保公民、國家不至於受到危害，另一種則是在「智慧政府」、「數位政府」大論述之下，嘗試建構一種新型態的國家（政府）與人民的內部治理關係，這種新型態的內部治理關係，融合了數位治理（新型態）、政府正當性（如執行機關必須確保公民權、隱私權不受侵犯）、甚至指涉生命政治（如 eID 是否包含相片、臉部等生物特徵等）等不同層面的思考。而值得再次提出的是，上述兩種內涵也經常產生相互牽連、辯證的關係，比如 eID 如採用公民相片作為顯露的個資，那麼在中國產製的監視器、辨識裝置大舉進入台灣之時，是否對於公民產生危害就是顯著的案例，其主要作用力在於產生新的政府與公民關係。

2. 半導體成為全球關鍵基礎設施，「護國神山」論述背後的國族建構工程

正如 Carse（2017）指出基礎設施是「意義的歷史性問題」（Historical problems of Meaning），可以發現台灣關鍵基礎設施的價值、意義，也隨著歷史時間遷移。2018 年之後的美中對抗關係，不僅持續地加深台灣關鍵基礎設施的「國土防禦」思維，也孕育出一種融合國際政治、經濟的情境。比如在 2021 年的立法院議程之中，此時受到較多關注的部會，已從國安局、國防部，轉移到經濟部，許多對關鍵基礎設施討論，轉而聚焦高科技半導體、晶片生產等高科技的企業與產品。比如，時任立法委員李貴敏指出：

> 我們知道台積電是台灣的護國神山，所以，也因為中美貿易的關係，我們現在看到很多的布局都是根據全球 IC 需求，Intel 也說要搶食代工的

> 市場，請問經濟部做了對台灣影響相關因應措施的沙盤推演了嗎？（立法院，2021a: 457）

除此之外，亦有將台灣半導體產業與關鍵基礎設施相互比擬者。如時任立法委員的葉毓蘭指出：

> 2017 年張忠謀就曾表示過，政府只要把基礎建設搞好就對了，其實國家基礎建設，也就是 critical infrastructure，…，如果我們的基礎建設沒有辦法支撐住高科技產業，會不會造成另外一個國安危機？（立法院，2021b: 398）

事實上，在 2020 年末起，台灣與關鍵基礎設施的討論，已提升到更為宏觀的美中競爭環境之中，牽引出更為複雜的政治性。半導體供應鏈在美中競爭格局之中成為了要角，此時，有關於關鍵基礎設施的討論可分為二：第一，關鍵基礎設施被視為是供應台灣半導體產業持續獲得競爭力的要素，包括能源、水資源等是維繫台灣半導體產業優勢的關鍵；第二，若以全球產業「供應鏈體系」來觀察，半導體即為全球高科技產業的關鍵基礎設施，而在全球半導體供應鏈體系中扮演要角的台灣，台灣的國家安全與主體性進一步上升為全球「供應鏈體系」的關鍵。

可以發現上述兩種討論內涵，支撐起 2020 年之後的關鍵基礎設施政治議程，其中，又以後者更具有創造性。值得留意的是，縱然其主題似乎圍繞在半導體、全球產業供應鏈，不過，如果細部觀察 2020 年之後台灣有關半導體的政治議程，不難發現到其創造性，而它是從「護國神山」的詞彙進一步延伸，使得「半導體」、「台灣」在國際安全為名的論述下進一步被黏合，當半導體成為全球產業供應鏈的關鍵基礎設施，而「台灣安全」就成為維護此一關鍵基礎設施的要件。「護國神山」等反覆出現在半導體與關鍵基礎設施的論述，便反映了台灣的國族工程。

再次回顧 Winner（2004）、Carse（2017）等基礎設施之技術政治的理論視角，台灣關鍵基礎設施的建構，背後不僅反映出不同的歷史情境、脈絡，背後更存在許多共同建構的政治意識與價值，而這樣的意識是存在於浮動、進行中的狀態，甚至不同的意識、價值還處於相互生產的關係，具有高度的創造性。藉由「數位身分識別証 eID」、「台灣半導體護國神山」兩個案例，可以再次驗證這樣的觀察。

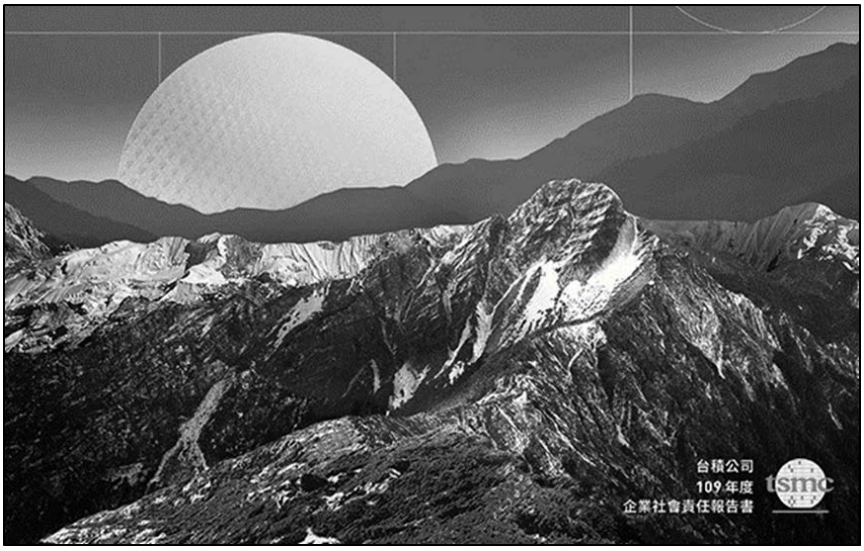

圖 3 台積電社會責任結合玉山、晶圓之企業意象（資料來源：台灣積體電路製造股份有限公司，2020）

再回到國家安全的問題上，可以發現台灣關鍵基礎設施的技術政治存在兩種相互扣合的作用力（或發展路徑）。首先，「限制中資投資台灣關鍵基礎設施」、「中國資通產品視為危害資安產品」、「東方海外航運公司承租高雄港」三個案例體現出一種外部防禦觀，它有非常明確的敵我關係，比如必須針對中資投資台灣關鍵基礎設施，建立強化審查機制，並且禁止具有「紅色供應鏈」色彩的企業與零組件，被採用在台灣關鍵基礎設施的組成成分之中，這代表著一種極為強烈的「國家邊界」劃定作用，意味著一種外部防禦。其次，「數位身分識別証 eID」、「台灣半導體護國神山」兩個案例，前者涉及一種新的國家與公民治理的新關係，而與台灣半導體高科技產業、產品的討論，則持續被扣合在美中競爭的語境之中，比如台灣半導體產業作為台灣「護國神山」的論述，除了顯現出「技術浪漫主義」（technological romanticism）內涵之外，它更藉由不間斷的政治辯論，使台灣的半導體的產品與特定企業，成為國家對內生產台灣民族、國族歸屬感的中介（interface），它蘊藏極精細的「新國族」的內部生產過程。兩種作用力同時發生，而兩種作用力都嘗試藉由不同的政治意識去定義何為關鍵基礎設施的「邊界」。

四、結論：未完成的關鍵基礎設施，在未完成的國家

回顧台灣關鍵基礎建設的政策、政治議程，台灣的關鍵基礎設施作為「空的意符」（empty signifier），其背後的意義，不斷地被產製；之所以會在不同的歷史

時間之中，出現不同的認知與評估思考，其實是反映出台灣與中國之間獨特國家關係之外，也反映出不同的宏觀政治經濟環境因素，比如美中的大國競爭格局，便牽引了台灣自 2012 年之後的關鍵基礎設施討論，而這樣的過程在 2020 年之後變得更加地強烈，比如是否限制中資投資台灣特定的基礎設施，就是明顯的例證。這也再次應證，基礎設施並非是單純的技術物，關鍵基礎設施也同樣是乘載各種政治價值、意識的載體。而且在 2013 年國安局提出「我國如何因應網軍與駭客攻擊並強化資訊安全措施」，衍伸出行政院提出國家級的關鍵基礎設施保護措施之後，關鍵基礎設施在台灣，已然成為獨立的政治議程，而它本身即是「政治性本身」（infrastructure as a site of the political itself）。

值得留意的是，雖然在 2015 年之前，已有許多有關於關鍵基礎設施的討論，指涉到台灣、中國之間的「國土防禦」問題，但在 2020 年後，諸如「危害資安產品廠商清單制訂作業」等更為嚴格的管制方案出現，可以發現到關鍵基礎設施作為劃定「國家邊界」的功能已然更加強化；此一強化的過程，不僅出現在實體與虛擬國土的防禦策略，也反映在台灣關鍵基礎設施的內部「成分」，必須排除中國產品與零組件的「滲透」，其中隱含著更為強烈的政治性，而這樣的政治性，無疑是圍繞在台灣與中國獨特的國家關係之上。除此之外，半導體同時需要關鍵基礎設施的支持，以及半導體同時作為關鍵基礎設施本身，也同樣是 2020 年後台灣關鍵基礎設施的兩大核心主題，有別於「危害資安產品廠商清單制訂作業」等措施，其作用是在劃定台灣與另一個國家的關係，半導體產業與關鍵基礎設施的連結之中，也不斷在內部發現到國家認同的元素，其核心作用在於－建立國家。

以台灣的經驗案例來看，關鍵基礎設施的認知與建構，與台灣國家建構工程是一種「共建」（co-construction）過程或者關係，然而，在台灣無論是關鍵基礎設施或是國家，都仍然處在「未完成」（Unfinished）的狀態，而這樣的過程預期將會持續發生，或者持續填充基礎設施內生的政治意義。

謝誌

本文修改前曾發表於 2022 年 4 月 16 日第二十六屆國土規劃論壇於成功大學。感謝黃麗玲老師於本文撰寫過程的指導，以及王志弘老師在「基礎設施的技術政治」課程中的指引。感謝本刊兩位評審的意見，協助澄清了本文核心的討論內容與論點。

參考文獻

內政部（2017）《與社會各界溝通之重要活動及 New eID 規劃內容重點》。台北：內政部。

內政部（2021）《數位身分識別證(New eID)-新一代國民身分證換發計畫》。台北：內政部。

內政部（2024）〈保二總隊擴編轉型編成典禮〉。https://www.npa.gov.tw/ch/app/news/view，取用日期：2024 年 9 月 19 日。

台灣積體電路製造股份有限公司（2020）《109 年度企業社會責任報告書》，新竹：台灣積體電路製造股份有限公司。

立法院（2009）《立法院公報》98（44）（委員會紀錄）。台北：立法院。

立法院（2012a）《立法院公報》101（13）（委員會紀錄）。台北：立法院。

立法院（2012b）《立法院公報》102（29）（委員會紀錄）。台北：立法院。

立法院（2012c）《立法院公報》103（29）（委員會紀錄）。台北：立法院。

立法院（2019）《立法院公報》108（68）（委員會紀錄）。台北：立法院。

立法院（2020）《立法院公報》109（101）（委員會紀錄）。台北：立法院。

立法院（2021a）《立法院公報》110（39）（委員會紀錄）。台北：立法院。

立法院（2021b）《立法院公報》110（50）（委員會紀錄）。台北：立法院。

行政院國土安全政策會報（2014）《國家關鍵基礎設施安全防護指導綱要》。台北：行政院。

行政院資通安全辦公室（2018）《國家資通安全戰略報告：資安即國安，打造安全可信賴的數位國家》。台北：行政院。

高雄市議會（2021）《高雄市議會第 3 屆第 5 次定期大會第 37 次會議議事錄》。高雄：高雄市議會。

經濟部投資審議委員會（2022）《跨部會密切合作確保高雄港營運安全》。台北：經濟部。

Balibar, Etienne, (2002). World Borders, Political Borders. *PMLA*, 117(1): 68-78.

Barros, Thomás Zicman, (2023). The polysemy of an empty signifier: the various uses of Ernesto Laclau's puzzling concept. *Journal of Political Ideologies*. Published online

Cantelmi, R. G. Di Gravio & R. Patriarca, (2021). Reviewing qualitative research approaches in the context of critical infrastructure resilience. *Environment Systems and Decisions* (41): 341–376.

Carse, Ashley and David Kneas (2019) Unbuilt and Unfinished: The Temporalities of Infrastructure. *Environment and Society: Advances in Research* (10): 9-28.

Carse, Ashley, (2017). Keyword infrastructure: How a humble French engineering term shaped the modern world. In P. Harvey, C.B. Jensen and A. Morita (eds.), *Infrastructures and Social Complexity: A Companion* (pp. 27-39). Abingdon, Oxon: Routledge.

Criqui, Laure, (2016). Delhi: Questioning urban planning in the electrification of irregular settlements. In Andrés Luque-Ayala and Jonathan Silver (eds.), Energy, Power and Protest on the Urban Grid: Geographies of the Electric City (pp. 86-111). Abingdon, Oxon: Routledge.

Crosby, Andrew, (2021). The racialized logics of settler colonial policing: Indigenous 'communities of concern' and critical infrastructure in Canada. *Settler Colonial Studies* 11(4): 411–430.

Cybersecurity and Infrastructure Security Agency, (2021). Critical infrastructure sectors. Retrieved from https://www.cisa.gov/critical-infrastructure-sectors (Date visited: Oct 31, 2021)

Edwards, Paul N., (2003). Infrastructure and modernity: Force, time and social organization in the history of sociotechnical systems. In Thomas J. Misa, Philip Brey, and Andrew Feenberg (eds.), *Modernity and Technology* (pp. 185-225). Cambridge, MA: The MIT Press.

European Commission (2021). European Critical Infrastructure. Retrieved from https://ec.europa.eu/home-affairs/whats-new/evaluations-and-impact-assessments/european-critical-infrastructure_en (Date visited: Oct 31, 2021)

European Parliament, (2008). European critical infrastructure. Retrieved from https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/662604/EPRS_BRI(2021)662604_EN.pdf (Date visited: Oct 31, 2021)

Executive Office of the President, (1996). Executive Order 13010-Critical Infrastructure Protection. Retrieved from https://irp.fas.org/offdocs/eo13010.htm.

Mastro, Oriana Skylar (2021). “The Taiwan Temptation: Why Beijing Might Resort to Force” Retrieved from https://www.foreignaffairs.com/articles/china/2021-06-03/china-taiwan-war-temptation (Date visited: Oct 31, 2021)

Gechkova, Teodora and Tiana Kaleeva, (2020). The European Refugee Crisis-A Threat to the National Critical Infrastructure. *Knowledge for sustainability* 41(5): 1007–1010.

Hemme, Kris, (2015). Critical Infrastructure Protection: Maintenance is National Security. *Journal of Strategic Security* 8(3): 25–39.

International Telecommunication Union, 2008, *Report on Best Practices for a National Approach to Cybersecurity: A Management Framework for Organizing National Cybersecurity Efforts*. Geneva: International Telecommunication Union.

Laclau, Ernesto, (2005). On Populist Reason. London: Verso.

Lundborg, Tom, (2011). Resilience, Critical Infrastructure, and Molecular Security: The Excess of ‘‘Life’’ in Biopolitics. *International Political Sociology* (2011) 5, 367–383.

Monaghan, Jeffrey and Kevin Walby , (2015). Surveillance of environmental movements in Canada: critical infrastructure protection and the petro-security apparatus. *Contemporary Justice Review* 11(4): 411–430.

Moteff, John, (2005). *Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences*. Washington, DC: Federation of American Scientists.

Li, Lauly, (2018). Taiwan quietly lets Chinese state company take over port area. Retrieved from https://asia.nikkei.com/Business/Companies/Taiwan-quietly-lets-Chinese-state-company-take-over-port-area (Date visited: Dec 19, 2023)

Nolte, Amina, (2016). Political infrastructure and the politics of infrastructure. *City, Taylor & Francis Journals* 20(3): 441-454.

Ongkowijoyo, Citra Satria and Hemanta Doloi, (2016). Determining Critical Infrastructure Risks using Social Network Analysis. *International Journal of Disaster Resilience in the Built Environment* 8 (2016): 5-15.

Pursiainen, Christer, (2016). Critical infrastructure resilience: A Nordic model in the making?. *International Journal of Disaster Risk Reduction* (27): 632–641.

Rumford, Chris. (2012). Towards a Multiperspectival Study of Borders. *Geopolitics*, 17(4): 887-902.

The White House, (2003). *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. Washington D.C.: U.S. Department of Homeland Security.

Theocharidou, Marianthi and Georgios Giannopoulos, (2015). *Risk assessment methodologies for critical infrastructure protection. Part II: A new approach*. Brussel: European Commission.

United Nations Office for Disaster Risk Reduction, 2024, “Critical infrastructure” Retrieved from https://www.undrr.org/terminology/critical-infrastructure (Date visited: Sep 19, 2024)

United States Department of Homeland Security, (2021). Critical Infrastructure. Retrieved from https://www.dhs.gov/science-and-technology/critical-infrastructure (Date visited: Oct 31, 2021)

Verdeil, Eric, (2016). Beirut, metropolis of darkness: The politics of urban electricity grids. In Andrés Luque-Ayala and Jonathan Silver (eds.), *Energy, Power and Protest on the Urban Grid: Geographies of the Electric City* (pp. 45-64). Abingdon, Oxon: Routledge.

Winner, Langdon（2004）〈技術物有政治性嗎?〉（方俊育、林崇熙譯），收於吳嘉苓、傅大為、雷祥麟編《科技渴望社會》（pp. 123-150）。台北：群學。

White, Richard, (2019). Risk Analysis for Critical Infrastructure Protection: Theories, Methods, Tools and Technologies. In Dimitris Gritzalis Marianthi, Theocharidou and George Stergiopoulos, *Critical Infrastructure Security and Resilience* (pp.35-54). Heidelberg: Springer.

内閣サイバーセキュリティセンター（2018）《重要インフラの情報セキュリティ対策に係る》。東京：内閣サイバーセキュリティセンター。

内閣サイバーセキュリティセンター（2021）《サイバーセキュリティ戦略》。東京：内閣サイバーセキュリティセンター。

附錄一：美國十六項關鍵基礎設施項目

基礎設施項目	說明
化工產業	化學品製造、儲存、使用，與具有潛在危險的化學品運輸
商業設施	可吸引人群進行商務辦公、購物、娛樂、住宿的部門場所
通訊部門	與人員、企業進行通訊與傳輸的基礎設施，與相關的維護
關鍵製造部門	初級金屬、機械製造、電氣設備與零組件、運輸設備製造
水壩	與水力發電、農業灌溉、洪水控制等相關的水壩基礎設施
國防工業	與軍事武器的研究、開發、設計、生產、維護相關的部門
緊急服務	包括警政機構、消防局、私人安全組織、緊急醫療機構等
能源	主要由電力、石油、天然氣所構成的能源基礎設施與系統
金融服務業	包括數以千計的存款機構、保險公司、信貸與融資機構等
食品與農業部門	與糧食與農業有關的水利、運輸、能源、化學品供應系統
政府設施	由聯邦、州、地方、部落等政府組織有關的機構、資產等
醫療保健與公衛	與醫療保健、傳染病與公共衛生、自然災害有關的機構等
資訊科技部門	資通訊部門有關的網路、硬體、軟體、系統等建構與維運
核反應堆與材料	包括核反應堆、核材料以及相關的核能廢棄物管理機構等
運輸系統	包括航空、公路、海上運輸、公共交通、運輸管道等系統
水利與廢水處理	提供安全公眾健康飲用水的系統，與廢水處理服務等機構

資料來源：Cybersecurity and Infrastructure Security Agency（2021）

Infrastructure as the Boundary of Nation: Techno-Politics and Transformation of Taiwan's Critical Infrastructure

Po-Jung, Shi[*]

Abstract

In most countries' definitions, the critical infrastructure (CI) is a collection of indispensable utilities and buildings or system that provide an essential support for economic and social well-being, for public security and for the functioning of key government responsibilities. This paper focuses on the historical formation of Taiwan's critical infrastructure and proposes an approach of techno-politics to illustrate its development transformation. Taiwan's critical infrastructure must be analyzed in its unique historical and political-economic context, as the paper argues, the formation of Taiwan's critical infrastructure can be seen a “process of national boundary delineation” in Taiwan. This paper first explores the policy formation of critical infrastructure in global context, such as United State, EU and Japan. Secondly, it depicts the policy value and thinking shift of Taiwan's critical infrastructure during the different historical periods. Thirdly, I show the core argument of this paper is that Taiwan's critical infrastructure simultaneously shape and is shaped by (in other words, co-construct) the engineering of “nation building”. However, both of the above in Taiwan still exist in in a dynamic and uncertain situation characterized as “unfinished”.

Keyword: critical infrastructure, techno-politics, national boundary, national identity, nation building

[*] PhD student, Graduate Institute of Building and Planning, National Taiwan University; Deputy Director, Market Intelligence & Consulting Institute.

Email: d10544002@ntu.edu.tw