行政暨政策學報　第七十八期
民國113年6月　　第33-66頁
Public Administration & Policy, No. 78
June 2024　　pp. 33-66
https://doi.org/10.29865/PAP.202406_(78).0002

以協力治理觀點探究我國資通安全區域聯防體系*

張鎧如**

摘要

本文以過往協力治理的文獻爲基礎，透過結合資通安全與災害防救的概念，提出資通安全協力治理理論架構，並聚焦探討影響資通安全協力治理的「驅力」、「協力治理過程」兩面向中的重要因素。其中驅力包含「資通安全風險」、「資通安全互賴性」、「參與誘因」，以及「中央政府領導力」；而協力治理過程則引用Emerson與Nabatchi（2015）的架構，包括「原則化參與」、「共享動機」、「聯合行動能量」。本文以所提出的理論架構爲基礎，透過深度訪談蒐集質性資料進行分析，嘗試從中央與地方政府視角來了解資通安全區域聯防體系的現況與挑戰。學理上，本文有助於進一步認識資通安全協力治理的重要面向與因素，建立理論架構並累積實證研究資料；實務上，亦有助於持續深入了解我國資通安全區域聯防政策現況，以提供未來發展之相關政策建議。

關鍵詞：資通安全、災害防救、協力治理、區域聯防

---

* 本文初稿曾發表於台灣公共行政與公共事務系所聯合會2022年會暨「邁向2030：永續公共治理的發展與實踐」國際學術研討會（9月30日），作者感謝莊文忠教授於研討會中之指正，以及學報兩位匿名審稿人與編輯委員會提供的修正建議，惟一切文責仍由本文作者自負。作者亦感謝所有研究參與者撥冗受訪分享個人經驗與觀點，以及政治大學公共行政學系碩士生王浦彥、林鼎翔在資料蒐集與彙整上的協助，讓本文得以完成。最後，本文受助於科技部（現改爲國科會）專題研究計畫「探究我國資通安全協力治理架構：政府、企業、與非營利組織之間的動態夥伴關係」（MOST 108-2410-H-004-162-）。

** 國立政治大學公共行政學系副教授，電子郵件：kchang@nccu.edu.tw。

收稿日期：民國111年11月23日。接受刊登日期：民國112年7月24日。

壹、前言

據世界經濟論壇（World Economic Forum）所公布的「2018 年全球風險報告」（Global Risks Report 2018）指出，除了環境氣候與污染風險、經濟不平等風險、國內外政治風險，對世界各地關鍵基礎設施[1]所進行的網路攻擊與網路犯罪事件亦是目前全球面臨最關鍵的風險之一（World Economic Forum, 2018）。面對日趨嚴峻的資通安全（cybersecurity）課題，[2]在聯合國國際電信聯盟（International Telecommunication Union, ITU）發布的 2020 年全球資通安全指數（Global Cybersecurity Index, GCI）報告中，以法律、技術、組織、能力建立、合作等五大面向，來評比各國的資通安全發展程度。[3]從研究報告的結果來看，透過建制法規、研擬策略、成立主管機關、提升資通安全意識、發展雙邊或多邊公私協力，來加強國家整體資通安全能量，已成爲各國政府持續精進的目標。

資通安全議題過去常被歸類爲技術領域的課題，近年來則是受到國際關係、國家安全領域的學者關注（Balzacq & Cavelty, 2016; Cavelty, 2013; Hansen & Nissenbaum, 2009; Yannakogeorgos, 2012; 彭慧鸞，2004）。過去國內公共行政學者多半將資通安全視爲電子化政府、電子治理的重要基礎（胡龍騰等人，2013；陳俊明等人，2014；潘競恒、蔣麗君，2013）。隨著各國陸續將資通安全規範法制化，強調建立情資分享、資通安全聯防體系的必要性後，資通安全議題便進入治理的領域。如何透過中央與地方政府既有的行政體系，與民間非政府組織、甚至一般公民共同合作確保資通安全，成爲當前值得關切的議題（Harknett & Stever, 2009, 2011; Manley, 2015）。從近幾年國內外關鍵基礎設施發生的知名資安事件案例來看，如我國 2020 年 5 月，中油、台塑內部系統遭不明人士植入勒索病毒，儲存的檔案無法開啓，導致營運受到嚴重影響（翁芊儒，2020）；美國 2021 年 5 月最大燃油供應業者 Colonial Pipeline 遭勒索軟體攻擊，導致暫停所有輸油管線運作，美國總統拜登宣布國家進入緊急狀態（Sanger et al., 2021）。這些國營或民營關鍵基礎設施提供者所發生的資安事件，後續都有政府相關單位介入調查並予以協助，以迅速降低對民生經濟所造成的影響與損害，這些實例皆顯示資通安全的公私協防有其實務上的必要性。若以區域聯防機制爲例，當某直轄縣市察覺到惡意程式對於本身政府機關的攻擊後，藉由情資分享，可立

---

[1] 針對關鍵基礎設施的定義，根據我國行政院通過的「國家關鍵基礎設施安全防護指導綱要」規定，係指公有或私有、實體或虛擬的資產、生產系統、網絡，因人爲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（行政院，2014）。

[2] 參照我國資通安全法之正式英文翻譯，本文統一將 “cybersecurity” 一詞譯成資通安全。

[3] 完整報告書請參見網址：https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

即將相關情資讓其他直轄縣市政府知悉，助其預先防範潛在資安威脅，也顯現出建立區域聯防機制的重要性。

另一方面，資通安全課題與災害防救其實息息相關（Walker, 2012），[4] 從災害防救中的減災、整備、應變、復原的角度來看，關鍵基礎設施資訊系統其資通安全的確保，需要平時進行重要資訊系統的風險評估、擬定緊急應變計畫並加以演練（Caruson et al., 2012）；偵測到惡意軟體或遭受網路攻擊時，能執行緊急應變對策，確保資訊系統安全或讓系統盡速復原；事後盤點災損，並透過分析檢討過往的資通安全事件，從錯誤中學習，提升資通安全知識與防禦技能。而且，建立與提升政府、民間、乃至一般民眾資通安全風險意識，培養資通安全相關基礎知識與自我安全防護的技能，也顯示資通安全課題呼應災害防救中的重視風險管理、全民防災精神（Harknett & Stever, 2009; Wirtz & Weyerer, 2017）。對於我國中央政府而言，2019年 1 月起已正式施行「資通安全管理法」（以下簡稱資安法），並希望藉由建立國家級的資通安全聯防體系，作爲確保整體國家資通安全能量的重要策略之一。而這個聯防體系實務上包含政府與中央目的事業主管機關，串連關鍵基礎設施提供者的公私協防，以及以六都爲核心，結合鄰近縣市，建立地方資通安全防護網的區域聯防兩者所組成（行政院國家資通安全會報，2021）。由此可見，我國目前推動的國家級資安聯防體系能否成功運作，取決於中央政府與地方政府之間、地方政府之間、政府與非政府組織（如石油公司、電信公司、銀行、醫院或其他關鍵基礎設施提供者等特定非公務機關）之間，針對所面臨的資安風險能否建立一套穩健的合作模式來有效預防與應變，以減低因人爲疏失或遭惡意攻擊所發生的資通安全事件，以至於我國公務機關或特定非公務機關之核心業務或機密資訊遭洩漏或系統受竄改，而導致服務中斷、無法正常運作，甚至危害民眾隱私與生命財產之情況的可能性，這便涉及到垂直與水平組織協力的課題（Harknett & Stever, 2009, 2011; Manley, 2015）。從第三代政策執行的角度來看，這樣的協力關係也顯示政策執行需仰賴各級政府機關之間的合作來確保其成果（李翠萍，2007）。而在 Shaw（2012）提出的韌性地方權威（resilient local authority）概念中，管理風險（managing risk）是其中一項重要的影響因素。因此，對地方政府而言，如何透過與中央、其他地方政府、或非政府組織合作，降低資通安全事件的發生，也是一種管理資安風險的策略，來確保該政府在地方權威的穩固性。

然而資通安全政策的推動並非易事，往往面臨多項重大挑戰，例如張書瑋

[4] “Emergency management” 一詞在國內有諸多翻譯，例如應急管理、緊急事務管理、災害管理、災難管理，本文以我國「災害防救法」爲依據，將該詞統一稱爲災害防救。同時依據該法第 2 條第 2 款之規定，災害防救意指「災害之預防、災害發生時之應變及災後之復原重建等措施」。

（2018）點出我國中央與地方各級公務機關專責資安人力不足、多爲兼職；陳泉錫與陳俊呈（2020）則指出我國政府機關內部因推動資訊業務委外政策，使政府機關資訊部門（單位）之設置與資訊人力配置受到限制，又因過度委外導致政府機關逐漸失去技術主控能力，資訊技術人員變成資訊採購行政人員，產生政府機關的資安危機。國外研究也已發現，地方政府對資通安全的投入往往不足，不僅欠缺採行建議的資安管理措施與導入相應政策，機關組織人員在資通安全上缺乏相關教育訓練，具備的資安科技相對落後，應變處理資安事件的能力有限，地方高層官員也對地方政府資通安全的需求不夠重視與支持，沒有擔負起維護地方政府資通安全的責任（Norris et al., 2021）。

雖然協力治理是近十多年來公共行政領域的重要研究主軸之一，相較於國外日趨蓬勃的資通安全網絡治理、公私協力等相關研究（Center for Strategic and International Studies, 2013; Germano, 2014; Greiman, 2015; Manley, 2015; Tagarev, 2020; Yanakiev & Tagarev, 2020），以及對於地方政府面臨資通安全威脅、急需整體提升地方政府資通安全能量等課題的關注（Norris et al., 2018, 2019, 2021; Preis & Susskind, 2022），目前國內公共行政領域相關研究仍鮮少以協力或網絡治理的理論觀點，結合災害防救思維，探討資通安全協力治理可能的理論架構與影響因素。有鑑於此，本文以過往協力治理的文獻爲基礎，透過結合資通安全與災害防救的概念，提出資通安全協力治理架構，後續透過深度訪談法蒐集質性資料進行分析，並聚焦在了解中央與地方政府對於建立我國資通安全區域聯防體系的看法。本文主要研究問題如下：一、資通安全的協力治理架構可能爲何？二、影響地方政府參與資通安全區域聯防體系彼此協力互動之關鍵因素又爲何？地方政府又面臨哪些困難與挑戰？

貳、文獻回顧

一、資通安全概念的範疇與界定

資通安全（cybersecurity），可從「安全」（security）與「網路空間」（cyber space）兩項概念來理解。首先，就「安全」的概念來說，基本上有兩個層次，即英文中的 “safety” 和 “security”，“safety” 意指沒有意外（no accident），“security” 意指沒有事件（no incident）（李宗勳，2016，頁 7）。當意外或事件發生時，便需要啓動緊急應變措施與系統來確保安全（李宗勳，2016）。而「網路空間」或是「賽博空間」之概念，根據賴曉黎（2012，頁 24）的詮釋，可將其理解爲「一個由電腦中介的、由抽象資訊構成的構造物，它並非物理空間，但人們可以通過電腦介入資訊系統

與網路中，並感覺它的存在。它既關乎控制也強調通信，將數位資訊儲存、處理能力結合網路的遠距傳輸、通訊，成就了一個嶄新的、多向交流的社會空間，一種依網路而存的空間、虛擬空間」。因此資通安全概念的範疇，可理解成透過相關防護措施或系統，確保依網路存在、透電腦中介、強調通信、由數位資訊建構的虛擬社會空間中沒有事件發生。若依據我國資安法中定義的資通安全，則指「防止資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性、完整性及可用性」。

從國家安全的角度來看，彭慧鸞（2004）指出，當前國家追求數位科技的同時，面臨不同層次數位科技層面的國家安全議題。若運用鑲嵌的概念來理解，國家整體的數位安全（digital security），涉及資訊安全（information security）、資通安全（cyber security）、網絡安全（network security）等三種層次。本文聚焦在「網路空間」層次上的安全議題，也就是資通安全。Cavelty（2013, p. 109）認爲資通安全可從政治與國家安全的角度來論述，背後其實反映三種不同層次的威脅，分別爲科技面、社會政治面、人類機器面。其中社會政治面的威脅例子包含駭客入侵、網路犯罪、網路間諜、網路恐怖攻擊事件等，而人類機器面威脅例子像是透過網路對關鍵基礎設施進行毀滅性攻擊等。後兩種層面的威脅，讓國家政府有了合理正當性透過執法強制力來介入，對於人類機器面可能造成重大災害的威脅，國家機器介入的名義，往往是爲了保護或是確保關鍵資訊基礎設施的「韌性」（resilience），也就是讓資訊系統有能力從外力衝擊自行復原或是到更新調整的狀態（Cavelty, 2013, pp. 115-116）。Wirtz 與 Weyerer（2017, p. 1088）認爲政府機關過去受網路攻擊的經驗、資通安全威脅的來源、不同層級機關對於資通安全脆弱性與威脅的風險評估、高層領導欠缺資通安全風險意識，可視爲影響政府機關之資通安全狀態的風險因素；資通安全防護措施、災害防救應變計畫、專業人力與知識技能、高層領導提供資源支持則可視爲資源因素。

如果從災害防救中的危害（hazards）概念來看資通安全，資通安全事件可視爲與電腦和資訊有關的科技危害（McEntire, 2015）。相較於其他類型的科技危害，與電腦或資訊有關的科技危害往往容易被組織決策者忽視，結果產生重大損失，例如交通運輸、電力系統等服務被中斷，或是因爲網路恐怖行動透過網路癱瘓資訊系統，導致有毒物質釋放或是讓關鍵基礎建設失靈（McEntire, 2015）。換言之，災害防救的運用，有助於預防、應變組織中與電腦或資訊有關的科技危害造成的後果，維護資通安全，進而提升網路韌性（cyber resilience）。當前災害防救領域也越發強調網路狀況感知（cyber situational awareness）的重要性，呼籲組織從事災害防救工作的同時，必須同步盤點與掌握手邊仰賴或連結的網路資產（cyber assets）有哪些，才能確保災害防救工作順利進行（Walker, 2012）。

二、資通安全的協力治理

（一）協力治理的意義與內涵

「協力」（collaboration）一般被認爲是具有目的性的行動，藉由參與者之間的緊密互動、分享、建立信任、取得共識，進而解決過於複雜或單一組織無法獨自解決的問題（Agranoff & McGuire, 2003）。其概念有別於互動關係普通的「協調」（coordination），以及互動關係較爲鬆散的「合作」（cooperation）（陳敦源、張世杰，2010）。而協力治理（collaborative governance）強調的是一種多元行動者緊密的互動關係，關係的建立以信任爲基礎，注重彼此的資源共享、責任分擔，以達成共同目標，進而創造及建立社會資本、共識認知與資源共享（李長晏、曾淑娟，2009；林淑馨，2017）。

Ansell 與 Gash（2008, pp. 544-545）對於協力治理採取較爲狹義的定義，聚焦在公私協力的面向，視爲一種統治安排（governing arrangement），由一個或是多個政府機關及非國家利害關係人共同決策的過程，該過程具有正式、共識及共同審議等特徵。若進一步分析協力治理的內涵，Ansell 與 Gash（2008）認爲協力治理基本上包含「初始情況」、「協力過程」、「制度設計」、「協助型領導」幾個要素。其中「協力過程」裡，如果各方利害關係人能有效促進「面對面對話」、「信任建立」、「參與者對互賴關係的承諾」、「共享理解」、「初期可感知到的合作利益」等這五個因素之間的正向循環時，有助於產生滿足各方期待的良好成果（陳敦源、張世杰，2010，頁 37-38）。

Emerson 與 Nabatchi（2015, p. 18）則提出較爲廣義的協力治理定義，認爲協力治理是一種公共政策決策制定與管理的過程、結構，以實踐公共目的爲目標，但僅能透過不同領域的政府單位、不同層級的政府機關、企業與第三部門，以及公民場域的人們一同參與的方式來達成。而這樣的定義，其實也將過去府際治理、公私夥伴關係、跨域治理、公民參與等概念含括在內。在 Emerson 等人（2012）、Emerson 與 Nabatchi（2015, p. 18）以各方文獻爲基礎所建構的協力治理模型中，「協力治理體制」（collaborative governance regime）被視爲協力治理的核心要素，會受到「驅力」（drivers）和「系絡」（system context）的影響。而後又透過「調適」（adaptation）回饋到「協力治理體制」和「系絡」。模型中指涉的驅力，Emerson 等人（2012）認爲包含「不確定性」、「互賴性」、「相應的誘因」、「啓動的領導力」等元素。「協力治理體制」是由「協力動能」（collaborative dynamics）與後續產生的「行動」（actions）組成。而協力動能內容則與「原則化的參與」、「共享動機」、「聯合行動能量」等三項概念有關，這三者又具有相互影響的齒輪關係。「原則化的參與」係

指協力的參與者互動合作時遵循的原則，包含各方參與者公開表述立場與利益，界定問題、需求與期待，爾後經過審愼地參與討論，最終獲致各方參與者認同的決定；「共享的動機」包含互信、理解、內部正當性、承諾等相互影響的要件；「聯合行動能量」與過程、制度安排、領導力、資源、知識有關。

在資通安全區域聯防的系絡下，協力動能可視爲促使各地方政府認同資通安全的重要性、願意參與區域聯防、中央和其他地方政府協力合作之重要因素，透過建立制度化的參與原則，形塑參與區域聯防的動機及凝聚共識，同步提升地方政府參與區域聯防的制度規範之依據、資源、知識、領導力等行動能量，讓地方政府積極參與所屬區域聯防體系，從事情資分享與交換，通報資通安全事件，並積極應變處理等行動，進而確保國家整體資通安全。

（二）協力治理作爲確保資通安全的防護策略

若進一步以協力治理定義與內涵來看資通安全，由於網路具有無遠弗屆的性質，網路空間可以超越政府行政區劃、公私部門範疇、甚至國土疆界，因此，若要發展成功的國家資通安全策略，來降低網路與資通科技可能造成的危害或災害損失，必須以穩健的府際關係、有效的公私部門合作，以及鼓勵公民參與作爲基礎（Harknett & Stever, 2009, 2011）。當資通安全議題升高至國家安全層次時，非政府組織行動者的積極參與往往是資通安全制度成功的關鍵，故國防與民防之間，更須建立合作共享資源與資訊的機制（彭慧鸞，2004）。

若將資通安全事件視爲一種數位災害（digital disaster），國家藉由推動垂直與水平組織協力，進行情資與資源分享，形成區域聯防體系，提升國家整體減災、整備、應變、復原的能力，進而降低或避免災害損失，那麼將導入協力治理作爲確保資通安全的策略，則有其必要性。舉例來說，各國政府對於其國內關鍵基礎建設的維運，大致遊走在國營與民營兩個途徑之間（Assaf, 2008）。因此，公部門有其必要與民間企業或第三部門協商合作，以確保關鍵基礎設施的資通安全，同時也彰顯協力概念在資通安全領域的重要性。從我國的實務上來看，針對八大關鍵基礎設施提供者，中央主管機關除了與關鍵基礎設施提供者平時建立良好的情資分享、通報應變，以及資安監控機制外，亦可透過定期與其合作舉辦公私聯合攻防演練，強化民間關鍵基礎設施提供者其資安人員對資安事件的警覺心與防護力；針對目前非受資安法規範的民間企業，可透過鼓勵民間企業參與「台灣 CERT/CSIRT 聯盟」，強化台灣電腦網路危機處理暨協調中心（TWCERT/CC）資安情資系統及服務，提升該組織對於企業資安事件諮詢及協調處理服務之能力，以增強民間企業資安防護能量及意識（行政院國家資

通安全會報，2021）。

當前國內外研究也呼籲透過加強公私協力以穩固資通安全（Center for Strategic and International Studies, 2013; Germano, 2014; Greiman, 2015; Manley, 2015; 張書瑋，2018；陳育正，2015）。進一步剖析影響資通安全公私協力關係的因素，大致包含領導者的支持、法規制度的配合、民間參與的誘因、推動時機等（Center for Strategic and International Studies, 2013; Greiman, 2015）。Manley（2015）則建議，促進資通安全的公私夥伴關係，須建立公私雙方的信任感，並且政府須提供清楚的法規指導、採取由下而上的協力合作模式，並鼓勵相關社群的投入參與。近期也有國外學者從協力的角度探討資通安全網絡治理。Yanakiev 與 Tagarev（2020）以歐盟近來積極發展的資安能力網絡（cybersecurity competence network）爲背景，探討治理協力網絡連結組織（collaborative networked organization, CNO）相關課題。透過文獻檢閱，該研究探討各項治理模式的樣態與建置，以及組織網絡連結的形式，其中便提到公平與信任關係對於運作與維繫協力網絡連結組織的重要性。Pala 與 Zhuang（2019）則從資訊分享（information-sharing）的角度分析美國資通安全的跨部門協力，探討資通安全相關行動者分享資訊可能面臨的利弊得失，相關行動者認爲分享資訊可獲得的好處包括可增強網路攻擊事件的防禦能力，以及可降低安全層面投資成本。

（三）透過協力治理推動資通安全的困難與挑戰

過去文獻已指出，運用協力治理作爲解決公共治理難題之策略，可能面臨的根本性挑戰，在於如何確保協力治理過程中多元利害關係人的實質參與，且在多元利益中建立共同目標滿足各自的期待，在過程中解決衝突取得共識，以及提出有效衡量協力治理所產出績效的評量方式（Gash, 2016）。公私部門在建立協力關係的過程中，可能面臨既競爭又合作、開放又封閉、追求彈性卻須考量可治理性、希望有效課責又須兼顧效率等兩難或弔詭的現象（陳敦源、張世杰，2010）。除了溝通協調可能耗時費力外，私人企業、非營利組織和公部門合作時，本身也常須承擔政治面與行政面的成本（林淑馨，2018；曾冠球，2010）。

在資通安全的系絡當中，Germano（2014）點出資通安全建立公私夥伴關係常面臨的難題，包含：1. 信任與控管的分際難以拿捏；2. 對於揭露義務存有疑問；3. 不明確的法規與公民責任義務背後可能帶來的風險；4. 跨國調查網路犯罪不易；以及 5. 跨國資料傳輸困難。Pala 與 Zhuang（2019）則指出，資通安全相關行動者分享資訊的同時，也面臨了隱私權與公民權保護，以及背負責任義務等課題。私部門行動者往往特別擔心會因此喪失客戶的信任、損失商譽、吸引更多網路攻擊，以及必須負擔資訊

外洩的風險與成本及參與資訊分享行動本身的成本。

三、我國資通安全區域聯防體系介紹

2018 年我國資安法經立法院三讀通過，2019 年 1 月 1 日起正式施行，該法規範對象除行使公權力的中央與地方機關（構）或公法人等公務機關外，非公務機關則以關鍵基礎設施提供者、國營事業及適用資通安全責任等級分級之政府捐補助法人爲主。而我國目前依該法定義的關鍵基礎設施包含能源、水資源、通訊傳播、交通運輸、銀行與金融、緊急救援與醫院、中央與地方政府機關、高科技園區等八類。[5] 此外，該法第 8 條規定主管機關應建立資通安全情資分享機制。而資通安全情資之分析、整合與分享之內容、程序、方法及其他相關事項之辦法，由主管機關訂定。目前已有「資通安全情資分享辦法」、「資通安全事件通報及應變辦法」相關辦法施行。

目前，我國全國性資通安全防護系統是由資訊安全監控中心（National-Security Operation Center, 以下簡稱 N-SOC）、資通安全資訊分享與分析中心（National-Information Sharing and Analysis Center, 以下簡稱 N-ISAC），以及電腦緊急應變小組（National-Computer Emergency Response Team, 以下簡稱 N-CERT）所組成。N-ISAC、N-SOC、N-CERT 由行政院國家資通安全會報技術服務中心來維運。N-ISAC 負責接收、統整及分析資通安全事件，並與國內外及不同領域進行情資分享，爲將可能發生的資通安全事件發出預警；N-SOC 負責偵測入侵及即時監控，與 N-ISAC 進行情資交換，有效掌握資訊安全之運行；N-CERT 則係在資通安全事件發生後提供緊急應變與處置，達到降低損失同時快速復原的效果。至於地方性的資通安全防護系統，則透過區域聯防的方式，中央政府提供計畫經費協助汰換基層地方政府超過使用年限或停產之資訊軟硬體設備，以強化政府資安端點防護，同時以六大直轄市政府爲核心，藉由結合其周邊鄰近縣市以及離島，[6] 設立區域級 ISAC、SOC、CERT，建構地方聯合資通安全防護網，進而與全國性資通安全防護系統進行整合，並希望能帶動地方政府與臨近學術研究機構合作，培育政府與學界的資通安全人才（行政院國家資通安全會報，2021）。

---

[5] 詳細介紹請見我國數位發展部資通安全署網站，網址：https://moda.gov.tw/ACS/operations/ciip/650

[6] 在目前資通安全區域聯防政策下，六大直轄分別帶領的縣市分別爲：臺北市：金門縣、連江縣、花蓮縣；新北市：宜蘭縣、基隆市；桃園市：新竹市、新竹縣、苗栗縣；臺中市：彰化縣、南投縣；臺南市：嘉義市、嘉義縣、雲林縣；高雄市：屏東縣、臺東縣、澎湖縣。

參、研究架構、方法與資料蒐集

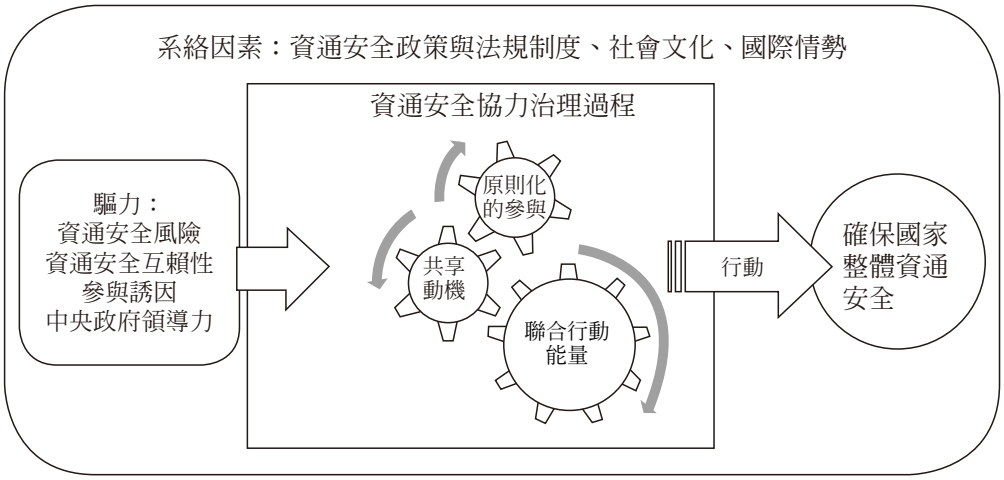
一、研究架構

本文以 Emerson 等人（2012）、Emerson 與 Nabatchi（2015）的協力治理架構爲基礎，結合 Wirtz 與 Weyerer（2017）的「風險與資源」資通安全架構，提出資通安全協力治理架構（見圖 1）。研究架構中「驅力」的部分，包含「資通安全風險」、「資通安全互賴性」、「參與誘因」、「中央政府領導力」等面向。「資通安全風險」，指涉影響機關組織資通安全狀態的風險因素；「資通安全互賴性」代表機關組織之間的相互依賴程度以確保資通安全狀態穩定，反映網路世界中，藉由互聯網跨越區域界線將各機關組織串連的特性，在此情況下，一旦發生資通安全事件，各機關組織往往難以置身事外，若要確保資通訊的安全性，就須仰賴各機關組織之間的互助合作；「參與誘因」的部分，意指機關組織參與資通安全協力行動的初始動機或誘因；「中央政府領導力」則意指中央政府對於全國資通安全協力治理體制的擘劃與資源投入程度，突顯當前資通安全議題受到國家層級的重視，並將資通安全視爲國家安全的一環，需要各國中央政府制定政策法規與投入資源，發揮領導力以促進國家整體資通安全協力治理體系的建置與維運。

「協力治理過程」的部分，引用 Emerson 與 Nabatchi（2015）的協力治理體系論點，包含「原則化的參與」、「共享動機」、「聯合行動能量」三大要素，因素之間彼此相輔相成。以資通安全區域聯盟的概念爲例，「原則化的參與」意指參與區域聯防的過程中，利害關係人如何表述立場、建立共識、對話溝通、做出合意的決定；「共享動機」顯示在參與區域聯防過程中，利害關係人之間藉由建立彼此的信任感，加深彼此的理解，建立內部合法性，投入推動區域聯防的承諾，建立起共享動機的基礎；「聯合行動能量」指涉支撐利害關係人共同產生與持續參與區域聯防行動，背後過程與制度性的安排、所擁有的資源、相關知識技能，以及促成協力的領導力。至於協力治理過程後所產生的「行動」的部分，本文認爲，對於資通安全的確保而言，參與區域聯防體系，進行跨組織機關之間的情資分享與應變作爲的配合是重要的行動，進而產生確保國家整體資通安全的成果，而成果也會回饋、影響協力治理的過程，產生調適的效果。同時，整個資通安全治理架構也必須考量系絡因素，這些涉及到國家的資通安全政策與法規制度、資通安全社會文化的養成，以及當下的國際情勢。有鑑於我國資通安全協力治理體系之建置仍處於前期階段，因此本文主要聚焦在探討驅力及協力治理過程的兩大環節上。

圖 1

資通安全協力治理理論架構



資料來源：修改自 “An integrative Framework for Collaborative Governance,” by K. Emerson et al., 2012, *Journal of Public Administration Research and Theory*, *22*(1), 1-29; *Collaborative Governance Regimes*, by K. Emerson, & T. Nabatchi, 2015, Georgetown University Press; “Cyberterrorism and Cyber Attacks in the Public Sector: How Public Administration Copes with Digital Threats,” by B. W. Wirtz, & J. C. Weyerer, 2017, *International Journal of Public Administration*, *40*(13), 1085-1100。

二、研究方法與資料蒐集

本文以中央與地方政府形成的資通安全區域聯防爲主要分析探討的研究範疇，以圖 1 提出的理論架構爲基礎，透過深度訪談的方式蒐集質性資料，採用譯碼分析法進一步探討影響地方政府參與資通安全區域聯防的驅力與過程因素。針對訪談對象的選取原則，本文參考數份官方文件與簡報，以及以我國資通安全發展策略爲主題的網路新聞雜誌報導，[7] 以中央政府與地方政府研擬與推動資通安全政策相關業務之單位、關鍵基礎設施主管機關與提供者，以及非政府組織等各類型機關組織作爲主要約訪對象。一開始採立意抽樣方式，先約訪中央政府層級受訪者，後透過滾雪球的方式，由受訪者推薦其他合適的受訪者，例如八大關鍵基礎設施主管機關之主管、資通安全服

[7] 本文參考之官方文件與簡報包括「2008 資通安全政策白皮書」、「2010 資通安全政策白皮書」、「國家資通訊安全發展方案（102 年至 105 年）」、「國家資通安全發展方案（106 年至 109 年）」、「國家資通安全戰略報告」、「國家關鍵基礎設施安全防護指導綱要」、「前瞻基礎建設—數位建設：強化政府基層機關資安防護及區域聯防計畫」、「從全球數位領土之防禦 談我國資安聯防機制之規劃」。至於網路新聞雜誌以 iThome 周刊於 2019 年針對〔全面盤點國家級資安情報力〕此主題所製作之系列報導爲主要參考來源。詳細說明請參見網址：https://www.ithome.com.tw/article/132228

務公司高階主管、技術中心高階主管、產業工會中階主管等，也嘗試主動聯繫關鍵基礎設施提供者。地方政府的部分，以目前我國以六都區分的六大資通安全聯防區域，分別聯繫六都市政府資通安全業務承辦單位高階或中層主管，以及區域內其他縣市政府的資通安全業務承辦單位高階或中層主管。訪談大綱的內容，則根據受訪者來自中央政府、地方政府、非政府組織或產業、關鍵基礎設施設計不同的訪談大綱。各類型的受訪者之訪談大綱提問內容主要環繞在了解受訪者對以下幾個議題的看法與經驗：（一）對於資通安全與災害防救概念，以及兩者之間關係的認知；（二）對於區域聯防概念、目的、功能與實務運作的闡述，（不）參與的原因與面臨的困難、實際案例的分享；（三）對於公私協防概念、目的、功能與實務運作的闡述，（不）參與聯防的原因與面臨的困難、實際案例的分享；（四）資通安全管理目前的現況與面臨的挑戰。

本文最後於 2020 年 3 月 12 日至同年 10 月 21 日之間，成功訪問 34 個機關組織或單位，總共 40 位受訪者（受訪者資訊見附錄一）。其中，3 位來自於中央政府層級之資通安全業務主管機關及其幕僚單位，如行政院資通安全處、[8]國家安全會議，時任或曾任高階主管或高階機要人員；19 位來自於 15 個地方直轄縣市政府層級之資通安全業務主管機關，如資訊局、資訊或科技中心、研考會、行政處或計畫處下之資訊科室，分布於北中南東部與離島地區，並涵括以六都爲首的六大區域；8 位來自八大關鍵基礎設施之中央主管機關單位，以及關鍵基礎設施提供者之資通安全業務單位，其中 2 位分別來自於國家級及民間技術中心，6 位來自於與公部門有業務往來之資通安全服務業者及公會。另由於資料蒐集階段正值 COVID-19 疫情爆發，因此本文除了採取實地面對面訪談，疫情期間亦搭配使用線上視訊軟體進行視訊訪談，每次訪談時間約 1.5 至 2 小時。其中有 1 位受訪者因時間無法配合受訪但仍有意願提供個人經驗，因此由受訪者提供書面資料回覆。

另基於研究倫理相關規範，受訪者皆須閱讀且填寫研究參與者知情同意書，研究團隊獲得受訪者的同意後才正式進行訪談，並透過現場錄音方式記錄訪談過程，若是線上視訊訪談則採錄影方式留存紀錄。後續的資料分析也皆採匿名方式呈現，並妥善保管訪談資料，以確保受訪者的個人權益。所留存的錄音或錄影檔後續繕打成逐字稿，以進行訪談資料的編碼與分析工作。

肆、資料分析與討論

本文以前述協力治理相關理論爲基礎，提出資通安全協力治理的可能架構後，進

[8] 隨著 2022 年 1 月 19 日數位發展部成立，行政院資通安全處現已併入數位發展部成爲資通安全署。

一步透過分析訪談資料，從驅力及資通安全協力治理過程等面向梳理出我國資通安全協力治理現況，探討影響地方政府參與資通安全區域聯防體系彼此協力互動之關鍵因素，以及所面臨的困難與挑戰。

一、驅力

（一）資通安全風險

1. 資通安全的特性

多位受訪者認爲災害防救與資通安全兩者在概念上有相通之處，例如在本質上，兩者面對的威脅都具有「隱性」特質，所以事件發生當下，很難即時知道災害發生的原因，因此只能先採取被動地防衛，並依賴即時應變來降低損害（CI1；CG2；LG-Z5-2）。在發生來源的特質上，相較於災害防救處理的事件一般屬於自然而且是物理層面（P5；LG-Z1-1a），資通安全事件所面對的多是人爲、有目的性的，且是虛擬的（P4b；P5；P3a；LG-Z1-1a）。因此，資通安全事件的發生會跟當前的政治社會因素有關，例如兩岸關係的緊張程度（P5）。此外，有受訪者認爲，相較於災害防救，資通安全事件可以是每分每秒持續地發生，因此資訊量極大（P5；LG-Z5-2）。而且天然災害一旦發生很難掩蓋，但資通安全事件的發生則有可被掩蓋或忽略的機率（P5）。

災害防救與資通安全兩者在管理層面上亦會採取相似的架構來應對風險（LG-Z1-1a；LG-Z5-2；P4a；P4b；CI3；CI5；P5）。例如，災害防救的「事前、事中、事後」及「減災、整備、應變、復原」架構，與美國國家標準與技術研究所（NIST）所提出的資通安全架構（cybersecurity framework）下，所列出的「辨識」（identify）、「保護」（protect）、「偵測」（detect）、「回應」（respond）、「復原」（recover），其核心概念有相對應之處（LG-Z5-2）。

若從事件發生的結果來看，受訪者認爲其實自然環境造成的天災與資通安全事件造成的人禍，後果其實是一樣嚴重的，而且無論是災害防救工作或資通安全工作，要展現其工作績效其實不容易，而且常被認爲做好工作是分內、應該的事情，其背後投注的心力不易展現（CI8）。受訪者表達從事資通安全工作的感受：

> 有功沒賞，打破要賠（臺語）。（CG2）

> 其實我常常講說，做資安跟做下水道工程是一樣，就是你看不見，然後沒事大家也不會鼓勵，出事大家就開始怪東怪西。（CG3）

由於資通安全這類的隱性特質，讓資源投入到資通安全領域，其成效難以立即被看見（LG-Z1-1b，CG3），導致資通安全業務單位更難說服地方政府首長及民意機關代表投入更多資通安全經費預算，或是爭取、分配到更優先的順序（LG-Z3-1a），以至於資通安全相較其他政策範疇更缺乏資源的投入，而忽視資通安全的後果就容易讓風險提高。此外，無論面對天然災害或是資通安全事件，兩者在事前防護的工作只有越來越多，要求越來越高，是一個永無止境的工作，故有受訪者以「軍備競賽」一詞來形容前述這種狀況（P5）。

2. 地方政府資通安全業務機關經費與人力資源之限制

地方政府資通安全人力資源的限制，成爲潛在的地方政府面臨的資安風險之一，其限制反映在人力不足與人才欠缺兩個部分。人力不足的部分，雖然資安法明定直轄縣市政府需要設有一定人數的專職資通安全人員，但實務上往往面臨資通安全專職人力不足，多由機關的資訊人員兼任（CI2）。而且不少受訪者也指出政府機關的員額，受總員額法之規範，且培育與訓練資通安全人才成本其實相當高（LG-Z1-1a；LG-Z1-1b；LG-Z5-2）。因此實務上許多工作其實仰賴委外廠商協助，但是即使如此還是需要一定程度的人力來執行相關業務（LG-Z3-1a）。

同時，人力不足也涉及人員流動的問題，而這個流動有向其他地方政府流動，或是向私部門流動。有地方政府受訪者指出，自己機關業務單位的公務員多來自不同縣市，並非在地人，因此當規定服務的期間一過，便可能申請調回其居住縣市政府單位，因此人力流動性高（LG-Z6-3）。而越是偏鄉的政府機關，前述的現象便更明顯。而且，以薪資來說，相比私部門可提供給具有資通安全專業技能人員的薪資，政府部門提供的薪資缺乏競爭力，因此也很難吸引或留住有經驗的資通安全人才（LG-Z1-1a；LG-Z3-1a；LG-Z4-1b）。

此外，由於資訊與資通安全相關知識、技術日新月異，往往需要不斷透過學習或受訓來提升本身知識與技能。但實務上，負責資訊與資通安全業務的公務人員，其實大部分工作時間都在處理行政協調上的問題，或是辦理委外、採購業務，長久下來，容易導致個人專業能力弱化。受訪者指出：

> 那我們資訊人員其實比較多的是辦採購，還有比較偏的是需求訪談、行政協調的部分……反而是比較偏這一塊。（LG-Z1-1a）

至於地方政府本身經費的限制上，不少地方政府受訪者指出，添購與維運資通安全相關資訊設備需要相當程度的經費支應，其中資訊過濾或是偵察軟硬體相當昂貴，添置成本已占大部分經費（LG-Z5-2；LG-Z1-1b），更不用說後續相關軟硬體設備的

維運（LG-Z1-1b）。經常與地方政府業務往來的資安服務業受訪者指出，當地方政府有經費時，更傾向先投注經費在換電腦或其他硬體設備上，這種情況在經常欠缺資訊經費的地方政府中更爲明顯（P3a）。

3. 地方政府機關內部資訊系統老舊及維運過度仰賴委外廠商

有受訪者則是從地方政府內部機關的系統開發與維運問題來看資通安全管理的困境，提到政府內部資訊系統一旦開發下去就會偏向持續沿用，但其實系統本身有生命週期，而各階段開發的系統對資通安全管理的要求標準高低不一，越老舊的系統就越可能面臨更高的資通安全風險（LG-Z1-1a）。同時，政府機關內部資訊系統又長年仰賴委外方式來採購與維運，一旦資訊系統廠商本身的資通安全管控不佳，或甚至面臨廠商本身結束營運，而政府機關內部後續又缺乏專業人力對該資訊系統的開發維運有詳細的認識時，發生資通安全事件就形成重大威脅（LG-Z1-1a）。

4. 城鄉差距帶來的困境

行政面積幅員廣且管理較多偏鄉地區，他們面對城鄉差距所帶來的問題也較明顯。舉例來說，一方面地方政府的資訊系統與資通安全系統多半仰賴委外廠商建置與維護，同時多偏鄉的縣市往往更缺乏資訊與資通安全相關專業人力，另一方面多偏鄉的縣市相對大城市缺乏商業誘因吸引資訊和資通安全設備和技術廠商進駐當地，讓當地的資訊基礎建設相對大城市落後，例如當地的鄉鎮市公所的網路頻寬會相對較不足。種種因素導致多偏鄉的地方政府在推動相關政策（例如資訊設備集中向上）面臨許多難題（LG-Z6-3）。

此外，位處偏鄉或是離島的地方政府，交通往往不如大城市便捷，導致縣市政府資通安全業務承辦人員跟公所進行資通安全輔導或提供相關技術支援時，所需付出的通勤成本更高（LG-Z6-4）。再者，偏鄉與一般都會區相比，資通安全的起跑點明顯落後，本來就需要更多經費購入設備，把資通安全做好，但偏鄉的地方政府得到經費比不上大城市，便更難做好資通安全，產生惡性循環。受訪者便指出：

> 「惡性循環」是說人家覺得你資安越差就越不能做，越不能補助；不能補助就越來越差……不是我們不想呀，好像防火牆的這一塊我已經花完，我就沒有錢啦。（LG-Z5-2）

5. 一般公務人員資通安全意識與素養不足

一般公務人員資通安全意識與素養不足，是地方政府受訪者們另一項常提到的現況（LG-Z4-1a；LG-Z4-1b；LG-Z1-1a；LG-Z1-1b；LG-Z6-3）。由於強調資訊系統的安全性，往往與系統操作的便利性有所衝突，機關成員不見得願意爲資通安全犧

牲方便性，例如設定一定長度複雜的密碼、限時登入系統等（LG-Z6-3；LG-Z1-1a；LG-Z1-1b）。

6. 政治的不確定性

若將資通安全視爲需要政府採取行動加以因應的政策問題時，多元利害關係人對於資通安全的不同認知，例如，政府關心資通安全背後涉及的「國安」問題，但民眾往往更擔心「隱私」權被侵犯，這些不同的價值觀點在民主政體下，最終透過民主的程序進行協商和妥協（CG2），但協商妥協的背後，可能隱含著政策的不延續性所帶來風險。舉例來說，目前多數地方政府獲得中央政府前瞻計畫經費來支應資通安全管理和參與區域聯防的業務支出，地方政府也對此表示支持。但是地方政府同時也擔心前瞻計畫所提供的階段性經費若未來未能延續，目前已投入資通安全的工作會因此白費（LG-Z6-3）。

（二）資通安全互賴性

受訪者指出，資通安全之鞏固，仰賴資安事件的情資分享，因爲網路是互聯的，這須落實在跨國之間的區域聯防，國內各級政府與中央之間的區域聯防，以及公私部門行動者之間的公私協防（CG2）。對於資安事件應變能量有限的地方政府而言，當發生嚴重的資通安全事件且影響範圍大，無法仰賴單一縣市處理時，須透過區域聯防才能發揮即時作用（LG-Z6-3）。

對於公部門而言，分享情資、事件通報是爲了資訊流通性，提高整體國家或機關對外部駭客事件的防禦，但分享情資、事件通報本身也同時承認了政府機關本身資通安全事件發生的存在（LG-Z6-4）。公部門基於保密及匿名的考量，一般傾向低調、保守的處理方式，不見得願意即時公開整體事情的全貌及自身資通安全防護對應策略與步驟。如果公開，也傾向會採先及時處理解決事件後再分享公開的做法（LG-Z6-4）。換言之，資通安全本身的性質與區域聯防理念可能會產生衝突的情況，一方面資通安全強調機密性及資料和隱私保護，但另一方面又希望透過區域聯防，藉由情資分享及事件通報達到互助的目標。有鑑於此，基於了解政府機關發生資安事件時，內部資安單位往往最擔心後續可能需擔負的責任，有受訪者在其轄區內建置標準作業流程機制（SOP），認爲只要內部資安單位已經遵照 SOP 完成相關要求與程序，就可以免責：

> 已經照了 **SOP** 來做了，那後面產生的與你無關。這些所謂的影響、權責不在於他……。（LG-Z3-1a）

此外，中央政府受訪者也建議，針對各級政府公務人員主動通報資通安全事件的態度和行動，應給予肯定和獎勵，而非讓公務人員擔心如果通報可能會受到懲處，這反而不利於鼓勵情資分享、進行資安聯防（CG2）。

（三）參與誘因

中央政府受訪者指出，中央透過前瞻計畫經費，補助地方政府投入區域聯防工作，給予其相當程度在經濟層面上的誘因（CG1；CG3；LG-Z3-1a），地方政府也認同，中央長期持續且多方面在資通安全演練、資產盤點、硬體升級等面向上的經費挹注是重要的支援（LG-Z1-1b）。不過中央政府也意識到，對地方政府而言，參與區域聯防體系，讓中央政府技術協助地方政府處理資安事件，達成問題解決的成果，也是重要的參與誘因之一（CG3）。此外，除了緊急時刻可透過區域聯防機制，協助地方政府處理重大資通安全事件（LG-Z6-3）外，平時也可藉由情資分享機制，掌握情資（LG-Z6-3），或參考學習區域成員成功的做法（LG-Z3-1a）。

（四）中央政府領導力

中央政府對於資通安全議題的重視，最早可見於 2000 年國家安全會議研擬提出之「建立我國資通訊基礎建設安全機制」建議書，後於 2001 年第 2718 次院會中核定通過第一期資通安全機制計畫，並成立行政院「國家資通安全會報」。十多年後，蔡政府爲有效因應日趨嚴峻的資通安全威脅，國家安全會議與行政院於 2016 年共同舉辦「資安即國安」策略會議，行政院接續於 2017 年通過 4 年期的「國家資通安全發展方案」，更於 2018 年通過資安法之立法，並搭配投入「資安旗艦計畫」及「前瞻基礎建設計畫」。後續也於 2018 年提出「國家資通安全戰略報告—資安即國安」，2021 年提出「國家資通安全戰略報告—資安即國安 2.0」。[9] 隨著 2022 年數位發展部的成立，行政院資通安全處改爲數位發展部資通安全署，以及 2023 年 1 月將國家資通安全技術服務中心與國家實驗研究院資安卓越中心規劃建置計畫合併，改制爲行政法人國家資通安全研究院。由此可見，中央政府透過立法與研擬相關政策，確立中央政府對於我國資通安全發展方向與主導地位，並透過計畫經費由上而下投入資源，同時透過機關組織的調整，來顯現中央政府對於資通安全課題的重視程度。

而中央政府的受訪者也指出，隨著 2018 年資安法通過，中央政府在資通安全推動上便有法令依據，且有相對明確的法遵事項要求關鍵基礎設施提供者配合

[9] 詳細內容請參見總統府網站之網頁內容說明，網址：https://www.president.gov.tw/Page/317/969

（CG2）。在受訪當時，受訪者認爲中央政府越來越意識到資通安全的重要性，拉高到「資安即國安」這個層次，透過國家安全會議、行政院資通安全處、國家通訊傳播委員會這樣的「資安鐵三角」組織架構領導來推動（CG2）。[10] 此外，中央政府也藉由參與年度資安大會、舉辦資安演練、資安稽核與資安健檢等活動，拉近中央與地方政府之間的關係，藉此協助地方政府提升資安能量（CG3）。

至於區域聯防策略的推動上，受訪者指出中央政府多會選擇尊重地方首長做法及在地脈絡來推動區域聯防（CG1；CG2），而獲得中央政府的實際支持、認同與鼓勵，對地方執行資通安全業務、建立資通安全防護能量來說，有重要的意義。地方政府受訪者便指出：

> 地方政府有各種思維、各種做法，可是當我提出一種好的想法、好的做法的時候，願不願意給一點支持？……。那如果說中央這邊也願意給一點力，那地方政府其實會覺得說：「不錯喔，那個想法是被支持的喔！」（LG-Z3-1a）

二、資通安全協力治理過程

（一）原則化的參與

目前我國資通安全的區域聯防，是以六大直轄市政府爲核心，逐步成立區域ISAC、SOC、CERT，目前由各直轄市維運，鼓勵結合其周邊鄰近縣市，推動及建立地方聯合資訊安全防護網。從訪談中發現，區域聯盟的成員對區域聯盟此政策的感受或認知，可能是影響各區域聯盟如何運作的前提。有受訪者認爲，區域聯防要能運作，得讓地方政府對於區域聯防此政策切身地感受，並認同有建立區域聯防的實際需求（LG-Z3-1a）。例如，有地方政府反映，從過去以來，本身的業務已經包括了情資分享，而區域聯防只是將情資分享對象從原本的中央層級的技服中心，增加多一個直轄市政府，但這個增加沒有讓他們感到更有效果，故產生政策上有疊床架屋之慮（LG-Z5-2；LG-Z6-3）。而區域聯防的概念下，雖然鼓勵地方政府彼此之間，以及向上與中央政府進行情資分享，但實際上到底要分享什麼，各地方政府對於情資分享概念，以及執行面上的做法與認知是否同步，其實也是區域聯防此策略能否有效運作

[10] 相關政策內容可參考 2018 年國家安全會議提出的「國家資通安全戰略報告」。詳細說明請參見網址：https://www.president.gov.tw/File/Doc/8f65b086-6be5-4481-b376-a4001204f003

的關鍵（LG-Z5-2）。

而目前各區域中直轄市政府與其區域成員縣市政府間推動區域聯防、創造溝通管道的模式不一，例如，採取定期開會交換意見，舉辦專案報告，參訪資安廠商活動，平時透過電子郵件等方式進行資訊分享（LG-Z1-1b；LG-Z3-1a）；採納多方利害關係人觀點，透過舉辦正式與非正式的交流活動來交換彼此意見，並從中了解需要提供哪些協助（LG-Z4-1b）；偏向透過建置自動化機制來串聯區域內成員，藉由自動化的防護派送機制，區域聯防內的成員間可以建立緊密的聯繫，並降低因人爲疏失帶來的問題（LG-Z6-1）。由於區域內成員都委託相同廠商提供服務，因此各地方政府習慣直接找廠商聯繫溝通，故相對而言，區域成員間較少透過會議或其他面對面活動進行聯繫溝通（LG-Z6-1）。

（二）共享動機

依據理論架構，建立信任、相互理解、內部正當性、承諾是形成共享動機的四項相互影響之要件。雖然如前所述有些區域聯盟成員之間的情資分享與交流，僅仰賴定期的會議或是 email 互通訊息，或是透過自動化機制派送情資，因此面對面的人際交流活動並不多。而且地方政府之間平時也常面臨競爭的關係，例如，彼此競爭中央政府的計畫經費補助，因此要建立信任感其實不容易（LG-Z5-2）。但也有地方政府特別重視區域內成員之間人際關係的建立，並強調信任對於建立與維繫區域聯防夥伴關係的重要性（LG-Z4-1a；LG-Z4-1b）。受訪者提到：

> 我覺得我們就一直等於是把○○○都當成夥伴。（LG-Z4-1a）

至於建立信任的方式，地方政府受訪者提到本身與區域夥伴會透過時常保持聯絡溝通且彼此熟絡來建立信任關係，以增加區域間合作意願，或是透過舉辦技術交流會，聚集技術人員彼此交換意見和探討資通安全事件，達成共識及建立信任關係，並強調成員間非正式交流活動的重要性（LG-Z4-1a；LG-Z4-1b）。故建議中央政府可以多舉辦增加非正式或半正式的交流活動，創造各區域間地方政府彼此互動與認識，建立與強化彼此的信任（LG-Z4-1b）。

此外，由於意識到各地方政府本身都是獨立的個體，因此受訪者會透過網絡管理的方式來串聯區域內不同地方政府，藉由交流各自的想法形成各自的政策（LG-Z4-1b），這同時也突顯出區域聯盟內各成員之間需要相互理解與尊重彼此的差異性。當各區域聯盟中成員之間建立足夠的信任感並能互相理解與尊重彼此的差異性和看法，

便能在過程中逐漸建立各區域聯盟的內部合法性，進而強化成員對於區域聯盟的承諾感。

（三）聯合行動能量

聯合行動能量指涉過程與制度性的安排、擁有的資源、相關知識技能，以及領導力等各項有助於促成區域聯防成員共同行動之因素。訪談內容中發現，推動區域聯防，地方政府本身資通安全能量的多寡是關鍵因素之一，除經費外，地方政府受訪者認同資通安全人力資源投入的重要性，並指出長遠而言需策略性地爭取員額的增加，但不能盲目只求人力的增加，而忽略整體資通安全領域人力市場結構的問題（LG-Z3-1a）。另外，也建議積極鼓勵及並提供經費支援，讓資通安全業務專責人員考取相關證照或給予相關訓練，把機關資通安全專責人員當作人才栽培而非僅是人力使用，藉此創造地方政府機關留住資通安全人才的誘因（LG-Z3-1a）。

也有地方政府對於參與區域聯防有所遲疑，這多與機關組織本身的資安能量多寡有關。第一，由於目前推動區域聯防的做法，地方政府多以臨時任務編組方式進行，沒有專責單位與人力負責此項業務，有受訪者認爲這可能會導致區域聯防所能發揮的效果有限（LG-Z6-3）。第二，原本地方政府機關內部資通安全人力已不足，業務量不勝負荷，參與區域聯防會增加現有業務量，同時也須花額外心力及時間與其他地方政府經營信任關係（LG-Z4-1a）。第三，地方政府資通安全業務單位參與區域聯防，無論是對外分享或是接收情資，或只是建置一般安全日誌（log 檔），其背後的資訊量其實都相當龐大，若要從中萃取分析以取得有價值的情資，其實需要專業資通安全人員投入心力，就算可依賴自動化資通安全系統篩選判別，但可能最終還是得由人力進一步判辨除錯或過濾（LG-Z5-2），導致面臨資訊過載的難題。

而獲得地方政府首長或機關單位長官的支持，也對地方政府資通安全能量能否提升產生重要影響。若地方政府首長或機關單位長官對資通安全業務有一定程度的了解，並抱持支持的態度，對於資通安全業務在經費預算、人力投入、資通安全人員在機關內的地位等面向，會帶來正面影響（LG-Z4-1b；LG-Z6-3）。

至於區域聯防能否達成預期效果，地方政府受訪者指出其實取決於直轄市作爲「母雞」是否有足夠能力主導區域內的「小雞」們（LG-Z5-2）。直轄市政府對於區域聯防的態度、主導力、能量是影響的關鍵。不過，也有受訪者強調，各地方政府本身是否具備一定程度的資通安全能量亦是重要前提，若僅仰賴直轄市本身外撥資源或投注心力帶領區域內的聯防夥伴，其實難以發揮區域聯防的成效（LG-Z3-1a）。

三、綜合討論

綜整以上訪談資料的分析結果，本文提出圖 2，彙整出當前我國資通安全協力治理的樣貌，並透過呈現驅力、協力治理過程中之要素，探討影響地方政府參與資通安全區域聯防體系彼此協力互動之關鍵因素，以及所面臨的困難與挑戰，並與文獻進行對話。

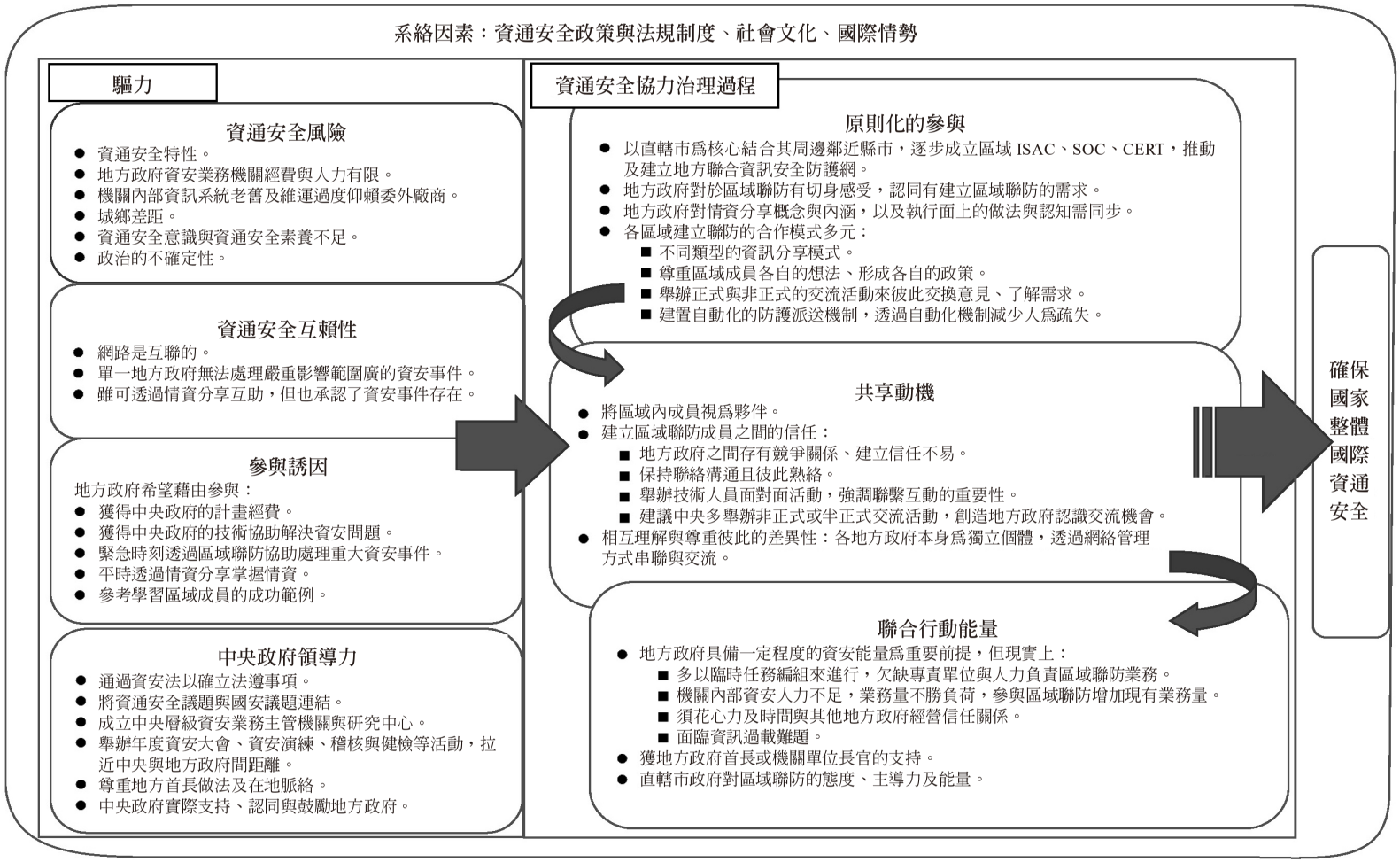
從趨力中的「資通安全互賴性」、「參與誘因」來看，地方政府確實有參與區域聯防體系的動機，一方面希望透過聯防機制與其他成員進行交流，彼此學習，並透過區域聯防下的情資分享機制掌握情資，另一方面，當發生嚴重的資通安全事件，無法仰賴單一縣市處理時，可透過區域聯防發揮即時應變的作用。這也呼應文獻中提到行動者參與資通安全區域聯防機制分享資訊往往希望能藉此提升組織本身的防禦能力或是降低防禦成本（Pala & Zhuang, 2019）。然而，雖然地方政府希望透過情資分享、事件通報及達到互助的目標，但分享情資、事件通報也意謂承認資通安全事件的存在，因此可能面臨究責的處境，同時也容易陷入資訊揭露，與內部資訊保密及隱私權保護的兩難，這也呼應過往文獻中提到行動者參與區域聯防機制可能須付出的成本或面臨的難題（Germano, 2014; Pala & Zhuang, 2019）。

至於驅力中的「中央政府領導力」則顯示，中央政府透過逐年建置資安相關政策與通過資安法，確立法遵事項，並將資通安全議題與國安議題連結，以及成立中央層級資安業務主管機關與研究中心，來領導與提升國家整體資安能量。同時，中央政府藉由參與資安大會、舉辦各項資安演練、資安稽核、資安健檢等活動與演習，強化中央與地方政府之間，以及地方政府之間的認識與交流。實務上各區域內部技術上如何建置聯防體系，中央政府採尊重各地方政府的立場。而對於地方政府而言，獲得中央長期持續地實際支持、認同與鼓勵，具有正面的鼓舞力量。此發現突顯文獻中強調領導力及建置相應的法規制度對於建立協力關係的重要性（Ansell & Gash, 2008; Center for Strategic and International Studies, 2013; Emerson & Nabatchi, 2015; Greiman, 2015; Manley, 2015）。

至於資通安全協力治理過程中，「原則化的參與」顯示，區域聯防能否成功運作，需仰賴地方政府對區域聯防此國家策略能有切身的感受，認同有建立區域聯防的實際需求，並體認能藉此提升其資通安全成效。同時也需讓地方政府同步清楚區域聯防下情資分享的界定範疇與可行做法，這也呼應協力治理文獻強調須建立共同目標與取得共識，方能有效推進協力行動之觀點（Emerson & Nabatchi, 2015）。目前各區域促進區域成員對於參與聯防之策略做法多元，有些區域重視跨地方政府之間的人際交流合作，有些區域則仰賴建置自動化系統串聯區域內成員，做法的差異性相當程度

圖 2

當前我國資通安全協力治理樣貌



資料來源：作者自行整理。

受直轄市政府採取的執行方式影響。

「共享動機」則顯示，建立夥伴關係，營造區域聯防內地方政府之間的信任，是促使區域聯防體系能有效運作的重要因素之一，此研究發現也與過往文獻強調信任的建立與維繫有助於確保資通安全公私協力之論點相契合（Manley, 2015; Yanakiev & Tagarev, 2020），即便建立與維繫區域夥伴之間的信任感並非易事。同時，區域聯盟內各成員之間亦需要相互理解與尊重彼此的差異性。當各區域聯盟中成員之間建立足夠的信任感並能互相理解與尊重彼此的差異性和看法，有助逐步建立各區域聯盟的內部合法性，進而強化成員對於區域聯盟的承諾感。

而「聯合行動能量」指出，區域內各地方政府本身具備一定程度的資通安全能量，除經費外，地方政府本身對於資通安全人力資源的重視和投入，以及獲得地方政府首長或機關單位長官的支持，這些都有助於該區域中聯防理念的實踐。而引領各區域的直轄市政府，對於區域聯防的態度、主導力，以及本身組織的資通安全能量，對於區域聯防能否成功運行也有相當程度的影響力。這項研究發現也呼應過往研究強調機關組織內部高階文官與領導者對資通安全議題的支持，對於維繫資通安全公私協力以及提升地方政府資安能量之重要性（Center for Strategic and International Studies, 2013; Greiman, 2015; Norris et al., 2021）。

至於驅力中的「資通安全風險」因素，則可能成爲地方政府對參與區域聯防怯步，或是偏向被動消極的理由，同時也點出地方政府面臨的困境與挑戰。例如，城鄉差距的問題，讓位處偏鄉或離島的地方政府，更容易面臨欠缺資訊與資通安全相關專業人力，缺乏商業誘因吸引資訊和資通安全設備和技術廠商進駐當地，維運資訊與資通安全設備成本高，以及資訊基礎建設相對落後等各項難題。再者，地方政府長久以來面臨資訊經費與專業人力不足的問題，加上參與區域聯防本身也需要人力與經費的投入，而資通安全在資訊領域之下，其人力與經費更顯捉襟見肘，面臨無法留住專業人才、資通安全專業難以與時俱進的難題。而資通安全本身的隱性特點，容易造成資源投入到資通安全領域，其成效較難立即呈現，因此難以持續爭取更多資源挹注的負向循環。另外，地方政府往往也處於機關內部資訊系統老舊及維運過度仰賴委外廠商的狀況，若要加以改善，需要長遠規劃與大量經費支應。前述提及的困境，除了呼應過往文獻提及地方政府資安人力不足、大量仰賴委外資安廠商維運衍生的問題外（張書瑋，2018；陳泉錫、陳俊呈，2020），突顯對於地方政府而言，資通安全管理的難題某種程度上也反映出地方政府間的數位機會仍存在一定程度差距的現象。而地方政府一般公務人員，其資通安全意識與資通安全素養普遍不足，容易忽視資通安全重要性，也讓地方政府容易面臨更多資通安全風險，這其實顯現出資安風險意識建立及相關訓練的必要性（Norris et al., 2021）。至於政治的不確定性對地方政府而言，則

反映在中央政府政策以及計畫經費的延續性議題上，由於地方政府往往面臨資訊經費短缺的狀況，當地方政府對於中央提供的計畫經費的存續性存疑時，可能進一步影響未來地方政府持續配合投入區域聯防政策之意願。

伍、結論與建議

一、結論

本文從探索性的角度，以協力治理文獻爲基礎，透過結合資通安全和災害防救的概念，提出資通安全協力治理架構，探討目前我國資通安全政策下推行的區域聯防體系之現況，以了解影響我國地方政府參與資通安全區域聯防體系，以及彼此協力互動之因素。本文認爲，探討資通安全協力治理、思考建置中央和地方資通安全區域聯防體系課題，必須先同步考量資通安全本身的特性，並且結合災害防救、風險管理、協力治理等理論基礎，才能系統性地思考區域聯防成員的參與動機和行動。因此，本文之貢獻，在學理上，藉由結合資通安全與公共行政與管理等跨專業領域，進一步認識資通安全協力治理的內涵與運作過程，建立理論架構並累積本土性實證研究資料；實務上，亦有助於持續深入了解我國資通安全區域聯防的政策現況，以提供未來發展之相關政策建議。

二、政策建議

本文建議，中央政府未來如果要穩固資通安全區域聯防體系，並鼓勵地方政府積極參與，可從以下幾個部分來考慮。首先，從驅力來看，如何強化地方政府對於資通安全互賴性的認知，並持續創造參與誘因，是重要的一步。由於情資分享與事件通報容易讓地方政府組織及其成員作爲區域聯防成員面臨道德風險的兩難，如何透過設計合理妥善的課責與獎懲制度，紓解地方政府及成員的疑慮，也與中央政府的態度和法令規範有關。面對此課題，本文建議中央政府藉此時機營造中央與地方政府之間，以及地方政府之間情資分享與相互合作的組織文化，使其認同推動區域聯防的必要性，並搭配法令規章積極鼓勵情資分享與跨機關組織合作，如「公務機關所屬人員資通安全事項獎懲辦法」第 3 條所列，並提供相應的經費資源和專業支援，協助地方政府逐步將區域聯防策略加以落實。而中央政府所頒布的資通安全相關法令與區域聯防政策，也需與時俱進並建立清楚的規範標準，作爲提供地方政府落實資安管理與投入區域聯防政策的依據。

至於如何協助地方政府減緩所面臨的資通安全風險，逐步提升各級政府機關本身

之資安成效，並建立長期且持續性的制度挹注資源到地方政府，給予支持，且理解地方政府本身同時面臨資通安全風險面的猶豫，促使地方政府感受參與資通安全區域聯防對其本身其實具有利大於弊的效果，是中央政府未來須長期關注的課題，持續檢視與評核地方政府的資安能量與管理成效爲可能的因應策略之一。目前我國政府參照國外做法，嘗試從資安治理成熟度的觀點來評估政府機關的資安治理成效，在評估項目上除檢視政府機關的資安防護與風險控管工作內容，亦同時考量政府機關資安相關人力與經費等資源之投入。[11] 本文建議後續可持續研議落實此評估機制的可行性，並納入地方政府的反饋意見來滾動修正相關做法。本文也呼籲，中央政府須正視並協助地方政府因應與解決資訊系統過度委外，連同資通安全系統過度委外，導致地方政府資安能量空洞化的問題。針對政府專業資安人才與人力不足的部分，本文建議除了結合大專院校專業及積極培育政府未來的資安人才外，培訓合格的資安志工，或透過舉辦實習計畫讓具有資安相關專業的優秀學生到公部門實習，協助提升地方政府資安能量，也是我國未來可參採的因應策略。[12]

若從資通安全協力治理過程來看，原則化的參與、共享動機、聯合行動能量這三個面向，顯示推動與維運資通安全區域聯防體制，需要區域成員間能對該體制有切身的感受，並認同有建立區域聯防的實際需求，能藉此提升其資通安全成效。同時也需讓地方政府能同步理解區域聯防下情資分享的界定範疇與可行做法，方能使其積極參與。此外，區域聯防成員之間須建立夥伴關係，形成以信任、互相理解爲基礎的共享動機，促使地方政府持續參與區域聯防，並且維持地方政府參與區域聯防的聯合行動能量，而這三者之間環環相扣。就現況而言，雖然中央政府各區域執行聯防的策略做法採尊重地方的態度，但區域聯防本身其實也涉及各區域內，以及各區域間，甚至與中央政府之間的水平面與垂直面的府際關係，但是目前現行制度對於地方自治、府際管理與資通安全管理課題的法制面之討論相對不足，例如，地方政府是屬於強制性亦或是自願性參與區域聯防體系，在相應的政策設計上該如何進行短、中、長期維運規劃並符合我國地方制度的特性，這些都有待進一步地討論。而直轄市政府作爲區域聯

[11] 針對我國政府機關資安治理成熟度相關討論可參見吳啓文與林晶瑩（2019）之文章。

[12] 目前已有私部門資安服務廠商開始啓動資安志工相關計畫，協助提升兒童、家庭、中小企業資通安全能量，以及大專院校資通安全教育，如趨勢科技教育計畫（詳請參見網址：https://www.trendmicro.com/zh_tw/initiative-education/about.html#team-tm-anchor）。而美國網路安全暨基礎設施安全局（Cybersecurity and Infrastructure Security Agency, CISA）也有啓動學生實習計畫，鼓勵具有資安相關專業的在學學生申請赴政府機關實習（詳情請參見網址：https://www.cisa.gov/careers/work-rolescyber-and-it-interns）。美國非營利組織 The Partnership for Public Service 則舉辦資安人才實習計畫（Cybersecurity Talent Initiative），鼓勵並協助擁有資安相關專長具公民身分的大專院校優秀在學學生申請到政府機構實習（詳情請參見網址：https://gogovernment.org/fellowship/cybersecurity-talent-initiative/）。

防的領頭羊，是否具有政策工具協助其凝聚區域內部成員，如何妥善利用自動化機制串聯區域成員，以及如何明確定位其角色任務並進行短、中、長期規劃設計，這些也是後續需考量的課題。本文建議中央政府未來應就上述課題，與地方政府進行對話，就區域聯防體系的參與機制與維運規劃做更細緻的設計。

最後，地方政府對於區域聯防政策的清楚認識與認同，以及區域成員之間的信任，是區域聯防能否成功建立與維運的關鍵之一，但區域成員彼此信任感的建立，往往需要各區域成員投入大量的時間、人力、相關資源來維繫，也需要直轄市政府作爲區域領袖，帶領區域成員，而這其實也與各地方政府本身參與區域聯防的能量高低有關。本文建議中央政府可透過定期舉辦正式與非正式活動，讓各地方政府能清楚了解區域聯防的核心概念、相關技術與實務可行做法，創造地方政府之間建立關係、累積信任的機會。

三、研究限制與未來研究課題

針對研究限制與未來研究課題的部分，本文依據訪談資料進行分析與歸納，雖然已嘗試涵納不同類型受訪者之觀點，但研究分析成果仍受限於受訪者個人的服務單位、位階、工作經驗所提供的觀點，以及作者本身的解讀，故仍存有一定程度的主觀性。此外，本文的實證分析主要聚焦於歸納研究架構所提出的驅力與協力治理過程面向中的因素，並未探討或比較各面向中各項因素重要程度，且協力治理過程因素對於行動結果之影響也尚待進一步分析與討論。最後，本文主要透過提出資通安全協力治理架構，以驅力與資通安全協力治理過程，探究影響地方政府參與我國以六都爲首的區域聯防體系和彼此協力互動之關鍵因素，以及其所面臨的困難與挑戰，並未就理論架構中涉及關鍵基礎設施提供者之公私協力的部分進行探討，故建議未來研究可針對前述幾項課題進行進一步的探索與分析。

參考文獻

一、中文部分

行政院（2014）。**國家關鍵基礎設施安全防護指導綱要**，12 月 29 日。https://ohs.ey.gov.tw/File/EF5E72C88077DE72 [Executive Yuan (2014). *Guojia guanjian jichu sheshi anquan fanghu zhidao gangyao*, December 29.]

行政院國家資通安全會報（2021）。**國家資通安全發展方案（110 年至 113 年）**。行政院，2 月。https://cloudschool.chc.edu.tw/open-message/074738/get-file/6041e464285d5d58af198572.pdf [Executive Yuan National Information Security Conference Report (2021). *Guojia zitong anquan fazhan fangan*. Executive Yuan, February.]

李宗勳（2016）。**危機管理與談判**（初版）。元熙。[Lee, T.-S. (2016). *Crisis management and negotiation* (1st ed.). Angle Publishing.]

李長晏、曾淑娟（2009）。北臺與高高屏區域聯盟治理營運之比較。**臺灣民主季刊，6**（2），1-60。[Lee, C.-Y., & Tseng, S.-C. (2009). A comparison on the governing operations of the northern Taiwan region alliance and the kao-kaoping region alliance. *Taiwan Foundation for Democracy*, *6*(2), 1-60.]

李翠萍（2007）。直轄市社政單位部際關係之研究：政策執行的觀點。**政治科學論叢**，（31），87-128。[Lee, T.-P. (2007). Welfare interagency relations at the local level: A policy implementation perspective. *Taiwanese Journal of Political Science*, (31), 87-128.]

林淑馨（2017）。從協力治理檢視日本的災害防救。**行政暨政策學報**，（65），1-37。[Lin, S.-H. (2017). Japanese disaster prevention from a partnership governance perspective: The example of the 2011 Tohoku earthquake. *Public Administration & Policy*, (65), 1-37.]

林淑馨（2018）。協力神話的崩壞？我國地方政府與非營利組織的協力現況。**公共行政學報**，（55），1-36。[Lin, S.-H. (2018). The fall of collaborative governance? Current collaboration between local governments and non-profit organizations. *Journal of Public Administration*, (55), 1-36.]

吳啓文、林晶瑩（2019）。政府機關資安治理成熟度評估機制。**國土及公共治理季刊，7**（4），80-91。[Wu, C.-W., & Lin, C.-Y. (2019). Zengfu jiquan zian zhili chengshudu pinggu jizhi. *Public Governance Quarterly*, *7*(4), 80-91.]

胡龍騰、曾冠球、張智凱、黃榮志（2013）。電子化跨域治理影響因素之研究：多個案之探索。**公共行政學報，**（45），1-39。[Hu, L.-T., Tseng, K.-C., Chang, C.-K., & Huang, R.-C. (2013). Influential factors of electronic cross-boundary governance: An exploratory study with multiple cases. *Journal of Public Administration*, (45), 1-39.]

翁芊儒（2020）。**【臺灣資安大會直擊】調查局完整揭露中油、台塑遭勒索軟體攻擊事件調查結果，駭客集團入侵途徑大公開**。iThome，8 月 12 日。https://www.ithome.com.tw/news/139331 [Weng, Q.-R. (2020). *[Taiwan zian dahu izhiji] Diaochaju wanzhen gjielu zhongyou taisu zao lesuo ruanti gongji shijian diaocha jieguo, haike jituan ruqin tujing dagongkai*. iThome, August 12.]

張書瑋（2018）。我國資通安全戰略及體系評估－兼論資通安全管理法草案。**安全與情報研究，1**（1），39-87。[Chang, S.-W. (2018). An evaluation on information and communication security strategy and system in Taiwan: Focus on the draft of the information communication security management act. *Security and Intelligence Studies*, *1*(1), 39-87.]

陳育正（2015）。美國資通安全防護經驗對我國資通安全情勢之啓示。**國防雜誌，30**（3），73-87。[Chen, Y.-C. (2015). The US experience of cyber security and its implications to Taiwan's national security. *National Defense Journal*, *30*(3), 73-87.]

陳俊明、朱斌妤、黃東益、蔣麗君、李仲彬、張鎧如（2014）。**數位國家治理：國情分析架構與方法**（編號：RDEC-MIS-102-001）。行政院研究發展考核委員會。[Chen, C.-M., Chu, P-Y., Huang, T.-Y., Chiang, L.-C., Lee, C.-P., & Cheng, K.-J. (2014). *Public value and electronic governance: Analytical and methodological reflections* (Project number: RDEC-MIS-102-001). Research, Development and Evaluation Commission.]

陳泉錫、陳俊呈（2020）。駭客無所不在，政府機關的資料安全嗎？載於陳敦源、朱斌妤、黃東益、廖洲棚、曾憲立（編），**政府數位轉型－一本必讀的入門書**（頁 327-342）。五南圖書。[Chen, C.-H., & Chen, C.-C. (2020). Haike wusuobuzai, zhengfu jiguan de ziliao anquan ma? In D.-Y. Chen, P.-Y. Chu, T.-Y. Huang, Z.-P. Liao, & H.-L. Tseng (Eds.), *Digital transformation in government: A must-read primer* (pp. 327-342). Wu-Nan Book Inc.]

陳敦源、張世杰（2010）。公私協力夥伴關係的弔詭。**文官制度季刊，2**（3），17-71。[Chen, D.-Y., & Chang, S.-J. (2010). The paradoxes of public-private partnerships. *Journal of Civil Service*, *2*(3), 17-71.]

彭慧鸞（2004）。數位時代的國家安全與全球治理。**問題與研究，43**（6），29-52。[Poong, H.-L. (2004). Digital security and global governance. *Journal of Issues and Studies*, *43*(6), 29-52.]

曾冠球（2010）。「問題廠商」還是「問題政府」？電子化政府公私合夥協力困境之個案分析。**公共行政學報，**（34），77-121。[Tseng, K.-C. (2010). Is the firm or the government agency a trouble maker? A case study of obstacles to successful public-private partnerships (PPPs) in e-government. *Journal of Public Administration*, (34), 77-121.]

潘競恒、蔣麗君（2013）。地方政府電子治理成效認知評估研究。**行政暨政策學報，**（56），43-83。[Pan, C.-H., & Chiang, L.-C. (2013). An evaluation framework of perceived performance of local e-governance. *Public Administration & Policy*, (56), 43-83.]

賴曉黎（2012）。資通科技的工具面向－從科技決定論談起。**資訊社會研究，**（23），1-35。[La, S.-L. (2012). The instrumental dimension of ICTs: Starting with technological determinism. *Journal of Cyber Culture and Information Society*, (23), 1-35.]

二、英文部分

Agranoff, R., & McGuire, M. (2003). *Collaborative public management: New strategies for local governments*. Georgetown University Press.

Ansell, C., & Gash, A. (2008). Collaborative governance in theory and practice. *Journal of Public Administration Research and Theory*, *18*(4), 543-571.

Assaf, D. (2008). Models of critical information infrastructure protection. *International Journal of Critical Infrastructure Protection*, *1*, 6-14.

Balzacq, T., & Cavelty, M. D. (2016). A theory of actor-network for cyber-security. *European Journal of International Security*, *1*(2), 176-198.

Caruson, K., MacManus, S. A., & McPhee, B. D. (2012). Cybersecurity policy-making at the local government level: An analysis of threats, preparedness, and bureaucratic roadblocks to success. *Journal of Homeland Security and Emergency Management*, *9*(2), 1-22.

Cavelty, M. D. (2013). From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse. *International Studies Review*, *15*(1), 105-122.

Center for Strategic and International Studies (2013). *Public-private partnerships for critical infrastructure protection*, August 19. https://www.csis.org/analysis/public-private-partnerships-critical-infrastructure-protection-0

Emerson, K., Nabatchi, T., & Balogh, S. (2012). An integrative framework for collaborative governance. *Journal of Public Administration Research and Theory*, *22*(1), 1-29.

Emerson, K., & Nabatchi, T. (2015). *Collaborative governance regimes*. Georgetown University Press.

Gash, A. (2016). Collaborative governance. In C. Ansell & J. Torfing (Eds.), *Handbook on theories of governance* (pp. 454-467). Edward Elgar Publishing.

Germano, J. H. (2014). *Cybersecurity partnership: A new era of public-private collaboration*. The Center on Law and Security.

Greiman, V. A. (2015). Public/private partnerships in cyberspace: Building a sustainable collaboration. *Journal of Information Warfare*, *14*(3), 30-42.

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen school. *International Studies Quarterly*, *53*(4), 1155-1175.

Harknett, R. J., & Stever, J. A. (2009). The cybersecurity triad: Government, private sector partners, and the engaged cybersecurity citizen. *Journal of Homeland Security and Emergency Management*, *6*(1), 1-14.

Harknett, R. J., & Stever, J. A. (2011). The new policy world of cybersecurity. *Public Administration Review*, *71*(3), 455-460.

Manley, M. (2015). Cyberspace's dynamic duo: Forging a cybersecurity public-private partnership. *Journal of Strategic Security*, *8*(3), 85-98.

McEntire, D. A. (2015). *Disaster response and recovery: Strategies and tactics for resilience* (2nd ed.). John Wiley and Sons.

Norris, D. F., Mateczun, L., Joshi, A., & Finin, T. (2018). Cybersecurity at the grassroots: American local governments and the challenges of internet security. *Journal of Homeland Security and Emergency Management*, *15*(3). https://doi.org/10.1515/jhsem-2017-0048

Norris, D. F., Mateczun, L., Joshi, A., & Finin, T. (2019). Cyberattacks at the grass roots: American local governments and the need for high levels of cybersecurity. *Public Administration Review*, *79*(6), 895-904.

Norris, D. F., Mateczun, L., Joshi, A., & Finin, T. (2021). Managing cybersecurity at the grassroots: Evidence from the first nationwide survey of local government cybersecurity. *Journal of Urban Affairs*, *43*(8), 1173-1195.

Pala, A., & Zhuang, J. (2019). Information sharing in cybersecurity: A review. *Decision Analysis*, *16*(3), 172-196.

Preis, B., & Susskind, L. (2022). Municipal cybersecurity: More work needs to be done. *Urban Affairs Review*, *58*(2), 614-629.

Sanger, D. E., Krauss, C., & Perlroth, N. (2021). Cyberattack forces a shutdown of a top U.S. pipeline. *The New York Times*, May 8. https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html

Shaw, K. (2012). The rise of the resilient local authority? *Local Government Studies*, *38*(3), 281-300.

Tagarev, T. (2020). Towards the design of a collaborative cybersecurity networked organisation: Identification and prioritisation of governance needs and objectives. *Future Internet*, *12*(4), 62.

Walker, J. (2012). Cyber security concerns for emergency management. In B. Eksioglu (Ed.), *Emergency Management* (pp. 39-59). IntechOpen.

Wirtz, B. W., & Weyerer, J. C. (2017). Cyberterrorism and cyber attacks in the public sector: How public administration copes with digital threats. *International Journal of Public Administration*, *40*(13), 1085-1100.

World Economic Forum (2018). *The global risks report 2018* (13th ed.), January 17. http://www3.weforum.org/docs/WEF_GRR18_Report.pdf

Yanakiev, Y., & Tagarev, T. (2020). *Governance model of a cybersecurity network: Best practices in the academic literature* [Conference presentation]. 21st International Conference on Computer Systems and Technologies, June19-20, Ruse, Bulgaria.

Yannakogeorgos, P. A. (2012). Internet governance and national security. *Strategic Studies Quarterly*, *6*(3), 102-125.

附錄一：受訪者資訊

表 A
受訪者背景與訪談資訊

受訪者編號	職稱	匿名後機關單位		訪談方式	訪談時間
CG 中央（3 人）					
CG1	高階主管	A 中央機關		面訪	2020/3/12
CG2	高階主管	B 中央機關		面訪	2020/3/27
CG3	高階機要人員	C 中央機關		面訪	2020/3/24
TEC 技術中心（2 人）					
TEC1	高階主管	D 資訊技術中心		面訪	2020/5/12
TEC2	高階主管	E 資訊技術中心		面訪	2020/7/16
LG-Z 地方（15 縣市，19 人）					
LG-Z1-1a	高階主管	Z1 政府爲首之區域	Z1-1 地方政府資安業務職掌部門	面訪	2020/4/1
LG-Z1-1b	基層主管				
LG-Z1-2	中階主管		Z1-2 地方政府資安業務職掌部門	線訪	2020/9/28
LG-Z2-1	中階主管	Z2 政府爲首之區域	Z2-1 地方政府資安業務職掌部門	線訪	2020/9/17
LG-Z3-1a	高階主管	Z3 政府爲首之區域	Z3-1 地方政府資安業務職掌部門	面訪	2020/6/18
LG-Z3-1b	高階主管				
LG-Z3-1c	中階主管				
LG-Z3-2	中階主管		Z3-2 地方政府資安業務職掌部門	線訪	2020/8/24
LG-Z3-3	中階主管		Z3-3 地方政府資安業務職掌部門	線訪	2020/9/18
LG-Z4-1a	高階主管	Z4 政府爲首之區域	Z4-1 地方政府資安業務職掌部門	線訪	2020/5/7
LG-Z4-1b	中階主管				
LG-Z4-2	中階主管		Z4-2 地方政府資安業務職掌部門	線訪	2020/6/11
LG-Z4-3	中階主管		Z4-3 地方政府資安業務職掌部門	線訪	2020/6/5

表 A（續）

受訪者編號	職稱	匿名後機關單位		訪談方式	訪談時間
LG-Z5-1	中階主管	Z5 政府爲首之區域	Z5-1 地方政府資安業務職掌部門	紙本	2020/9/15
LG-Z5-2	中階主管		Z5-2 地方政府資安業務職掌部門	線訪	2020/10/21
LG-Z6-1	中階主管	Z6 政府爲首之區域	Z6-1 地方政府資安業務職掌部門	線訪	2020/8/11
LG-Z6-2	中階主管		Z6-2 地方政府資安業務職掌部門	線訪	2020/9/11
LG-Z6-3	中階主管		Z6-3 地方政府資安業務職掌部門	線訪	2020/9/4
LG-Z6-4	中階主管		Z6-4 地方政府資安業務職掌部門	線訪	2020/9/7
CI 關鍵基礎設施（8 人）					
CI1	高階主管	CI1 關鍵基礎設施主管機關		面訪	2020/7/1
CI2	高階主管	CI2 關鍵基礎設施主管機關		線訪	2020/4/24
CI3	高階主管	CI3 關鍵基礎設施主管機關		面訪	2020/4/9
CI4	高階主管	CI4 關鍵基礎設施主管機關		面訪	2020/8/20
CI5	高階主管	CI5 關鍵基礎設施主管機關		面訪	2020/8/20
CI6	高階主管	CI6 關鍵基礎設施主管機關		面訪	2020/8/10
CI7	高階主管	CI7 關鍵基礎設施服務提供者		面訪	2020/9/9
CI8	中階主管	CI8 關鍵基礎設施服務提供者		線訪	2020/10/13
P 企業（5 家企業，7 人）					
P1	高階主管	P1 資安服務業者		面訪	2020/4/14
P2	高階主管	P2 資安服務業者		面訪	2020/5/26
P3a	高階主管	P3 資安服務業者		面訪	2020/7/2
P3b	高階主管			面訪	2020/7/13
P4a	高階主管	P4 資安服務業者		面訪	2020/7/27
P4b	高階主管				
P5	高階主管	P5 資安服務業者		面訪	2020/8/27
U 產業公會					
U1	中階主管	某資訊產業平臺組織		面訪	2020/7/13

資料來源：作者自行整理。

Exploring Cybersecurity Regional United Defense System in Taiwan: The Perspective of Collaborative Governance

Kaiju Chang[*]

Abstract

This paper proposes a cybersecurity collaborative governance framework rooted in theories of collaborative governance, cybersecurity, and emergency management, focusing on dimensions of drivers and collaborative governance process. The Dimension of Drivers contains "cybersecurity risks", "cybersecurity interdependency", "participation incentives", and "central government leadership." The Dimension of Collaborative Governance Process is based on Emerson and Nabatchi's (2015) framework, comprising "principled engagement", "shared motivation", and "joint action capacity". This paper conducts an analysis of interview data using the proposed theoretical framework to comprehend the current situation and challenges of cybersecurity regional united dense system in Taiwan This analysis takes into consideration viewpoints from both central and local governments. This paper aims to contribute to the establishment of a theoretical framework and the accumulation of empirical research, thereby enriching the study of cybersecurity collaborative governance and regional united dense system in Taiwan from both academic and practical standpoints.

Keywords: cybersecurity, emergency management, collaborative governance, regional united defense system

[*] Associate Professor, Department of Public Administration, National Chengchi University.
Email: kchang@nccu.edu.tw